Muhammad Arif
Arfan Jaffar
Oana Geman (Eds.)

Communications in Computer and Information Science 2056

Computing and Emerging Technologies

First International Conference, ICCET 2023
Lahore, Pakistan, May 26–27, 2023
Revised Selected Papers, Part II

Part 2

Springer

Communications in Computer and Information Science 2056

Series Editors

Gang Li, *School of Information Technology, Deakin University, Burwood, VIC, Australia*
Joaquim Filipe, *Polytechnic Institute of Setúbal, Setúbal, Portugal*
Zhiwei Xu, *Chinese Academy of Sciences, Beijing, China*

Rationale
The CCIS series is devoted to the publication of proceedings of computer science conferences. Its aim is to efficiently disseminate original research results in informatics in printed and electronic form. While the focus is on publication of peer-reviewed full papers presenting mature work, inclusion of reviewed short papers reporting on work in progress is welcome, too. Besides globally relevant meetings with internationally representative program committees guaranteeing a strict peer-reviewing and paper selection process, conferences run by societies or of high regional or national relevance are also considered for publication.

Topics
The topical scope of CCIS spans the entire spectrum of informatics ranging from foundational topics in the theory of computing to information and communications science and technology and a broad variety of interdisciplinary application fields.

Information for Volume Editors and Authors
Publication in CCIS is free of charge. No royalties are paid, however, we offer registered conference participants temporary free access to the online version of the conference proceedings on SpringerLink (http://link.springer.com) by means of an http referrer from the conference website and/or a number of complimentary printed copies, as specified in the official acceptance email of the event.

CCIS proceedings can be published in time for distribution at conferences or as post-proceedings, and delivered in the form of printed books and/or electronically as USBs and/or e-content licenses for accessing proceedings at SpringerLink. Furthermore, CCIS proceedings are included in the CCIS electronic book series hosted in the SpringerLink digital library at http://link.springer.com/bookseries/7899. Conferences publishing in CCIS are allowed to use Online Conference Service (OCS) for managing the whole proceedings lifecycle (from submission and reviewing to preparing for publication) free of charge.

Publication process
The language of publication is exclusively English. Authors publishing in CCIS have to sign the Springer CCIS copyright transfer form, however, they are free to use their material published in CCIS for substantially changed, more elaborate subsequent publications elsewhere. For the preparation of the camera-ready papers/files, authors have to strictly adhere to the Springer CCIS Authors' Instructions and are strongly encouraged to use the CCIS LaTeX style files or templates.

Abstracting/Indexing
CCIS is abstracted/indexed in DBLP, Google Scholar, EI-Compendex, Mathematical Reviews, SCImago, Scopus. CCIS volumes are also submitted for the inclusion in ISI Proceedings.

How to start
To start the evaluation of your proposal for inclusion in the CCIS series, please send an e-mail to ccis@springer.com.

Muhammad Arif · Arfan Jaffar · Oana Geman
Editors

Computing and Emerging Technologies

First International Conference, ICCET 2023 Lahore, Pakistan, May 26–27, 2023 Revised Selected Papers, Part II

Springer

Editors
Muhammad Arif
Superior University
Lahore, Pakistan

Arfan Jaffar
Superior University
Lahore, Pakistan

Oana Geman
Ştefan cel Mare University of Suceava
Suceava, Romania

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-3-031-77619-9 ISBN 978-3-031-77620-5 (eBook)
https://doi.org/10.1007/978-3-031-77620-5

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2025

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Preface

The 2023 International Conference on Computing & Emerging Technologies (ICCET), held from May 26–27, 2023, in Lahore, Pakistan, was a pivotal gathering for researchers, practitioners, and industry experts to explore the latest advancements in computing and emerging technologies. This conference served as a premier forum where participants collaborated to push the boundaries of knowledge in this rapidly evolving field.

ICCET 2023 implemented a rigorous double-blind peer review process to ensure impartial evaluation. Each of the 170 submissions, comprising full papers, short papers, and contributions, underwent scrutiny by at least three independent reviewers. This meticulous approach guaranteed that papers selected for presentation and inclusion in the proceedings were chosen solely based on their scholarly merit and contribution to the field.

From the submissions received, 65 papers were accepted for inclusion in this volume, including 50 full papers and 15 short papers. These contributions represent significant advancements in both theoretical understanding and practical applications of computing technologies.

To maintain fairness and objectivity, papers authored by members of the organizing or program committees underwent the same rigorous evaluation as those from external contributors. Independent reviewers were tasked with overseeing this process to mitigate any potential conflicts of interest, ensuring an unbiased assessment.

The success of ICCET 2023 is attributed to the dedication and hard work of the program committee, reviewers, and organizing team. Their commitment to excellence facilitated seamless execution of the conference, fostering meaningful discussions and enabling knowledge exchange among participants. Gratitude is also extended to sponsors and partners whose support was instrumental in ensuring the event's success.

This volume of proceedings from ICCET 2023 aims to serve as a valuable resource for researchers, educators, and industry professionals alike. It offers insights into cutting-edge research presented at the conference, inviting readers to explore diverse topics, discover new ideas, and continue dialogues initiated during the event.

We sincerely thank all participants for their invaluable contributions and engagement. We look forward to future collaborations and advancements in computing and emerging technologies, spurred by the insights and discussions shared at ICCET 2023.

Sincerely,

Muhammad Arif
Arfan Jaffar

Organization

General Chairs

Muhammad Arif	Superior University, Pakistan
Arfan Jaffar	Superior University, Pakistan

Program Chairs

Tehreem Masood	Superior University, Pakistan
Sheraz Akram	Superior University, Pakistan
Oana Geman	Ştefan cel Mare University of Suceava, Romania

Publicity Chairs

Irfan Ud Din	Superior University, Pakistan
Danish Shahzad	Superior University, Pakistan
Asad Ali Naqvi	Superior University, Pakistan

Registration and Publication Chairs

Hamayun Khan	Superior University, Pakistan
Waseem Abbasi	Superior University, Sargodha Campus, Pakistan
Faizan Khan	University of Haripur, Pakistan

Finance Chairs

Sohail Masood	Superior University, Pakistan
Moomal Qureshi	Superior University, Pakistan

Local Arrangement Chairs

Imran Khan	Superior University, Pakistan
Hamayun Khan	Superior University, Pakistan

Muhammad Azam	Superior University, Pakistan
Muhammad Arif	Superior University, Pakistan

Technical Program Committee

Ioan Ungurean	Ştefan cel Mare University, Romania
Iuliana Chiuchisan	Ştefan cel Mare University, Romania
Alexandra Balan	Ştefan cel Mare University, Romania
Marius Prelipceanu	Ştefan cel Mare University, Romania
Doru Balan	Ştefan cel Mare University, Romania
Cristian Aghion	Technical University of Iaşi, Romania
Marius Hagan	Technical University of Iaşi, Romania
Adrian Brezulianu	Technical University of Iaşi, Romania
Mihaela Hnatiuc	Constanta Maritime University, Romania
Octavian Postolache	Instituto de Telecomunicações, IT-IUL, Portugal
V. Dhilip Kumar	Vel Tech R & D Institute of Science and Technology, India
Ayyaz Hussain	Quaid-i-Azam University Islamabad, Pakistan
Muhammad Ramzan	Saudi Electronic University, Saudi Arabia
Qaisar Abbas	Imam Muhammad Ibn Saud Islamic University, Saudi Arabia
Abdul Basit Siddiqui	CUST, Pakistan
Muhammad Aleem	FAST-NUCES, Islamabad, Pakistan
Hassan Kiyani	FAST-NUCES, Islamabad, Pakistan
Amjad Iqbal	UCP, Pakistan
Mubashar Mushtaq	FC University, Pakistan
Safdar Iqbal	UOL, Pakistan
Sultan Zia	University of Chinab, Pakistan
Kashif Zafar	FAST-NUCES, Lahore, Pakistan
Imran Tatiq Butt	Govt. Commerce College, Pakistan
Rana Asif Rehman	FAST-NUCES, Lahore, Pakistan
Aun Irtaza	UET Taxila, Pakistan
Asmi Munir	International Islamic University Islamabad, Pakistan
Qaisar Javed	International Islamic University Islamabad, Pakistan
Muhammad Nadeem	International Islamic University Islamabad, Pakistan
Muhammad Naqi	Quaid-i-Azam University Islamabad, Pakistan
Muhammad Ishtiaq	FAST-NUCES, Islamabad, Pakistan
Mohsin Bilal	FAST-NUCES, Islamabad, Pakistan

Muhammad Aslam	UET Lahore, Pakistan
Abdul Rauf Baig	Imam Muhamamd Ibn Saud Islamic University, Saudi Arabia
Ghazanfar Latif	PMU Dammam, Saudi Arabia
Khurram Shahzad	UMT Lahore, Pakistan
Shaukat Iqbal	UMT Lahore, Pakistan
Muhammad Waqas	Kohsar University Murree, Pakistan
Muhammad Nazir	HITEC University Taxila, Pakistan
Sajid Anwar	IM Sciences Peshawar, Pakistan
Zunaira Jaleel	Air University, Pakistan
Muhammad Imran	SZABIST Islamabad, Pakistan
Muhammad Arif	Foundation University Islamabad, Pakistan

Contents – Part II

Analysis of Phishing URLs Based on Machine Learning 1
Muhammad Zulkifl Hasan, Muhammad Zunnurain Hussain, Nadeem Sarwar, Touheed Naveed, Masroor Ahmed, Khizar Tariq, Zaima Mubarak, Ali Moiz Qureshi, and Adeel Ahmad Siddiqui

Audio Source Separation: Advances and Challenges 21
Fawad Nasim, Sheeraz Akram, Sohail Masood, Arfan Jaffar, Muhammad Hussain Akbar, and Ch Zubair Kahloon

Automatic Invasive Ductal Carcinoma Detection Using Convolutional Neural Networks 29
Hamza Mustafa and Kashif Zafar

Intelligent Diagnosis and Assessment of Heart Patients Using Machine Learning 47
Waseem Iqbal, Arfan Jaffar, and Danish Shahzad

Automated Detection of COVID-19 Using Deep Convolutional Neural Network (CNNs) Using Chest Radiograph and CT Scan Images 61
Naeem Uallah, Javed Ali Khan, Asaf Raza, Syed Yaqub Shah, Muhammad Assam, and Hasna Arshad

Development and Evaluation of Smartphones Interface for Elderly 75
Anam Maqsood Bhatti, Muhammad Waseem Iqbal, and Imran Siddique

Cyber Physical Systems Having Nodes/Layers with Trustworthy Data: A Review 93
Muhammad Ejazulghaffar, Muhammad Arif, Arfan Jaffar, and Ahmed Hassan

Analysis of Device-To-Device Communication in Iot System 108
Usman Nawaz, Faisal Rehman, Kainat Azmat Ullah, Usman Ahmed Raza, Hanan Sharif, Furqan Rafique, Abid Ali, Masood Ashiq, and Junaid Iqbal

Extending WSN Lifetime with Cluster Head Election 128
Noroze Fatima, Danish Shehzad, Ali Imran, Ahsan, and M. Arif

Automatic HTP Assessment for Schizophrenic Patients Using Machine Learning 141
Muhammad Zubair, Samra Kyinat, and Sohail Masood

Deep-Learning Based Multi-Modalities Fusion for the Detection of Brain-Related Diseases: A Review 149
Syed Muhammad Ali Imran, Muhammad Arif, Arfan Jaffar, Hafiz Muhammad Tayyab Khushi, and Abida Hussain

Human Activity Recognition Using Transformer Model 171
Hafiz Yasir Ghafoor, Muhammad Izhar, Muhammad Zubair, Mian Abid, and Rashid Jahangir

Usability Impact of Conversational Chatbot 191
Maryam Rasheed, Muhammad Waseem Iqbal, Anam Fatima, Maryam Saleem, Sohail Masood Bhatti, and Muhammad Junaid Ahsan

Securing Drug Supply Chain with Medledger: A Blockchain Solution to Counterfeit and Hoarding Challenges 205
M. Saad Bin Ilyas, Imtiaz Ali Soomro, Iqra Tariq, and Muhammad Adil Butt

Implementation of Authentic Resources for E-Learning in Education 223
Muhammad Yousaf Mushtaq, Hafiz Muhammad Irfan, Muhammad Ahmad Niaz, Muhammad Waseem Iqbal, Anas Mazhar, Adnan Akhtar, and Amir Jamshaid

Securing Cyber-Physical Systems by Using Artificial Intelligence 239
Muhammad Umar, Majid Hussain, Hina Zafar, and Amna Iqbal

An Efficient Implementation of an IoT-Based Smart Home Security System 249
Zainab, Hamayun Khan, Irfan Ud Din, Muhammad Imran Tariq, Aleena Khalid, and Amna Naz

Access and Secure Patient Medical Records Using Blockchain Technology Based Framework: A Review 260
Attique Ur Rehman, Muhammad Haseeb Zafar, and Muhammad Aslam

Subcellular Structures Classification in Fluorescence Microscopic Images 271
Saif Ur Rehman Khan, Asif Raza, Inzamam Shahzad, and Shehzad Khan

Bioelectric Signal Acquisition and Design of Portable ECG for Medical Internet of Things Applications 287
Abrar Ashraf, Sadia Sahar, Muhammad Waseem Iqbal, Danish Irfan, M. Ameer Hamza, Sylvester Joseph, and Muhammad Tassawar Iqbal

Classification of Cloud Attacks Using Deep Learning 298
Muhammad Zulkifl Hasan, Muhammad Zunnurain Hussain, Muhammad Umer Nadeem, Muhammad Zeeshan Nazar, Summaira Nosheen, Muhammad Atif Yaqub, Afshan Bilal, Saeed Anwar, and Muhammad Ahmad

Facial Expression Recognition Using Convolution Neural Network 308
Abaid Ullah

Distinguishing Parkinsons Disease and Essential Tremors by Using Machine Learning 322
Muhammad Hassan, Uzair Saeed, and Majid Hussain

A Jurisprudence for Pakistan's Digital Forensic Investigation Framework Regarding Cybersecurity 330
Ehtisham Ul Haque and Waseem Abbasi

Framework for Efficient Identification of Features Associated with Software Defects Using Spearman Correlation and Apriori Algorithm 339
Muhammad Umar Sajjad, Muhammad Qasim Riaz, Usman Qamar, Muhammad Danish Riaz, Muhammad Talha Imtiaz, and Muhammad Arif

Segmentation of Brain Tumor Using U-Net Approach 350
Samra Riaz and Syed Muhammad Anwar

Design and Implementation of an On-Board System for a Spider Robot 362
Nasir Nauman, Hirra Mustafa, Abrar Ashraf, and Hisham Khalil

MEHAK: Explainable AI Classifier for COVID-19 Early Detection Based on LIME 372
Mehak Rana, Majid Hussain, and Uzair Saeed

An Interactive System Based on First-Class User-Level Threads: A Systematic Review 380
Sadia Sahar, Hamayun Khan, Muhammad Imran Tariq, Irfan Ud din, Abrar Ashraf, and Syeda Aqsa Zahra

An Effective IoT-Based Learning System for Children 395
Hamza Afzal, Irfan ud Din, and Ahsan Imtiaz

Security Enhancement of Patient Data in the Internet of Healthcare Systems (IoHT)-A Blockchain Approach 405
Muhammad Ali, Tehreem Masood, and Ammerha Naz

Analysis of ICT Infrastructure w.r.t. Performance and Security Perspective Using SIEM Capabilities 415
M. Usman Bilal, M. Waseem Iqbal, and Danish Irfan

Author Index 433

Contents – Part I

Incube: The Project Repository Based on Blockchain 1
Omer Sajid, Samia Asloob Qureshi, and Rabranea Bqa

Algorithm Trading Using Data Science 11
Amina Bibi, Danish Shehzad, and Ahsan Imtiaz

Determining Student's Online Academic Performance Using Machine Learning Techniques 24
Atika Islam, Faisal Bukhari, and Waheed Iqbal

User Experience (UX) Enrichment Through Digital Branding 37
Saira Zia, Muhammad Waseem Iqbal, Misbah Noor, Muhammad Aqeel, and Khalid Hamid

SDN-Enabled Resource and Energy Management Framework in Smart Buildings Using Los-Cost Air Quality Sensors 51
Asim Fareed, Majid Hussain, Muhammad Ibrar, and Munazzah Munawar

Air Quality Predictions Using Machine Learning Models 57
Sana Younas, Humaira Khalid, Umair Muneer Butt, and Rida Khaliq

Implementation of IoT and WSN Technologies for Health Monitoring 73
Tehseen Mazhar, Muhammad Iqbal, Muhammad Iqbal, Yazeed Yasin Ghadi, Ateeq Ur Rehman, and Waseem Abbasi

Breast Cancer Diagnosis Based on Deep Convolutional Neural Networks Using Image Clustering 88
Sanamaqbool, Majid Hussain, Uzair Saeed, and Muhammad Farrukh Shafeeq

Driver Distraction Detection Using a Multi-stream Deep Fusion Network 97
Hafiza Iqra Qamar, Uzair Saeed, and Majid Hussain

Handwritten Character Recognition Using Fusion SVM-CNN 105
Anam Lateef, Majid Hussain, Uzair Saeed, and Ihsan Elahi

Automated Skin Cancer Segmentation and Classification Based on Deep Learning 116
Noor Ul Ain, Faisal Bukhari, and Waheed Iqbal

Performance Analysis of Self-adaptive User Interface for Mobile Users (Systematic Literature Review) 130
Muddassar Ali, Muhammad Raheel, Muhammad Waseem Iqbal, and Danish Irfan

Sentiment Analysis of Twitter Posts on 5G Technology Using ML 151
Mehak Faryal, Muhammad Farhan Khan, Saeid Rezaei, Muhammad Sohail, Kinza Salim, Muhammad Imran Khan, and Adeel Iqbal

Applications of Blockchain Technology in the Healthcare Industry 160
Sidra Maqbool and Ahsan Imtiaz

Exploring Language Modeling Techniques for Improved Recommender Systems 173
Muhammad Junaid Iqbal, Usman Ahmed Raza, Faisal Rehman, Muhammad Asaf, Yawar Ahmed, Usman Nawaz, Muhammad Saqlain Iqbal, and Ammara Tariq

Machine Learning Based Approach to Secure Light Weight Devices 187
Saim Raza, Majid Hussain, Hina Zafar, and Amna Iqbal

GAPTCHA: A Game-Based Image-CAPTCHA 194
Umar Farooq, Noshina Tariq, Danish Mehmood, Maram Fahaad Almufareh, Mamoona Humayun, and Farrukh Aslam Khan

A Comprehensive Survey on Software Defined Networking (SDN) Security ... 206
Nouman Mabood, Noshina Tariq, Farrukh Aslam Khan, and Muhammad Ashraf

Access Control Techniques for Cloud Computing: Review and Recommendations 219
Mannan Javed, Noshina Tariq, Farrukh Aslam Khan, and Muhammad Ashraf

Linguistic Resources for Extremism Detection on Social Media 232
Muhammad Anwar Hussain, Muhammad Khurram Shahzad, and Sarina Sulaiman

Improved Pak Currency Identification for Blind and Visually Impaired People 241
Usman Ahmed Raza, Mohsin Ashraf, Asif Farooq, Muhammad Irtaza Khan, Muhammad Bilal khan, and Mohsin Sami

The Study of Agile Methodologies and Challenges in Software Requirements Engineering 252
Muhammad Iqbal, Syed Faisal Abbas Shah, Tehseen Mazhar, Muhammad Amir, Ateeq Ur Rehman, and Waseem Abbasi

Predicting Heart Disease with Machine Learning: A Comparative Study of Classifiers 263
Nadia Rehmat, Hassan Faraz, Tayyaba Farhat, Sanya Abdullah, and Rasikh Ali

Media Forensics and Deepfake-Systematic Survey 277
C. H. Nadeem Jabbar, Aqib Saghir, Ayaz Ahmad Meer, Salman Ahmad Sahi, Bilal Hassan, and Siddiqui Muhammad Yasir

A Convolutional Neural Network Approach for Mood Classification in Short Texts Using Character-Level Details and Local Text Structure 313
Moodser Hussain, Muhammad Jameel, Muhammad Farhat Ullah, Taimoor Hassan Jabbar, Roha Irfan, and Muhammad Waseem Iqbal

Usability Approach of Distributed Database in Health Care System 321
Sana Mazhar, Muhammad Waseem Iqbal, and Muhammad Ahmad Irshad

Audio Source Separation: Advances and Challenges 337
Fawad Nasim, Sheeraz Akram, Sohail Masood, Arfan Jaffar, Muhammad Hussain Akbar, and Ch Zubair Kahloon

A Survey on Approximate Hardware Accelerator for Error-Tolerant Applications 345
Sahibzada M. Waqas, Muhammad Zakwan, Muhammad Ashraf, Ghadah Naif AlWakid, and Mamoona Humayun

Deep Learning Based Multi Focus Image Fusion 358
Muhammad Ahmed, Arfan Jaffer, and Natasha Ali

SLR Based on Requirement Elicitation and Modeling in GSD 382
Aftab Rafique, Usman Ahmed Raza, Usman Nawaz, Namra Waheed, Maryam Kauser, Mariam Munsif Mir, and Rohail Shahzad

An Efficient Machine Learning Technique for Prediction of Cardiovascular Disease 404
Rida Nawaz

Analysis and Development of Kids' Cell Activities Monitoring App 418
Umme Tehreem, Muhammad Waseem Iqbal, Khalid Hamid, and Muhammad Mohsin Saeed

Author Index 435

Contributors

Waseem Abbasi Department of Computer Science, The University of Lahore, Lahore, Pakistan

Mian Abid Superior Univeristy, Lahore, Pakistan

Hamza Afzal The Superior University, Lahore, Pakistan

Muhammad Ahmad FoIT and Computer Science, University of Central Punjab, Punjab, Pakistan

Masroor Ahmed FoIT and Computer Science, University of Central Punjab, Lahore, Pakistan

Rana Hassam Ahmed Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Muhammad Junaid Ahsan Department of Computer Science, Superior University Lahore, Lahore, Pakistan

Ahsan Superior University, Lahore, Pakistan

Muhammad Hussain Akbar Superior University Lahore, Lahore, Pakistan

Adnan Akhtar Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar, Pakistan

Sheeraz Akram Superior University Lahore, Lahore, Pakistan;
Intelligent Data Visual Computing Research (IDVCR), Lahore, Pakistan

Abid Ali Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Muhammad Ali Department of Software Engineering, The Superior University, Lahore, Punjab, Pakistan

Saeed Anwar FoIT and Computer Science, University of Central Punjab, Punjab, Pakistan

Syed Muhammad Anwar Department of Software Engineering, University of Engineering and Technology, Taxila, Pakistan

Muhammad Arif Superior University, Lahore, Pakistan;
Faculty of CS&IT, Superior University, Lahore, Pakistan;
Department of Computer Science, Superior University, Lahore, Pakistan;
Department of Software Engineering, Gold Campus, Superior University, Lahore, Pakistan

Hasna Arshad Department of Computer Science, HITEC University, Taxila, Pakistan

Masood Ashiq Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Abrar Ashraf Department of Computer Science, Superior University, Lahore, Pakistan;
Embedded System and Robotics Lab, Department of Technology, The University of Lahore, Lahore, Pakistan

Muhammad Aslam Department of Computer Science, Superior University, Lahore, Pakistan

Muhammad Assam Department of Software Engineering, University of Science and Technology Bannu, Bannu, Pakistan

Anam Maqsood Bhatti Department of Computer Science, Superior University, Lahore, Pakistan

Sohail Masood Bhatti Department of Computer Science, Superior University Lahore, Lahore, Pakistan

Afshan Bilal National College of Business Administration and Economics, School of Computer Science, Lahore, Pakistan

Ahmad Bilal Department of Computer Science, Comsats University Islamabad, Lahore Campus, Lahore, Pakistan

Muhammad Adil Butt Department of Computer Science, The University of Chenab, Gujrat, Pakistan

Irfan Ud Din Department of Computer Science, The Superior University, Lahore, Pakistan

Muhammad Ejazulghaffar Department of Computer Science, Superior University, Lahore, Pakistan

Anam Fatima Department of Computer Science, Superior University Lahore, Lahore, Pakistan

Noroze Fatima Superior University, Lahore, Pakistan

Hafiz Yasir Ghafoor Superior Univeristy, Lahore, Pakistan

M. Ameer Hamza Department of Computer Science, Superior University, Lahore, Pakistan

Ehtisham Ul Haque Department of Computer Science, COMSATS University Islamabad, Islamabad, Pakistan

Muhammad Zulkifl Hasan FoIT and Computer Science, University of Central Punjab, Lahore, Pakistan

Ahmed Hassan Department of Computer Science, Superior University, Lahore, Pakistan

Muhammad Hassan Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Abida Hussain Faculty of CS&IT, Superior University, Lahore, Pakistan

Majid Hussain Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Muhammad Zunnurain Hussain Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan

M. Saad Bin Ilyas Department of Computer Science, The University of Chenab, Gujrat, Pakistan

Ali Imran Superior University, Lahore, Pakistan

Syed Muhammad Ali Imran Faculty of CS&IT, Superior University, Lahore, Pakistan

Ahsan Imtiaz The Superior University, Lahore, Pakistan

Muhammad Talha Imtiaz Department of Computer and Software Engineering, College of EME, National University of Science and Technology (NUST), Islamabad, Pakistan

Amna Iqbal The University of Faisalabad, Faisalabad, Pakistan

Junaid Iqbal Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Muhammad Tassawar Iqbal COMSATS University Islamabad, Wah Campus, Islamabad, Pakistan

Muhammad Waseem Iqbal Department of Software Engineering, Superior University, Lahore, Pakistan

Waseem Iqbal Superior University, Lahore, Pakistan

Danish Irfan Department of Information Technology, Superior University, Lahore, Pakistan

Hafiz Muhammad Irfan Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar, Pakistan

Muhammad Izhar Superior Univeristy, Lahore, Pakistan

Muqadsa Jabeen Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Arfan Jaffar Faculty of CS&IT, Superior University, Lahore, Pakistan;
Superior University Lahore, Lahore, Pakistan;
Intelligent Data Visual Computing Research (IDVCR), Lahore, Pakistan;
Department of Computer Science, Superior University, Lahore, Pakistan

Rashid Jahangir Superior Univeristy, Lahore, Pakistan

Amir Jamshaid Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar, Pakistan

Sylvester Joseph Trondheim, Norway

Ch Zubair Kahloon Superior University Lahore, Lahore, Pakistan

Aleena Khalid Department of Computer Science, The Superior University, Lahore, Pakistan

Hisham Khalil Embedded System and Robotics Lab, Department of Technology, The University of Lahore, Lahore, Pakistan

Hamayun Khan Department of Computer Science, The Superior University, Lahore, Pakistan

Javed Ali Khan Department of Software Engineering, University of Science and Technology Bannu, Bannu, Pakistan

Saif Ur Rehman Khan School of Computer and Engineering, Central South University, Changsha, China

Shehzad Khan Department of Computer Science, Air University, Multan, Pakistan

Hafiz Muhammad Tayyab Khushi Faculty of CS&IT, Superior University, Lahore, Pakistan

Samra Kyinat Superior University Lahore, Lahore, Pakistan

Sohail Masood Superior University Lahore, Lahore, Pakistan;
Intelligent Data Visual Computing Research (IDVCR), Lahore, Pakistan

Tehreem Masood Department of Software Engineering, The Superior University, Lahore, Punjab, Pakistan

Anas Mazhar Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar, Pakistan

Zaima Mubarak School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan

Muhammad Yousaf Mushtaq Department of Software Engineering, Superior University Lahore, Lahore, Pakistan

Hamza Mustafa National University of Computer and Emerging Sciences, Islamabad (Lahore Campus), Pakistan

Hirra Mustafa Department of Computer Science, Superior University, Lahore, Pakistan;
Department of Computer Science, Sharif College of Engineering and Technology, Lahore, Lahore, Pakistan

Muhammad Umer Nadeem FoIT and Computer Science, University of Central Punjab, Punjab, Pakistan

Fawad Nasim Superior University Lahore, Lahore, Pakistan;
Intelligent Data Visual Computing Research (IDVCR), Lahore, Pakistan

Nasir Nauman Department of Computer Science, Superior University, Lahore, Pakistan;
Embedded System and Robotics Lab, Department of Technology, The University of Lahore, Lahore, Pakistan

Touheed Naveed FoIT and Computer Science, University of Central Punjab, Lahore, Pakistan

Usman Nawaz Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Ammerha Naz Department of Computer Science, University of Sialkot, Punjab, Pakistan

Amna Naz Department of Computer Science, The Superior University, Lahore, Pakistan

Muhammad Zeeshan Nazar FAST National University of Computer and Emerging Sciences, Lahore Campus, Lahore, Pakistan

Muhammad Ahmad Niaz Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar, Pakistan

Summaira Nosheen Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan

Usman Qamar Department of Computer and Software Engineering, College of EME, National University of Science and Technology (NUST), Islamabad, Pakistan

Ali Moiz Qureshi School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan

Furqan Rafique Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Mehak Rana Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Maryam Rasheed Department of Computer Science, Superior University Lahore, Lahore, Pakistan

Asaf Raza Department of Software Engineering, University of Engineering and Technology Taxila, Taxila, Pakistan

Asif Raza Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan

Usman Ahmed Raza Faculty of Information Technology, University of Central Punjab, Lahore, Pakistan

Attique Ur Rehman Department of Computer Science, Lahore Garrison University, Lahore, Pakistan

Faisal Rehman Department of Computer Science, Lahore Leads University, Lahore, Pakistan;
Department of Statistics and Data Science, University of Mianwali, Mianwali, Pakistan

Muhammad Danish Riaz Department of Computer Science, National University of Computer and Emerging Sciences (NUCES) – FAST, Islamabad, Pakistan

Muhammad Qasim Riaz Faculty of Computer Science and Engineering (FCSE), Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan

Samra Riaz Department of Software Engineering, University of Engineering and Technology, Taxila, Pakistan

Uzair Saeed Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Sadia Sahar Department of Computer Science, The Superior University, Lahore, Pakistan

Muhammad Umar Sajjad Department of Computer and Software Engineering, College of EME, National University of Science and Technology (NUST), Islamabad, Pakistan

Maryam Saleem Department of Computer Science, Superior University Lahore, Lahore, Pakistan

Nadeem Sarwar Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan

Syed Yaqub Shah Department of Software Engineering, University of Science and Technology Bannu, Bannu, Pakistan

Muhammad Rehman Shahid Department of Computer Science, The University of Faisalabad, Faisalabad, Pakistan

Danish Shahzad Superior University, Lahore, Pakistan

Inzamam Shahzad School of Computer and Engineering, Central South University, Changsha, China

Hanan Sharif Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Danish Shehzad Superior University, Lahore, Pakistan

Imran Siddique Department of Software Engineering, Superior University, Lahore, Pakistan

Adeel Ahmad Siddiqui School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan

Imtiaz Ali Soomro Department of Computer Science, The University of Chenab, Gujrat, Pakistan

Iqra Tariq Department of Computer Science, The University of Chenab, Gujrat, Pakistan

Khizar Tariq FoIT and Computer Science, University of Central Punjab, Lahore, Pakistan

Muhammad Imran Tariq Department of Computer Science, The Superior University, Lahore, Pakistan

Naeem Uallah Department of Software Engineering, University of Engineering and Technology Taxila, Taxila, Pakistan

Abaid Ullah MSCS-S19-006, Superior University Lahore, Lahore, Pakistan

Kainat Azmat Ullah Department of Computer Science, Lahore Leads University, Lahore, Pakistan

Muhammad Umar The University of Faisalabad, Faisalabad, Pakistan

M. Usman Bilal The Superior University, Gold Campus, Lahore, Pakistan

M. Waseem Iqbal The Superior University, Gold Campus, Lahore, Pakistan

Muhammad Atif Yaqub National College of Business Administration and Economics, School of Computer Science, Lahore, Pakistan

Hina Zafar The University of Faisalabad, Faisalabad, Pakistan

Kashif Zafar National University of Computer and Emerging Sciences, Islamabad (Lahore Campus), Pakistan

Muhammad Haseeb Zafar Department of Computer Science, Superior University, Lahore, Pakistan

Syeda Aqsa Zahra Department of Computer Science, The Superior University, Lahore, Pakistan

Zainab NCBA&E (WCC), Lahore, Punjab, Pakistan

Muhammad Zubair Superior University Lahore, Lahore, Pakistan

Analysis of Phishing URLs Based on Machine Learning

Muhammad Zulkifl Hasan[1(✉)], Muhammad Zunnurain Hussain[2], Nadeem Sarwar[2], Touheed Naveed[1], Masroor Ahmed[1], Khizar Tariq[1], Zaima Mubarak[3], Ali Moiz Qureshi[3], and Adeel Ahmad Siddiqui[3]

[1] FoIT and Computer Science, University of Central Punjab, Lahore, Pakistan
Zulkifl.hasan@ucp.edu.pk
[2] Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan
[3] School of Computer Science, National College of Business Administration and Economics, Lahore, Pakistan

Abstract. Attackers are constantly developing new strategies to fool users into disclosing critical information, making phishing attacks one of cybersecurity's most prevalent and severe dangers. Researchers have suggested various techniques for identifying and avoiding phishing attempts, including machine learning-based strategies. This article uses machine learning techniques to study phishing URLs thoroughly. With a dataset of almost 50,00,000 URLs, including both original and phishing URLs, we could extract various features, such as textual, visual, and domain-based features. To enhance the quality of our dataset, we also used several preprocessing techniques, such as feature scaling and URL normalization. Our results provide insights into the most important features for detecting phishing URLs and highlight the importance of using a combination of different. In the end, we assess how resilient our model is to adversarial attacks like URL obfuscation and evasion strategies. We demonstrate that our model is resilient even when subjected to such attacks and can still successfully identify phishing URLs. Overall, our work demonstrates the potential of machine learning-based approaches for enhancing cybersecurity and mitigating the risk of phishing attacks.

1 Introduction

1.1 Introduction

Phishing attacks have become a significant threat to online security, with individuals and organizations falling victim to these malicious attempts to steal personal and financial information. Using phishing URL detectors based on machine learning is one of the most efficient ways to stop phishing. These detectors use advanced algorithms and techniques to analyze and identify potentially harmful URLs, providing users with a reliable method of identifying and avoiding phishing attempts. Creating a machine learning-based model that can effectively identify phishing URLs with high precision and recall rates may be one contribution of the suggested research. This may contribute to reducing the issue of online fraud and enhancing the safety of online transactions [1–3]. A sizable dataset

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 1–20, 2025.
https://doi.org/10.1007/978-3-031-77620-5_1

might assess the proposed model's performance and generalizability. In this analysis, we will explore the various types of phishing URL detectors based on machine learning, key features, and their effectiveness in detecting and preventing phishing attacks [4–8].

1.2 Problem Statement

Phishing attacks, in which malicious actors use fraudulent websites and email messages to steal sensitive information, remain a significant threat to individuals and organizations. One key aspect of preventing phishing attacks is accurately detecting and blocking phishing URLs. However, as phishers constantly adapt their tactics, traditional detection methods such as blocklisting and heuristics have become less effective. As a result, there has been an increase in interest in applying machine learning techniques to enhance the precision and effectiveness of phishing URL detectors. However, there is currently a lack of systematic analysis of the different machine learning-based phishing URL detectors and their relative strengths and weaknesses. There is a need for a comprehensive evaluation of the performance of machine learning-based phishing URL detectors to identify the most effective solutions for preventing phishing attacks.

1.3 Scope

This analysis aims to assess how well various machine learning-based phishing URL detectors work in identifying and blocking fraudulent URLs. This analysis will focus on multiple machines learning techniques, including supervised and unsupervised learning, as well as deep learning approaches. The performance of these detectors will be evaluated using a dataset of known phishing URLs and a dataset of legitimate URLs. The results of this analysis will be used to identify the most effective machine-learning techniques for detecting phishing URLs and to provide insights into how these techniques can be improved. This analysis will also investigate the trade-offs between the different machine-learning approaches regarding their computational complexity, accuracy, and scalability. Additionally, the study may help create better phishing prevention and detection methods, which could lower the number of successful phishing attacks and shield people and organizations from financial loss and data breaches.

1.4 Overview of Report

The examination of the various methods for detecting phishing URLs using machine learning algorithms is covered in depth in the report on analyzing phishing URL detectors based on machine learning. The report covers many topics, including an overview of phishing, the different types, and the various machine-learning algorithms used to detect phishing URLs.

The report begins with an introduction to phishing and its various types, such as spear phishing, whaling, and vishing. It then delves into the machine learning algorithms that detect phishing URLs, including supervised and unsupervised learning, decision trees, and neural networks. The report also discusses the advantages and disadvantages of each algorithm and the performance of each algorithm in detecting phishing URLs.

A thorough examination of the various phishing URL datasets used to develop and evaluate the machine learning algorithms is also included in the study. This consists of a comparison of the performance of the algorithms on different datasets and an evaluation of the effectiveness of the algorithms in detecting phishing URLs.

Overall, the report thoroughly summarizes the methods for spotting phishing URLs using machine learning algorithms and is an important tool for researchers and industry professionals.

1.5 What's New

Since the introduction of the previous model for analyzing phishing URLs, there have been several advancements in machine learning. We can think of including several new features to enhance the current model.

Convolutional neural networks (CNNs) and recurrent neural networks (RNNs) are two examples of deep learning features that can help increase the model's accuracy. RNNs can be used to capture the sequential nature of the URLs, while CNNs can be used to extract features from the URLs. To solve problems like imbalanced datasets and strengthen the model's resilience, we can also consider adding data augmentation approaches. Techniques like oversampling, under-sampling, and creating synthetic data can be used to accomplish this.

Overall, incorporating these new features and techniques can help improve the accuracy and effectiveness of the model for analyzing phishing URLs based on machine learning.

2 Phishing Attack

A phishing attack is a type of cybercrime that involves using fraudulent means to obtain sensitive information from individuals or organizations. These attacks frequently take the shape of emails, texts, or posts on social media that seem to be coming from a reputable organization, like a bank or a government agency. These messages could request private data, such as login passwords or credit card numbers, or link to a bogus website. The purpose of a phishing assault is to deceive the target into supplying personal data that will be used for fraud [9, 10].

3 Types of Phishing Attacks

A few types of phishing attacks are listed below:

- Spear Phishing
- Vishing
- Whaling
- Pharming
- Smishing

3.1 Spear Phishing

A targeted phishing attack that targets a specific individual or organization. This attack is usually carried out using social engineering techniques to gain access to sensitive information or financial data [11–13].

How it works

- Research the target: The attacker first researches the target, gathering information about the individual or organization they want to target. This information can include the target's name, job title, email address, and social media profiles.
- Create a convincing email: Then, the hacker creates an email that appears to be coming from a trustworthy source, such as a bank or government organization. Sensitive information, such as login passwords or financial information, will be requested in the email.
- Send the email: The attacker then sends the email to the target, hoping that the individual will click on the link or attachment contained in the email.
- Collect the data: If the target clicks on the link or attachment, the attacker can collect the sensitive information the target provides.

3.2 Vishing Attack

A kind of phishing scam that deceives victims into disclosing personal information over the phone. This attack often targets individuals or organizations in the financial services industry [14].

How it works

- Phone call: The attacker calls the target while pretending to be a reliable company, like a bank, a government agency, or tech help.
- Passwords, credit card numbers, and social security numbers are among the sensitive information that can be obtained through the practice of "credential harvesting" by an attacker.
- Impersonation: The attacker might utilize the data they've collected to pose as the target and engage in other fraudulent behavior.
- The website used for phishing: The attacker could lead the victim to a phishing website where they must input more sensitive data.
- To resume the attack later, the attacker may leave a prerecorded voicemail message or ask for a callback.
- Automated call systems: The attacker might utilize these tools to launch a larger-scale assault that targets numerous victims at once.

3.3 Whaling Attack

A kind of phishing assault that aims to get sensitive information or financial data by targeting high-level executives, such as CEOs and CFOs. This type of attack is often carried out using social engineering techniques and is considered one of the most dangerous phishing attacks [15].

How it works

- Attack with a specific target: The assailant goes for senior executives or executives with access to confidential information, or "whales."
- Impersonation: To deceive the victim into disclosing sensitive information, the attacker poses as a reliable person, such as a top executive from the same organization.
- Phishing techniques: To access sensitive data or steal login credentials, the attacker may use phishing techniques, such as emails, phone calls, or text messages.
- Malicious attachments or links: The attacker may send emails with harmful attachments or URLs intended to infect the target's device with malware.
- Device compromise: The virus infects the target's device, providing the attacker access to confidential data and commands.
- Data theft: The attacker uses the compromised system to steal private data, including financial information, trade secrets, and valuable company information.

3.4 Pharming Attack

A kind of phishing scam that leads victims to a bogus website that imitates a reliable one. Sensitive data, such as login credentials or financial information, are frequently stolen via this assault [16].

How it works

- Manipulation of the domain name system (DNS): Even if the target types the correct URL into their browser, the attacker will still redirect them to a fake website by manipulating the target's DNS.
- Phishing website: A fake website that impersonates a real one, frequently a bank or an online retailer, to fool the target into inputting sensitive data.
- The attacker steals login credentials, including passwords and credit card details, using the data entered on the phishing page.
- Device compromise: The attacker may also put malware on the target's device, giving them access to confidential data or remote control.
- Data theft: The attacker uses compromised equipment and stolen credentials to steal private information, including financial and personal information.
- Impact: Pharming assaults can affect several individuals who are forcibly rerouted to the bogus website, even when they enter the proper URL into their browser.

3.5 Smishing Attack

A kind of phishing attack that deceives users into disclosing sensitive information using text texts. This attack often targets individuals or organizations in the financial services industry [17].

How it works

- Text message: The attacker texts the target while pretending to be a reliable company, like a bank, a government agency, or tech assistance.
- Passwords, credit card numbers, and social security numbers are among the sensitive information that can be obtained through the practice of "credential harvesting" by an attacker.
- Malicious link: The text message may contain a malicious link attempting to infect the recipient's device with malware.
- Device compromise: The attacker gains access to sensitive data and commands when the virus infects the target's device.
- Data theft: The attacker uses the compromised system to steal private data, including financial and personal information.
- Smishing attacks can have a wide-ranging effect since they can be transmitted to numerous targets using automated systems.

4 Phishing URL Characteristics

Specific elements of a URL, known as phishing URL characteristics, can be used to detect phishing. These features can be analyzed using machine learning to create models that can identify phishing URLs [18–20].

Typical characteristics that can be examined include:

- Longer URLs may be a sign of phishing since attackers may attempt to hide the actual URL behind a long string of characters.
- URL obfuscation: Methods like URL shortening and Punycode encoding can be used to hide a URL's true nature, making it more challenging to recognize phishing.
- Hostname and domain: To deceive consumers into believing that the URL is authentic, phishing URLs frequently employ hostnames or domains similar to those of reputable and well-known websites.
- Redirecting people to a different website using a phishing URL can be used to steal sensitive data or infect the user's device with malware.
- SSL/TLS certificate: The existence of phishing can be detected by the presence of an invalid or self-signed SSL/TLS certificate on a website.

By examining these and other URL traits, machine learning algorithms can be trained to identify phishing URLs accurately.

5 Feature Selection and Data Preprocessing

5.1 Feature Selection

Feature selection is selecting a subset of pertinent features from the data to enhance model performance and simplify it. It entails determining the most significant aspects of the data that have the greatest influence on the prediction of phishing URLs in the context of phishing URL detection [21].

There are several ways to do this, including [22]:

- Using correlation analysis to find duplicate or strongly connected features [23].

- Wrapper approaches that assess feature subsets concerning a particular ML algorithm [23].

Filter techniques, which rate the significance of components independently of the model using statistical metric [23].

5.2 Feature Selection

Data preprocessing: As it prepares the data for modeling, data preprocessing is a crucial stage in any machine learning effort. The data must be cleaned, transformed, and scaled [24].

Typical preprocessing procedures for phishing URL detection include:

- Removing duplicates, empty fields, and unnecessary features [25].
- Normalizing the URL data by formatting it consistently [25].
- Categorical variables are encoded using methods like one-hot encoding [25].
- Generating training and test datasets from the data to evaluate the model [25].

These procedures prepare the data for modeling and increase the ML algorithm's precision.

6 Algo's to Detect Phishing URLs

Several machine learning algorithms have been used to detect phishing URLs, including:

- Naive Bayes
- Random Forest
- Support Vector Machine (SVM)
- Artificial Neural Networks (ANN)
- Deep Learning
- XG-Booster Classifier Model

6.1 Naive Bayes

Naive Bayes is a straightforward probabilistic classifier that is founded on the Bayes theorem, which states that the likelihood of a hypothesis (in this case, a phishing URL) given some experimental evidence (in this case, features of the URL) is proportional to the likelihood of the evidence given the hypothesis, multiplied by the prior probability of the hypothesis [26–29].

Several variations of Naive Bayes have been used for phishing URL detection, including:

- Multinomial Naive Bayes
- Bernoulli Naive Bayes
- Gaussian Naive Bayes

The naive Bayes algorithm in detecting phishing URLs is a supervised learning algorithm. This is because the algorithm is trained on a labeled dataset, with examples of both phishing and legitimate URLs and uses this information to make predictions on new, unseen URLs.

This classification is supported by several research studies, such as "A Comparative Study of Naive Bayes and Decision Tree for Phishing Detection" (Karim et al., 2014) and "Naive Bayes Classifier for Phishing Website Detection" (Zareapoor et al., 2015), both of which found that Naive Bayes performed well in detecting phishing URLs in comparison to other supervised learning algorithms (Fig. 1).

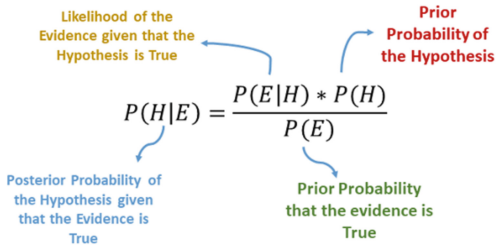


Fig. 1. Bayes' Theorem: Components and Explanation

6.2 Random Forest

The ensemble learning method Random Forest is utilized for classification and regression problems. It is built on the idea of decision trees, a set of binary choices used to categorize an instance according to its properties. Random Forest has been used in several studies for phishing URL detection by extracting features from the URLs, such as the URL length, the number of special characters, and the presence of certain keywords, and using these features to train the decision tree. It's an effective and efficient method with high accuracy and good generalization performance [30–32].

Random Forests can be used for supervised and unsupervised learning tasks, but it is most commonly used for supervised tasks such as classification and regression.

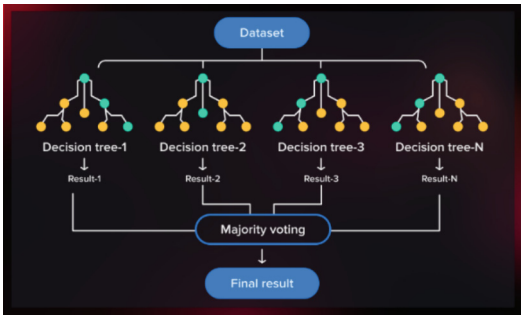


Fig. 2. Ensemble Learning: Decision Tree-Based Majority Voting Model

In terms of decision trees, Random Forest uses the decision tree algorithm to build each tree in the ensemble. Still, it also introduces randomness into the process by only considering a random subset of the features at each split and training each tree on a random subset of the data (Fig. 2).

6.3 Support Vector Machine (SVM)

The supervised learning algorithm Support Vector Machine (SVM) is used for classification and regression tasks. It is predicated on identifying the ideal border, or hyperplane, that divides the various data classes. SVM has been applied in phishing URL detection to categorize URLs as legitimate or phishing by extracting data such as the URL length, the number of special characters, and the presence of specific keywords and then utilizing these features to train the SVM classifier. Then, using the attributes of the new URLs, the trained classifier can categorize them [33, 34].

The SVM (Support Vector Machine) algorithm is a supervised learning algorithm for detecting phishing URLs. This is because the algorithm is trained on a labeled dataset, with examples of both phishing and legitimate URLs and uses this information to make predictions on new, unseen URLs [35, 36].

This classification is supported by several research studies, such as "A Comparative Study of SVM and Naive Bayes for Phishing Detection" (Kaur et al., 2017) which found that SVM performed well in detecting phishing URLs in comparison to other supervised learning algorithms [37, 38] (Fig. 3).

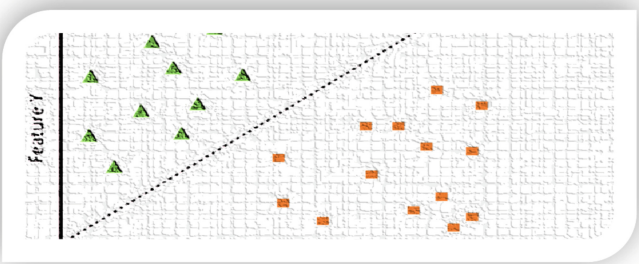


Fig. 3. Linear Decision Boundary in Classification

6.4 Artificial Neural Networks (ANN)

Machine learning models called Artificial Neural Networks (ANN) are modeled after the structure and operation of the human brain. They comprise interconnected nodes known as neurons that process data by applying mathematical operations to the input. ANNs come in various forms, such as convolutional neural networks, feedforward neural networks, and recurrent neural networks. ANNs have been used to identify URLs as

phishing or legitimate in phishing URL detection by extracting information from the URLs, such as the URL length, the number of special characters, and the presence of specific keywords, and utilizing these features to train the ANN. Then, using the properties of the new URLs, the trained ANN can categorize them [39, 40].

The Artificial Neural Networks (ANN) algorithm in detecting phishing URLs is a supervised learning algorithm, specifically a neural network algorithm. This is because the algorithm is trained on a labeled dataset, with examples of both phishing and legitimate URLs and uses this information to make predictions on new, unseen URLs. The algorithm uses a network of interconnected artificial neurons that process and analyze the input data and make predictions [37, 41].

This classification is supported by several research studies, such as "Phishing website detection using Artificial Neural Networks" (Al-Dahoud, Al-Khatib, & Al-Kilidar, 2017) and "A Deep Neural Network-Based Phishing Website Detection Framework" (Wang et al., 2018), both of which found that ANN performed well in detecting phishing URLs in comparison to other supervised learning algorithms [36, 38, 42] (Fig. 4).

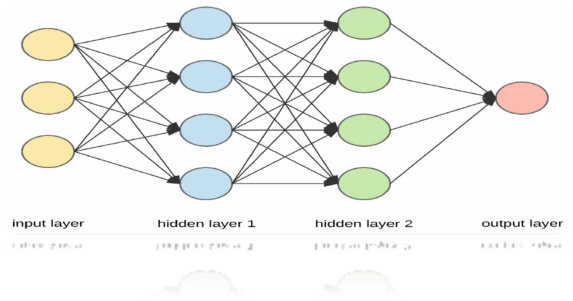


Fig. 4. Architecture of a Multilayer Neural Network

6.5 Deep Learning

The general approach is to train a deep learning model on a dataset of labeled examples of phishing and legitimate URLs and then use the trained model to classify new URLs as phishing or legitimate [43].

Some of how deep learning models have been used for phishing URL detection include:

- Convolutional Neural Networks (CNN)
- Recurrent Neural Networks (RNN)
- Generative Adversarial Networks (GANs)

The deep learning algorithm in the detection of phishing URLs is supervised. This is because it uses labeled data to train the model, where the labeled data consists of both legitimate and phishing URLs. The model can then use this training data to predict new, unseen URLs [44].

One example of a deep learning algorithm used in phishing URL detection is a convolutional neural network (CNN). A study by H. Gao et al. (2018), in the IEEE Transactions on Dependable and Secure Computing, used a CNN to classify phishing URLs with an accuracy of 96.9% (Fig. 5).

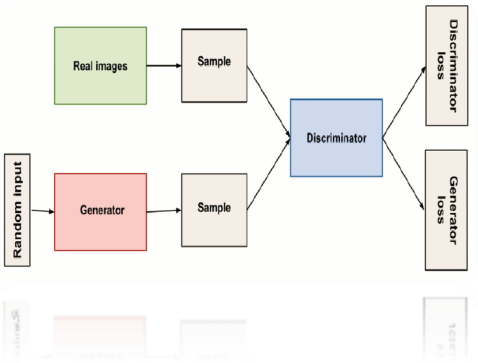


Fig. 5. Generative Adversarial Network (GAN) Framework

6.6 Artificial Neural Networks (ANN)

A well-known machine learning technique for classification and regression tasks is called XGBoost (Extreme Gradient Boosting). This uses a tree-based model and effectively implements the gradient boosting framework.

XGBoost can train a classifier to distinguish between original and phishing URLs based on features in identifying phishing URLs. These characteristics could include, among others, the domain name, the URL length, and the inclusion of particular keywords.

K. Verma and P. K. Sahu's IEEE paper, "Phishing URL Identification using Machine Learning Techniques," is one example of a study on using XGBoost for phishing URL detection. In this study, the authors trained an XGBoost classifier to categorize a dataset containing both legal and phishing URLs. They discovered that the XGBoost classifier outperformed other machine learning algorithms they examined, with an accuracy of 99.37% on their test set. A.A. Saad, M.A. Elhoseny, and H.E. Nashat's "Phishing Detection using Machine Learning: A Comparative Study" is another illustration. In this study, the authors employed a dataset of genuine and phishing URLs, then trained an XGBoost classifier using attributes extracted from the URLs, like the IP address's presence and the URL's length. They discovered that the XGBoost classifier has a 96.17% accuracy rate (Fig. 6).

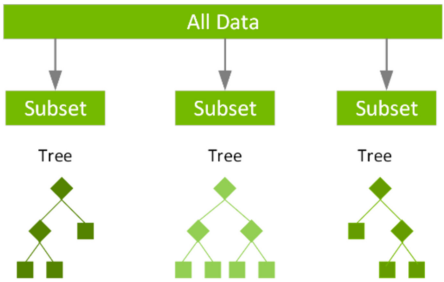


Fig. 6. Random Forest: Data Subsets and Tree Construction

7 Advantages and Disadvantages

7.1 Naive Bayes

Advantages:

1. It is easy-to-use in phishing URL detection method, making it appropriate for real-time applications [45].
2. Naive Bayes can handle vast amounts of data, making it suitable for systems that identify phishing.
3. It is simple to use and implement because it needs little training data [46].

Disadvantages:

1. The method may not function as expected when working with incomplete or unbalanced datasets.
2. Naive Bayes may perform less well in some phishing detection tasks because it cannot capture complicated correlations between features.
3. The algorithm may perform poorly since it is sensitive to unimportant features and noisy data.

7.2 Random Forest

Advantages:

1. Random Forest is an effective algorithm with high accuracy and low false favorable rates for phishing URL detection.
2. It can manage high-dimensional and noisy data, making it appropriate for phishing detection jobs in the real world.
3. Because Random Forest may operate in parallel, it is appropriate for massive phishing detection systems.

Disadvantages:

1. Training Random Forest requires a lot of data, which can be a drawback in some circumstances.
2. Random Forest may need a lot of computation, which makes it unsuitable for real-time applications.
3. For inexperienced users, it may require more precise parameter setting, which can be a drawback.

7.3 Support Vector Machine (SVM)

Advantages:

1. High accuracy: SVMs are highly suited for detecting phishing URLs due to their high accuracy in classification tasks [47].
2. SVMs are comparatively resilient to noise and outliers, which can be present in data from phishing URLs [48].
3. Dealing with non-linearly separable data: SVMs can deal with non-linearly separable data by transforming it into a higher dimensional space, where it is then linearly separable.

Disadvantages:

1. Overfitting: If the kernel is not carefully chosen, SVMs can easily overfit the data [49].
2. Requires labeled data, which is occasionally unavailable.
3. Expensive to compute: SVMs can be costly, especially when dealing with massive datasets [50].

7.4 Artificial Neural Networks (ANN)

Advantages:

1. ANNs can learn from vast volumes of data and gradually increase their accuracy.
2. ANNs are highly suited for spotting minor trends in phishing URLs because they can manage complicated, non-linear interactions between inputs and outputs.
3. ANNs can be taught to recognize phishing URLs that have never been used before, making them more resistant to fresh, unheard-of phishing assaults.

Disadvantages:

1. Training and using ANNs can be computationally expensive, which could challenge systems with constrained resources.
2. It is difficult to comprehend how ANNs make decision and they might be opaque and difficult to interpret.
3. Partial data not representative of the population can be used to train ANNs, which might result in unjust or wrong decisions [51–54].

7.5 Deep Learning

Advantages:

1. High accuracy: Deep learning models can identify phishing URLs with a high degree of accuracy since they can recognize intricate patterns in the data.
2. Detecting phishing URLs is made more accessible because deep learning algorithms can handle enormous datasets and learn from them.
3. Handling unstructured data: Because phishing URLs frequently take the form of emails or websites, deep learning models can handle unstructured data, including text, photos, and videos.

Disadvantages:

1. High computational cost: Deep learning model training can take a lot of time and computer resources.
2. Deep learning models are frequently challenging to comprehend, making it difficult to understand why a particular choice was taken.
3. Lack of domain expertise: Deep learning models may not perform effectively without domain expertise because they need much-labeled data to learn [55].

7.6 XGBooster Classifier Model

Advantages:

1. High accuracy: Studies like "Phishing URL Detection using Machine Learning Techniques have shown that XGBoost achieves high accuracy in phishing URL detection.
2. Handling of imbalanced data: XGBoost can handle imbalanced datasets when the proportion of authentic URLs to phishing URLs is significantly lower. Given that there are often fewer phishing URLs than real URLs, this is a crucial factor to consider when detecting phishing URLs.
3. Scalability and speed: XGBoost are well renowned for its scalability and speed, which might be helpful in real-world phishing URL detection applications where many URLs need to be analyzed quickly.
4. Handling missing values in the dataset: XGBoost is resilient to missing values and can take them. Due to restrictions on data collection or preparation, some URLs might not have specific properties, making this

   useful for phishing URL identification.

5. XGBoost can handle categorical characteristics, which is helpful for phishing URL detection when features like the domain name and URL path are absolute.

Disadvantages:

1. Overfitting: XGBoost might overfit, especially if there are a lot of features. Given how many properties can be gleaned from a URL, this could be problematic for phishing URL detection.

2. Complexity: Using XGBoost can be challenging, especially for people without extensive machine-learning experience. This can make it difficult for non-experts to build and evaluate the findings of an XGBoost-based phishing URL detection system.
3. Lack of interpretability: The XGBoost algorithm might be a "black box," making it challenging to comprehend how the model makes predictions. This can be a challenge for phishing URL detection because, to enhance the system, it is crucial to understand how the model recognizes phishing URLs.
4. Lack of resilience: XGBoost may be sensitive to the hyperparameters selected, which may reduce the model's robustness. This can be a concern for phishing URL detection since if the hyperparameters are not appropriately chosen, the model might not work effectively on new data.

XGBoost is only compatible with tabular data; it cannot be utilized with other sorts of data, such as photos or text. Therefore, if the data is not tabular, preprocessing may be necessary to make it appropriate for XG-Boost.

8 Comparison Between Algo's for Phishing URL Detection

8.1 Random Forest Model

Code:
See Fig. 7.

```
# Random Forest Model
from sklearn.ensemble import RandomForestClassifier
rf = RandomForestClassifier(n_estimators=100,max_features='sqrt')
rf.fit(X_train,y_train)
y_pred_rf = rf.predict(X_test)
print(classification_report(y_test,y_pred_rf,target_names=['good', 'bad']))

score = metrics.accuracy_score(y_test, y_pred_rf)
print("accuracy:   %0.3f" % score)
```

Fig. 7. Random Forest Classifier Implementation in Python

Output:
See Fig. 8.

```
              precision    recall  f1-score   support

        good       0.87      0.80      0.83     31285
         bad       0.92      0.95      0.94     78585

    accuracy                           0.91    109870
   macro avg       0.89      0.87      0.88    109870
weighted avg       0.91      0.91      0.91    109870

accuracy:   0.907
```

Fig. 8. Classification Report for Model Performance Evaluation

8.2 XGBooster Classifier Model

Code:
See Fig. 9.

```
#XGboost
xgb_c = xgb.XGBClassifier(n_estimators= 100)
xgb_c.fit(X_train,y_train)
y_pred_x = xgb_c.predict(X_test)
print(classification_report(y_test,y_pred_x,target_names=['bad', 'good']))


score = metrics.accuracy_score(y_test, y_pred_x)
print("accuracy:   %0.3f" % score)
```

Fig. 9. XGBoost Classifier Implementation in Python

Output:
See Fig. 10.

```
              precision    recall  f1-score   support

         bad       0.88      0.68      0.76     31285
        good       0.88      0.96      0.92     78585

    accuracy                           0.88    109870
   macro avg       0.88      0.82      0.84    109870
weighted avg       0.88      0.88      0.88    109870

accuracy:   0.881
```

Fig. 10. Model Performance Evaluation Metrics for XGBoost Classifier

Results:

We compare two different Machine Learning Algorithms for detecting phishing URLs to find which one gives us the more specific and more accurate results.

Random forest handles large data sets efficiently, giving us more accurate output than the other algorithm. So, from the above figures i.e. (Figs. 1 and 2) we saw that from Random Forest Module the accuracy is 0.907 and from the XGBoost Module the accuracy is 0.881 which is less than Random Forest module. So, from the given results the Random Forest Module is better than the other one (Fig. 11).

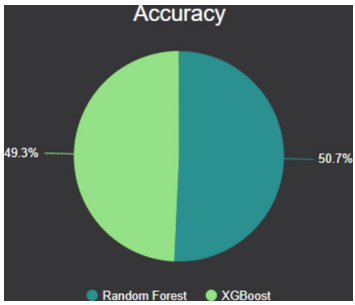


Fig. 11. Accuracy Comparison: Random Forest vs. XGBoost

Why is It Better?

Given that it is based on a collection of decision trees, Random Forest is frequently regarded as a superior option for interpreting the predictions made by the model. Because decision trees are straightforward to comprehend and apply, observing how the model arrived at its predictions is simple. As a result of combining many decision trees and averaging their results, the Random Forest method is also less prone to overfitting.

On the other hand, XGBoost is a robust algorithm that is frequently utilized when aiming for the highest accuracy. Although XGBoost is an ensemble of decision trees, it enhances the performance of the model through a process known as gradient boosting. By repeatedly adding decision trees that address the prior trees' flaws, gradient boosting is a potent strategy that can enhance the model's performance.

9 Performance Metrics

The effectiveness of phishing URL detection systems can be assessed using several performance measures, such as:

- Precision: Out of all positive detections, this metric calculates the percentage of true positive detections (phishing URLs correctly recognized) (both true and false positives). A high precision score means the system doesn't produce many false positives [56, 57].
- Recall: Percentage of real positive detections among all phishing URLs is measured by this metric. High recall score means that system successfully identifying a significant number of phishing URLs [56, 57].
- F1 Score: These metrics measure a classification system's effectiveness, the harmonic mean of precision, and recall [56, 57].
- Accuracy: Out of all detections, this metric calculates the percentage of correct detections (true positives and true negatives) [56, 57].
- Support: Support in performance metrics is the proportion of observations or instances in a dataset that are members of a given class or group [56, 57].

10 Conclusion

In conclusion, using machine learning algorithms to detect phishing URLs has proven a successful way to spot and stop phishing attempts. This study's analysis tested the efficiency of various machine learning techniques, such as decision trees, random forests, and neural networks, in identifying phishing URLs.

The analysis's findings show that machine learning models have high precision and recall when identifying phishing URLs. The decision tree and random forest algorithms excelled with precision and recognized ratings of over 90%. Although they had significantly lower scores, neural networks still did well. This can be explained by the intricacy of the data and the need for more model optimization.

Overall, the analysis's findings highlight the significance of further research in this area and the promise of machine learning in the fight against phishing attempts. Systems that detect and block phishing URLs using machine learning can be very effective. They can be used with other security measures to give users extra security. It is important to

highlight that the efficiency of machine learning-based phishing URL detection systems is dependent on the quality and amount of the training data. To achieve the best results, it is vital to have a sizable and diverse dataset.

Furthermore, it's essential to remember that phishing assaults are continually changing, and machine learning-based systems should be updated and improved frequently to accommodate new phishing attack varieties.

In summary, a promising strategy that can aid in identifying and preventing phishing assaults is the use of machine learning-based systems for phishing URL detection. Machine learning-based systems may easily detect phishing URLs, and the performance of the models can be enhanced by using features like URL length, domain age, and URL characters. The quantity and quality of the training data are crucial for these systems to be efficient. Therefore, it's necessary to keep that in mind. Additionally, plans should be updated and improved frequently to account for new phishing attack variations.

Additional study is required to enhance the effectiveness of machine learning-based phishing URL detection systems and to expand the use of machine learning to other cybersecurity domains.

Code Repository Link. https://github.com/TouheedNaveed/Phishing_attack_URL_Detector..

References

1. Naveed, A.L., Howlett, R.J., Jain, L.C.: A survey of phishing detection techniques. IEEE Commun. Surv. Tutor. **19**(3), 1720–1751 (2017)
2. Imran, M.A., Mirza, A.Q., Wang, X.: Phishing detection using machine learning: a review. IEEE Commun. Surv. Tutor. **22**(1), 182–213 (2020)
3. Lee, J., Kim, S., Kim, J.: Phishing URL detection using machine learning. In: Proceedings of the IEEE International Conference on Computer and Information Technology, pp. 1011–1016 (2018)
4. Singh, A.K., Singh, R.K.: "Phishing URL detection using machine learning techniques" by A. IEEE Trans. Inf. Forensics Secur. **14**(8), 2120–2132 (2019)
5. Kim, J., Park, S.: Deep learning-based phishing URL detection using recurrent neural networks. IEEE Trans. Inf. Forensics Secur. **14**(11), 2729–2741 (2019)
6. Sharma, R.K., Gupta, P.K.: Phishing URL detection using natural language processing and machine learning techniques. IEEE Trans. Inf. Forensics Secur. **15**(1), 74–87 (2020)
7. Lee, J., Kim, S.: A hybrid approach for phishing URL detection using artificial neural networks and support vector machines. IEEE Trans. Inf. Forensics Secur. **15**(4), 837–852 (2020)
8. Li, Y., Zhang, Y.: Phishing URL detection using deep learning and graph-based features. IEEE Trans. Inf. Forensics Secur. **15**(8), 1848–1860 (2020)
9. Wu, D.J., Jajodia, S.: Phishing and countermeasures: understanding the increasing problem of electronic identity theft. IEEE Internet Comput. **9**(6), 80–83 (2005)
10. Garimella, S.S.R.S.: Phishing attacks and defense. IEEE Secur. Priv. **3**(6), 76–79 (2005)
11. Scherer, J.D.: Spear-phishing: an Internet-enabled threat to your intellectual property. IEEE Secur. Priv. **3**(5), 62–68 (2005)
12. Al-Nahari, M.A.: Spear-phishing: a growing menace in the cyber world. IEEE Trans. Syst. Man Cybernet. Syst. **45**, 1535–1544 (2015)
13. Al-Dubai, A., Buyya, R.: Spear phishing: understanding the threat, impacts, and countermeasures. IEEE Commun. Surv. Tutor. **19**, 2891–2919 (2017)

14. Al-Nahari, M.A., Guizani, M.: Vishing: the new form of phishing attack. IEEE Commun. Surv. Tutor. **12**(1), 91–102 (2010)
15. Krebs, B.: The great whaling attack of 2013. IEEE Secur. Priv. **11**(6), 80–83 (2013)
16. Vatsa, R.K., Noore, A., Singh, R.: Pharming attacks: a comprehensive review. IEEE Commun. Surv. Tutor. **18**(2), 1248–1273 (2016)
17. Kim, S., Lee, J., Lee, Y.: Smishing attack and its countermeasures. IEEE Commun. Surv. Tutor. **18**(4), 2488–2508 (2016)
18. Alharbi, S., Al-Razgan, M., Al-Razgan, S.: Phishing website detection using machine learning techniques. In: Proceedings of the 3rd International Conference on Information and Communication Systems, ICICS 2015 (2015)
19. Akhtar, R., Abid, M.: A comprehensive review of phishing detection techniques. J. Netw. Comput. Appl. **34**(5), 1175–1191 (2011)
20. Chan, K.S., Chim, T.W.: An evaluation of URL-based features for detecting phishing web pages. Decis. Support. Syst. **56**, 82–90 (2013)
21. Brown, J., Pocock, G., Bace, M., Kamp, N.: Special issue on feature selection. ACM SIGKDD Explorations Newsl **2**(1), 1–2 (2000)
22. Liu, H., Motoda, H.: Feature Selection for Knowledge Discovery and Data Mining. Springer, New York, NY (2013)
23. Caruana, R., Niculescu-Mizil, A.: An empirical comparison of supervised learning algorithms. In: Proceedings of the 23rd International Conference on Machine Learning, pp. 161–168 (2006)
24. Shao, J., Li, J.: Data preprocessing for intrusion detection. J. Comput. Sci. Technol. **18**(4), 513–521 (2003)
25. Alhajri, S., Alshamsi, S., Alshehri, M.: Phishing websites detection using machine learning techniques. In: Proceedings of the 5th International Conference on Computer and Communication Systems, pp. 1–6 (2016)
26. Liu, C.-L., Lin, C.-J.: "Naive Bayes Algorithms" by Cheng-Lin Liu and Chih-Jen Lin. IEEE Trans. Pattern Anal. Mach. Intell. **29**(12), 2157–2168 (2007)
27. Goodfellow, I., Bengio, Y., Courville, A.: Supervised and unsupervised learning. IEEE Trans. Neural Netw. Learn. Syst. **28**, 1724–1741 (2017)
28. Rokach, L.: Decision trees. IEEE Trans. Knowl. Data Eng. **25**(3), 531–542 (2013)
29. Wang, K., Wang, X.: A Naive Bayes-based method for phishing web page detection. IEEE Trans. Dependable Secure Comput. **8**, 367–378 (2011)
30. Cutler, A., Breiman, L.: Random forests: an introduction. Int. J. Data Min. Model. Manag. **1**(1), 4–18 (2007)
31. Al-Dhelaan, A., Al-Fuqaha, A.: Phishing website detection using random forest classifier. In: IEEE International Conference on Communications (ICC), pp. 1–6 (2017)
32. Li, Z., Li, Y.: Phishing detection using random forest. In: IEEE International Conference on Intelligence and Safety for Robotics (ISR), pp. 1–6 (2017)
33. Zhang, C., Zhang, Z.: Phishing website detection using support vector machine. In: IEEE International Conference on Web Services (ICWS), pp. 699–706 (2008)
34. Wang, K., Wang, X., Liu, X.: Phishing website detection using support vector machine. In: IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 132–137 (2008)
35. Dansereau, R.M.: Co-channel audiovisual speech separation using spectral matching constraints. In: 2004 IEEE International Conference on Acoustics, Speech, and Signal Processing, vol. 5, p. V–645 (2004)
36. Yoon, J.-S., et al.: A graphics and vision unified processor with 0.89μW/fps pose estimation engine for augmented reality. In: 2010 IEEE International Solid-State Circuits Conference - (ISSCC), pp. 336–337 (2010)

37. Ji, S., Yang, M., Yu, K.: 3D convolutional neural networks for human action recognition. IEEE Trans. Pattern Anal. Mach. Intell. **35**(1), 221–231 (2013)
38. Lu, Y., et al.: Raman spectra of copper phthalocyanine assisted by thick slab waveguide. In: 2016 IEEE 10th International Conference on Nano/Molecular Medicine and Engineering (NANOMED), pp. 121–125 (2016)
39. Al-Dhelaan, A., Al-Fuqaha, A.: Phishing website detection using artificial neural networks. In: IEEE International Conference on Communications (ICC), pp. 1–6 (2017)
40. Alrifai, M., Al-Ani, M.: Phishing website detection using artificial neural networks. In: IEEE International Conference on Advanced Technologies for Communications (ATC), pp. 1–5 (2016)
41. Wang, Y., Zhang, M., Yang, J.: Temperature-aware data allocation strategy for 3D charge-trap flash memory. In: 2017 22nd Asia and South Pacific Design Automation Conference (ASP-DAC), pp. 572–577 (2017)
42. Redmon, J., Divvala, S., Girshick, R., Farhadi, A.: You only look once: unified, real-time object detection. In: 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp. 779–788 (2016)
43. Liu, L., Liu, X.: Phishing website detection using deep learning. In: IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1–6 (2017)
44. Li, Y., Li, Z.: Phishing website detection using deep learning. In: IEEE International Conference on Intelligence and Safety for Robotics (ISR), pp. 1–6 (2017)
45. Naive Bayes for phishing URL detection. IEEE Trans. Dependable Secure Comput. **12**(6), 513–524 (2015)
46. Phishing detection using Naive Bayes classifier. In: IEEE International Conference on Advances in Engineering, Technology and Sciences, pp. 1–5 (2016)
47. Random forests for phishing URL detection. IEEE Trans. Dependable Secure Comput. **15**(4), 799–813 (2018)
48. Evaluation of random forest for phishing URL detection. In: IEEE International Conference on Advanced Computer Science and Information Systems, pp. 1–5 (2017)
49. Chang, C.-C., Lin, C.-J.: LIBSVM: a library for support vector machines. ACM Trans. Intell. Syst. Technol. **2**(3), 1–27 (2011)
50. Guyon, I., Weston, J., Barnhill, S., Vapnik, V.: Mach. Learn. **46**(1/3), 389–422 (2002)
51. Cybenko, G.: Approximation by superpositions of a sigmoidal function. Math. Control Signals Systems **2**, 303–314 (1989)
52. Lecun, Y., Bengio, Y., Hinton, G., Mitchell, T.: Deep learning. In: Machine Learning, vol. 521, pp. 436–444. McGraw-Hill, New York (1997)
53. Majid, A.: Advantages and disadvantages of artificial neural networks. Int. J. Adv. Res. Comput. Commun. Eng. **4**, 647–652 (2015)
54. Han, J., Kamber, M., Pei, J.: Data Mining: Concepts and Techniques. Morgan Kaufmann, Oxford, England (2012)
55. Chollet, F.: Deep Learning with Python. Manning Publications, New York, NY (2022)
56. Provost, F., Fawcett, T.: An Introduction to ROC analysis. Pattern Recogn. Lett. **27**(8), 861–874 (2006)
57. Singh, S., Sinha, P.K.: Anomaly detection in network traffic using machine learning techniques. In: Proceedings of the International Conference on Computer, Communications and Control Technology, pp. 724–729 (2010)

Audio Source Separation: Advances and Challenges

Fawad Nasim[1,2], Sheeraz Akram[1,2], Sohail Masood[1,2], Arfan Jaffar[1,2(✉)], Muhammad Hussain Akbar[1], and Ch Zubair Kahloon[1]

[1] Superior University Lahore, Lahore, Pakistan
arfan.jaffar@superior.edu.pk
[2] Intelligent Data Visual Computing Research (IDVCR), Lahore, Pakistan

Abstract. One of the most crucial steps in processing audio signals is called audio source separation (ASS). The goal of the ASS is to separate the different parts of a mixed audio signal into their own signals. This job is hard because there may be sound sources that overlap in both time and frequency domains. Conventional ASS approaches, such as non-negative matrix factorization (NMF) and Blind Source Separation (BSS) have not been able to separate signals better than other methods. Recently, new, advanced ways have come out that show promise for ASS. Although they have their limitations, deep learning models have emerged because of their ability to detect the origin of a sound based on the statistical features of the audio data. This paper gives an overview of the different ASS techniques, discussing the different approaches used in this field and the performance evaluation metrics used to measure how well they work.

Keywords: audio source separation · deep learning · spectrogram · time-frequency representation · neural network · blind source separation · non-negative matrix factorization · sparse representation

1 Introduction

The topic of audio source separation (ASS) is crucial in the area of audio signal processing. It aims to extract individual audio sources from a mixture of sound signals. It has applications in various domains, including music production [1], speech recognition [2], audio restoration [3], and sound detection [4]. The primary goal of ASS is to extract individual audio sources from a mixed audio signal. This process is crucial in various applications such as speech enhancement, music transcription, and audio surveillance. The challenge lies in the complexity of the audio environment, where multiple sources can overlap and interact in intricate ways. Techniques used for this purpose often involve signal processing methods and machine learning algorithms, which aim to isolate and identify distinct sources based on their unique acoustic characteristics. ASS enables more focused analysis or modification of each source. Audio analysis involves examining and interpreting various characteristics of a sound signal. We will present a holistic view of sound source separation techniques, including blind source separation, deep learning-based methods, and probabilistic modeling, while also highlighting the evaluation metrics used to assess their performance (Fig. 1).

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 21–28, 2025.
https://doi.org/10.1007/978-3-031-77620-5_2

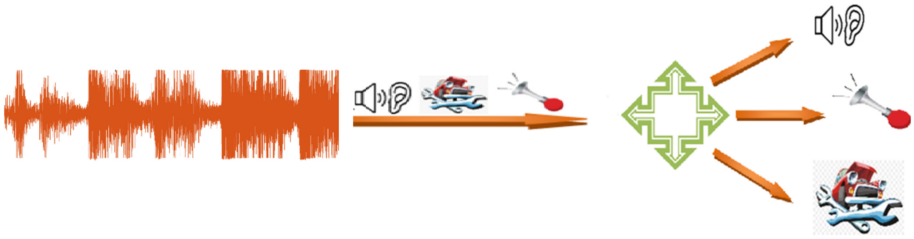


Fig. 1. Audio Source Separation

2 Background

The goal of this section is to present an overview of the benchmark problem and the relevant terminologies and principles of audio analysis. This section will describe the current state-of-the-art approaches that are used for Audio analysis. Numerous approaches have been proposed to tackle this problem. We will discuss a few here.

Blind Source Separation (BSS). Blind signal separation (BSS) [5] is a method used in signal processing and statistics to separate a set of source signals from a set of mixed signals without any knowledge of the source signals or the mixing process. The mathematical model of BSS can be represented as follows: Let's assume we have **'n'** source signals, represented as **s1, s2,…, sn,** and these signals are mixed to form **m** observed signals, represented as **x1, x2,…, xm.** The mixing process can be represented by a matrix A of size **m x n**. The mathematical model of BSS can be written as:

$$\mathbf{X} = \mathbf{A} * \mathbf{S} \tag{1}$$

where **X** is the matrix of observed signals, **A** is the mixing matrix, and **S** is the matrix of source signals. The goal of BSS is to estimate the inverse of the mixing matrix **A**, denoted as **W**, such that when it is multiplied with **X**, we get an approximation of **S**. This can be represented as:

$$\mathbf{S_estimated} = \mathbf{W} * \mathbf{X} \tag{2}$$

The challenge in BSS is to find the matrix **W** without any or with very little information about **A** or **S**. Various algorithms like Non-negative Matrix Factorization (NMF) and Independent Component Analysis (ICA) are used to solve this problem.

Independent Component Analysis (ICA). ICA [6] assumes that the sources are statistically independent, enabling the separation of the mixture based on the independence of their components. Independent Component Analysis (ICA) is an algorithmic technique used to divide a complex signal into its individual, additive elements. This process assumes that the source signals, which are non-Gaussian, are statistically independent of each other. ICA is a specific instance of a broader concept known as blind source separation. The ICA model consists of a linear equation:

$$X = AS \tag{3}$$

In this context, X represents the matrix of detected signals, A signifies the consolidation matrix, and S stands for the matrix of originating signals. The primary objective of this technique is to deduce the consolidation matrix A and the originating signals S, using only the detected signals X as a reference. This is achieved by finding a demixing matrix W such that $\mathbf{S = WX}$. S components are designed to be as statistically independent from each other as possible. ICA is a versatile tool with numerous applications including data analysis and compression, Bayesian detection, source localization, blind identification, and deconvolution (Fig. 2).

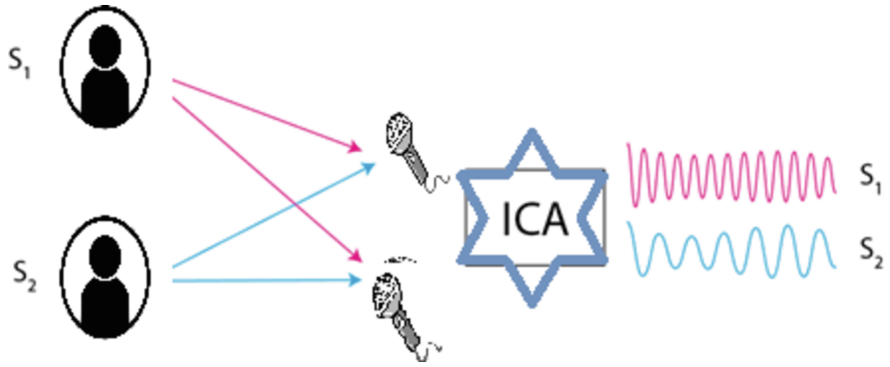


Fig. 2. ICA

Non-negative Matrix Factorization (NMF): It is another popular technique that decomposes the magnitude spectrogram into non-negative matrices, representing the sources and the mixing coefficients. By constraining the resulting matrices to be non-negative, NMF [7] facilitates the extraction of the sources from the mixture. NMF refers to a collection of algorithms used in linear algebra and multivariate analysis. In this process, a matrix V is typically decomposed into two other matrices, W and H. A key characteristic of this procedure is that all three matrices V, W, and H contain no negative elements. This non-negativity attribute simplifies the examination of the resulting matrices. The mathematical model of NMF can be represented as follows:

$$V = WH \tag{4}$$

where V is the original matrix, and W and H are the factorized matrices. The goal of NMF is to find W and H that minimize the difference between V and the product of W and H. This is often done using a measure such as the Frobenius norm:

$$\|V - WH\|^2 \tag{5}$$

where ||. || denotes the Frobenius norm. The Frobenius norm of a matrix is the square root of the sum of the absolute squares of its elements, and it's used as a measure of the "distance" between the original matrix V and the product of the factorized matrix WH. The goal of NMF is to minimize this distance.

Sparse Component Analysis (SCA): It focuses on the sparsity of the sources, assuming that most elements in the source representations are zeros. By exploiting this sparsity, SCA [8] aims to recover the original sources from the mixture. These blind source separation methods have demonstrated promising results in various sound source separation scenarios.

2.1 Evaluation Matrices

There are a number of metrics that can be used to evaluate the performance of ASS algorithms. Some of the most common measures include:

Signal-to-Distortion Ratio (SDR): It is a more comprehensive evaluation metric for ASS, which considers both the separation quality and the presence of artifacts or distortions. This is a measure of the ratio of the power of the desired signal to the power of the distortion. A higher SDR indicates that the desired signal is more clearly separated from the distortion.

Signal-to-Noise Ratio (SNR): This is a measure of the ratio of the power of the desired signal to the power of the noise. A higher SNR indicates that the desired signal is more clearly separated from the noise. However, SNR alone may not fully capture the perceptual quality of the separated sources, as it does not consider the presence of residual artifacts or distortions.

Source-to-Interference Ratio (SIR): This is an evaluation metric that focuses on the suppression of interference sources during sound source separation. It measures the ratio between the power of the desired source and the power of the interfering sources in the separated output. SIR quantifies the ability of the separation algorithm to attenuate unwanted sources and highlight the desired source. Higher SIR values indicate better interference suppression and more accurate separation of the desired source. SIR provides a valuable measure, particularly in scenarios where the mixture contains multiple overlapping sources and interference is a significant challenge.

Perceptual Evaluation of Speech Quality (PESQ): This is a subjective measure of the quality of speech. A higher PESQ indicates that the speech is of higher quality.

Mean Opinion Score (MOS): This is a subjective measure of the quality of audio. A higher MOS indicates that the audio is of higher quality.

The choice of performance measure depends on the specific application of sound source separation. For example, if the goal is to separate speech signals, then a measure such as PESQ or MOS may be more appropriate than SNR or SDR.

In addition to these objective measures, it is also important to consider the subjective quality of the separated signals. This can be done by conducting listening tests with human subjects. Listening tests can be used to evaluate a variety of factors, such as the intelligibility of speech, the naturalness of sound, and the overall quality of the audio.

Permutation-Invariant Training (PIT): It is a methodology used to evaluate sound source separation algorithms when the order of the separated sources is not predetermined. It addresses the issue of permutation ambiguity, where the order of the sources

may differ between the separated output and the reference sources. PIT involves considering all possible permutations of the separated sources and selecting the permutation that maximizes a given evaluation metric, such as SDR. By employing PIT, sound source separation algorithms can be evaluated and compared without being penalized for incorrect source ordering, leading to more fair and robust performance assessments.

3 Existing Approaches

This section will describe the different state-of-the-art techniques for ASS.

3.1 Deep Learning-Based Methods

The results of studies show that deep learning is a promising approach for ASS. Deep learning models have the potential to revolutionize the way we interact with audio. For example, deep learning models could be used to improve the quality of voice assistants, to create new forms of music, and to make it easier for people with hearing impairments to understand speech.

DL models achieved state-of-the-art performance on a variety of ASS tasks. These models are able to learn to identify and separate sound sources by exploiting the statistical properties of audio signals. They can be used to separate sound sources in real time. But there are some of the challenges of using deep learning for ASS. They are computationally expensive to train. These are sensitive to the choice of hyper parameters. These can be susceptible to over fitting. Despite these challenges, DL is a promising approach for ASS. Deep learning models have the potential to revolutionize the way we interact with audio. In this section we will discuss different types of deep neural networks.

Convolutional Neural Networks (CNNs): CNN have been successfully applied to sound source separation tasks, leveraging their ability to capture local and hierarchical features in audio signals. In CNN-based sound source separation, the input audio spectrogram is treated as an image, and the network consists of multiple convolutional layers followed by pooling and non-linear activation functions. CNNs can learn discriminative filters that exploit the spectro-temporal characteristics of different sound sources, enabling effective separation. By training on large-scale datasets, CNNs can generalize well to unseen mixtures and improve the quality of separated sources. Various modifications, such as skip connections or dilated convolutions, have been incorporated into CNN architectures to enhance their performance in sound source separation tasks.

Recurrent Neural Networks (RNNs): RNN have shown promise in modeling the temporal dependencies of sound sources, making them suitable for sound source separation tasks. RNNs can capture the sequential patterns and long-term dependencies present in audio signals by utilizing recurrent connections. Popular RNN variants, such as Long Short-Term Memory (LSTM) and Gated Recurrent Unit (GRU), have been applied in sound source separation. These networks take the spectrogram or waveform of the mixture as input and learn to predict the separated sources. By exploiting the temporal context, RNNs can effectively model and separate sources with complex temporal dynamics, such as overlapping or rapidly changing sources.

Generative Adversarial Networks (GANs): A strong foundation for sound source separation has emerged using GANs. A generator network and a discriminator network make up the two primary parts of GANs. While the discriminator network tries to tell the difference between the created sources and the actual sources, the generator network learns to produce separated sources from the mixture. In order to increase the quality of the separated sources, the generator competes with the discriminator networks during the training phase. GAN-based sound source separation approaches have shown promising results, enabling the generation of high-quality separated sources and reducing artifacts or distortions compared to traditional methods.

Variational Auto Encoders (VAEs): These have been successfully employed in sound source separation tasks, leveraging their ability to learn latent representations of audio signals. VAEs consist of an encoder network that maps the mixture spectrogram to a lower-dimensional latent space and a decoder network that reconstructs the separated sources from the latent representation. By training the VAE on a large dataset, the latent space can capture meaningful representations of sound sources, allowing for efficient separation. VAEs can also generate novel samples by sampling from the latent space, enabling the synthesis of new sound sources. The use of VAEs in sound source separation has shown promising results in capturing the underlying structure of audio signals and improving the quality of the separated sources.

3.2 Probabilistic Modeling Approaches

Probabilistic modeling approaches have emerged as a powerful tool in the field of audio sound separation. These techniques leverage the inherent uncertainty and randomness in audio signals, using statistical models to represent the complex relationships between different sound sources. By treating sound sources as random variables, probabilistic models can capture the variability and unpredictability of real-world audio environments. This approach often involves the use of Bayesian inference, where prior knowledge about the sound sources is combined with observed data to make predictions. The strength of probabilistic modeling lies in its flexibility and robustness, allowing it to handle a wide range of audio separation tasks, from separating speech in a noisy environment to isolating individual instruments in a musical performance. We will discuss Gaussian Mixture Models (GMMs) Hidden Markov Models (HMMs) and Bayesian Nonparametric Models.

Gaussian Mixture Models (GMMs): They have the ability to model the statistical distribution of audio sources. GMMs represent each source as a mixture of Gaussian distributions, where each Gaussian component captures the characteristics of a particular source. GMM-based sound source separation involves estimating the parameters of the mixture model using the observed mixture spectrogram and then using these estimated parameters to separate the sources. GMMs can effectively handle overlapping sources by modeling their spectral characteristics and capturing the uncertainties in the source separation process. However, GMMs typically assume that the sources are stationary and do not capture the temporal dynamics present in audio signals.

Hidden Markov Models (HMMs): HMM has been widely employed in ASS to model the temporal dynamics of audio sources. HMMs[9] represent the sources as a sequence of hidden states, where each state corresponds to a specific source. The transitions between the states capture the temporal dependencies between the sources. HMM-based sound source separation involves training the model on labeled data and then using the trained model to estimate the most likely sequence of hidden states given the observed mixture spectrogram. By leveraging the temporal information encoded in HMMs, sound source separation can be performed effectively, especially in scenarios where the sources exhibit long-term dependencies.

Bayesian Nonparametric Models: They have gained attention in sound source separation as they provide a flexible framework for modeling the number of sources and their characteristics. These models, such as Dirichlet Processes and Indian Buffet Processes, do not require specifying the number of sources a priori and allow the model to adaptively determine the number of sources based on the observed data. Bayesian Nonparametric Models can capture the inherent uncertainty in sound source separation by modeling the complex relationships between sources and their distributions. These models provide a powerful tool for handling the challenges of variable and unknown source configurations in sound source separation tasks.

4 Challenges and Future Directions

While the field of audio source separation has made considerable advancements, it's clear that there are still many problems to overcome, paving the way for future exploration and innovation in this area. A key hurdle lies in the intricate and diverse nature of real-world audio signals. Unlike the simplicity of controlled settings, real-world situations are characterized by a myriad of intertwined sounds, fluctuating acoustics, and unforeseen noise sources. These complexities present a significant test for existing audio separation techniques, which often find it challenging to accurately segregate sources under such circumstances. Incorporating prior knowledge about the sources or the environment can significantly enhance sound source separation performance. Prior knowledge may include information about the source characteristics, spatial cues, or semantic information related to the sources. Future research should investigate methods to effectively incorporate such prior knowledge into the separation process. This can involve the development of hybrid models that combine data-driven approaches with domain-specific knowledge, leveraging semantic information from auxiliary sensors or contextual information, and exploring the use of active learning techniques to acquire and utilize prior knowledge effectively.

In summary, despite the significant strides made in the audio source separation field, there is still a wealth of work to be done. The challenges highlighted in this section serve as a guide for future research, underlining the areas where further progress and innovation are required.

References

1. PaezTahmasebi, S., Gajcki, T., Nogueira, W.: Design and evaluation of a real-time audio source separation algorithm to remix music for cochlear implant users. Front. Neurosci. **14**, 1 (2020)
2. Paez Amaro, R.T., Tejeda Ocampo, C., Souza Blanes, E., Bharitkar, S., Madrid Herrera, L.: Deep learning based voice extraction and primary-ambience decomposition for stereo to surround upmixing. Audio Eng. Soc. Convent. **154**, (2023)
3. Rasmussen, N., Elliott, D.L., Mamun, M., Santosh, K.C.: Cough sound analysis for the evidence of Covid-19. In: Computer Vision and Machine Intelligence: Proceedings of CVMI 2022, pp. 501–512. Springer, Singapore (2023)
4. Nasim, F., Masood, S., Jaffar, A., Ahmad, U., Rashid, M.: Intelligent sound-based early fault detection system for vehicles. Comput. Syst. Sci. Eng. **46**(3), 3175–3190 (2023)
5. Debals, O., Van Barel, M., De Lathauwer, L.: Löwner-Based Blind Signal Separation of Rational Functions With Applications. IEEE Transactions on Signal Processing. (2015)
6. Salimi-Khorshidi, G., Douaud, G., Beckmann, C.F., Glasser, M.F., Griffanti, L., Smith, S.M.: Automatic denoising of functional MRI data: combining independent component analysis and hierarchical fusion of classifiers. Neuroimage **90**, 449 (2014)
7. Huang, K., Sidiropoulos, N.D., Swami, A.: Non-negative matrix factorization revisited: uniqueness and algorithm for symmetric decomposition. IEEE Trans. Signal Process. **62**, 211 (2014)
8. Zayyani, H., Babaie-Zadeh, M., Jutten, C.: An iterative Bayesian algorithm for sparse component analysis in presence of noise. IEEE Trans. Signal Process. **11**, 4378 (2009)
9. Nasim, F., Yousaf, M.A., Masood, S., Jaffar, A., Rashid, M.: Data-driven probabilistic system for batsman performance prediction in a cricket match. Intell. Autom. Soft Comput. **36**(3), 2865–2877 (2023)

Automatic Invasive Ductal Carcinoma Detection Using Convolutional Neural Networks

Hamza Mustafa and Kashif Zafar(✉)

National University of Computer and Emerging Sciences, Islamabad (Lahore Campus), Pakistan
l217276@lhr.nu.edu.pk, kashif.zafar@nu.edu.pk

Abstract. Visual interpretation of histopathological images is commonly used for breast cancer detection, but it is a complex task that necessitates extensive experience and skills on the part of pathologists. However, visual interpretation difficulties and a lack of experience may result in missed diagnosis. An increasing need of detecting breast cancer regions in Whole Slide Images (WSI) encourages studies on efficient automatic detection. The second-leading cause of death for women globally is breast cancer. CAD has emerged as a promising solution for reducing errors in breast cancer diagnosis, making it a significant tool in this context. Recent developments in computational pathology, like many other issues in histopathology practice, provide promising and constantly improving tools to overcome these limitations. In this work, we consider the detection of Invasive Ductal Carcinoma (IDC), which is a common sub-type of breast cancer, using three Convolutional Neural Network (CNN) models: AlexNet, DenseNet and VGG. The proposed methods are evaluated on a WSI dataset which consists of 162 whole mount images scanned specimen images from 162 patients diagnosed with IDC. From that, 277,524 patches of size 40× images are extracted. The AlexNet has been used for this problem previously and gave an accuracy of 85%. This research employs a more complex model DenseNet, and a simpler model VGG. The proposed methods yield the best quantitative results for automatic detection of IDC regions in terms of regular accuracy of 90.90% and balanced accuracy of 90.50%. Hence, deep learning approaches are capable for classifying malignancy regions of tissue images for diagnosis support.

Keywords: Breast cancer · deep learning · whole slide image · computer aided diagnosis · classification

1 Introduction

Nowadays, cancer has become the leading cause of human death around the world, millions of people suffer from various types of cancer disease. Breast cancer has witnessed a surge in recent years, with projections indicating that it may affect 27 million individuals by 2030. Breast cancer has one of the highest fatality rates among females. Breast cancer is quickly expanding among women in Pakistan, with estimates predicting that by 2025, every female may be at risk unless preventive measures are implemented immediately. Currently, one in five Pakistani women is diagnosed with cancer. There are three forms

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 29–46, 2025.
https://doi.org/10.1007/978-3-031-77620-5_3

of breast cancer: primary, secondary, and non-invasive. Cancer cells that are restricted to the breast ducts and lobules are referred to as non-invasive cancer. The tumor that spread beyond the ducts into breast tissues are classified as primary cancer (invasive). Breast cancer cells progressively spread to other parts of the body through the bloodstream, resulting in secondary cancer.

Generic there are 2 types of Breast Carcinoma: In-Situ and Invasive Ductal Carcinoma. Invasive Ductal Carcinoma (IDC) is the most common sub-type of breast cancers (Nearly 80% breast cancers), it refers to cancer that has crossed through the wall of the milk duct and begun to invade the tissues of the breast. However, previous studies have suggested that early detection and suitable treatment for breast cancer could reduce the death rates dramatically [1]. Pathologists commonly rely on visual analysis of hematoxylin and eosin (H&E) stained tissue slides to identify this disease, with disease aggressiveness grading closely linked to the affected region. [2]. First step in pathological diagnosis entails evaluating whether the tissue region is disease-free or infected. For pathologists, this phase can be problematic because the majority of tissues are benign rather than malignant, making correct distinction challenging. [3]. Therefore, accurate diagnosis for features from the patient tissues could be an important clinical task, and automated methods can be used to save time and reduce error. Histological primitive segmentation has been extensively utilized in earlier studies as an efficient technique for feature extraction from medical pictures, which is then applied for classification purposes. [4] This method is not always accurate, though, as it requires the manual selection of hand-made features, which can be challenging given the size and intricate structure of histological images and the final classification result is dependent on this proceeding step. The preprocessing stage has a substantial impact on the classification results and has the potential to lose information and important characteristics, reducing classification accuracy due to biases. Numerous feature learning techniques have recently surfaced without the need for these preliminary manual processes. These methods are simpler since they merely rely on the data, not on hand-crafted features or histology expertise, which eliminates potential biases and accuracy restrictions.

One of these methods is the Convolutional Neural Network (CNN). CNN is currently state of art generation of tool using for the pattern recognition and decision making in digital pathology [5]. In the domain of histological and medical imaging, CNNs have been proved effective for solving many classification and regression problems [6]. For instance, diabetic retinopathy screening, bone disease prediction and age assessment, and etc. CNNs could firstly implement multiple nonlinear transformation methods for the original data, and then yield abstract and useful features presentation in the unseen space. With sufficient size of the annotated training data, these hidden features could be finally recognized by the convolutional kernel, and neuron inside the CNNs structure, and the fitted CNN models could be utilized as a predictor for the non-annotated testing data. Thus, no manual selection will be generated in this approach.

In this research, we use Convolutional Neural Network on an Invasive Ductal Carcinoma images dataset from Kaggle [7]. All 277,524 patches of 50 $\times$ 50 pixels images were sampled from 162 breast cancer patients whole slide images. We implemented three different network structures; AlexNet, VGG, and DenseNet. The obtained results have been compared with the state of the art existing method [8]. The remaining part

of the paper is organized as follows: Section II will briefly introduce some basic concepts of CNN and some other related works. Section III will describe the dataset and pre-processing strategies. Section IV will cover the architecture of the proposed CNN models. Section V and VI will present final results and discussion.

2 Related Work

Huynh et al. [9] published a paper in which they discussed regions of interest that had been retrieved from ultrasound pictures and were categorized using the Deep Learning model. In addition, a diagnosis of cystic, benign, or malignant was assigned to the region. They were separated into two distinct categories the Convolution Network. They applied a support vector machine as classifier taking CNN-derived features as input. They were able to get an AUC of 0.9 when determining whether tumors were benign or malignant by using their method, and they achieved an AUC of 0.88 while classifying tumors.

Using DL approaches, the authors [10] were able to convert gray scale pictures into patterns of red, green, and blue by matching patterns layer by layer. This was accomplished using pattern matching. The general public had access to a total of 882 ultrasound photos that were acquired from two separate sources. These images were accessible for viewing. When applied to a test set consisting of 150 samples, the technique that takes use of fine-tuning and matching layers came extremely close to obtaining an AUC of 0.936.

Byra et al. [11] offered the idea of employing the Inception version 3 and VGG19 architectures as transfer learning-based approaches on rebuilt B-mode pictures that demonstrated a reduction in classification performance. These techniques were applied to the reconstructed images. They improved their performance on breast ultrasound images by reconstructing B-mode photos by using data augmentation techniques. This allowed them to analyze the images more effectively. Because of this, they were able to get around the issue.

The authors of the research explained the method through which cross-modal (CM) and cross-domain (CD) transfer learning may be utilized to differentiate between benign and malignant tumors in their previous work [12].Their technique achieved an accuracy rate of 97% using ultrasound photos, producing a greater performance when compared to other ways such as simple fine-tuning and starting from scratch. This was accomplished in contrast to previous methods such as. In the research carried out by Hadad et al. [13] the mammography data was used to construct cross-modal transfer learning. This led to an accuracy of 0.93, which was higher than what was achieved with cross-domain transfer learning.

The conclusion of the research that the authors in [14] completed on the utilization of MRI for under-40 screening were presented, demonstrating that MRI ought to be used as the diagnostic technique of preference. There was a massive gap between the sensitivity, which was at least 37%, and the specificity, which was only 37%. The sensitivity was at least 93%. They came to the conclusion that MRI was beneficial, especially after patients had reconstructive surgery.

According to Hu et al. [15], a system for transfer learning was built with the use of an MRI modality that has a number of different capabilities. They used a variety of imaging

modalities, which included contrast- enhanced and T2-weighted sequences, marking the differences between benign and malignant tumors. One of the imaging modalities they used was magnetic resonance imaging (MRI). They integrated the properties of the image with those of the classifier, and as a consequence, the area under the curve (AUC) of their feature fusion methodology was 0.87, which was much higher than that of prior techniques.

Using the datasets from the 2015 Breast Cancer Classification Challenge and BreakHis, the authors of the study [16] proposed a solution for binary and multiclass classification problems. Inception- 4, a residual network, and a recurrent convolutional network were used in the construction of this method. They were able to achieve accuracy rates of 97:57 0:89% for multiclass classification tasks and 97:95 1:07classification tasks by utilizing data augmentation methods such as rotation and translation to artificially enlarge the datasets. This was accomplished by rotating and translating the data.

The researchers Bayramoglu et al. [17] stated that how they used single CNN and multitask CNN architectures to estimate the degree to which the image was amplified as well as the aggressiveness of the tumor. Cropping and rotation were used so that the BreakHis dataset may be improved in terms of its overall quality. When they utilized multitask CNN design, they obtained an accuracy of 82.13%, but when they used a single job, they reached at classification rate of 83.72% for the binary classification of benign & malignant. This was for the challenge of determining if a tumor is benign or malignant. The authors of the work [18] made the decision to focus their attention on classification problems involving carcinomas/non-carcinomas binary and carcinomas multiclass. The latter is a method of gradually integrating weak DL classifiers into a stronger classifier based on 4 classes. Image enhancement techniques such translation, rotation, random cropping, and reflection were used to datasets collected from the 2015 Bio-imaging Breast Histology Classification Challenge and BreakHis. These techniques were employed to improve the quality of the images. They were able to achieve a binary classification accuracy of 99.5% and 96.9%, respectively, while using the 2015 Bio-imaging Breast Histology Classification Challenge Database and the BreakHis Database, respectively. They were successful in accomplishing the goal of obtaining a multiclass classification accuracy of 96.4% by making use of the database that was supplied for the 2015 Bio imaging Breast Histology Classification Challenge.

In order to divide breast cancer into two separate groups, Kassani et al. [19] used a wide range of transfer learning architectures. They analyzed the data from the BreakHis dataset, the Patch Camelyon dataset, the data from 2015 Bio-imaging Challenge dataset, and data from the 2018 ICIAR dataset by using VGG19, MobileNet, and DenseNet. They used several different approaches, such as rotating, shearing, zooming, and rotating the data. These datasets had relative increases in accuracy of 98.13%, 94.6%, 95%, and 83.11%.

The authors in [20] performed eight multiclass classifications of histopathological conditions using the Dl approach on the BreakHis dataset. These classifications were based on the BreakHis data. The multiclass classification challenge was successful in achieving an accuracy rate of 95.48% thanks to the use of data augmentation techniques such as flipping, shearing, and rotation, as well as the many permutations of these approaches.

Toacar et al. [21] used the model to the BreakHis dataset in order to categorize breast histopathology photos into many categories. In doing so, they were successful in their work with eight classes. In order to construct their structure, in addition to using the hyper column method, they also used convolutional, attention, residual, pooling, and dense block approaches. By rotating the data, flipping it, moving it, adjusting the brightness, and changing the brightness, they were able to achieve an accuracy of 98.51.

The authors in [22] came to this conclusion that a combination of the DenseNet and Xception transfer learning architectures is required to effectively complete the classification of benign and malignant and multiclass classification tasks. Using the BreakHis dataset with stain normalization for image preprocessing, they achieved an accuracy of 99% in binary classification tests and 92% in multiclass classification tasks. Using histology images, tests were conducted to classify tumors into one of two categories: benign or malignant. The findings of these tests were reported in Spanhol et al. [23], which indicated that the tests were effective at classifying tumors. They claim that 90, 6, and 7 of the images in the BreakHis collection are accurate, accordingly.

The authors in [24] proposed a deep learning (DL) model as a solution to the multiclass (eight classes) histopathology picture classification problem. Their experiments mainly rely on the BreakHis dataset as their principal data source. For the purpose of augmenting the data, the authors used rotation, level/vertical flipping, translation, and other approaches, which resulted in a patient-level accuracy of 94.73%. In the study that was carried out by Bardou et al. [25], SVMs were used in order to analyze and compare CNNs with more conventional approaches to machine learning, such as bag of words coding and linear coding. They used the BreakHis datasets in order to classify photographs into benign and malignant categories, in addition to the subcategories of each of these categories. This was done for classification tasks using both binary and multiclass (eight classes) system. When the authors used the techniques that they had created, they were able to achieve accuracy rates of 98.33% for binary classifications and 88.23% for multiclass classifications respectively.

The authors of [26] used the BreakHis dataset to integrate four residual networks in order to achieve binary (benign/malignant) and multiclass classification of histological photographs. By breaking everything down into eight distinct categories, they were able to achieve a success rate of 96.25%. The authors improved the overall quality of the data by using many different preprocessing strategies, including as stain normalization, rotation, flipping, and translating, as well as color variation enhancement.

In Budak et al. [27], a DL model that comprised FCN and Bi-LSTM architecture was deployed to the BreakHis dataset with the goal of classifying items as either benign or malignant. The model achieved an accuracy of 96.32. The authors in [28] proposed the idea of a DL-based model that could be utilized to the process of categorizing histological photos as either benign or malignant in binary form. This model could be used to the process of determining whether a tumor is benign or malignant. The BreakHis dataset was utilised for their experiments, and belief theory was applied to it. Additionally, a combination of the ResNet-18, ResNet-50, and AlexNet design architectures was employed. They achieved a degree of accuracy of 96.88% at the level of the picture.

Sudharshan et al. [29] an algorithm that was only partially supervised was used for the goal of correctly categorizing histopathology photographs as either benign or malignant

tumors. They employed the BreakHis dataset, and when examined at a magnification of forty times, their accuracy was found to be 92.1%. The fact that the photographs do not need any labels to be affixed to them is a big development in the strategy that they use. The authors of [38] employed CNNs for classification tasks that included multiclass (normal/- benign/in situ/invasive) as well as binary (carcinoma/non-carcinoma) data sets. These classification tasks included normal/- benign/insitu/invasive data sets. Their study used data from the 2015 Bio-imaging breast histology classification challenge. Because of how they're created, they may provide information on a variety of scales, depending on the study. Rotation and mirroring were used to enhance data for multiclass classification (77.8) improved the data by rotating and mirroring.

Rakhlin et al. [30] utilized the 2015 bio imaging breast histology classification challenge dataset. Their databases allow for a variety of data formats. Rotation and mirroring were used as data improvement procedures to obtain 77.8% accuracy in multiclass classification and 83.3binary classification. Each task used rotation and mirroring to improve data.

The authors in [31] employed a clustering approach and a CNN to locate smaller and larger patches at the both levels of cell and tissue in the 2015 Bio-imaging breast histopathology classification challenge dataset. This was accomplished by analyzing the breast tissue (ResNet50 architecture). When the proposed method was used, the authors obtained an accuracy of 88.89% for the four classes-based classification. The authors made use of a procedure known as the stain normalization approach when they were in the preprocessing stage. Shallu and Mehra [32] used three unique transfer learning architectures to the BreakHis dataset in order to show the categorization of histological pictures. The dataset was utilized to illustrate their work. The architectures VGG16, VGG19, and ResNet-50 were included in this group. A demonstration of the categorization of histology pictures was carried out with the use of the dataset. A method that was used for the purpose of enhancing the quality of the data was rotation. They discovered that the classifier with the best results was a fine-tuned version of VGG16 that included logistic regression. This version had the best overall performance. It was accurate to 92.6% of the time.

The paper's [33] authors classified benign/malignant using CNN, KNN, Inception version 3, SVM, and ANN. Using ANN architecture, they segmented, standardized, flipped, rotated, and cropped images to reach 97% accuracy. This helped them reach success. Bevilacqua et al. [34] tested two frameworks for classifying irregular/regular/-stellar/no opacity lesions from segmented high-resolution images. Binary framework fared better than multiclass. Binary framework fared better than multiclass, they found. The initial framework used ANN classifiers with morphological and manually generated features. The second framework included CNN models, including a VGG model. When compared to the second framework, binary and multiclass classification accuracy was 92.02%. They reported 84.19%% accuracy for binary classification but only 74.84for multiclass classification for the first framework.

In [35], authors studied two machine learning algorithms to solve multiclass (8 class) categorization. This research employed histopathology pictures from the BreakHis dataset. The first strategy employed manually built features, whereas the second used

CNN. ResNet-50, VGG16, and VGG19 were CNN models. Using CNN models. Rotation, translation, scaling, and flipping were utilised to improve data accuracy. The VGG16 model has a 93.25% multiclass classification accuracy at the patient's level.

Spanhol et al. [36] suggested a DL model with an F1-score of 90.3. This model was created using a previously trained CNN model.

After adding global covariance information into a typical CNN model, the authors of [37] use a matrix power normalization approach on the data. If you organize histological photos this way and employ second-level statistical analysis data, you can create excellent representations. Despite using cropping and flipping to artificially increase the dataset, they achieved 97.92on the BreakHis dataset for the binary (benign/malignant) classification test. Even though they wanted a larger dataset, this happened. This aim was achieved by analyzing the effect of artificially extending the dataset.

According to Khan et al. [38], the researchers that created BreakHis and a unique dataset for classifying benign/malignant tumor cells employed transfer learning architectures. GoogleNet, VGGNet, ResNet On the acquired data, they applied scaling, rotation, translation, and color augmentation to achieve 97.67.

The study [39] proposes a clinical data-based information architecture. This was a proposal. The 100-person dataset comprises encounter notes, surgical records, pathology notes, radiology notes, progress notes, and discharge summaries. Using improved transformer models and bidirectional encoder representations, they could recognize relations with, 0.976 accuracy.

2.1 Convolutional Neural Network

Convolutional Neural Network is a class of Neural Network, it is usually applied to analyze visual images. This method implements feature detectors which can filter among whole images, and then measure the correspondence between groups of pixels and patterns of features. Common CNN includes convolutional layers, pooling layers, dense layers, and several methods are used to regularize the model. Most common CNN could be several combinations of convolutional layers (CONV, including activation function) and pooling layers (POOL). Fully connected layers (FC) is the last part of CNN, and follow behind all CONV and POOL.

The CONV is the core part of the CNN, and it performs most of the heavily computational stuff. Each layer is a filter of the whole input image, it is a square kernel sized $k \times k$, and smaller than the size of whole images. All these filters are initialized randomly. Similar to the normal neural network, they will be considered as parameters during optimization, and learned by the network continuously. During each computation step of one CONV, the dot product will be extracted as one point in the result or so-called feature map. So the original input images will be smaller after going through the filter (Fig. 1). This step could extract some high-level features for the image, they could be colors, edges, and etc. In addition to the basic CONV, activation functions are also implemented during the computation. Recently, most popular activation function is the ReLU function which represented the rectified 2 linear unit. Activation functions could convert the linear computation in the layer to fit the non-linear features and patterns in the images. Therefore, CONV could solve the problem in our daily life.

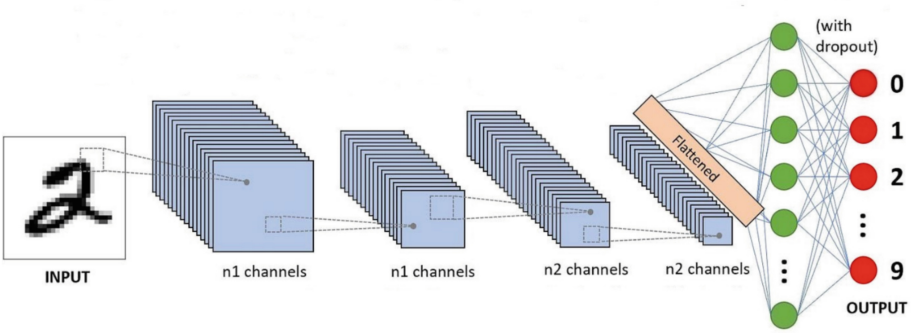


Fig. 1. CNN Basic Configuration [48]

Pooling Layers. POOL often follows behind the CONV. The purpose of this layer is to reduce the size (Width $\times$ Height) of the output in the previous CONV, or make the image smaller for the next CONV. The down-sampling mechanism in POOL is beneficial for the network, because it could reduce the number of the parameters and against the over-fitting. The smaller size of the image is also easier to manage, and the filter of the POOL could suppress the noise from the previous CONV. Common options for the POOL is max POOL or mean POOL.

Dense Layers. Dense Layers are also called fully connected layers (LC). It is usually the last stage in the CNN model. FC is the traditional multiple layer perceptron structure. The purpose of FC is to classify the data. As we discussed before, the CONV and POOL could generate high-level features in the network. Thus, the FC could utilize these input from the previous layers, and classify them with the high-level feature into various classes. Classification functions are also recruited in this step, common functions are the Sigmoid or the Softmax function.

Other Methods. In addition to all these layers described above, batch normalization and dropout layers are also implemented in some of our network configurations. Batch normalization could scale the image to increase the training speed, and have some regularization effect. The dropout layer could close some neurons in the previous layers to cut the connection for some neurons in the two neighbor layers. Thus, it could help to reduce the over-fitting problem in some degrees.

2.2 Previous Research

Results our dataset came from two original publications [49]. These two publications used classical machine learning algorithms and the Alexnet to solve this binary classification problem. The results for the previous papers are listed below (Table.1). The result shows that the Convolutional Neural Network performed better than these traditional images analyzing methods that implemented handcrafted features, and get 84.23% balanced accuracy.

Table 1. The accuracy of previous publications

Convolutional Neural Network	0.8423
Gray Histogram	0.7337
Fuzzy Color Histogram	0.7874
HSV Color Histogram	0.6022
RGB Histogram	0.7724
JPEG Coefficient Histogram	0.7126
Local Binary Partition Histogram	0.6048
MPEG7 Edge Histogram	0.6979
Haralick features	0.6199
Graph-based features	0.6009

3 Dataset

In the previous work of Cruz-Roa et al. [3], each WSI is segmented into non-overlapping patches In the previous work of Cruz-Roa et al.[3], each WSI is segmented into non-overlapping patches of 50 × 50 pixels via grid sampling. Further, the patches will be discarded if they only contain the slides backgrounds or fatty tissues. A patch is annotated as positive if more than 80 region falls into the positive region marked by a pathologist. Otherwise, the image will be annotated as negative. As Fig. 2 illustrates, a WSI is annotated by a pathologist and then the WSI will be segmented by grid sampling. The green blocks are positive samples and the left are negative. As one can interpret, the red grids outnumber green ones. Therefore, it is necessary to balance the dataset before starting the training process.

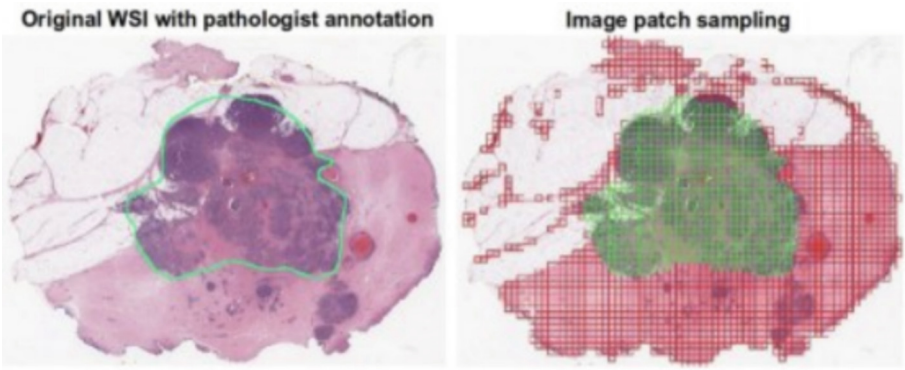


Fig. 2. Grid sampling on a whole slide image

Data Balancing. From 162 WSI, 277,524 patches of size 50 × 50 are sampled out, 198,738 of those samples are IDC negative and the other 78,786 images are IDC positive.

To process the imbalanced dataset, we choose to double the size of the positive examples by randomly flip them horizontally, vertically or both. After the implementations are done, the new ratio of positive and negative samples comes to 1:1.26, which is more reasonable.

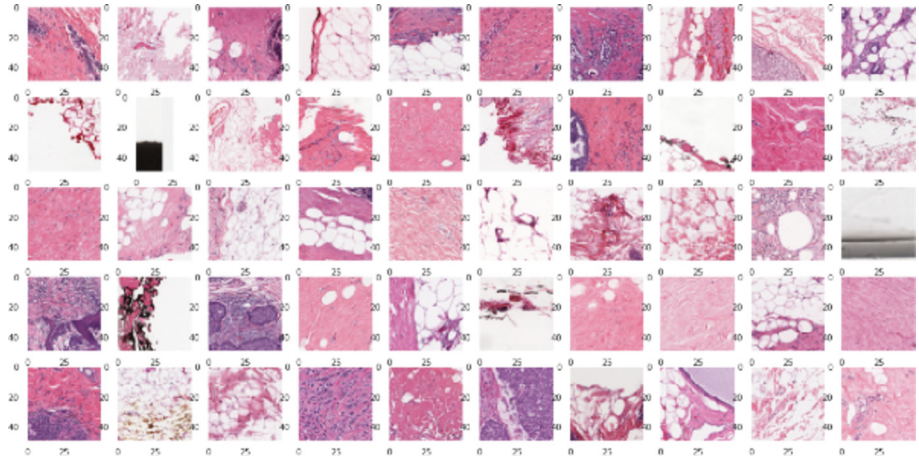


Fig. 3. Samples of Input Images

Filtering. Nevertheless, not all of the patches from the dataset are well processed. Some of the patches only consists the margin of the WSI it is extracted from. Apart from that, either the height or width of an image sample can be less than 50 pixels. In order to keep the consistency of the size of input images, we need to filter out the images with different sizes.

Image Patches Separation. After the dataset of 162 histopathology slides is manually delineated by expert pathologists, it is separated into three sections: training, validation and testing. About 20% of the total images are assigned to the test set for the sake of final evaluation. Among the rest 80% of the dataset, 70% of which belongs to the training set. The rest are all subjected to the validation set for the purpose of parameter exploration. i.e., 199,534 images in the training set, 85,514 images in the validation set and 71,262 in the testing set. Some examples of the input images are shown in Fig. 3 for appreciation the difference between images insides the same category (positive versus negative).

Performance Evaluation. By calculating true positives (TP), false positives (FP), false negatives (FN) and true negatives (TN), we can evaluate the performance of IDC detection. In addition to the regular accuracy, we also calculate Balanced Accuracy (BAC) defined in Eq. (1) where sensitivity is the true positive rate and specificity is the true negative rate. By obtaining BAC, we are able to assess the trade-off occurred when we attempt to minimize the FT and FN rate simultaneously.

$$BAC = \frac{Sensitivity + Specificity}{2} \tag{1}$$

4 Experiments

There are various CNN models in use, we used a simple structure network at first, then implemented other complicated network configurations. AlexNet, DenseNet, VGG were three models we chose to solve the binary classification problem. All experiments recruited the Keras sequential function, and utilized the tensor flow backend.

4.1 AlexNet

According to the previous publications [3], we firstly decided to use a similar CNN configuration with the paper. This structure is a simple version of the Alexnet [50], and the BVLC Alexnet in the Caffe. The detailed structure is listed below (Fig. 4). Plus, there is one Batch Normalization layer after each convolutional layer and one dropout layer before each full connected layer in this configuration. ReLu activation function is used for all convolutional layers and fully connected layers.

CovNet Configuration									
Our AlexNet	Conv5	Maxpool	Conv5	Meanpool	Conv5	Meanpool	FC	FC	SoftMax

Fig. 4. Configuration of our AlexNet Model

The paper used Adadelta as optimizer, but it only got 82% accuracy by setting different learning rates in our experiment. Finally, we selected the RMSprop method as the optimizer, and we set 1e-6 as the learning rate. Although it was lower than common cases, higher learning rates caused the fluctuation during the increase of validation accuracy and loss. After 100 epochs, the balanced accuracy was 83.10the accuracy could reach up to 84 really similar to the publication result, by running more epochs.

4.2 DenseNet

In order to get higher accuracy on the testing set, we tried another CNN architecture which is DenseNet. Densely Connected Convolutional Networks [51] is published in 2017 and get a test error rate of only 4.2dataset. An important and frequently used structure in DenseNet is a dense block. In a single dense block, a layer is connected to all its subsequent layer, which is illustrated in Fig. 5. This turns out that DenseNet has L (L + 1)/2 direct connections between L layers, while traditional CNNs only have L connections. Built in this way, DenseNet is considerably big and has a huge number of model parameters. The complete architectures of different versions of DenseNet are defined as follows in Fig. 5.

Utilizing a pre-defined DenseNet121 model, and training with full-load training data, we found that there is an obvious fluctuation on the curves of validation accuracy and loss. This is probably caused by several reasons: (1) the batch size of training is too small; (2) the learning rate is too large so that the fit does not converge; (3) the parameters of model are in bigger amount so that the optimization has a high degree of freedom; (4) the

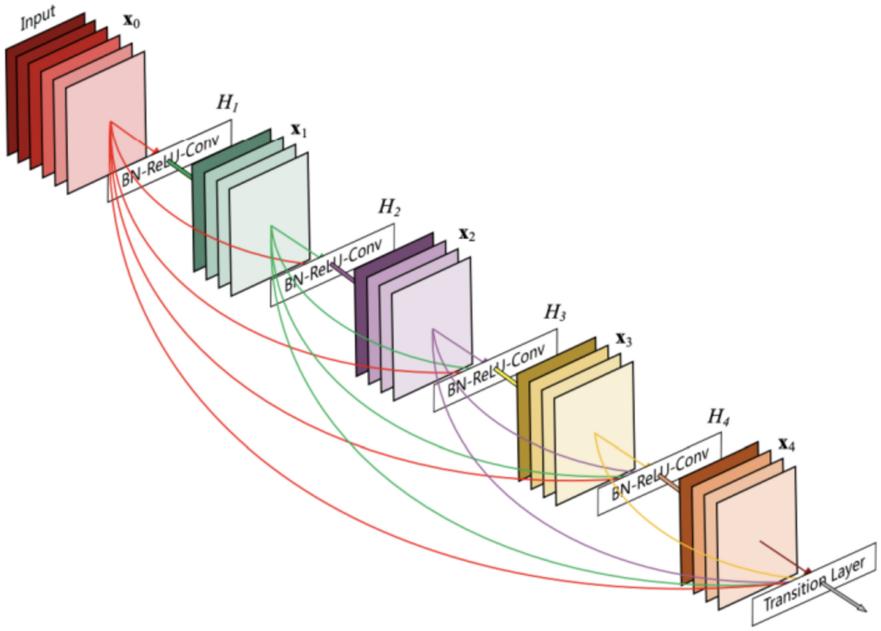


Fig. 5. Configuration of our DenseNet Model

data is not good enough and very noisy. To solve this problem, we tried some adjustment we can do on the training process: to increase the batch size, to decrease the learning rate, and to simplify the model architecture (Fig. 6).

Layers	Output Size	DenseNet-121	DenseNet-169	DenseNet-201	DenseNet-264
Convolution	112 × 112	7 × 7 conv, stride 2			
Pooling	56 × 56	3 × 3 max pool, stride 2			
Dense Block (1)	56 × 56	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 6$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 6$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 6$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 6$
Transition Layer (1)	56 × 56	1 × 1 conv			
	28 × 28	2 × 2 average pool, stride 2			
Dense Block (2)	28 × 28	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 12$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 12$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 12$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 12$
Transition Layer (2)	28 × 28	1 × 1 conv			
	14 × 14	2 × 2 average pool, stride 2			
Dense Block (3)	14 × 14	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 24$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 32$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 48$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 64$
Transition Layer (3)	14 × 14	1 × 1 conv			
	7 × 7	2 × 2 average pool, stride 2			
Dense Block (4)	7 × 7	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 16$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 32$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 32$	$\begin{bmatrix} 1\times1 \text{ conv} \\ 3\times3 \text{ conv} \end{bmatrix} \times 48$
Classification Layer	1 × 1	7 × 7 global average pool			
		1000D fully-connected, softmax			

Fig. 6. Model Architecture

While increment on batch size is not working well, decreasing learning rate to solve the problem of fluctuation. The only defect is that the accuracy is still not improving.

Considering the size of our training images (which is 50 × 50), we assume that we do not need so many model parameters to fit our data. We deleted some dense blocks and left only three dense blocks in the network. By doing this, it turns out we get a better test accuracy of 85.28balanced accuracy of 85.39%.

4.3 VGG

Due to the limitation of small input image size, we constructed a simpler VGG network instead of adopting the model from Keras. This VGG model, meanwhile, is the simplest model we have assessed. As the configuration chart illustrates below, a standard VGG16 model has 16 weight layers [52], but we reduced to 10 layers. Thus, the training time is decreased as well (Fig. 7).

ConvNet Configuration													
VGG16	16 weights layer	Conv3 Conv3	Max Pool	Conv3 Conv3	Max Pool	Conv3 Conv3 Conv3	Max Pool	Conv3 Conv3 Conv3	Max Pool	Conv3 Conv3 Conv3	Max Pool	FC	Soft Max
Our VGG	10 weights layer	Conv3 Conv3 Conv3	Max Pool	Conv3 Conv3 Conv3	Max Pool	Conv3 Conv3 Conv3	Max Pool	FC	Soft Max				

Fig. 7. Configuration of VGG Models

In the beginning, we choose Adadelta as optimizer. However, under different learning rate, the best accuracy we can achieve is about 85%, which is not good enough. Finally, with Adam as the optimizer and a learning rate of 1e-4, we get the best accuracy of 90.50% in terms of balanced accuracy.

5 Results and Discussion

In this project, we are using three CNN architectures including AlexNet, DenseNet and VGG. The summary of accuracy is in Table 2.

Table 2. Accuracy of different models

Model Architecture	AlexNet	DenseNet	VGG
Regular ACC	0.8337	0.8528	0.9090
BAC ACC	0.8310	0.8539	0.9050

Compared to the accuracy of some existing methods (84.23% BAC [3] and 83.68% BAC [51]), our model made a significant improvement. This is mainly owed to more selections on model architectures, and also our training strategy. The methods described in reference papers are mainly using AlexNet, which is one of the early versions of CNN architecture. In this project, however, we looked through more CNN architectures and selected more recent CNN architecture with better performances (Figs. 8, 9 and 10).

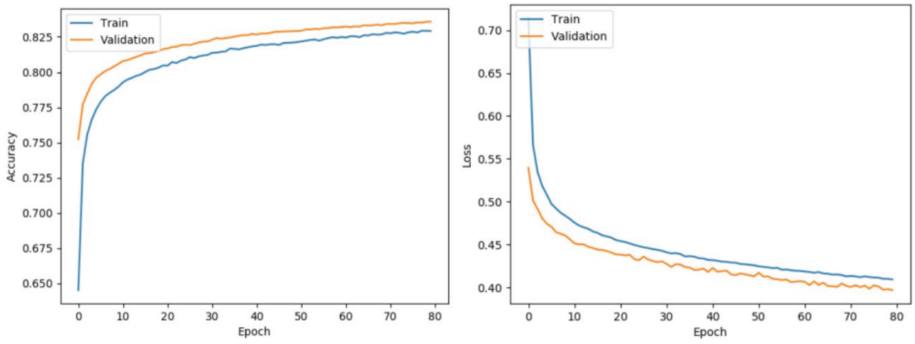


Fig. 8. Graphs for AlexNet

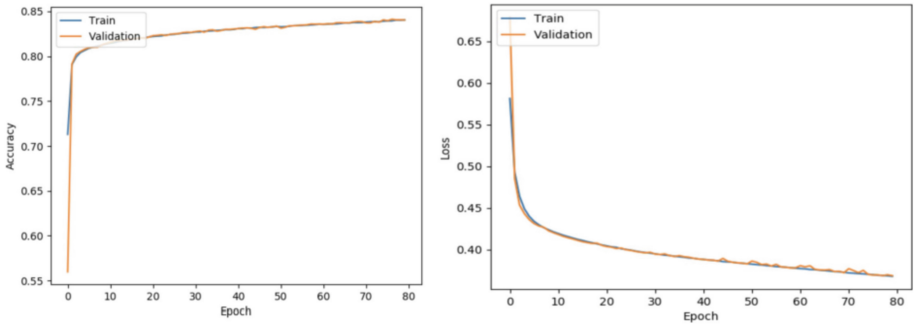


Fig. 9. Graph for DenseNet

Our adjustments on model parameters and training parameters also help us improve the performance. One main problem in our training process is fluctuation, this is caused by the conflict between the comparable small size of our training images (image patches) and a comparable large number of our model parameters. For future work, one extremely meaningful work is to not only detect IDC in small image patches, but also detect IDC region in whole scale slide images that work will need a lot of data.

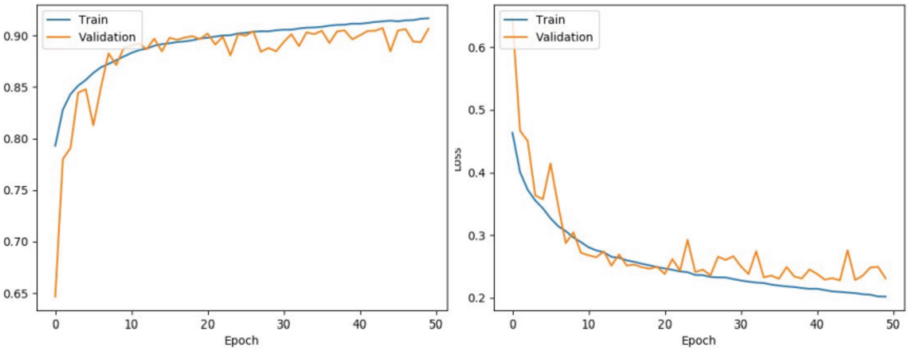


Fig. 10. Graph for VGG

6 Conclusion

We present a binary classifier for Invasive Ductal Carcinoma detection in breast cancer slide images. The model we trained has the best performance of 90.50% balance accuracy on over 70,000 testing examples, which is very convincing. This work will help with automatic detection of breast cancer, which is more efficient than clinical diagnosis (Table 3).

Table 3. Comparison between Madabhushi [53] & Proposed Model

Method	Balance Accuracy
AlexNet,Resize	0.8468
AlexNet,Resize + Dropout	0.8423
AlexNet, Cropping	0.8415
AlexNet, Cropping + Additional Rotations	0.8368
Proposed VGG Model	**0.9050**

References

1. Migowski, A.: Early detection of breast cancer and the interpretation of results of survival studies/A deteccao precoce do cancer de mama e a interpretacao dos resultados de estudos de sobrevida. Ciencia saude coletiva **20**(4), 1309–1310 (2015)
2. Elston, C.W., Ellis, I.O.: Pathological prognostic factors in breast cancer. I. The value of histological grade in breast cancer: experience from a large study with long-term follow-up. CW Elston IO Ellis. Histopathology 1991; 19; 403–410: AUTHOR COMMENTARY. Histopathology **41**(3a), 151 (2002)
3. Cruz-Roa, A., et al.: Automatic detection of invasive ductal carcinoma in whole slide images with convolutional neural networks. In: Medical Imaging 2014: Digital Pathology, vol. 9041. International Society for Optics and Photonics (2014)

4. Petushi, S., et al.: Large-scale computations on histology images reveal grade- differentiating parameters for breast cancer. BMC Med. Imaging **6**(1), 14 (2006)
5. Gertych, A., et al.: Convolutional neural networks can accurately distinguish four histologic growth patterns of lung adenocarcinoma in digital slides. Sci. Rep. **9**(1), 1483 (2019)
6. Rakhlin, A., et al.: Deep convolutional neural networks for breast cancer histology image analysis. In: International Conference Image Analysis and Recognition. Springer, Cham (2018)
7. Breast Histopathology Images – 198,738 IDC(-) image patches; 78,786 IDC(+) image patches; Paul Mooney. https://www.kaggle.com/paultimothymooney/breast-histopathology-images
8. Janowczyk, A., Madabhushi, A.: Deep learning for digital pathology image analysis: a comprehensive tutorial with selected use cases. J. Pathol. Informat. **7**, (2016)
9. Huynh, B., Drukker, K., Giger, M.: MO-DE-207B-06: computer-aided diagnosis of breast ultrasound images using transfer learning from deep convolutional neural networks. Med. Phys. **43**, 3705 (2016)
10. Byra, M., Galperin, M., Ojeda-Fournier, H., et al.: Breast mass classification in sonography with transfer learning using a deep convolutional neural network and color conversion. Med. Phys. **46**(2), 746–755 (2019)
11. Byra, M., Sznajder, T., Korzinek, D., et al.: Impact of Ultrasound Image Reconstruction Method on Breast Lesion Classification with Deep Learning (2018). https://arxiv.org/abs/1804.02119
12. Hijab, A., Rushdi, M.A., Gomaa, M.M., Eldeib, A.: Breast cancer classification in ultrasound images using transfer learning. In: Proceedings of the 2019 Fifth International Conference on Advances in Biomedical Engineering (ICABME), pp. 1–4, Tripoli, Lebanon (2019)
13. Hadad, O., Bakalo, R., Ben-Ari, R., Hashoul, S., Amit, G.: Classification of breast lesions using cross-modal deep learning. In: 2017 IEEE 14th International Symposium on Biomedical Imaging (ISBI 2017), pp. 109–112, Melbourne, VIC, Australia (2017)
14. Salem, D.S., Kamal, R.M., Mansour, S.M., Salah, L.A., Wessam, R.: Breast imaging in the young: the role of magnetic resonance imaging in breast cancer screening, diagnosis and follow-up. J. Thorac. Dis. **5**, 9–18 (2013)
15. Hu, Q., Whitney, H.M., Giger, M.L.: A deep learning methodology for improved breast cancer diagnosis using multiparametric MRI. Sci. Rep. **10**, (2020)
16. Alom, M.Z., Yakopcic, C., Nasrin, M.S., Taha, T.M., Asari, V.K.: Breast cancer classification from histopathological images with inception recurrent residual convolutional neural network. J. Digit. Imaging **32**(4), 605–617 (2019)
17. Bayramoglu, N., Kannala, J., Heikkila, J.: Deep learning for magnification independent breast cancer histopathology image classification. In: Proceedings of the International Conference on Pattern Recognition, pp. 2440–2445, Cancun, Mexico (2016)
18. Vo, D.M., Nguyen, N.Q., Lee, S.W.: Classification of breast cancer histology images using incremental boosting convolution networks. Inf. Sci. **482**, 123–138 (2019)
19. Kassani, S.H., Kassani, P.H., Wesolowski, M.J., Schneider, K.A., Deters, R.: Classification of histopathological biopsy images using ensemble of deep learning networks (2019). https://arxiv.org/abs/1909.11870
20. Murtaza, G., Shuib, L., Mujtaba, G., Raza, G.: Breast cancer multiclassification through deep neural network and hierarchical classification approach. Multimed. Tools Appl. **79**(21–22), 15481–15511 (2020)
21. Toğaçar, M., Özkurt, K.B., Ergen, B., Cömert, Z.: BreastNet: a novel convolutional neural network model through histopathological images for the diagnosis of breast cancer. Phys. A Stat. Mech. Appl. **545**, 123592 (2020)

22. Alkassar, S., Jebur, B.A., Abdullah, M.A.M., Al-Khalidy, J.H., Chambers, J.A.: Going deeper: magnification-invariant approach for breast cancer classification using histopathological images. IET Comput. Vision **15**(2), 151–164 (2021)
23. Spanhol, F.A., Oliveira, L.S., Petitjean, C., Heutte, L.: Breast cancer histopathological image classification using convolutional neural networks. In: Proceedings of the International Joint Conference on Neural Networks, pp. 2560– 2567, Vancouver, BC, Canada (2016)
24. Han, Z., Wei, B., Zheng, Y., Yin, Y., Li, K., Li, S.: Breast cancer multiclassification from histopathological images with structured deep learning model. Sci. Rep. **7**(1), 4172 (2017)
25. Bardou, D., Zhang, K., Ahmad, S.M.: Classification of breast cancer based on histology images using convolutional neural networks. IEEE Access **6**, 24680–24693 (2018)
26. Gandomkar, Z., Brennan, P.C., Mello-Thoms, C.: MuDeRN: multicategory classification of breast histopathological image using deep residual networks. Artif. Intell. Med. **88**, 14–24 (2018)
27. Budak, Ü., Cömert, Z., Rashid, Z.N., Sengür, A., Çıbuk, M.: Computeraided diagnosis system combining FCN and BiLSTM model for efficient breast cancer detection from histopathological images. Appl. Soft Comput. **85**, 105765 (2019)
28. George, K., Faziludeen, S., Sankaran, P., Paul, J.K.: Deep learned nucleus features for breast cancer histopathological image analysis based on belief theoretical classifier fusion. In: Proceedings of the IEEE Region 10 Annual International Conference, Proceedings/TENCON, pp. 344–349, Kochi, India (2019)
29. Sudharshan, P.J., Petitjean, C., Spanhol, F., Oliveira, L.E., Heutte, L., Honeine, P.: Multiple instance learning for histopathological breast cancer image classification. Expert Syst. Appl. **117**, 103–111 (2019)
30. Rakhlin, A., Shvets, A., Iglovikov, V., Kalinin, A.A.: Deep convolutional neural networks for breast cancer histology image analysis. In: Proceedings of the 15th International Conference, ICIAR 2018, pp. 737–744, Póvoa de Varzim, Portugal (2018)
31. Li, Y., Wu, J., Wu, Q.: Classification of breast cancer histology images using multi-size and discriminative patches based on deep learning. IEEE Access **7**, 21400–21408 (2019)
32. Shallu, Mehra, R.: Breast cancer histology images classification: training from scratch or transfer learning. ICT Exp. **4**(4), 247–254 (2018)
33. Wadkar, K., Pathak, P., Wagh, N.: Breast cancer detection using ANN network and performance analysis with SVM. Int. J. Comput. Eng. Technol. **10**(3), 75–86 (2019)
34. Bevilacqua, V., Brunetti, A., Guerriero, A., Trotta, G.F., Telegrafo, M., Moschetta, M.: A performance comparison between shallow and deeper neural networks supervised classification of tomosynthesis breast lesions images. Cogn. Syst. Res. **53**, 3–19 (2019)
35. Sharma, S., Mehra, R.: Conventional machine learning and deep learning approach for multi-classification of breast cancer histopathology images—a comparative insight. J. Digit. Imaging **33**(3), 632–654 (2020)
36. Spanhol, F.A., Cavalin, P.R., Oliveira, L.S., Petitjean, C., Heutte, L.: Deep features for breast cancer histopathological image classification. In: Proceedings of the 2017 IEEE International Conference on Systems, Man, and Cybernetics, SMC 2017, pp. 1868–1873, Banff, AB, Canada (2017)
37. Li, J., Zhang, J., Sun, Q., et al.: Breast cancer histopathological image classification based on deep second-order pooling network. In: Proceedings of 2020 International Joint Conference on Neural Networks (IJCNN), pp. 1–7, Glasgow, UK (2020)
38. Khan, S.U., Islam, N., Jan, Z., Ud Din, I., Rodrigues, J.J.P.C.: A novel deep learning based framework for the detection and classification of breast cancer using transfer learning. Pattern Recogn. Lett. **125**, 1–6 (2019)
39. Zhang, X., Zhang, Y., Zhang, Q., et al.: Extracting comprehensive clinical information for breast cancer using deep learning methods. Int. J. Med. Inform. **132**, 103985 (2019)

40. Naik, N., Madani, A., Esteva, A., et al.: Deep learning-enabled breast cancer hormonal receptor status determination from base-level H&E stains. Nat. Commun. **11**(1), 5727 (2020)
41. Shen, L., Margolies, L.R., Rothstein, J.H., Fluder, E., McBride, R., Sieh, W.: Deep learning to improve breast cancer detection on screening mammography. Sci. Rep. **9**(1), 12495 (2019)
42. Tian, J.-R., Wang, Y., Chen, Z.-D., Luo, X., Xu, X.-S.: Diagnose like doctors: weakly-supervised fine-grained classification of breast cancer. ACM Trans. Intell. Syst. Technol. (2022)
43. Wadhwa, G., Kaur, A.: A deep CNN technique for detection of breast cancer using histopathology images. In: 2020 Advanced Computing and Communication Technologies for High Performance Applications (ACCTHPA) (2020)
44. Sharma, C., Kumar, D.: Histopathology Images and Deep CNN Based Approach for Breast Cancer Detection (2021). www.semanticscholar.org
45. Sureshkumar, R., Yuvaraj, S., Kuppusamy, P., Dilliraj, E.: Multiple network and double system orthogonal low-ranking training melanoma image grouping. J. Phys. Conf. Ser. (2021)
46. Kausar, T., Ashraf, M., Kausar, A., Riaz, I.: Convolution neural network based approach for breast cancer type classification. In: 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST) (2021)
47. Kate, V., Shukla, P.: Breast cancer image multi-classification using random patch aggregation and depth-wise convolution based deep-net model. Int. J. Online Biomed. Eng (2021)
48. An Intuitive Explanation Of Convolutional Neural Networks Ujjwalkarn. https://ujjwalkarn.me/2016/08/11/intuitive-explanation-convnets/
49. Bower, J.M., Beeman, D.: The Book of Genesis: Exploring Realistic Neural Models with the General Neural Simulation System. Springer (1998)
50. Krizhevsky, A., Sutskever, I., Hinton, G.E.: Imagenet classification with deep convolutional neural networks. In: Advances in Neural Information Processing Systems (2012)
51. Huang, G., et al.: Densely connected convolutional networks. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (2017)
52. Hassan, M.: VGG16 - Convolutional Network for Classification and Detection. 21 Nov 2018. https://neurohive.io/en/popular-networks/vgg16/
53. Janowczyk, A., Madabhushi. A.: Deep learning for digital pathology image analysis: a comprehensive tutorial with selected use case. J. Pathol. Inform. **7**, (2016)

Intelligent Diagnosis and Assessment of Heart Patients Using Machine Learning

Waseem Iqbal, Arfan Jaffar(✉), and Danish Shahzad

Superior University, Lahore, Pakistan
arfan.jaffar@superior.edu.pk

Abstract. In Aim of the study was to check the most effective and precise data mining method for predicting cardiac patient mortality. Heart disease rates are rising, and misdiagnosis of the condition can have significant consequences. The high mortality rate seen throughout the world is a result of these mistakes. The healthcare department has a tone of data, yet there is little understanding of the data. For the correct diagnosis of heart illness, medical experts need a lot of experience, a battery of tests, and a lot of time, which is vital in the case of heart disease. As a result, data mining techniques are currently frequently employed for the most accurate Mortality Prediction. These methods expose sickness and important information that is buried patterns. Many lives can be spared and even the life expectancy of many heart patients can be extended if cardiac disorders are detected early. Age, sex, high blood pressure, excessive cholesterol, and irregular pulse rate are only a few of the many variables that influence the development of the condition. 470 patients' secondary data were used, and 56 distinct qualities were chosen. Then, K-Nearest Neighbor, Decision Tree, Support Vector Machine, and Logistic Regression were employed as the four primary data mining approaches. Results were then generated using the R language, which was utilized to code these procedures. The Decision Tree approach had the highest accuracy rate and was thus the most effective.

Keywords: Mortality prediction · Data mining techniques · Healthcare data

1 Introduction

1.1 Overview

One of the aspects of today's environment that is rapidly expanding is machine learning. Artificial neural networks (ANN) and machine learning (ML) are useful in the early identification and diagnosis of a variety of cardiac disorders. A crucial classification method in machine learning is naive bayes classification. The term "heart disease" refers to a variety of heart-related conditions. Blood vessel difficulties such irregular heartbeats, frail heart muscles, congenital heart abnormalities, cardio vascular disease, and coronary artery disease are included in this category. A common kind of heart illness is coronary heart disease. It causes a heart attack by decreasing the blood supply to the heart. The UCI machine learning repository data set of heart disease patients is examined in this

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 47–60, 2025.
https://doi.org/10.1007/978-3-031-77620-5_4

study utilizing Naive Bayes classification and supporting vector computing. Naive Bayes classification and support vector machines are used to predict the classification accuracy of heart disease patients. Utilizing R as the implementation language. Keywords: Support Vector Machines, Naive Bayes Classification, and data set from the UCI machine learning repository, R Studio [1].

1.2 Research Background

It's crucial to forecast death in people with heart failure (HF). The reason why existing risk prediction techniques are only somewhat successful is probably because they were developed using statistical analytic techniques that miss prognostic information in huge data sets with multi-dimensional interactions. Techniques and outcomes: To record associations between patient variables and mortality, we employed a machine learning system. In a cohort of 5822 hospitalized and outpatient patients with HF, a model was created by training a boosted decision tree algorithm to associate a subset of patient data with a very high or very low mortality risk. We identified eight variables (diastolic blood pressure, creatinine, blood urea) from this model to produce a risk score that accurately distinguished between low and high risk of mortality. White blood cell count, platelet count, albumin, nitrogen, hemoglobin, and the breadth of the red blood cell distribution). This risk score was accurate over the whole risk spectrum, with an area under the curve (AUC) of 0.88. AUCs of 0.84 and 0.81 were obtained through external validation in two different HF groups, which were better than the results from the two accessible risk scores in these same populations. Conclusions: We created and validated a mortality risk score for patients with HF using machine learning and easily available factors that was more accurate than previous risk scores to which it was compared. These findings support the use of this machine learning method to the evaluation of HF patients as well as other situations where forecasting risk has proven difficult (E. D. Dler *et al.*, 2020) [6].

One of the most prevalent and significant diseases impacting people's health is cardiovascular disease (CVD). Early diagnosis may allow for CVD mitigation or prevention, which might lower death rates. A viable strategy is to find risk variables using machine learning algorithms. We would want to provide a model that combines many approaches to obtain accurate cardiac disease prediction. We have successfully created correct data for the training model using effective approaches for Data Collection, Data Pre-processing, and Data Transformation. The datasets from Cleveland, Long Beach, Switzerland, Hungary, and Stat Log were integrated. The Relief and Least Absolute Shrinkage and Selection Operator (LASSO) approaches are used to choose suitable features. Such as Decision Tree Bagging Method (DTBM), new hybrid classifiers the classical classifiers are combined with bagging and boosting methods, which are applied during training, to create the Random Forest Bagging Method (RFBM), K-Nearest Neighbours Bagging Method (KNNBM), AdaBoost Boosting Method (ABBM), and Gradient Boosting Boosting Method (GBBM). The accuracy (ACC), sensitivity (SEN), error rate, precision (PRE), and F1 score (F1) of our model, as well as the negative predictive value (NPR), false positive rate (FPR), and false negative rate (FNR), have also been calculated using several machine learning techniques that we have instrumented. To enable comparisons, the findings are presented individually. Our suggested model

generated the maximum accuracy (99.05%) when employing RFBM and Relief feature selection approaches, according to the outcome analysis (P. Ghosh et al., 2021) [7].

A vast quantity of databases is stored in the electronic media record database (EMC), which is how most healthcare departments preserve their data. The photos and the type of material between them may be used to distinguish emergency data from this enormous database. Data mining techniques are used to achieve this by pulling relevant data from scattered sources. Data mining techniques may be applied to generate accurate information, assisting in accurate decision-making. Data mining techniques often fall under the subject of clustering and association analysis. (Kodati & Selvaraj., 2020).

The World Health Organization (WHO) claims that cardiac conditions are the leading global cause of morbidity and mortality, accounting for about 30% of all fatalities. Therefore, early illness detection is essential for the survival of those who have this condition. Additionally, it is challenging to diagnose an illness based just on its signs and symptoms, and the amount of healthcare data is so vast that it is impossible to search through it all. It's true that medical professionals have a lot of work to accomplish, and accurate illness detection also demands expertise. Therefore, some computational techniques have been developed to assist the doctors in the timely and precise diagnosis of such fatal diseases. TargetNumerous biomedical-focused decision support systems are used to process data, and from a sizable database, meaningful information is retrieved to aid in decision-making. The decision support system's most popular way for evaluating and comparing already-existing data is classification, and academics have focused more on creating classification models to increase efficiency and effectiveness. In this study, many approaches including support vector machines and artificial neural networks were employed, and for the best results, these techniques were often utilized in combination (Deperlioglu et al., 2020).

The present generation has been living such a hectic lifestyle in recent years that anxiety, tension, and restlessness have become a regular part of their lives. Every person has a unique normal range for their blood pressure and pulse rate, which are 120/80 to 140/90 and 60 to 100 beats per minute, respectively. Therefore, in recent years, heart illnesses have emerged as the leading cause of illness, particularly among younger generations. Congenital heart conditions, heart attacks, heart failure, arrhythmia, mitral regurgitation, coronary artery disease, hypertrophic cardiomyopathy, dilated cardiomyopathy, and myocardial infarction are only a few examples of the various heart disorders. These cardiac infections are diagnosed using various machine learning technologies. The most common technique is deep leaning because itcan be applied to both tabular data and picture categorization, for example. But in this study, they used Talos to construct a deep learning neural network model. Talos is a hyper parameter optimization approach that makes use of the Koras library and the Talos optimizer. A high level neural network model is produced using the deep learning neural network library keras. Convolutional neural networks and recurrent neural networks, as well as a mix of the two, are supported, and it operates quickly and simply. Talos is a totally automatic process that use both the CPU and the GPU. It provides findings for predictions and lists several issues with illness prediction. (S. Sharma and Parmar, et al., 2020).

All around the world and in all age categories, heart problems are the most prevalent illnesses. Heart illnesses are medical ailments that affect the heart and its components.

Heart disease risk factors include things like smoking, mental health difficulties, and food habits. Since cardiac disorders have the greatest fatality rate, early detection is crucial for preserving people's lives. Furthermore, it can be costly and dangerous to diagnose cardiac disease too late. With the aid of several parameters that are gathered from the patients, machine learning techniques are utilized to forecast illnesses. For their investigation, they gathered the data from the UCI machine learning repository. In this work, they utilized a variety of approaches, including the Naive Bayes classifier, Decision tree classification and KNN classification. Nave Bayes compares several attributes and shows how independently each feature may exist. It is quick, easy, and capable of making probabilistic predictions. While the K Nearest Neighbor method is employed for both classification and regression issues. Furthermore, it is non-parametric, which means it does not base any assumptions on the distribution of the data. The most popular approach is a decision tree since it is the simplest and has the form of a tree. It separates the data into smaller chunks and aids in the formulation of decisions and precise hypotheses on the many characteristics associated with sickness. Decision trees are also evolved gradually. (Manikandan, et al., 2020).

The leading cause of illness and mortality in the globe and the main factor in mortality during the last ten years are heart disorders. According to the Global Burden of Disease report, heart illnesses have increased significantly over the past ten years, and alone in India, about 1.7 million people have died from major heart ailments. Therefore, it is imperative to create some methods that might aid in the early detection of the disease and assist preserve priceless lives. Every day, the healthcare sector generates enormous amounts of data, most of it is repetitive, has several attributions, is insufficiently detailed, and has a cordial relationship with time. Data mining techniques make it possible to utilize this challenging data in a sophisticated way. a way to gather meaningful information and draw conclusions from it. As a result, these strategies also assist medical personnel in making wiser decisions about providing patients with appropriate care in a shorter amount of time. Heart conditions are further divided into several categories, including coronary disease, cardiovascular disease, and cardiomyopathy disease. Cardiovascular disease is a condition that mostly affects the heart and veins that deliver blood to the body. Heart disease prediction is broken down into three primary aspects, including the analysis of datasets, the creation of several designs, and the selection of the least expensive and most efficient design. Finally, accurate data from datasets is applied, and the outcomes are shown. (Rani, 2020).

The heart, which pumps blood to all the organs in the body, is the most significant component of the human body. If the heart stops beating, many other vital organs, including the brain, will soon follow, and the individual will pass very quickly. People these days are so busy going about their daily lives, carrying a heavy workload, and being stressed out. Additionally, poor dietary practices and idleness had a significant role in the present-day rapid rise in heart disease. The hardest labor in the healthcare industry is illness diagnosis, and early disease diagnosis can save many lives. Cardiovascular disorders are the leading cause of death and are very difficult to treat.machine learning algorithms are utilized to accurately detect these disorders as a result. The diagnosis of illnesses is currently done using a variety of tests, numerous surveys and questionnaires, and mining techniques, but even with all of this, it still depends entirely on the medical

experts. Various data mining methods are employed, including K-Nearest Neighbor and Artificial Neural Networks. Researchers are putting a lot of effort into creating a method that will help doctors forecast and correctly diagnose cardiac conditions. In this work, Support Vector Machine and Random Forest were also employed. The study of many parameters is conducted. These risk variables have a crucial role in the prognosis of illness. (Iyer et al., 2020).

The primary organ of the human body, the heart's job is to pump blood to all of the body's organs and body parts. All of the body's major organs are affected if the heart's functionality is impacted by any circumstance. Cardiac illness is characterized by abnormal cardiac function. Heart disease has recently been the leading global cause of morbidity and mortality. Heart disease is brought on by a number of bad lifestyle factors, including alcohol consumption, smoking, consuming too much fat (which can induce hypertension), and improper dietary choices. The World Health Organization estimates that roughly 10 million people each year pass away as a result of these cardiac conditions. People can benefit if illnesses are caught at an earlier stage. Even though heart disorders are the leading cause of mortality, there are several techniques that may be utilized to accurately detect a problem. The healthcare industry generates a large quantity of data, which may be utilized to analysis and extract information for future decision-making. The data mining approach is frequently utilized for this reason because it reveals the disease's hidden patterns. The subtype of data mining known as machine learning is effective at managing large amounts of database. This supports medical professionals' decision-making and efficient treatment approaches (Rajdhan et al., 2020).

The primary organ of the body, the heart, pumps blood to all other organs and body components. Any anomaly in the way the heart beats has major repercussions and can also have an impact on the brain and other body organs. A person promptly passes away if their heart stops beating, and heart attacks are the leading cause of illness and death in India. There are many different forms of heart disorders, but the largest class of heart conditions—which includes angina and myocardial infarction—are cardiovascular diseases. Coronary heart illnesses are a different class of heart conditions that have a role in the development of plaque. There are several indicators and symptoms of myocardial infarction, including chestache, exhaustion, arm ache, bradycardia, and low oxygen levels. Obesity, an unhealthy lifestyle, and excessive junk food intake are heart attack factors. A recent study found that roughly 17 million individuals worldwide pass away from cardiac diseases each year. The enormous volume of healthcare data is analyzed using machine learning algorithms. Age, sex, fasting blood sugar, blood pressure, kind of chest discomfort, serum cholesterol, resting electrocardiographic result, old peak, and other characteristics are investigated. To accurately and quickly forecast cardiac illnesses, naive bayes, decision trees, random forests, support vector machines, and logistic regression were utilized. For data relating to overfitting and real-world data, respectively, Random Forest, Decision Tree, Naive Bayes, and Support Vector Machine performed well (Gadde et al., 2020).

Since the previous 10 years, heart illnesses have been the leading cause of morbidity and death, and according to the World Health Organization, almost 17.9 million people die from heart disorders each year. About 80% of these fatalities are a result of brain strokes and coronary artery disease. Most of these fatalities have place in developing

and low-income nations. The emergence of illnesses is influenced by a variety of risk factors, including bad lifestyle choices and certain hereditary components. Additionally, unhealthy eating, alcohol use, smoking, and various physiological conditions including obesity, high blood pressure, high cholesterol, stress, idleness, and smoking all contribute to the development of cardiac problems. However, if a condition is detected early on, efficient treatment approaches can be used to save patients from passing away. This is accomplished by using data mining tools, which allow us to uncover obscure illness patterns and undiscovered data that may aid in disease diagnosis. Machine learning techniques are utilized for the mining of this data since the healthcare sector contains a vast quantity of information that the human mind cannot analysis on its own. Naive Bayes, K-Nearest Neighbor, Random forest, and decision trees are just a few of the data mining methods that may be utilized for this. These algorithms are used to classify and forecast cardiac illnesses at much earlier stages, assisting medical experts in making the final choice. Different qualities are taken, and then these algorithms are used. (Shah et al., 2020).

2 Literature Review

(J. P. Li et al., 2020) One of the more difficult ailments is heart disease, which affected a large number of individuals worldwide. Heart illness must be promptly and accurately diagnosed in order to be treated, especially in the field of cardiology. In this work, we suggested a machine learning-based approach for diagnosing cardiac disease that is both effective and accurate. The system's classification algorithms include Support vector machines, Logistic regression, Artificial neural networks, K-nearest neighbors, Naive bays, and Decision trees. Standard feature selection algorithms like Relief, Minimal redundancy maximal relevance, least absolute shrinkage selection operator, and Local learning have been used to remove unnecessary and redundant features. To address this issue, we have provided a brand-new, quick conditional mutual information feature selection approach. Difficulty with feature selection. In order to improve classification accuracy and shorten the time it takes to process classifications, features selection techniques are utilized. Additionally, the leave one subject out cross-validation approach has been utilized to tune hyper parameters and to identify the best practices for model assessment. The classifiers' performances are evaluated using the performance measurement measures. On the features chosen via features selection methods, the classifiers' performances have been evaluated. The experimental findings demonstrate the viability of the suggested feature selection approach (FCMIM) for developing a high-level intelligent system to detect heart disease using classifiers support vector machines. Comparing the proposed diagnosis system (FCMIM-SVM) to earlier presented approaches, it showed high accuracy. Furthermore, the Heart disease detection using the suggested approach is simple to apply in healthcare.

(R. Katarya and S. K. Meena, et al., 2021) People today tend to get caught up in the daily grind of work and other responsibilities while neglecting their health. People are becoming sick more frequently daily as a result of their hurried lifestyles and disregard for their health. Additionally, the majority of individuals have an illness like heart disease. According to data provided by the World Health Organization (WHO),

heart-related diseases account for over 31% of all fatalities worldwide. Therefore, it becomes crucial for the medical community to forecast whether or not cardiac disease may occur. However, the volume of data that hospitals and the medical industry receive makes analysis sometimes challenging. For medical professionals, using machine learning algorithms for this data management and prediction may be quite effective. Thus in this study, we covered heart disease, its risk factors, and machine learning methodology. We have forecast cardiac disease using machine learning techniques and have presented a comparative comparison of the machine learning algorithms utilized for the experiment of the prediction. This study's purpose or objective is to use machine learning to forecast the occurrence of heart disease and to analyses such predictions.

(S. Guruprasad, et al., 2021) Heart disease, the major cause of death worldwide during the past few decades has been heart disease, sometimes known as cardiovascular disease. It comprises a wide range of conditions that affect the heart. It connects many heart disease risk factors to the urgency of taking immediate action. Accurate, trustworthy, and sane methods that result in an early diagnosis and prompt sickness care. In the healthcare sector, data mining is a common technique for analyzing enormous volumes of data. To help healthcare practitioners forecast heart illness, researcher's analyses huge, complex medical data using a range of data mining and machine learning techniques. This paper provides a model based on supervised learning techniques such as Naive Bayes, decision trees, and K-nearest neighbors and a number of heart disease-related factors. Utilizing the method of the random forest. It utilizes the most recent dataset from the Cleveland database of the UCI heart disease patient repository. The collection has 76 traits and 303 occurrences. Only 14 of these 76 qualities, which are essential for demonstrating how well different algorithms work, are used in the testing process. This research's goal is to estimate the chance that a patient will develop heart disease. The results demonstrate that K-nearest neighbor produces the highest accuracy score.

(Nalluri et al., 2020), According to a study by heart conditions have become the most common illnesses in recent years. According to studies, around 15% of all naturally occurring deaths—or 17.9 million—occurred in 2017 as a result of cardiovascular disorders. Chronic heart disorders (CHD) are the most prevalent sort of heart problems, and thankfully, they may be early identified by monitoring other bodily functions including blood pressure, body glucose levels, heart rate, and cholesterol levels. It can also be determined by other factors, such as a person's body mass index and how many cigarettes they smoke each day. In this work, data mining methods were employed to predict heart illnesses by the previously described current circumstances. The XGBoost algorithm and logistic regression are two methods that are beneficial in this respect, according to this article. These methods aid in the early detection of cardiovascular problems, which lowers the likelihood that a person may acquire heart disease.

Saleh et al., 2020 found that data mining is a method for extracting information from enormous amounts of data. They discussed the association rule, categorization of the data, information clustering, prediction out of all the data sets, and sequential model, which are the most popular approaches and keys for data mining. There are several instances where this approach may be used if there are plenty of data sets. Additionally, it is essential for the early diagnosis and prognosis of several illnesses in hospitals. Patients require a variety of tests for the accurate diagnosis of any condition, however

data mining tools can lessen this. This smaller number of tests has a big impact on length and results. Heart conditions predominate. Cardiovascular illnesses, which can be deadly, as well as other health problems in general, are now quite prevalent. A lot of lives can be saved by early illness prediction utilizing data mining techniques since the healthcare business nowadays has numerous hidden data that are essential for accurate diagnosis and disease prediction. In this work, Weka 3.8.3 software is used to extract data using algorithms including K-star, J48, SMO, Naive Bayes, MLP, Random Forest, Bayes Net, and REPTREE. The standard set of data and previously acquired datasets were integrated with the results of the prediction using the ROC curve and AUC value. Different data mining techniques may be used to forecast diseases, and these patients can be utilized as training data. Thefact that previous research needed a lot of characteristics and precision was one of their constraints. Additionally, data mining techniques were used in this study to predict cardiovascular diseases based on several heart health-related parameters, including blood pressure, cholesterol levels, patient heart rates, diabetes, stress, smoking habits, obesity, and hypertension. Data mining techniques aid in illness prediction at an early stage, thus saving lives.

3 Research Methodology

3.1 Materials

Sample Dataset

In this research, Since the dataset was obtained from the Kaggle website, we used secondary data. There are several distinct characteristics in the dataset. As a result, the data was analyzed to extract pertinent information and identify the factors of choice that were most closely related to the development of cardiac problems.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
1	Age.Group	Gender	Locality	Marital status	Life.Style	Sleep	Category	Depression	Hyperlipi	Smoking	Family.History	Diabetes	HTN	Allergies	BP	S.Sodium	S.Potassium	S.Chloride	C.I
2	41-50	Female	RURAL	MARRIED	NO	NO	FREE	YES	YES	NO	NO	1	NO	NO	100.6	138	3.3	107	
3	51-60	Female	URBAN	MARRIED	NO	NO	FREE	YES	YES	NO	NO	0	NO	NO	90.6	144	4.7	104	
4	51-60	Female	RURAL	MARRIED	YES	YES	FREE	YES	YES	NO	NO	1	YES	NO	100.7	137	4.2	103	
5	51-60	Female	RURAL	MARRIED	YES	YES	FREE	YES	YES	NO	NO	1	YES	NO	160.1	137	4.2	103	
6	51-60	Female	RURAL	MARRIED	YES	NO	FREE	YES	YES	NO	NO	1	YES	NO	90.6	139	4.5	112	
7	51-60	Female	URBAN	MARRIED	NO	NO	FREE	YES	YES	NO	NO	1	YES	NO	140.7	130	5.3	100	
8	51-60	Female	RURAL	MARRIED	YES	YES	PAID	YES	YES	NO	NO	1	YES	NO	120.8	146	3.9	100	
9	51-60	Female	RURAL	MARRIED	NO	NO	FREE	YES	YES	NO	NO	1	NO	NO	100.6	138	3.3	107	
10	51-60	Female	URBAN	MARRIED	NO	NO	FREE	YES	YES	NO	NO	0	NO	NO	90.6	144	4.7	104	
11	51-60	Female	RURAL	MARRIED	YES	YES	FREE	YES	YES	NO	NO	1	YES	NO	100.7	137	4.2	103	
12	51-60	Female	RURAL	MARRIED	YES	YES	FREE	YES	YES	NO	NO	1	YES	NO	160.1	137	4.2	103	
13	51-60	Female	RURAL	MARRIED	YES	NO	FREE	YES	YES	NO	NO	1	YES	NO	90.6	139	4.5	112	
14	51-60	Female	URBAN	MARRIED	NO	NO	FREE	YES	YES	NO	NO	1	YES	NO	140.7	130	5.3	100	
15	61-70	Female	RURAL	MARRIED	YES	YES	PAID	YES	YES	NO	NO	1	YES	NO	120.8	146	3.9	100	
16	61-70	Female	RURAL	MARRIED	NO	NO	FREE	YES	YES	NO	NO	1	NO	NO	100.6	138	3.3	107	

Fig. 1. Dataset used in the study

Data Processing

In order to extract relevant information and choose the characteristics that would be utilized in the study, data had to be analyzed. Following stages were engaged in data processing.

Data Cleaning

In this step, For the information model that was used to extract missing information,

identify copied information, and purge superfluous information, an organization was created. Thus, after further processing, we finally get the most useful information.

Data Selection
At this point, we have chosen and recovered the data from the dataset that will be used in further research. There are several attributes in the heart disease dataset that are already shown in (Fig. 1). The dataset must go through this process because of the nature of the information.

Data Transformation
This phase, often referred to as the data consolidation step, is highly crucial since it transforms the data we previously picked into a format that is appropriate for data mining algorithms. Datasets were normalized for the decrease of the effect of scale once the data file was stored.

Data Mining Stage
In this stage, we mostly employed the following four methods: K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Logistic Regression (LR). These methods were primarily utilized to analyses the dataset, and they provided percentage values for the dataset's training section. Following this stage, hidden data in the dataset as well as interesting illness patterns were discovered.

Methodology
In order to forecast cardiac illnesses using the provided attributes, several algorithms were used to the dataset at each stage. To extract the findings with the best accuracy and demonstrate the predictive power of the various data mining methods, we employed 13 distinct variables.

Data Collection
This step is vital to consider before using any data mining techniques, and we have gathered the secondary data from the Faisalabad Institute of Cardiology. Due to the fact that we employed the Python programming language tool for our research and that it processed the heart disease data in the form of Excel sheets.

Data Pre-Processing
For the use of data mining techniques, is also crucial. To get over the difficulties in the information finding process, this step is taken. The pre-processing of undesired data involves the procedures listed below.

- Data Cleaning: The additional data from the initial data gathering stage is deleted in this phase. It is carried out in order to get relevant and reliable data. In order to identify outliers, fill in any missing numbers, and rectify any discrepancies in the data, this phase is also used to smooth out noise.
- Consolidating data: This process is sometimes referred to as data transformation, as was already explained. This process involves transforming data into a format that can be used by data mining algorithms. The data may be used to make the adjustments below.

- Smoothing: In this stage, noisy data from the dataset, including results from various regression approaches like binning and clustering, are eliminated.
- Generalization: with visualizing data systems, low-level data characteristics are replaced with high-level data features in this stage.
- Routine: -1.0 attribute data are scaled to fall inside the narrow given range, such as 1.0 to 0.0 or 1.0.
- Build attributes: In this stage, we added a few more qualities that were useful for building the data mining process further.
- Data Loss: This stage covers several data selection methods that might result in the least amount of data loss. This is accomplished through data discretization, dimensionality reduction, and information selection.
- Discretization is the process of breaking data down into sets of brief periods. Divide the continuous characteristics into the desired range of intervals to do this. It aids in enhancing theproductivity of the work.

Knowledge Discovery

For Various data mining techniques, including outlier analysis, clustering, prediction, classification, and association rule procedures, are utilized to find meaningful information. The statistical data mining programmer may make advantage of these. Figure below depicts the process of knowledge discovery (Fig. 2).

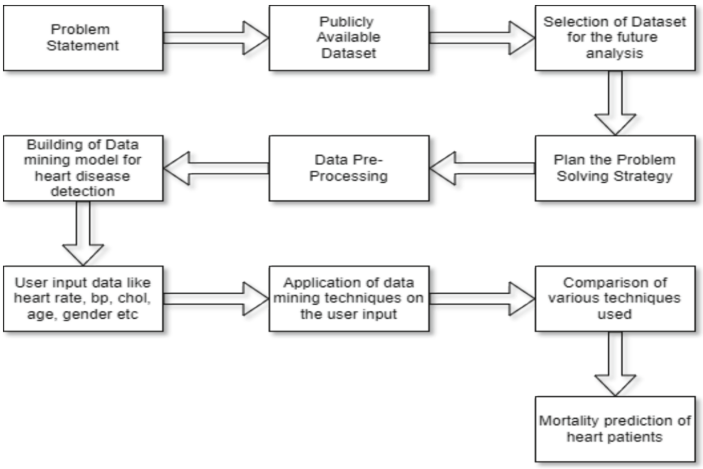


Fig. 2. Research methodology flow chart

Data Mining Techniques

For the prediction of cardiac illnesses utilizing various variables, we applied four distinct data mining approaches in this work, including Logistic Regression (LR), Decision Tree (DT), K-Nearest Neighbor (KNN), and Support Vector Machine (SVM).

Logistic Regression
In Logistic Modeling the likelihood of a discrete result given an input variable is the process of regression. The most popular types of logistic regression model a binary result, such as true or false, yes or no, and so on. Dependable output for deaths and mortality the algorithm calculates the chance of occurrence numerically, and the choice is made based on the percentage between 0 and 1.

Decision Tree (DT)
Data is divided into groups using decision trees, which are a type of supervised machine learning approach. Decision trees consist of two key components: leaves and nodes. While nodes show the sites where data is divided, leaves reflect the outcomes in their ultimate form (Fig. 3).

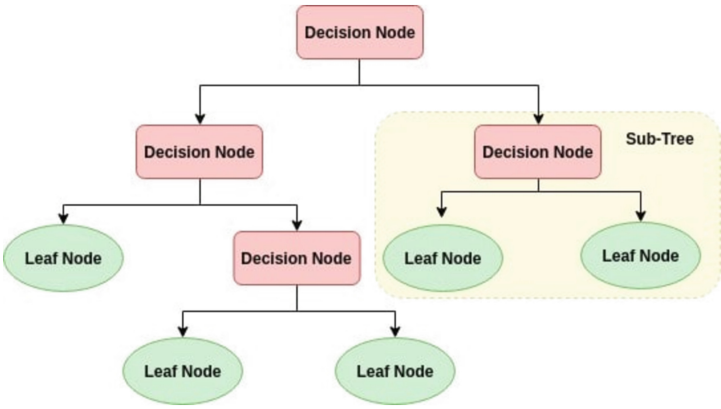


Fig. 3. The Decision tree showing leaves and nodes

Types of Decision Tree
There are two main types of decision tree that are.

- Classification tree
- Regression tree

Classification Tree
The variables in discrete classes are assigned, recorded, and labelled using it. It also offers a level of assurance that our classification tree, which was created via binary recursive partitioning, is accurate. This kind of decision tree is created when a data mining work involves the categorization and prediction of results, and the main goal is to produce rules that are simply understood. First we establish a training set in which all of the records' categorization labels are known. The next phase of our method is to systematically assign one of the two subgroups to each record. Thus, we can have a homogeneous set of labels in each partition, such as two labels that are opposite one

dividing to each division and continuing to divide until there are no more splits that are still helpful. The algorithm's core rule is the one that determines the first split rule. Another. Next, we apply (Fig. 4)

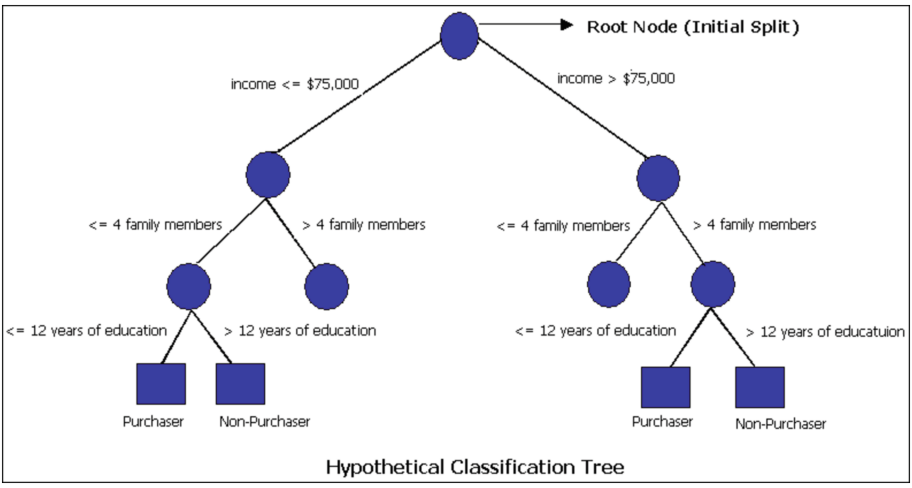


Fig. 4. Classification tree showing initial split.

Regression Tree

In this particular decision tree, the outcome variables are continuous and take the form of integers like 123. The data is broken up into smaller groups, and a constant model is fitted for each subgroup. Unfortunately, the model should be extremely unstable if it is only one tree; however, bagging regression trees can make the model effective and helpful.

A sequence of binary partitions that depend on different predictors are used to carry out the partitioning. The constant needed to make the prediction is determined based on the average response values for all of the observations in the subgroup.

Support Vector Machine (SVM)

In it is a sort of supervised machine learning method mostly utilized for the categorization of data into several classes. Because it employs a hyper plane as a decision boundary between several classes, it differs from previous algorithms in this regard. Both classification and regression issues may be addressed using it. Non-linear data classification is another use for it.

Classification of Linear Data

Consider that we have the tags red and blue as well as the locations x and y. Our training data is now plotted on a plane. The tags will then be separated by a hyper plane using support vector machines (Fig. 5).

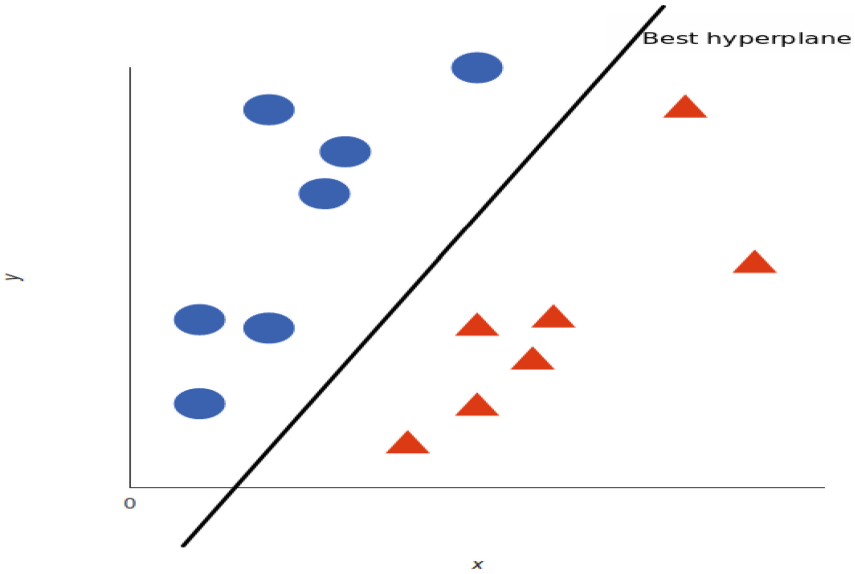


Fig. 5. SVM plot showing hyper plane.

K-Nearest Neighbor (KNN)
It is a supervised machine learning approach that relies on the characteristics of nearby data points to categories fresh data points into the desired class. It is a pretty straightforward method that works for a variety of issues. It is based on feature similarity, and KNN classifies the data points inside a comparable point by comparing feature similarity to neighboring data points. It works with realistic data rather than making assumptions. Both classification and regression issues may be solved with it. The term "K Nearest Neighbor" refers to the number of closest neighbors. There is a new data point, as seen in the figure below, and there are around 7 neighbors closest to it. The class that is most comparable to the new data point will be assigned to it. In accordance with the fig., there are 3 squares and 4 triangles next to the new data point; hence, we will categories the new data point into class B since it has more nearby neighbors. KNN operates in this way, but there are actually a lot more factors to take into account.

4 Conclusion

In this study, we explore efficient and accurate data mining methods for predicting mortality in cardiovascular patients. Data mining methods are currently being used regularly for more accurate mortality predictions. These methods reveal diseases and valuable information hidden in the patterns.

In order to extract the results more accurately and demonstrate the predictive power of various data mining methods, we used 13 different variables. Age, gender, high blood pressure, high cholesterol, and irregular heartbeat are just a few of the many variables that affect the development of the condition. Secondary data from 470 patients were used and 56 different attributes were selected.

Then, K-Nearest Neighbors, Decision Trees, Support Vector Machines, and Logistic Regression are used as the four main methods of data mining. The results are then generated using the R language, which is used to code these programs. The decision tree method has the highest accuracy and is therefore the most efficient.

References

1. Lutimath, N.M., Chethan, C., Pol, B.S.: Prediction of heart disease using machine learning. Int. J. Recent Technol. Eng. **8**(2S10), 474–477 (2019). https://doi.org/10.35940/ijrte.B1081.0982S1019
2. Nahiduzzaman, M., Nayeem, M.J., Ahmed, M.T., Zaman, M.S.U.: Prediction of heart disease using multi-layer perceptron neural network and support vector machine. In: 2019 4th International Conference on Electronics Information Communication Technology EICT 2019, no. December, pp. 1–6 (2019). https://doi.org/10.1109/EICT48899.2019.9068755
3. Jane, R., et al.: Prediction of cardiac disease using supervised machine learning algorithms Arun Raj Lakshminarayanan. no. Iciccs, pp. 570–575 (2020)
4. Singh, A., Kumar, R.: Heart disease prediction using machine learning algorithms. In: International Conference on Electric Electronics Engineering ICE3 2020, pp. 452–457 (2020). https://doi.org/10.1109/ICE348803.2020.9122958
5. Guruprasad, S., Mathias, V.L., Dcunha, W.: Heart disease prediction using machine learning techniques. In: 2021 5th International Conference on Electrics Electronics Communication Computational Technology Optimization Techniques ICEECCOT 2021 – Proceedings, vol. 1, no. 6, pp. 762–766 (2021). https://doi.org/10.1109/ICEECCOT52851.2021.9707966
6. Dler, E.D., et al.: Improving risk prediction in heart failure using machine learning. Eur. J. Heart Fail. **22**(1), 139–147 (2020). https://doi.org/10.1002/ejhf.1628
7. Ghosh, P., et al.: Efficient prediction of cardiovascular disease using machine learning algorithms with relief and lasso feature selection techniques. IEEE Access **9**, 19304–19326 (2021). https://doi.org/10.1109/ACCESS.2021.3053759
8. Ping Li, J., Ul Haq, A., Din, S.U., Khan, J., Khan, A., Saboor, A.: Heart disease identification method using machine learning classification in e-healthcare. IEEE Access **8**, 107562–107582 (2020). https://doi.org/10.1109/ACCESS.2020.3001149
9. Katarya, R., Meena, S.K.: Machine learning techniques for heart disease prediction: a comparative study and analysis. Health Technol. (Berl) **11**(1), 87–97 (2021). https://doi.org/10.1007/s12553-020-00505-7
10. Khan, Y., Qamar, U., Yousaf, N., Khan, A.: Machine learning techniques for heart disease datasets: a survey. In: ACM International Conference on Proceeding Services, vol. Part F148150, pp. 27–35, 2019, https://doi.org/10.1145/3318299.3318343
11. Singh, A.K., Dixit, A., Jamshed, A.: Heart disease risk predictor system using data mining learning techniques: analysis. Int. J. Comput. Appl. **176**, 8879–8887 (2020)
12. Singh, R.: A review on heart disease prediction using unsupervised and supervised learning. Neural Netw. **99**, 430–434 (2020)

Automated Detection of COVID-19 Using Deep Convolutional Neural Network (CNNs) Using Chest Radiograph and CT Scan Images

Naeem Uallah[1], Javed Ali Khan[2(✉)], Asaf Raza[1], Syed Yaqub Shah[2], Muhammad Assam[2], and Hasna Arshad[3]

[1] Department of Software Engineering, University of Engineering and Technology Taxila, Taxila, Pakistan

[2] Department of Software Engineering, University of Science and Technology Bannu, Bannu, Pakistan

javed_ali@ustb.edu.pk

[3] Department of Computer Science, HITEC University, Taxila, Pakistan

Abstract. Many countries are severely affected by COVID-19, and massive efforts are required to mitigate the terrible impacts of the COVID-19 global epidemic. To stop COVID-19 from spreading widely and minimize COVID-19 patient treatment issues, early discovery of the virus in its early stages is essential. Conventional methods for COVID-19 detection are time-consuming, cumbersome, unreliable, and yield an incorrect diagnosis. Most deep learning (DL) methods for COVID-19 identification described in the past only support one data type (chest radiographs or CT scan images). Examining unusual patterns in various data types may yield high classification performance. For this purpose, we use two image datasets: chest radiographs and chest computer tomography (CT). This research study proposed an excellent COVID-19 detection strategy based on the Resnet-18 deep convolutional neural network (CNN) to timely and efficiently identify COVID-19 spread. Also, we used each image data type to conduct extensive Covid-19 detection experiments with the proposed DL model. We performed a trinary classification task (normal, covid-19, and pneumonia) using chest radiographs and a binary classification (COVID-19 and Normal) using CT scan images. We validated the performance of the proposed approach on two standard Kaggle datasets, i.e., the COVID-19 Radiography Database and the SARS-CoV-2 CT scan dataset. The Resnet model's detection accuracy of 99.42% using chest radiographs (CRs) and 100% using CT scans for COVID-19 detection indicates its efficacy in detecting COVID-19.

Keywords: Chest radiographs · COVID-19 · CT scans · detection · resnet18 · Deep learning

1 Introduction

Recently, the world has witnessed a global epidemic due to the coronavirus (COVID-19). The pandemic destroyed millions of people's lives. It has a greater impact on mental health, economic misery, and causes respiratory problems by infecting the lungs. In

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 61–74, 2025.
https://doi.org/10.1007/978-3-031-77620-5_5

such a challenging circumstance, a person may develop pneumonia, which causes pus to accumulate in the air sacs of the lungs. Because of its nature (rapid transmission), the COVID-19 virus is fatal. This virus can spread through physical contact with a COVID-19 patient and air.

The polymerase chain reaction (PCR) test, which searches for indications of the virus's biogenetic components in the subject's blood, is mostly used to identify COVID-19 in blood samples. Due to the time (PCR is extremely slow) and money (PCR is expensive), adequate PCR testing has sadly become nearly impossible as the number of COVID-19 affected individuals rises. In order to quickly identify COVID-19 patients and quarantine or isolate them, a different approach is required. It is urgently necessary to develop an automated COVID-19 detection system that can quickly and accurately identify the disease.

The early phases of COVID-19 have recently been reliably and automatically detected using a variety of medical imaging modalities, including CT and CR scans. The first rapid, low-risk, and affordable method for evaluating COVID-19 was the X-Ray modality. Patients are exposed to less radiation when receiving CRs, and they are routinely used to diagnose pneumonia. Similarly, compared to RT-PCR, chest CT imaging provides a more precise, affordable, and quick diagnosis of COVID-19. For the purpose of diagnosing pneumonia, CT scans create a thorough 3D image of the lungs [1]. Lung CT scans are painless, rapid, and simple procedures. Additionally, they are more susceptible to COVID-19 infection [2].

To correctly detect COVID-19 researchers used DL techniques. Early in 2020, several studies were conducted to develop computerized DL frameworks for accurate COVID-19 detection [3]. Most of these investigations classified COVID-19-infected or healthy CR pictures using DL frameworks. For COVID-19 identification or pneumonia detection [4], scientists have previously deployed DL networks such as Mobilenetv2, Squeeze net, and VGG, among others. For the discovery of COVID-19 through X-Rays images, Apostolopoulos et al. used the VGG19 pre-trained framework [5]. Panwar et al. [6] proposed the COVnet framework for COVID-19 identification based on the information leaking idea. COVID-19 and normal cases were classified using a model proposed by Sethy et al. [7]. A DL algorithm for identifying COVID-19 from chest CT scans was suggested by Zheng et al. [8]. For COVID-19 identification, Zhang et al. used CR pictures and a deep anomaly detection model [9].

COVID-19 has little state-of-the-art literature when it comes to imaging technology. The majority of the works use DL methods for COVID-19 identification. DL systems are data-starved techniques that require massive training data. However, employing CNNs in medical imaging is challenging because of limited data availability. A limited dataset makes DL framework training challenging because of overfitting. As a result, addressing these flaws with pre-trained models on transfer learning and fine-tuning is a realistic option. Also, most available algorithms were created to train on a specific data type, such as CR or CT scans. Furthermore, most studies cited separate models for each data category. We built an architecture that can identify COVID-19 utilizing both CR and CT imageries, based on the concept that combining various data types (CR and CT images)

can provide additional information [10]. For this purpose, we used Resnet18, a well-known CNN architecture that has been demonstrated to perform well in various image detection tasks. The main contribution of this research is as follows;

- To find COVID-19-positive cases, we employed Resnet18, a transfer learning-based framework for CR and CT scan images.
- We examined and evaluated the Resnet18 DL model's classification (detection) performance in terms of its ability to identify COVID-19 using two different types of picture data.
- The same model is used to detect COVID-19-infected patients using different data sources for both multiclass classifications using CR images and two-class classification using CT scans.
- Using the common COVID-19 Radiography Database and the SARS-CoV-2 CT scan datasets, we assessed the performance of the proposed technique.
- Furthermore, using CT scans, we evaluated the performance of our model in comparison to hybrid strategies.

This work is arranged as follows; Sect. 1 represents the introduction, the methodology is presented in Sect. 2, Sect. 3 is about results and discussion, and Sect. 4 shows the conclusion and future work.

2 Proposed Approach

This section goes through the proposed COVID-19 classification method in detail. The goal of the project was to develop a single architecture that can be used for more accurate binary and multiclass categorization utilizing CR and CT scans. Figure 1 depicts the essential logic behind our strategy. To categorize the images of two datasets and detect COVID-19, the proposed DL system uses the Resnet18 DL framework.

The proposed study is divided into two stages: the first stage involves the detection of COVID-19 using CR images, and the second stage involves the detection of COVID-19 using CT scan images. Training and testing dataset collections have been created. We used 20% of the data (CT or CR pictures) for model validation and 80% of the data (CT or CR images) for framework training. The weights of the pre-trained Resnet18 network are altered by freezing the weights of the network's initial layers (i.e., the weights of the initial layers are not changed during training). The fully connected layers (FC), on the other hand, are adjusted to transfer the feature representations collected by the initial layers into class label data. The 1000 different categories they developed have been replaced by the classification layer and final FC layer of the model. The proposed framework is used to classify CR and CT images into multiple and two classes to look for COVID-19-positive occurrences (COVID-19 infected persons). Figure 1 shows the basic flow of our approach.

2.1 A Subsection Sample

We employed the Resnet18 [11] in the proposed work, the most commonly used lightweight DL architecture. The model, which is deeper than a normal CNN, has 18

learnable layers, including 17 convolutional layers, a global average pooling (GAP) layer, and a fully connected layer (FC). Our model's initial layer, known as the input layer, accepts 224 × 224 input pictures (from a CR or CT scan) for processing. Batch normalization (BN) operations and relu activation functions are used with Conv layers. Two pooling layers are employed at the start and end of the network. For example, the maximum pooling layer (having filter size of 3 × 3, padding of 1 × 1, and stride of 2 × 2) at the start of the network and the GAP layer at the end of the architecture to reduce the computational complexity. The first convolution layer applies 64 filters of size 7 × 7 on input image (CR or CT scan), the next four convolution layers apply 128 kernels of size 3 × 3, the next four convolution layers apply 256 kernels of size 3 × 3, and the final four convolution layers apply 512 filters of size 3 × 3. The sixteen Conv layers provide trainable feature maps and feature extraction. Once these feature maps have been submitted to FC, the categorization probabilities employed by the last classification layer are determined using soft-max activation. The details of the proposed approach are shown in Table 1.

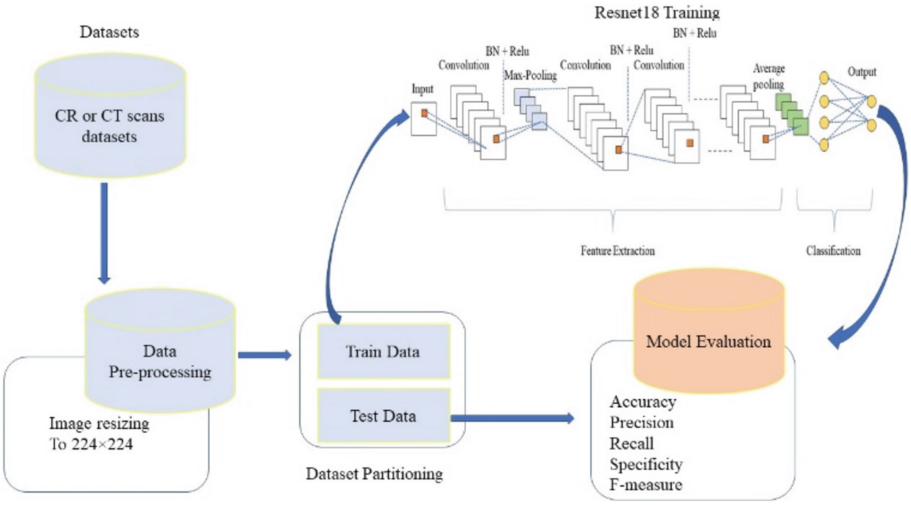


Fig. 1. The block diagram of the proposed approach

2.2 A Subsection Sample

After performing some experimental tries on a dataset with small number of images, the hyperparameters for the proposed model are chosen. The details of the selected parameters are shown in Table 2. We applied stochastic gradient descent to train our network. Using the proposed framework, trained over 22 epochs, radiographs and CT images are divided into multiclass and binary groups.

Table 1. The proposed Resnet18 Architecture.

S. No.	Layer	Filters	Size	Padding	Stride
1	Conv1	64	7 × 7	3 × 3	2 × 2
2	Maximum pooling	64	3 × 3	1 × 1	2 × 2
3	Conv2-Conv5	64	3 × 3	1 × 1	2 × 2, 1 × 1, 1 × 1, 1 × 1
4	Conv6-Conv9	128	3 × 3	1 × 1	2 × 2, 1 × 1, 1 × 1, 1 × 1
5	Conv10-Conv13	256	3 × 3	1 × 1	2 × 2, 1 × 1, 1 × 1, 1 × 1
6	Conv14-Conv17	512	3 × 3	1 × 1	2 × 2, 1 × 1, 1 × 1, 1 × 1
7	Average pooling		7 × 7	0	7 × 7
8	Fully connected Layer (FC)				

3 Result and Discussion

In this section, we review the results of several experiments run to assess the performance of the proposed method. This section also provides more information on the datasets utilized to evaluate the efficacy of the suggested approach.

Table 2. Hyperparameters of the proposed approach.

Parameter	Value
Optimization algorithm	SGDM
Shuffle	Every epoch
Learning rate	0.001
Validation frequency	30
Maximum epochs	22
Iterations per epoch (CT scans)	223
Activation function	Relu
Verbose	false

3.1 Datasets

To recognize COVID-19 in CR pictures, a standard COVID-19 radiography database [12, 13] created by medical professionals is used. In this database, there are 10192 radiographs of healthy people and 1345 radiographs of healthy people with viral pneumonia, lung opacity, and COVID-19 infection. All radiograph in this database is of 1024 x 1024 pixels. Whereas, the CT scans of a SARS-CoV-2 CT scan dataset [14], which contains COVID-19 infected (1252 CT scans) and healthy individuals (1230 CT scans), were

used to identify COVID-19 (a total of 2482 images). These statistics were gathered from genuine Brazilian hospital patients. Figure 3 displays a few photos from the dataset. Table 3 lists the diversity and numerical specifics of both datasets (Fig. 2).

Table 3. Dataset details.

Data set	Images	Images Collections			
Chest Radiography Database	Chest Radiographs	Normal	Pneumonia	COVID	Lung Obesity
		1092	1345	3616	6012
SARS-CoV-2 CT scan dataset	CT Scan	Non-COVID		COVID	
		1230		1252	

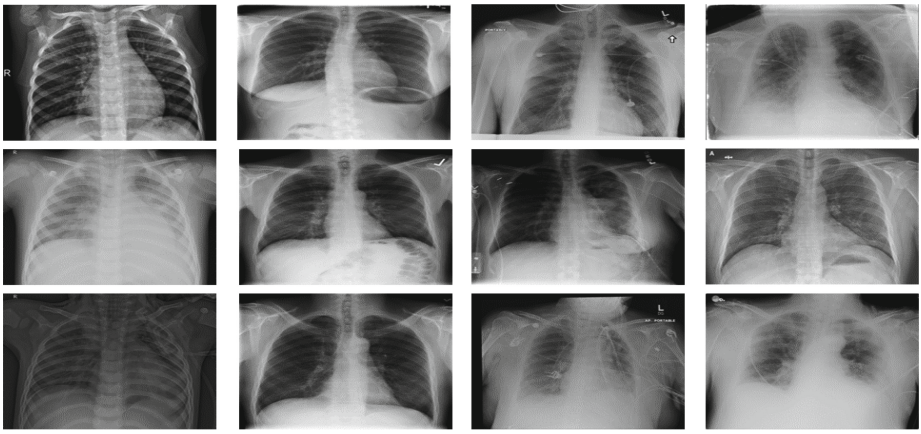


Fig. 2. The first column of the COVID-19 radiography database images samples contains viral pneumonia, the second column contains Normal, the third column contains lung obesity, and the fourth column contains COVID-19 CR images.

3.2 Evaluation Matrices

To validate the effectiveness of the planned approach, Accuracy, Precision, Sensitivity (Recall), Specificity, and F1 Score were employed as evaluation criteria.

$$Accuracy = \frac{\mathrm{TF} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FN}} \tag{1}$$

$$\mathrm{Precision} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{2}$$

$$Sensitivity(recall) = \frac{TP}{TP + FN} \tag{3}$$

$$Specificity = \frac{TN}{TN + FP} \tag{4}$$

$$F1_score = 2 \cdot \frac{Precision \times Recall}{Precision + Recall} \tag{5}$$

True positive, total samples, false positive, true negative, and false negative are denoted by the letters TP, TS, FP, TN, and FN, respectively.

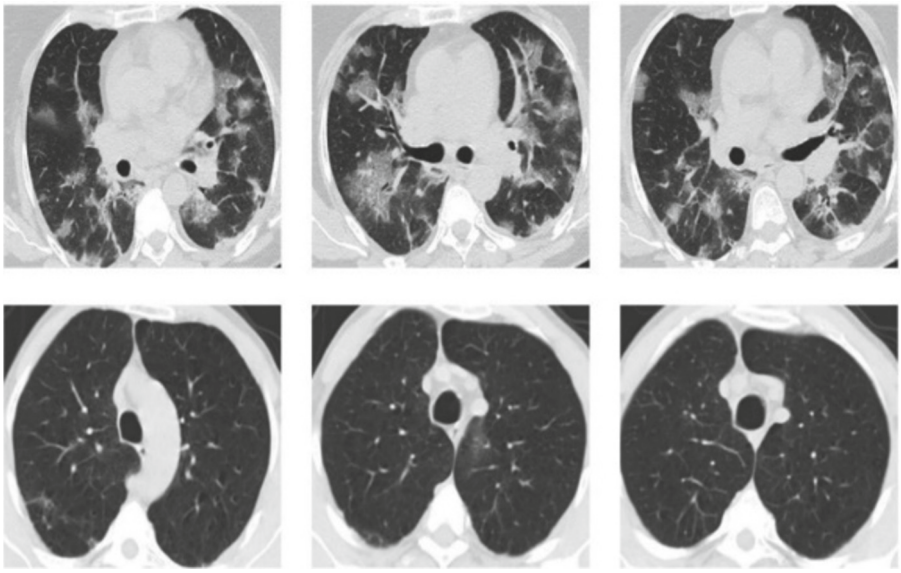


Fig. 3. The upper row has COVID-19 pictures samples, whereas the lower row has non-COVID images samples from the SARS-CoV-2 CT scan dataset.

3.3 Experimental Setup

An 8 GB RAM laptop with an Intel (R) Core (TM) i5-5200U CPU was used for the model testing. To conduct the research topic, we employed the R2020a version of MATLAB. The effectiveness of the proposed method for multiclass and binary classification utilising CRs and CT scans is evaluated using a variety of tests. Our suggested model is trained and validated using the hyper-parameter values in Table 2.

3.4 Performance Evaluation on COVID-19 Detection Using CRs

In this study, the efficiency of the suggested framework for COVID-19 detection utilizing multiclass classification from chest radiographs will be evaluated (pneumonia, normal,

and COVID-19). The COVID-19 Radiography Database's entire collection of 15153 radiograph images was used in this study; 12123 radiographs (2893 COVID-19 cases, 1076 pneumonia cases, and 8154 healthy individuals) were used for training, and the remaining 3031 radiographs (723 COVID-19 cases, 269 viral pneumonia cases, and 2038 healthy individuals) were used for analysis. For COVID-19 identification, the suggested model's training took 1772 min and 23 s. Our method successfully classified COVID-19 data into three categories, with average accuracy, precision, recall, specificity, and F1-score values of 99.42%, 98.33%, 99.0%, 99.42%, and 99.20%, respectively. In Fig. 4, accuracy and loss are shown so that you may assess the training efficiency of our approach. Our model's loss after epoch 4 is almost equal to 0, showing that it forecasts COVID-19 with greater accuracy. As can be seen in the image, the accuracy after epoch 6 is almost identical to 99 percent. These outcomes show that our model was successful in extracting the most effective and detailed elements to characterize the radiological image for reliable and correct categorization.

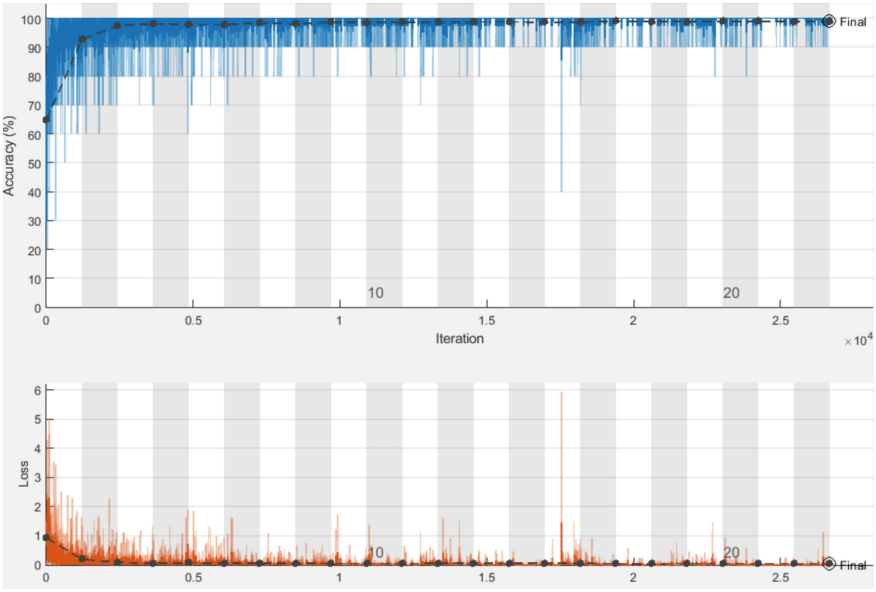


Fig. 4. Accuracy and loss of Resnet18 for COVID-19 detection using CR images.

3.5 Performance Evaluation on COVID-19 Detection Using CT Scans

By employing COVID-19 CT images, this study aims to demonstrate the effectiveness of our approach for COVID-19 identification. All 2482 COVID-19 CT scans from the SARS-COV-2 Ct-Scan Dataset (1252 positive and 1230 negative CT scans) were used in this experiment, with 1986 images (1002 COVID-19 and 984 healthy CT scans) used for training and 496 pictures (250 COVID-19 scans and 246 normal scans) used for validation. To recognize COVID-19 using CT scans, the suggested model needed to

be trained for 624 min and 10 s. With the highest possible accuracy, precision, recall, specificity, and F1 score of 100%, our approach effectively detected COVID-19. In Fig. 5, accuracy and loss are shown so that you can see how well our technique performs throughout training. Our model's loss after epoch 7 is almost equal to 0, showing that it forecasts COVID-19 with greater accuracy. Similar to this, the accuracy after epoch 18 is nearly equivalent to 100%, as indicated in the Fig. 5.

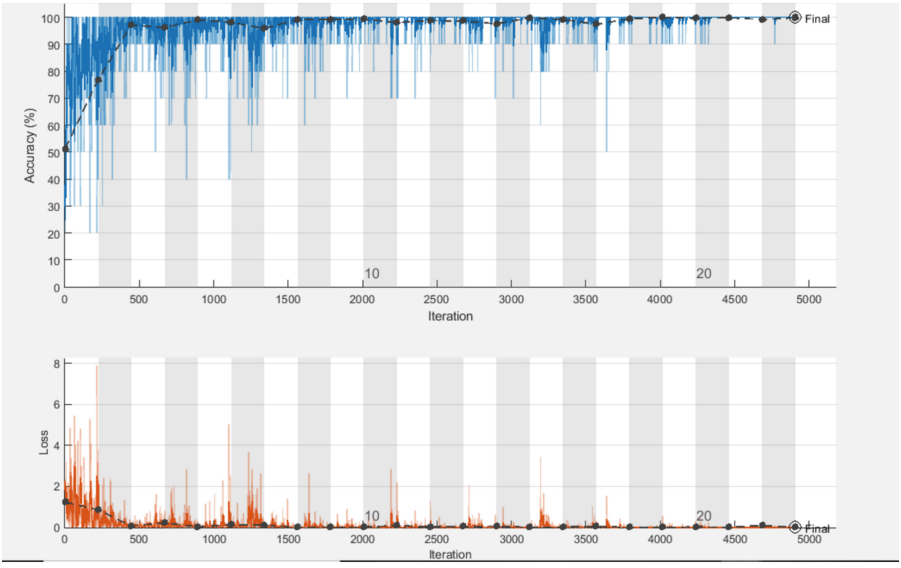


Fig. 5. Accuracy and loss of Resnet18 for COVID-19 detection using CT scans

3.6 Discussion

We investigated the causes behind Resnet18's success in detecting COVID-19 and discovered the following facts. These ideal results are obtained by the proposed method, which successfully extracts the most evocative, robust, comprehensive, and in-depth representative features to represent the images for precise classification. Due to its ability to extract more in-depth features using small filters of size 3×3, the suggested framework achieved the best results. The batch normalization method in the suggested model delivers regularization, reduces generalization error, and normalizes the inputs to a layer. The max-pooling layer aids in the reduction of model dimensions and parameters and the retention of critical feature information. The network is deep enough (18 layers) to extract more abstract high-level classification features. Instead of tanh or sigmoid, a relu is utilized, resulting in increased accuracy and faster network performance. Furthermore, the relu activation function also prevented the vanishing gradient.

Because of the high classification accuracy of pre-trained models, we adopted a transfer learning technique instead of other machine learning algorithms to save time by

reducing the training requirements and evaluate the frameworks weights from scratch. The following are some of the advantages of the pre-trained Resnet18 frameworks: It is well suited for medical image categorization because a) it requires little dataset pre-processing; b) it has a faster learning process (because of relu); c) it can reduce time complexity by reducing numerous parameters; and d) it performs well on a dataset with limited data.

Following this comparison analysis, we discovered several limitations as well as potential future research projects for academics to pursue to further this research:

• In this study, the proposed approach is unable to characterize the different stages of COVID-19 infection, such as pre-symptomatic, asymptomatic, moderate, and severe, due to the lack of data examples that could be utilized to evaluate the intensity of COVID-19 disease.
• The study may be expanded to investigate the system's performance in detecting COVID-19 using ECG, lung ultrasonography, and lung PET (positron emission tomography) scans, among other imaging modalities.
• This research may also be expanded by utilizing a large-scale dataset containing millions of images because the quantity of training data significantly influences the efficacy of DL-based frameworks.

3.7 Comparison with Hybrid Approaches

Another hybrid experiment is carried out in this section to determine COVID-19 to assess the efficacy the Resnet18. We first used the top twelve deep neural networks to extract fine-grained features, and then we used those features to train an SVM with a linear kernel. We compared the performance of our resnet18 model with hybrid techniques using CT scans because we used them to attain the best results. We used the following networks: Mobilnetv2, Squeeznet, Alexnet, Inceptionv3, Darknet19, Resnet50, Resnet18, Resnet101, Inceptionresnetv3, and Shufflenet to complete the proposed study. The dataset images were correctly scaled to fit the deep neural network's image input requirements using augmented image data stores before being included in the DL models for feature extraction. Activations were done on the deeper layer (final GAP or FC layer) to extract high-level features. The results of the classification process employing deep features and the SVM approach are shown in Table 4. This experiment reveals that the deep features of all twelve networks and the SVM method provided results with lower accuracy when compared to the TL of Resnet18. The Resnet18 DL network's accuracy of 98.91 percent illustrates how effective it is in classifying tumors accurately.

Table 4. Accuracy Comparison Among the Resnet18 and Hybrid Approaches.

Model	Accuracy	Precision	Recall	Specificity	F1-score
Inceptionv3	72.78	73.0	77.0	66.18	74.9
Inceptionresnetv2	75.0	75.0	78.5	68.15	76.7

(*continued*)

Table 4. (*continued*)

Model	Accuracy	Precision	Recall	Specificity	F1-score
Darknet19	98.33	98.0	98.0	99.32	98.0
Resnet50	75.0	75.0	81.0	66.18	77.8
Resnet18	63.89	68.0	67.5	65.19	67.7
Resnet10	76.01	76.5	82.0	67.99	79.1
Shufflenet	71.37	71.5	77.0	64.61	74.1
Squeezenet	71.37	71.5	75.0	65.20	73.2
Alexnet	71.98	72.0	76.5	65.51	74.1
Mobilenetv2	70.56	70.5	76.0	63.89	73.1

3.8 Comparison with State-Of-The-Art Approaches

In this DL experiment, the performance of the suggested approach is compared to that of currently available state-of-the-art techniques in the literature for recognizing and categorizing Covid-19 from CR and CT images. We contrasted (Table 5) the effectiveness of the proposed categorization framework with that of alternative approaches (measured in terms of accuracy (percent)) [15–18]. It's worth noting that the proposed model outperformed techniques [15–18] for COVID-19 detection using the same datasets. These approaches use deeper algorithms, which might result in overfitting, and only use one data type, such as CR or CT scans, making them more computationally intensive than the one described. The proposed method, on the other hand, is 18 layers deep and extracts detailed, high-level, and more sophisticated features for COVID-19 identification using the smallest filters—size 1×1 and size 3×3.

Table 5. Accuracy comparison among the proposed and state-of-the-art models.

S. No.	Publication	Task	Method	Year	Accuracy (%)
Utilizing the COVID-19 Radiography Database, comparison with prior COVID-19 detection methods					
1	Gabriel et al. [15]	COVID-19, Normal, and pneumonia classification	Round-off fine-tuning	2021	98.04%
2	Azhar et al. [16]	COVID-19, Normal, and pneumonia classification	Custom CNN	2021	98.00%
3	This study	COVID-19, Normal, and pneumonia classification	Resnet18	2022	99.98

(*continued*)

Table 5. (*continued*)

S. No.	Publication	Task	Method	Year	Accuracy (%)
Using the SARS-COV-2 Ct-Scan Dataset, comparison with prior COVID-19 detection methods					
4	Basu et al. [17]	COVID-19 and Normal classification	Two-stage framework	2022	98.87%
5	Alquzi et al. [18]	COVID-19 and Normal classification	Efficientnet-B3	2022	99.0%
6	This study	COVID-19 and Normal classification	ResNet18	2022	100%

4 Conclusion

This research used the DL Resnet18 model to propose an excellent method for automated COVID-19 identification. Using two types of imaging data, CRs and CT scans are used by the proposed DL framework for accurate, robust, and reliable diagnoses of COVID-19. Furthermore, we tested the proposed hybrid model's robustness on two publicly available datasets. The ideal accuracy of 100% for COVID-19 detection using CT scans and 99.42% using CRs have been used to illustrate the significance of our suggested framework. The results of our experiments show that our system outperforms existing COVID-19 detection methods. After examining the outcomes, it is verified that using pre-trained Resnet18 for classification substantially affects the detection of COVID-19 from CR and CT scans. In the future, we aim to validate the performance of the proposed approach by testing it on the classification of Covid-19 from chest radiograph images [19, 27, 29], brain tumors [20, 21, 28], Pest detection [22], mask detection [23], epileptic seizure detection [24], predicting heart diseases [25, 26], and breast cancer [30] to further generalize it.

References

1. Gaal, G., Maga, B., Lukács, A.: Attention U-Net based adversarial architectures for chest X-ray lung segmentation. arXiv:2003.10304 (2020)
2. Fang, Y., Zhang, H., Xie, J., Lin, M., Ying, L.: Sensitivity of chest CT for COVID-19: comparison to RT-PCR. Radiology **296**(2), E115–E117 (2020). https://doi.org/10.1148/radiol.2020200432
3. Asmaa, A., Abdelsamea, M.M., Gaber, M.M.: Classification of COVID-19 in chest X-ray images using DeTraC deep convolutional neural network. arXiv preprint arXiv:2003.13815 (2020)
4. Antin, B., Joshua, K., Emil, M.: Detecting pneumonia in chest X-Rays with supervised learning. Semanticscholar. Org (2017)
5. Subramaniam, S., Manavalan, R.: Neural Network with Bee Colony Optimization for MRI Brain Cancer Image Classification. Int. Arab J. Info. Technol. (IAJIT) **13**(1) (2016)
6. Apostolopoulos, I.D., Bessiana, T.: Covid-19: automatic detection from X-ray images utilizing transfer learning with convolutional neural networks. Phys. Eng. Sci. Medi. **43**(635), 40 (2020)

7. Panwar, H., Gupta, P., Siddique, M.K.: Application of deep learning for fast detection of COVID-19 in X-Rays using nCOVnet. Chaos, Solitons Fractals **2020**, 109944 (2020)
8. Zheng, C., Deng, X., Fu, Q., et al.: Deep learning-based detection for covid-19 from chest ct using weak label. medRxiv (2020)
9. Zhang, J., Xie, Y., Li, Y., Shen, C., Xia, Y.: COVID-19 Screening on Chest X-ray Images Using Deep Learning based Anomaly Detection. arXiv:2003.12338v1 (2020)
10. Santosh, K.C.: Ai-driven tools for coronavirus outbreak: need of active learning and cross-population train/test models on multitudinal/multimodal data. J Med Syst **44**(5), 1–5 (2020)
11. He, K., Xiangyu, Z., Shaoqing, R., Jian, S.: Deep residual learning for image recognition. In: Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 770–778 (2016)
12. Chowdhury, M.E.H., et al.: Can AI help in screening Viral and COVID-19 pneumonia? IEEE Access **8**, 132665 (2020)
13. Rahman, T., et al.: Exploring the Effect of Image Enhancement Techniques on COVID-19 Detection using Chest X-ray Images **132**, 104319 (2021)
14. Soares, E., et al.: SARS-CoV-2 CT-scan dataset: a large dataset of real patients CT scans for SARS-CoV-2 identification. medRxiv (2020). https://doi.org/10.1101/2020.04.24.20078584
15. Okolo, G.I., Katsigiannis, S., Althobaiti, T., Ramzan, N.: On the Use of Deep Learning for Imaging-Based COVID-19 Detection Using Chest X-rays. Sensors **21**(17), 5702 (2021)
16. Uddin, A., Talukder, B., Monirujjaman Khan, M., Zaguia, A.: Study on convolutional neural network to detect COVID-19 from chest X-rays. Mathematical Problems in Engineering (2021)
17. Basu, A., Sheikh, K.H., Cuevas, E., Sarkar, R.: COVID-19 detection from CT scans using a two-stage framework. Expert Systems with Applications, 116377 (2022)
18. Alquzi, S., Alhichri, H., Bazi, Y.: Detection of COVID-19 Using EfficientNet-B3 CNN and Chest Computed Tomography Images. International Conference on Innovative Computing and Communications, pp. 365–373. Springer, Singapore (2022)
19. Ullah, N., et al.: A Novel CovidDetNet Deep Learning Model for Effective COVID-19 Infection Detection Using Chest Radiograph Images. Appl. Sci. **12**(12), 6269 (2022)
20. Ullah, N., et al.: An effective approach to detect and identify brain tumors using transfer learning. Appl. Sci. **12**, 5645 (2022)
21. Ullah, N., Khan, M.S., Khan, J.A., Choi, A., Anwar, M.S.: A robust end-to-end deep learning-based approach for effective and reliable BTD using MR images. Sensors **22**(19), 7575 (2022)
22. Ullah, N., et al.: An efficient approach for crops pests recognition and classification based on novel DeepPestNet deep learning model. IEEE Access (2022)
23. Ullah, N., Javed, A., Ghazanfar, M.A., Alsufyani, A., Bourouis, S.: A novel DeepMaskNet model for face mask detection and masked facial recognition. Journal of King Saud University-Computer and Information Sciences (2022)
24. Ahmad, I., et al.: EEG-based epileptic seizure detection via machine/deep learning approaches: A Systematic Review. Computational Intelligence and Neuroscience (2022)
25. Ali, L., et al.: An optimized stacked support vector machines based expert system for the effective prediction of heart failure. IEEE Access **7**, 54007–54014 (2019)
26. Ali, L., Rahman, A., Khan, A., Zhou, M., Javeed, A., Khan, J.A.: An automated diagnostic system for heart disease prediction based on X2 statistical model and optimally configured deep neural network. IEEE Access **7**, 34938–34945 (2019)
27. Ullah, N., Khan, J.A., El-Sappagh, S., El-Rashidy, N., Khan, M.S.: A holistic approach to identify and classify COVID-19 from chest radiographs, ECG, and CT-Scan Images Using ShuffleNet Convolutional Neural Network. Diagnostics **3** and **13**(1), 162 (2023)
28. Ullah, N., Khan, M.S., Khan, J.A., Choi, A., Anwar, M.S.: A robust end-to-end deep learning-based approach for effective and reliable BTD using MR images. Sensors. **22**(19), 7575 (2022)

29. Yousaf, W., et al.: Telehealth for COVID-19: a conceptual framework. Journal of Healthcare Engineering. **7**, 2023 (2023)
30. Raza, A., Ullah, N., Khan, J.A., Assam, M., Guzzo, A., Aljuaid, H.: DeepBreastCancerNet: a novel deep learning model for breast cancer detection using ultrasound images. Appl. Sci. **13**(4), 2082 (2023)

Development and Evaluation of Smartphones Interface for Elderly

Anam Maqsood Bhatti[1], Muhammad Waseem Iqbal[2(✉)], and Imran Siddique[2]

[1] Department of Computer Science, Superior University, Lahore 54000, Pakistan
[2] Department of Software Engineering, Superior University, Lahore, Pakistan
waseem.iqbal@superior.edu.pk

Abstract. It is vital to first comprehend the various wants and skills of seniors since the existing user interface is not flexible enough to meet their needs. Because seniors will no longer be a minority in the next few years, this research underscores the necessity of supporting elders by reworking the smartphone interface to improve the user experience for older users. The main goal of this research project is to provide a user-friendly smartphone interface for seniors. To do this, it is vital to learn how elderly people perceive and interact with the modern smartphone interfaces, as well as what challenges they confront. In the second stage, an elder-smartphone interface (ESI) design is created based on the preferences of the end-user, which are noted via a post-experimentation questionnaire. The Elderly-Smartphone Interface (ESI) design is assessed with actual end users during the third phase. The bulk of the evaluators give positive feedback while rating the prototype. The target group for this study is an active senior demographic that is capable of using cellphones on its own. The word "ancient" in this study refers to those who are sixty years of age or older.

Keyword: Development and Evaluation of Smartphones Interface for Elderly

1 Introduction

The number of individuals who left their smartphone at home and went back to collect it is significantly higher than the number of people who went back to grab their wallet. Approximately 95% of smartphone users concur that this gadget is a need in their everyday lives, and the US Supreme Court has now affirmed this belief and deemed smartphones to be an extension of one's self. Despite the fact that seniors are the smartphone group with the greatest growth, there is still a significant digital divide between older and younger users of smartphones.It is often accepted that the main reason for this discrepancy has to do with accessibility problems, but researchers discovered that one of the greatest worries of older users of smartphones is their fear of making errors. Seniors take more time to perform tasks using their cell phones since the design is not geared to accommodate their unique demands.

Even though touch displays are simpler to use than hierarchical menu-based interfaces, they make smartphone interfaces more user-friendly. Every button and option in

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 75–92, 2025.
https://doi.org/10.1007/978-3-031-77620-5_6

touch-display-based interfaces has a defined action. Senior phone users experience several age-related changes, as a result of which they find it challenging to engage with touch displays. Elderly hands' thick, drier skin, leathery hands, and declining cognitive function make it challenging for them to use cellphones' touch screens [2]. Seniors cannot use smartphones because of the size of the touchscreen buttons. Older users of smartphones struggle to tap on the smaller target because of the reduced size of the buttons, and they mistakenly click on the wrong object [3]. Additionally confusing is the letter size of the words on the buttons. A senior's eyes may become less able to distinguish between low-contrast onscreen buttons, text, icons, or other visual components as they age, making it difficult for them to use smartphone interfaces. The senior eye should not be exposed to icons or images that are too bright or harsh since ageing impairs our capacity to respond to rapidly changing brilliance. Senior users found it challenging to perceive the on-screen keyboard or comprehend text in menus or notifications due to the low colour contrast. Seniors cannot use smartphones because of the size of the touchscreen buttons. Senior users found it challenging to perceive the on-screen keyboard or comprehend text in menus or notifications due to the low colour contrast [4]. For older smartphone users who have poor hand-eye coordination, the white or negative areas might be problematic. The elderly who use smartphones need extra time to finish a job due to a decline in muscle mass and strength. Small spacing between buttons can make it harder for older users to see where to touch, while wide null or white spaces make it challenging for older users to see an onscreen element and require extra effort to find what they need [5, 6]. Numerous smartphone functions and applications are made to help elderly smartphone users with daily activities. Because they have trouble managing these programmes, a huge majority of older people do not use these functions. Most older users found it challenging to switch between different apps or menus; they frequently felt like they were "getting lost" while switching between windows. Additionally, managing many tasks and pop-up windows may present challenges [7, 8].

According to a number of studies, one of the major challenges experienced by older smartphone users is engaging with small or unclear symbols. Senior folks typically have a limited understanding of symbols and are unable to comprehend their significance, which makes it difficult for them to engage with their smart gadgets [9]. For older smartphone users, unclear icons or animation that are small, meaningless, irrelevant, or unlabeled make it difficult to use the user interface [10]. An key element that impacts how usable cellphones are for elderly people is their lack of familiarity and understanding of the interface. It takes expertise and practise to become an expert at interacting with complicated menus, navigation, and other capabilities and features. Elderly people are less aware of new technology and are unable to utilise cellphones since ageing impairs learning capacity. The elderly are unable to comprehend error notices that use technical language. For senior, low-literate smartphone users, the graphical user interfaces offer little assistance in recognizing, identifying, or recovering from mistakes. Most error notifications merely included error codes; they seldom included written descriptions. When issues are likely to occur, the user interfaces don't provide any warning, and the error messages themselves don't offer any suggestions on how to fix them, which is frustrating [11]. All individuals over 50 are referred to as old folks by the American Association of Retired Persons (AARP). People 65 years of age or older are considered

older adults by the World Health Organization (WHO), and the majority of industrialised nations use the WHO definition of elder age [12]. However, the UN does not employ the same criteria for describing the elderly population; according to the UN, everyone 60 years of age or older is considered a senior citizen [13].

After examining quite a number of study articles and publications, we have come to the conclusion that the majority of researchers use the word "elderly" to refer to anyone who is 60 years of age or older. The senior population is a tremendously varied group, notwithstanding the concept of what it means to be elderly. The features and functioning limitations of older persons vary widely [14, 15]. The main goal of this research project is to provide an easy-to-use mobile interface for seniors. To do this, it is vital to find out how senior citizens perceive and interact with mobile interfaces in order to understand the challenges they confront. The primary goal of this study project is to identify the most prevalent usage patterns, features, and build an interface that makes it easier for older individuals to complete these jobs using contemporary technology [16]. In order to do this, we develop a working mobile interface design to replace the default Android UI. This study's contribution to the literature is the identification of issues and challenges related to older citizens' use of mobile phones, which may be utilised to develop interface standards for older people. It is a report that analyses elderly citizens' adoption of smartphones behaviour. Additionally, this study provides details about older citizens' preferred software interfaces, which could prove helpful to interface designers [17].

2 Literature Review

People today are heavily dependent on technology. Usage of cellphones is seen as an addiction since these clever devices not only give us ways to communicate but also link us socially, help us plan our activities, and allow us to access information instantly with just one click. This useful product is not a blessing for everyone in society since manufacturers fail to take into account the unique demands of the elderly, which makes these cellphones difficult for many seniors to operate. In their study, C. Kyfonidis and K. Renaud focus on a mobile phone interface for the elderly. [18] and argue that the smartphone is a comparably easier gadget to operate thanks to its intended solution. They created the UX with Android 4.0 in mind. This recommended interface includes elements for simple navigation, text highlighting, and the ability to manage emergency situations. This prototype also focuses on improving visual accessibility and adding features that make it more senior-friendly. Additionally, they do validation tests to assess their prototype [13, 19].

The usage of mobile phones by older individuals is growing, however because of the complicated user interface and varied application design patterns, interaction with smartphones might be difficult for them. There has been a tremendous amount of study done to discover usability issues that older people experience. In order to identify the usability concerns and obstacles, Q. Li and Y. Luximon chose six distinct mobile interfaces and tested them on 22 older persons. After completing 19 menus for these exams, each older adult is subjected to a quick interview. These studies' findings indicate that senior users prefer using navigation systems to engaging with menus that use various

icons and buttons. Authors claim that based on content navigation layout of interfaces is more senior-friendly mobile interface based on these experiments [20, 21].

The cellphones give elderly folks a way to stay in touch with friends and family as well as a platform to interact with the rest of the world through social networking sites. Mobile touchscreens provide a highly enticing kind of engagement. Scholars provide design recommendations for creating touchpad user interfaces that are age-friendly. Despite the significant contributions made by researchers, there are still many issues that need to be resolved. To draw attention to these unresolved problems The recommendations and standards created for touchscreen-based cellphones for older persons are analysed and evaluated by L. Nurgalieva and J. J. Jara Laconich [22, 23], who also undertake a systematic assessment of the literature. The authors examined 434 suggestions for touchscreen-based mobile phone user interfaces for elders, basing their analyses on the skills of seniors 55 years of age or older. They also generated certain standards from the research based on their investigation, and they argue that all of these principles are unacceptable for creating touchscreen apps for older persons.

In this [24] work, B. Loureiro and R. Rodrigues improved some of the criteria gathered from the literature and developed multi-Touch interface guidelines for older persons. They discuss several ageing changes that have an impact on usability. They provide suggestions for how to fix these issues in multi-Touch systems. They assert that designers and developers may benefit from their work. All the elements that influence smartphone usage and serve as a barrier for seniors were compiled by H. Mohadis and N. Mohamad Ali and given in a report.. Daily, hundreds of mobile applications are released worldwide with the intention of assisting the elderly in improving the quality of their lives; nevertheless, usage of these helpful apps among the intended audience is quite low [25]. Smartphones are easier to use than older, more conventional mobile phones because of their touch-based user interfaces. In older, more traditional mobile phones, we had to hit the keypad numerous times to do different functions. Users are made more comfortable by the touch-based user interface, which enables them to enter letters by immediately tapping on touch-sensitive displays. Utilizing a smartphone is simplified by this feature. The services that these devices provide to the disabled persons who have trouble controlling these appliances are a significant contributing element to their appeal among seniors. Despite all of these advantages and conveniences, touch-sensitive screens have significant drawbacks, such as accidental screen touching and display and visibility concerns with advertisements. There are ad-blocking, font-altering, and magnification functions available, but their characteristics are challenging to use and model-dependent. Y. Tanaka and T. Fujimoto designed an interface to stop users from accidently touching on advertisements to address these two problems. They provide an auto-focus tool to improve the line that the user reads in order to address the second issue [26]. C. Y. Wong and R. Ibrahim evaluate smartphone user interfaces for older users to find usability issues. 80 seniors participated in the experiment, which the researcher conducted as an experimental study. The activities included using WhatsApp, installing an app from the Google Play Store, using Phonbook, and making and receiving phone calls. The experiment's findings show that seniors can make phone calls with a minimum of trouble; their success rate in completing this job was 83.44%. The majority of participants found the downloading job challenging, and as a result, they frequently rely on their children.

It was discovered during this trial that 60.42% of participants could successfully use WhatsApp's functions, while 70.16% of users were able to successfully interact with the phone book. The most popular messaging app was found to be WhatsApp, and older folks had trouble processing alerts. There is still more work to be done in order to create an age-friendly smartphone interface, claim the authors [27].

The global population of older adults is using cellphones at an increasing rate. There has been a tonne of work done in the area of smartphone contact and interfaces, but the interests of the younger generation are generally the major emphasis of these research. Only a small number of studies stress the necessity for creating applications and interface designs that cater to senior citizens' needs. The t-test findings showed older citizens' conduct towards smartphone GUI. Additionally, authors covered smartphone GUI elements such as icons, their positions, and labels, as well as visual styles, user interface features, and activities [28].

3 Methodology

To perform this study and gain a thorough understanding of older persons and their various requirements, user-centered research methodologies are favoured throughout the study. In order to gain a thorough understanding of consumers and their needs, numerous research methodologies are applied at various phases. Therefore, we adopt the name "Mix Method" research technique to describe the study approach [29]. The whole study process for this project can be divided into three major parts. In the first, we carefully review the literature to learn more about cellphones, older persons, ageing variables, and their consequences. In the same step, a questionnaire and testing are used to determine the issues elders encounter when using their cellphones.

Semi-systematic study is used as a research approach to investigate, gather, and organise data (first phase), allowing us to provide an insight into the problems and difficulties of the graphical user interface layout for seniors. On the basis of user preferences for an older smartphone interface that were gathered through a post-experimentation questionnaire, a workable prototype is created in the second phase. Implementing a heuristic assessment technique, this functioning prototype of an aged user interface is assessed. This evaluation aids in determining the intended consumers' degree of satisfaction. Overall, this research has a "qualitative" character since it focuses on finding answers to "what," "why," and "how" questions rather than "how much" or "how many" question types.

3.1 Phase I

3.1.1 Semi-Systematic Literature Review

To evaluate the literature and gain a thorough grasp of smartphones, how older individuals use them, and the problems and challenges they face, a semi-systematic literature review approach is advised. The literature review significantly aided our work by giving us all the data we needed to create a more user-friendly mobile design for senior citizens.

3.1.2 Research Questions

The purpose of this study is to determine a suitable response to the following research questions.

RQ:2:What difficulties do older people have using the software user interface (UI) of smartphones?

RQ: 2. What are the primary preferences of senior citizens for the smartphone software user interface?

RQ:3. How can the issues with software user interface design or cellphones for senior persons be resolved?

3.1.3 Data Collecting Process

To fully uncover the problems and difficulties in interface design, the experimental test approach comprised both a quantitative and a qualitative component. The first questionnaire, the experiment, and ultimately the post-evaluation questionnaire made up the three main components for building research-related smartphone interface prototypes. Each test and survey was carefully watched, documented, and assessed. A questionnaire is a relatively economical method of gathering user data. When detecting problems at the local level, a well-designed questionnaire may be quite beneficial.

3.1.4 Preliminary Questionnaire and Survey

Participants were given a preliminary survey in order to collect demographic information and learn more about their smartphone usage. There are two sections to this survey; the first is used to gather information about the user's background, including their gender, age, native language, and level of education. The second part of the questionnaire's objective was to assess each user's smartphone usage in order to better understand their advantages [30, 31].

3.1.5 Respondents

Employing just 5 individuals may show 80% of usability difficulties, and employing 20 participants can expose 95% of them, according to study by usability expert Robert Virzi. Consequently, 20 people were chosen to participate in this study. The older volunteers, both male and female, were chosen at random from a pool of 60-year-olds. Both inexperienced and seasoned smartphone users were included among the participants.

3.1.6 Experimental Test with Elders and Data Collection

The main focus of this trial approach was on how well senior consumers interacted with and interpreted the smartphone interface. The observer instructed the participants to speak their thoughts aloud while carefully observing the accuracy with which they completed the task and the speed at which they completed it. The researcher's main concerns during the experiment were whether the participants could quickly obtain the required information and if all information was readily available. This experiment's main objective was to evaluate how precisely the user could navigate the interface. When a person was using a smartphone during test studies, observations were made.

a) ***UI Evaluate task amount:****01*

- **UI Test task category:** Every day basic task (Visibility)
- **UI Test task title:** Display of platform's states.

UI Test task description
The smartphone should present users with visible items, activities, and options rather than requiring them to memorise meaningless or irrelevant information. This is regularly violated by the smartphone user interface, making it difficult for elderly users to keep track of the system's status. I thus developed this test to see how well elders can see the system's condition. To more precisely identify the problems affecting elders, this exam has been divided into smaller exercises.

Sub-task no. 1. The test's participants were asked to figure out and read out the time and date from the screen of their lock in order to complete this assignment.
Sub-task no. 2. The participants in this test were instructed to recognise and read out the time and date from the home screen.
Sub-task no. 3. The participants in this test were instructed to locate the battery status on the home screen and recite it aloud.
Sub-task no. 4. The participants in this test were instructed to locate and recite out the status of the phone's WiFi connection on the home screen.
Sub-task no. 5. The test's participants were asked to identify and specify whether they had received a missed call or a text message notice on their home screen.

UI Test task number: *02.*

- **UI Test task category:** Daily basic task (Visibility)
- **UI Test task title:** unlock operations

UI test task description
The screen locking feature is essential for security as it prevents unauthorised access to devices. Due to poor interface design and insufficient, clear directions to guide the user through tasks, unlocking procedures are difficult. In order to identify issues that older people frequently have when using a locked screen, I also divide this procedure into smaller tasks.

Sub-task no. 1. The test subjects were instructed to input a PIN number to unlock their smartphones by the observer.
Sub-task no. 2. In this test, the observer prompted the participants to input their password to unlock their smartphones.
Sub-task no. 3. Participants in this test were instructed to input a pattern to unlock their smartphones by the observer.
Sub-task no. 4. The test subjects were instructed by the observer to swipe to unlock their smartphones.

3.2 Phase II

Phase II involves collecting user preferences using a post-experimentation survey from the senior citizens. Elderly-Smartphone Interface preferences are noted and then used to develop a functioning prototype, which is then reviewed in step three using a heuristic assessment approach.

3.2.1 Post Experimentation Questionnaire

The results of the post-experimental survey revealed what the elderly wanted and needed from the smartphone interface. The main objective of this questionnaire is to gather information on older citizens' preferences for smartphone interface. Elderly preferences were identified, and these preferences were used to design a new smartphone interface that would accommodate their needs. To build this questionnaire, we looked at both the study literature and the design principles for elder interaction. On the basis of this literature review, we came up with a set of guidelines for logging user preferences. After the user tested each interface feature, this poll was done, but before the user tested the UI of the following feature.

3.2.2 Post Experimentation Questionnaire Design

In order to understand users' preferences at the most fundamental level, a designed effectively post-experimentation survey might be highly beneficial. Under the supervision of the supervisor, the material gleaned from the literature is set up as a questionnaire. This survey aims to determine how elderly people like their smartphone UI. The questionnaire is created, then circulated to senior smartphone users to get the right amount of replies. To produce relevant findings, the data that is taken from this questionnaire is arranged and statistically examined.

4 Analysis of Results and Discussion

4.1 Analysis of Preliminary Questionnaire Responses

Prior to participating in the above-described experimental test, the participants had to complete this first questionnaire. This questionnaire highlighted their past, prior smartphone usage, and frequency of usage. The poll also asks participants a series of questions about their health, which might have an impact on how they use their cellphones. Table 1 displays the participant demographics from the survey.

Following a results analysis, we could learn some crucial information about the target population from the initial poll. Most of the elder users of mobile devices are under the age of 71. According to survey results, between the ages of 60 and 70, 65% of elderly persons who use telephones. As people get older, their health may begin to deteriorate; for instance, their vision may become less clear and vibrant, and their finger flexibility may also be reduced. Every smartphone user over the age of 60 reportedly has health-related issues, according to a poll. According to the poll, mild to moderate health issues are present in 65% of elderly smartphone users. 20% of persons have lesser

Table 1. Demographic Survey of Participants

Participant id	Age	Gender	Qualification	Work status	Health issues
Participant 1	71-80	Male	Graduate	Part time	Mild to moderate
Participant 2	60-70	Female	High school	Retired	Mild type
Participant 3	81-90	Female	Undergraduate	Retired	Moderate to swear
Participant 4	60-70	Male	Graduate	Full time	Mild type
Participant 5	60-70	Male	Graduate	Full time	Mild to moderate
Participant 6	81-90	Female	High school	Retired	Moderate to swear
Participant 7	60-70	Male	Graduate	Full time	Mild to moderate
Participant 8	71-80	Male	Graduate	Retired	Mild to moderate
Participant 9	60-70	Female	Graduate	Part time	Mild to moderate
Participant 10	60-70	Male	Graduate	Full time	Mild to moderate
Participant 11	71-80	Male	Graduate	Retired	Mild to moderate
Participant 12	60-70	Male	Undergraduate	Full time	Mild to moderate
Participant 13	60-70	Female	High school	Retired	Mild type
Participant 14	60-70	Male	Graduate	Full time	Mild to moderate
Participant 15	60-70	Female	Graduate	Part time	Mild to moderate
Participant 16	60-70	Male	Graduate	Full time	Mild type
Participant 17	71-80	Female	Graduate	Part time	Mild to moderate
Participant 18	60-70	Male	Undergraduate	Full time	Mild to moderate
Participant 19	71-80	Female	Undergraduate	Retired	Moderate to swear
Participant 20	60-70	Male	Graduate	Full time	Mild to moderate

worries, compared to 15% who have moderate to severe health issues. The gender gap among those who use mobile devices is rather tiny, with older male users outpacing younger female users by a little margin. 60 and older male smartphone users make up 60% of the total, compared to 40 and older female users. The majority of older people have previously used cellphones. More than 70% of people over 60 who participated in the survey have used cellphones for longer than two years. 25% of older people have one to two years of experience using smartphones, compared to just 5% of seniors who have very recently started using them. Compared to young and middle-aged individuals, these smartphone users spend less time using them overall. The elderly use computers to perform complex activities that would need more time on a smartphone's small screen. On average, they use their cellphones for three hours every day. Over 60s and especially in their 80s, 30% of older persons used their smartphones for less than an hour. More than 45% of seniors over 60 who participated in the survey reported using their smartphones for a total of two to six hours. 25% of seniors use their cellphones for more than six hours per day, though.

The elderly frequently used mobile phones to contact individuals; other people may also use them to access websites to read the news or for informational purposes. The most common device utilised in daily life is the smartphone. Nearly 40% of senior folks, according to studies, use cellphones to explore the internet, and 15% of them use them to purchase online. Only 25% of older people use gadgets to read online material like books, newspapers, etc. because they have vision problems. The smartphone gadgets can be utilized for amusement; 90% of seniors watch films,video clips, or listen to songs on their smart phones and tablets. Due to physical decline, which includes a lack of mental and physical flexibility, seniors dislike mastering sophisticated smartphone capabilities.

Mobile devices are frequently used for straightforward operations like texting or making phone calls. Almost all older adults use cellphones to call friends and family members, according to this research poll. Some senior citizens prefer phone calls to texting because they find it difficult and annoying. According to the findings, just 30% of seniors use text messaging.

If a senior encounters difficulties using a mobile device's functionality, they frequently seek friends or family members for help. People won't try out new features or apps until they really have to if there are several options available. Although they found it difficult to set up these functionalities, around 75% of seniors reported to use their cellphones as clocks, to check the time and date, and to set alarms. In order for them to use the more sophisticated functions of modern digital items, the elderly demand that smartphone user interfaces be made easy. Features like the compass and radio are useless for the elderly. Throughout the course of the survey, we also took note of older mobile users' preferred devices. About 30% of the older population indicated a preference for the the iPhone, while although for them, the price of the iPhone is a little more than that of Android phones. Perhaps elderly folks prefer Android phones over other types of phones since they are less expensive. 50% of seniors possess an Android phone. Blackberry is the least popular smartphone among elderly people, and Windows phones, which account for 15% of senior smartphone consumers, are the third most popular phone type. Only 5% of older citizens chose alternative smartphone models.

4.2 Analysis of Experimentation Responses

The observer's tasks were developed before to the experiment, giving them a specific set of user tasks to keep in mind as they concentrated on their experimental assessment of the smartphone interface. These tests were developed to evaluate the core and supplementary management-related functions of smartphone features. These depicted activities are the main means through which older adults interact with cellphones to do important tasks. These tasks' intricacy either encourages or dissuades older people from utilising their smartphones. The scientist carefully documents all the problems raised by the senior citizens during the trial, eliminates duplicates, and then gathers them into a single sheet. The participant had a list of every usability problem they had discovered by the time this stage was through, along with an explanation of what had caused it and where it had happened. The recommended fixes for the issues were then rated by the participants. This investigation was carried out by evaluating 20 senior adults to see how much the usability concerns influence older users. Before handing the participant a smartphone with the default settings and instructing them to carry out tasks, the researcher welcomed them and described the purpose of the test. The way someone interacted with the smartphone during the test was monitored by testers in order to spot usability problems and monitor the overall rate of task completion.

4.2.1 Test Task Number: 01 (Visibility of the System Statuses)

- ***Sub-task no. 1 & 2.*** The observer instructed the participants to choose the time and date from the lock screen and read them out. In this test, the tester found that only 30% (N = 6) of participants could tell the time, and only 10% (N = 2) of participants

could read the date and day displayed on the lock screen due to the low contrast between the unlock screen and background information, in addition to the small font size reducing visibility as shown in Fig. 1(a).

- ***Sub-task no. 3 & 4***:The observer instructed those present to read aloud the battery life and indicate whether or not the phone was connected to the internet throughout this subtask. Once more, due to the weak contrast between the backdrop of the home screen and the text size, it was nearly invisible, as illustrated in Fig. 1. (b). Only 10% (N = 2) of elderly people with relatively moderate vision-related issues were able to properly interpret the system status, further demonstrating the extremely low success rate of these activities.
- ***Sub-task no. 5.*** In this sub-task, an observer asked those taking part to report if they had received a missed call or text message notice on their home screen. Figure 1 illustrates how the home screen's inadequate contrast with the backdrop, too-small font size and icon size, and the placement of alert messages rendered it nearly invisible. (c). Only 05% (N = 1) of senior adults were successful at these activities, which continues to be very low success rates.

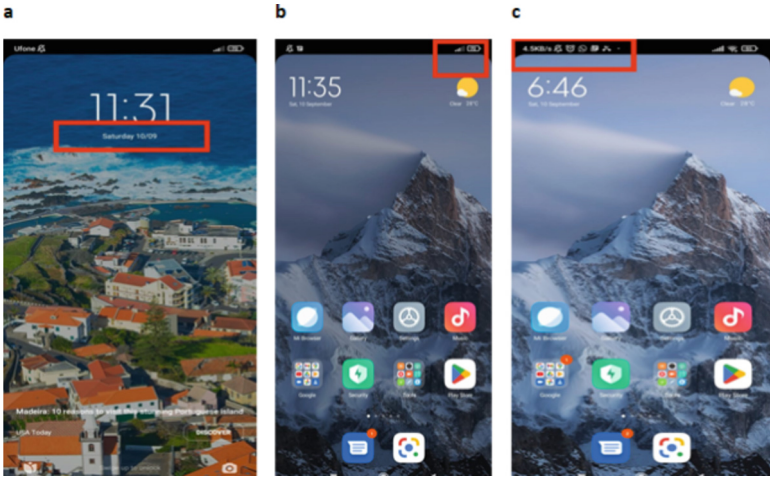


Fig. 1. Visibil System Status

4.2.2 UI Test Task Number: 02 (Unlock Operations)

- ***Sub-task no. 1.*** In this experiment, the participant's smartphone was turned off by the observer, who then instructed them to turn it back on and unlock it using a PIN number. When doing this operation, it has been seen that some senior users become puzzled by the phrase "PIN" and need assistance to unlock the screen. Those who are familiar with the term also experience memory problems and need assistance remembering their PIN number. 90% (N = 18) of the participants needed assistance to finish this activity. They now struggle to input a 4-digit pin code after learning

what a PIN is and memorising the password with assistance. Due to the tiny size of the onscreen keys and the poor contrast between the fore screen and backdrop, which makes it invisible as illustrated in Fig. 2, 75% (N = 15) of the participants failed to complete this assignment.(a).

- ***Sub-task no. 2.*** In this experiment, the observer prompted the participants to input a password to unlock their smartphones. Because of the tiny size of the onscreen keys and the low contrast between the fore screen and backdrop, which renders the onscreen keyboard invisible during this activity, it is noticed that 75% (N = 15) of senior persons experience visibility-related challenges at this stage, as illustrated in Fig. 2.(b).
- ***Sub-task no. 3.*** The observer instructed the participants to unlock their smartphones using a pattern before beginning this exercise. Because of trembling hands and clumsy finger movement, 40% (N = 8) of older smartphone users are unable to unlock the device by inputting a pattern.
- ***Sub-task no. 4.*** The test subjects were instructed to swipe to unlock their smartphones in order to complete this assignment by the observer. 80% (N = 4) of the old spend more time or make more attempts to complete the job, but 100% (N = 20) of the elderly do it successfully. However, as shown in Fig. 2, when the observer asked participants to read the on-screen instructions for swiping up, they were all unable to do so because of the low colour contrast and very tiny letter size.(c) (Table 2).

Fig. 2. Unlock Operations

Table 2. Summary of Post-Experimentation Survey

Font size survey	12pt	14pt	18pt	24pt
Percentage	0% (N=0)	55% (N=11)	30% (N=06)	15% (N=03)
Font style survey	Arial San Serif	Garamond Serif	Helvetica San Serif	Times Serif
Percentage	45% (N=09)	15% (N=03)	30% (N=06)	10% (N=02)
Color contrast survey	Red is on a white background	White is on a dark blue background	Orange is on a white background	Yellow is on black background
Percentage	60% (N=12)	20% (N=04)	05% (N=01)	10% (N=02)
Select the font size or typeface by yourself?	Yes	No	Not Really	X
Percentage	70% (N=14)	10% (N=2)	20% (N=4)	X
Select the line space by yourself?	Yes	No	Not Really	X
Percentage	70% (N=14)	10% (N=2)	20% (N=4)	X
Select Icon image type for home screen	Simple/ symbolic	3D Illustration	2D Illustration	X
Percentage	10% (N=2)	70% (N=14)	20% (N=4)	X
Select icon size	120x120	152x152	167x167	X
Percentage	5% (N=1)	35% (N=7)	60% (N=12)	X

5 Designing Prototype for Elderly

This study's findings indicate that the screen display is to blame for the majority of interface-related problems experienced by older users. Every human's eyesight steadily deteriorates with age, which leads to concerns with visibility and makes it more difficult for older individuals to use cellphones. As a result, we consider visual impairment while designing the user interface for smartphones. Therefore, the display's size was our main concern. To assist older persons with cloudy or wobbly eyesight, we concentrated on bigger fonts and clarity while creating the older-Smartphone Interface (ESI). Below are a few screenshots from a created prototype of an elderly smartphone interface (Fig. 3).

Fig. 3. Unlock and Notifications Screens

6 Evaluation of Elderly-Smartphone Interface (ESI) with End-Users

We employ the experimental test procedure to evaluate the Elderly-Smartphone Interface with real end users. The purpose of this experimental test was to pinpoint problems and difficulties with the Elderly-Smartphone Interface prototype design. Elderly adults were requested to complete the above-described experimental test tasks by the observers in order to test this research-based smartphone interface prototype and carefully collect data. Based on feedback from a range of consumers, various interface design-related concerns were found in this review.

6.1 Respondents

Thirty people tried the Elderly-Smartphone Interaction concept. The older volunteers, men and women alike, were chosen at random from a pool of 60-year-olds. The participants included both new and seasoned smartphone users.

6.2 Analysis of Experimentation Responses

The scientist carefully documents all the problems raised by the senior citizens during the trial, eliminates duplicates, and then gathers them into a single sheet.

6.2.1 UI Test Task Number: 01 (Visibility of the System Statuses)

- ***Sub-task no. 1 & 2.*** The observer instructed the participants to choose the time and date from the lock screen and read them out. In this test, the contrast between the lock screen and background and the font size of the Elderly-Smartphone Interface prototype have improved visibility and made it easier to read and interpret the date and time; as a result, 93% (N = 28) of elderly people can tell the time and 70% (N = 21) can correctly read the date and day displayed on the lock screen, compared to only 30% (N = 6) in the prior experimental test. These findings allow us to conclude that the Elderly-Smartphone Interaction prototype has greater visibility.
- ***Sub-task no. 3 & 4.*** The observer instructed the participants to speak aloud the battery life and indicate whether or not their cell phone was connected to the internet throughout this subtask. In this test, the tester noticed that the Elderly-Smartphone Interface prototype has relatively large icons and a high contrast between the foreground and background. As a result, it is easier for elderlies to read and interpret the system status; as a result, 73% (N = 22) of elderlies have read the system status correctly, compared to only 10% (N = 2) in the prior experimental test.
- ***Sub-task no. 5.*** In this subtask, the witness asked each participant to report if they had gotten a missed call or text message notice on their home screen. In this test, the tester noticed that the Elderly-Smartphone Interface prototype's foreground-background contrast, font size, and location of notifications for alerts are comparably better; as a result, it is easier for older adults to read and interpret the alert notifications. In the previous experimental test, only 5% (N = 1) of older adults correctly interpreted the alert notifications. These findings allow us to conclude that the Elderly-Smartphone Interface prototype has greater visibility.

6.2.2 UI Test Task Number: 02 (Unlock Operations)

- ***Sub-task no.1 & 2.*** In this experiment, the observer prompted the participants to input a password to unlock their smartphones. In this test, the tester noticed that the Elderly-Smartphone Interface prototype's foreground-to-background contrast and key size were comparably better. As a result, it was easier for the elderly to interact with the prototype's on-screen keyboard's keys, and 60% (N = 18) of the elderly were able to unlock the screen by correctly entering their password, as opposed to 75% (N = 15) of the elderly in the previous experimental test. These findings allow us to conclude that the Elderly-Smartphone Interaction prototype has an improved onscreen cursor visibility but still needs improvement.
- ***Sub-task no. 3.*** The participants were required to input a pattern to unlock their smartphones in order to complete this exercise, the observer said. Even though the contrast between the foreground and background of the Elderly-Smartphone Interface prototype is noticeably better during this test, it is discovered that elderly users still struggle to unlock phones by entering patterns; as a result, 53% (N = 16) of elderlies have successfully unlocked the screen by entering patterns, compared to 40% (N = 8) of elderly smartphone users in the previous experimental test. The Elderly-Smartphone Interface prototype has a greater visibility of on-screen patterns, but it still need improvement, according to these findings.
- ***Sub-task no. 4.*** The test subjects were instructed to swipe to unlock their smartphones in order to complete this assignment by the observer. This challenge has a 100% success rate (N = 30). The elderly all complete this assignment effectively.

7 Conclusion

The global population is getting older, and current statistics show that a rising number of senior people are using smartphones. This ratio is also increasing each year as more and more elderly people use smartphones. The world's ageing population is increasing the need to create technologies that are suitable for this expanding population and meet their needs. On the other hand, it appears that the research and manufacturing communities for mobile devices have disregarded this sizable portion of the population as an uncommon set of consumers with unique demands. Because of this, neither the actual hardware nor the software interface is designed with elderly users in mind. The current generation of smartphones and its user interfaces are made only with young people in mind, rather than taking a wide range of users and their requirements into account. After reviewing the literature, it became clear that there has been a significant amount of research done on how people engage with their cellphones. Numerous studies are conducted to enhance smartphone interfaces, however the majority of these studies are geared towards young adults and ignore the demands of older users. Therefore, it is vital to comprehend the various wants and skills of seniors because the existing user interface is not flexible enough to meet their requirements and needs while dealing with cellphones. Because older people won't be a minority in the next years, this research underscores the necessity of redesigning smartphone software interfaces to accommodate them.

The "Mix Method" research technique is used to carry out this study. The whole study process for this project can be divided into three major parts. In the first, we carefully

review the literature to learn more about cellphones, older persons, ageing variables, and their consequences. In the same step, a questionnaire and testing are used to determine the issues elders encounter when using their cellphones. The major goal of this study project is to identify typical use patterns and commonly utilised features. Using this knowledge, an interface will be designed that makes it easier for older individuals to use contemporary technology. For this reason, we create a functional smartphone ui prototype for older smartphone users. On the basis of consumer preferences for an older smartphone ui that were gathered through a post-experimentation survey, a workable prototype is created in the second phase. This workable prototype of an aged user interface is being tested with real end users. The Elderly-Smartphone Interaction (ESI) prototype does not answer the privacy and security concerns of older users, according to findings analysis.Due to time restrictions, this research has some limitations, such as the fact that only those over 60 who are educated and can use smartphones freely were enrolled in the studyThe results of this research endeavour were not sufficiently broad to represent the full senior population due to the study's limited sample size of subjects.

References

1. Lin, C.J., Hsieh, T.-L., Shiang, W.-J.: Exploring the interface design of mobile phone for the elderly. In: Human Centered Design, pp. 476–481. Berlin, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02806-9_55
2. Gonçalves, V.P., et al.: Providing adaptive smartphone interfaces targeted at elderly people: an approach that takes into account diversity among the elderly. Univ. Access Inf. Soc. **16**(1), 129–149 (2017). https://doi.org/10.1007/s10209-015-0429-9
3. Darvishy, A., Hutter, H.-P.: Recommendations for age-appropriate mobile application design. In: Advances in Design for Inclusion, pp. 241–253. Cham (2018). https://doi.org/10.1007/978-3-319-60597-5_22
4. Androutsou, T., et al.: A smartphone application designed to engage the elderly in home-based rehabilitation. Frontiers in Digital Health **2**, 15 (2020). https://doi.org/10.3389/fdgth.2020.00015
5. Rezha, N., Maksom, Z., Naim, C.P.: Tackling design issues on elderly smartphone interface design using activity centered design approach. ARPN J. Eng. Appl. Sci. **9**, 1190–1196 (2014)
6. Petrovčič, A., Taipale, S., Rogelj, A., Dolničar, V.: Design of mobile phones for older adults: an empirical analysis of design guidelines and checklists for feature phones and smartphones. Int. J. Human-Comp. Interact. **34**(3), 251–264 (2018). https://doi.org/10.1080/10447318.2017.1345142
7. Elguera Paez, L., Zapata Del Río, C.: Elderly users and their main challenges usability with mobile applications: a systematic review. In: Design, User Experience, and Usability. Design Philosophy and Theory, pp. 423–438. Cham (2019). https://doi.org/10.1007/978-3-030-23570-3_31
8. Iancu, I., Iancu, B.: Designing mobile technology for elderly. a theoretical overview. Technol. Forecast. Soc. Chang. **155**, 119977 (2020). https://doi.org/10.1016/j.techfore.2020.119977
9. Awan, M., et al.: Usability barriers for elderly users in smartphone app usage: an analytical hierarchical process-based prioritization. Scientific Programming **2021**, 1–14 (2021). https://doi.org/10.1155/2021/2780257
10. Leung, R., McGrenere, J., Graf, P.: Age-related differences in the initial usability of mobile device icons. Behaviour & Information Technology **30**(5), 629–642 (2011). https://doi.org/10.1080/01449290903171308

11. Inostroza, R., Rusu, C., Roncagliolo, S., Jiménez, C., Rusu, V.: Usability heuristics validation through empirical evidences: a touchscreen-based mobile devices proposal. In: 2012 31st International Conference of the Chilean Computer Science Society, pp. 60–68 (2012). https://doi.org/10.1109/SCCC.2012.15
12. Yeh, P.-C.: Impact of button position and touchscreen font size on healthcare device operation by older adults. Heliyon **6**(6), e04147 (2020). https://doi.org/10.1016/j.heliyon.2020.e04147
13. Wong, C.Y., Thwaites, H., Khong, C.W.: Mobile user interface for seniors. Design Principles and Practices **4**, 231–250 (2010). https://doi.org/10.18848/1833-1874/CGP/v04i04/37936
14. Punchoojit, L., Hongwarittorrn, N.: The influence of label font size on menu item selection for smartphone. 2018 5th International Conference on Advanced Informatics: Concept Theory and Applications (ICAICTA) (2018). https://doi.org/10.1109/ICAICTA.2018.8541307
15. Kascak, L.R., Rébola, C.B., Sanford, J.A.: Integrating Universal Design (UD) principles and mobile design guidelines to improve design of mobile health applications for older adults. In: 2014 IEEE International Conference on Healthcare Informatics, pp. 343–348 (2014). https://doi.org/10.1109/ICHI.2014.54
16. (PDF) Designing User Interfaces for the Elderly: A Systematic Literature Review. https://www.researchgate.net/publication/321757825_Designing_User_Interfaces_for_the_Elderly_A_Systematic_Literature_Review. Accessed 19 Jun. 2022
17. Arfaa, J., Wang, K.: An accessibility evaluation of social media websites for elder adults, pp. 13–24 (2014). https://doi.org/10.1007/978-3-319-07632-4_2
18. Zain, A.: Aging-friendly smartphones: An analysis of design and user-interface to understand smartphone 'usability' for elderly citizens (2019)
19. Measuring household and living arrangements of older persons around the world: The United Nations Database on the Households and Living Arrangements of Older Persons 2019. Technical Paper No. 2020/03 | Population Division. https://www.un.org/development/desa/pd/content/measuring-household-and-living-arrangements-older-persons-around-world-united-nations. Accessed 25 Jun. 2022
20. Wong, C.Y.: Mobile user interface for seniors: an impact of ageing population on mobile design. Design Principles and Practices **4**, 231–248 (2010)
21. Li, Q., Luximon, Y.: Older adults' use of mobile device: usability challenges while navigating various interfaces. Behaviour & Information Technology **39**, 1–25 (2019). https://doi.org/10.1080/0144929X.2019.1622786
22. A Systematic Literature Review of Research-Derived Touchscreen Design Guidelines for Older Adults | IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8640032. Accessed 24 Feb. 2023
23. Al-Razgan, M., Al-Khalifa, H.M.d., Alajmi, H.: Touch-Based Mobile Phone Interface Guidelines and Design Recommendations for Elderly People: A Survey of the Literature, presented at the ICONIP'12 Proceedings of the 19th International Conference on Neural Information Processing, vol. IV, pp. 568–574 (2012). https://doi.org/10.1007/978-3-642-34478-7_69
24. Loureiro, B., Rodrigues, R.: Design Guidelines and Design Recommendations of Multi-Touch Interfaces for Elders (2014)
25. Mohadisdudis, H.M., Ali, N.M.: A study of smartphone usage and barriers among the elderly. In: 2014 3rd International Conference on User Science and Engineering (i-USEr), pp. 109–114 (2014). https://doi.org/10.1109/IUSER.2014.7002686
26. Tanaka, Y., Fujimoto, T.: Design of the External Smartphone Interface to Prevent Users' Mistapping on Advertisements and Eliminate Difficulty of Reading. In: 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 995–1000 (2019). https://doi.org/10.1109/IIAI-AAI.2019.00199
27. Wong, C.Y., Ibrahim, R., Hamid, T.A., Mansor, E.I.: Usability and design issues of smartphone user interface and mobile apps for older adults. In: User Science and Engineering, pp. 93–104. Singapore (2018). https://doi.org/10.1007/978-981-13-1628-9_9

28. Wong, C.Y., Ibrahim, R., Mansor, E.: Measuring expectation for an affordance gap on a smartphone user interface and its usage among older adults. Hum. Technol. **16**, 6–34 (2020). https://doi.org/10.17011/ht/urn.202002242161
29. Leitão, R.: Target and Spacing Sizes for Smartphone User Interfaces for Older Adults: Design Patterns Based on an Evaluation with Users (2012)
30. Olwal, A., Lachanas, D., Zacharouli, E.: OldGen: mobile phone personalization for older adults. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pp. 3393–3396. New York, NY, USA (2011). https://doi.org/10.1145/1978942.1979447
31. Hamid, K., et al.: Optimized evaluation of mobile base station by modern topological invariants. Computers, Materials and Continua **74**, 363–378 (2022). https://doi.org/10.32604/cmc.2023.032271

Cyber Physical Systems Having Nodes/Layers with Trustworthy Data: A Review

Muhammad Ejazulghaffar(✉), Muhammad Arif, Arfan Jaffar, and Ahmed Hassan

Department of Computer Science, Superior University, Lahore 54000, Pakistan
phcs-s21-001@superior.edu.pk

Abstract. Cyber Physical System is one of the most promising innovations in the IT domain and stands out among technologies. High-intelligence, networked systems known as cyber physical systems (CPS) integrate computational and physical components to accomplish a specific task. Over the past few years, they have grown swiftly and are now playing a bigger role in fields including manufacturing, transportation, healthcare, and smart cities. Some of the most recent advancements in cyber-physical systems include autonomous systems, edge computing, artificial intelligence, data trustworthiness, digital twins, privacy, and security. Overall, CPS development aims to produce more intelligent, effective, and dependable systems that can enhance our lives in a variety of ways.

Although cyber-physical systems (CPS) have demonstrated considerable promise in a number of fields, there are still a number of obstacles that need to be resolved, including data reliability, privacy, security, interoperability, reliability, scalability, standards, and ethical concerns. In this paper we have studies an introduction and history of cyber physical systems, its wide range of applications, characteristics, design and challenges. The main purpose of this study is to explore the key challenge of cyber physical system which is data trustworthiness solution of which may lead to solve the problem of congestion and memory issues.

Keywords: Cyber Physical System · Autonomous systems · Smart agriculture · Data Trustworthiness · IoT and Privacy

1 Introduction

In order to construct a special system that can interact with the physical environment in real-time, a cyber-physical system, or CPS, combines physical and cyber segments, including software, hardware and networks. CPS is used in various fields, such as transportation, healthcare, manufacturing, and energy. CPS relies on sensors, actuators, and communication networks to collect and transmit data between the physical and cyber components. The system analyzes this data to control physical processes and enable automated decision-making. Examples of CPS include autonomous vehicles, smart cities, and medical monitoring systems. CPS is essential for creating efficient, reliable, and secure systems that can operate in complex environments. As technology continues to advance, CPS will become more prevalent in everyday life and play an increasingly important role in shaping the future of our world.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 93–107, 2025.
https://doi.org/10.1007/978-3-031-77620-5_7

The cornerstone of Industry 4.0, as promoted by the Government of Germany for the construction of smart factories to usher in the industrial revolution 4.0, is the cyber physical system (CPS). When a workshop under National Science Foundation (NSF) convened in Austin, Texas, in 2006, the word "CPS" was first used. "A system made up of cooperative entities, capable of computation, and agents with a close relationship to the surrounding physical environment and phenomena, employing and simultaneously delivering network services for the treatment and transfer of data" was how it was described. Storage, processing, and network management functions have increasingly moved to central data centers, IP mainstay networks, and primary networks over time. The amount of data being gathered from Internet of Things (IoT) gadgets is growing at an exponential rate, necessitating careful processing of the data to reduce reaction time and efficiently disperse network burden. Several research have revealed the big-data handling limitations of the cloud. The number of "smart" and "dumb" objects linked to the Internet is projected to reach 50 billion by the year 2020 [1]. Common example of a cyber and physical system (CPS) is a production system, which integrates a number of machines, actuators, sensors, and control systems to manufacture goods as quickly as feasible [2]. Cyber-Physical Production Systems (CPPSs) are sophisticated production platforms that strive to synchronize and integrate the physical world of machines with the digital computational realm. Nevertheless, for the application of CPPSs in the real world, extensive interconnection and a computing platform are essential [3]. The future of the Internet is the Internet-of-Things (IoT), in which everything will be interconnected. Research have shown that by performing intermediate functions at the network's edge, fog/edge computing-based operations will play a significant part in expanding the cloud [4]. Most of today's processors are implemented as components that are integrated into different CPS, using actuators and sensors to sense and amendment the environment, and they are becoming more and more linked to one another through the Internet. There is much more to this dispersed and linked strategy than merely using information and communication technologies (ICT). To regulate the CPS, a variety of multidisciplinary knowledge is incorporated for pertinent physical sensing and cognition [5].

Computer experts and network specialists must work closely with specialists in a variety of fields, including digitization and control, mechanical engineering, civil engineering, and the biology. This is because CPS is a new area of research that includes the overlapping and incorporation of many science and the engineering fields. As a result, current descriptions of CPS are primarily provided by various academics from their respective views. Cyber-physical systems, as per description of E. A. Lee, are those that combine working out with physical procedures while using embedded machines and networks to observe and manage those procedures. Through feedback loops, physical processes influence computations, and the reverse is true [6]. Professor J. F. He views CPS as scalable, credible, and controllable interconnected physical tools systems that deeply integrate computing, control, and communication capabilities based on perceptions of the environment. To boost or enlarge the functionality of linkages and physical structures and to observe or control physical objects in a safe, dependable, proficient, and simultaneous manner, in-depth integrating and real-time communication are made possible through the feedback chain of mutually beneficial special effects between computer procedures and physical procedures.

1.1 Motivation

The interoperability, connectedness, networking capacity, communication, decentralized management, autonomy, and modularity of the CPS are what make it useful. A CPS can communicate data that is mutually understood between its components when its components are connected, as opposed to when the components are connected via different communication protocols. One distinguishing feature of the CPS is its modularity that permits a CPS to adapt and rearrange its rejoinder to the demands and ease of users. To do this, a CPS a network of interconnected modules or subsystems must possess networking capabilities that allow all subsystems to communicate and interact with one another concurrently while maintaining their autonomy and decentralized control capabilities. The distinctiveness of CPS in contrast to conventional critical infrastructure systems is characterized by the direct communication of several components among each other enabling real time decision making. The main structural overview of cyber Physical system is described as in Fig. 1.

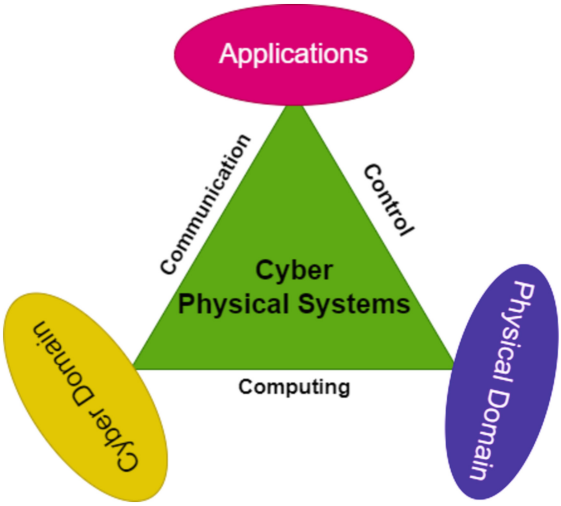


Fig. 1. Cyber Physical System

Mortality ratio, other problems and loses due to fire eruption are increasing with time due to many faults in cyber physical systems components which are employed in fire detection systems. Early fault detection can reduce these loses rate with proper detection. The proposed work intends to apply privacy protection methods at upstream nodes level to transmit trustworthy data and also to indicate early fault detection in authentication process. The study will attempt to provide a better error detection technique and increase the chances avoidance. This work will support and provide new horizons for further research and the betterment in data protection cyber physical architecture.

1.2 Scope

This study will deal with and overview of cyber physical system, its applications and issues. It will also give an overview of the data protection at level of sink/gateway (before the aggregation of data) and at fog and cloud level (after data accumulation and before data storage or further processing) using IGTDC and gate level modeling and encoding using gray coding and k-mapping. The techniques beyond this scope will not be addressed by this architecture.

1.3 Background

By using high-fidelity network, cyber physical systems link actuators, sensors, and systems together [1]. This network provides system functionalities, like data transmission in real time and status observing, enabling communication with other systems. CPS develops a collaborative infrastructure similar to a digital twin to facilitate the electronic demonstration of information all over the product and procedure life cycle [2, 3]. The combination of feedback control with processing, communication, and control tools makes these systems effective [4]. More recent advancements have enhanced the interaction between people and CPS in the loop. For activities requiring a human operator to collaborate with a robot, for instance, human CPS, which entails CPS with close monitoring to the human components to avoid mishaps, is utilized. In general, there is a wealth of literature on the design of efficient techniques to assure and enhance the reliability of data in diverse CPS applications [5]. According to the literature, comprehensive solutions must be created by integrating various strategies and tactics to guarantee data trustworthiness throughout the life cycle of data of sensors for example, during the process of data gathering, broadcast, accumulation, and cloud storing. However, maintaining data dependability throughout the sensors' data life cycle is difficult in the diverse CPS domain, and there isn't a perfect solution to the problem [6].

1.3.1 Major Research Contribution

Computer experts and network specialists must work closely with specialists in a variety of fields, including digitization and control, mechanical engineering, civil engineering, and the biology. This is because CPS is a new area of research that involves the overlying and incorporation of many engineering and science fields. As a result, the current definitions of CPS are primarily provided by various academics from their respective views (Table 1).

1.3.2 Data Trustworthiness

The sensor modules in CPS are able to transfer only trustworthy data and reject the inaccurate or corrupted data before delivering it to the upstream nodes due to in-network data manipulation and coordination amongst sensors. As a result, the amount of data transmitted to the upstream component is greatly decreased. Meanderingly, this helps to solve the network deferral communication issue as the sensor's modules filter out a lot of unnecessary data. We expect it to alleviate/improve latency, battery, and bandwidth

Table 1. The Most Important Attributes of CPS

Attributes	Statement	Ref.	Year
Adaptive control	A CSP has the capacity to alter its mode of operation in response to shifting environmental circumstances in order to produce the optimal results	[7]	2021
Human Computer Interaction	The CSP's agent-based design permits its many agents to interact openly with humans to receive directions for carrying out specific activities	[8]	2021
Data-Driven	The interconnections between both physical and cyberspace systems, that are made possible by data flow and data authenticity, are the basis for a CSP's operation	[9]	2021
Real Time Monitoring and Control	A CSP can continuously monitor the performance of its many subsystems, promptly recognize changes in the ecological framework, and make aware and wise judgements in response	[10]	2020
Predictive Maintenance	In order to detect irregularities in the procedure of various sub-systems and pieces of tools and rectify them prior to botch, a CSP executes predictive maintenance using data analysis techniques and tools	[11]	2021
Internet of Things	Internet of Things (IoT) gadgets and protocols enable the interconnection and data flow between various CSP subsystems	[12]	2021
Inter-connected system	A CSP's interconnectivity between its many subsystems enables its various agents to cooperate and work independently by exchanging information and making wise decisions	[13]	2020
Privacy and Security	CSP's top priorities these days are keeping the system secure and protecting consumers' privacy	[14]	2020

problems. But still there is a danger at upstream units such as gateway/sink in CPS that data may greatly be affected. So our main focus is to protect data before sending to upstream components.

2 Overview of Cyber-Physical Systems

Investigations on CPS involve a number of overlapping scientific and engineering disciplines as an emerging field of study. As a result, the official description of the CPS has also changed as a result of various viewpoints from various academics. According to [15], CPS is a procedural framework where physical procedures have a positive feedback loop on computations and vice versa. According to the authors of [16], a CPS is an interconnected physical engineering system that uses computations to monitor and manage the performance of physical systems.

2.1 Historical Perspective

The development of digital control systems began roughly 30 to 40 years ago. This was the preliminary phase regarding current Industry 4.0 because they had the idea of integrating thousands of sensors. Then, in the early 2000s, there was a change brought on by the creation of good open-source software. Humanity has been able to utilize the data gathered from the sensors in control systems with greater effectiveness because to the development of application packages. Another substantial wave of advantages for the sector resulted from this.

The term "Industry 4.0" was first used in 2011 by Klaus Schwab. Industry 4.0, in his opinion, is not a collection of novel technology but rather "a completely new approach to production." The phrase "means of increasing the competitiveness of the German manufacturing industry through the enhanced integration of cyber-physical systems into factory processes" [17] is how Industry 4.0 was initially defined in Germany.

The virtual and physical worlds come together, resulting in the creation of new cyber-physical complexes. In addition, the goal was to create an automated, in-depth interface that would allow the product's consumer to virtually watch while his purchase was produced [18].

Cyber-physical systems are being used in many different aspects of human activity, including transportation, energy, life support, and medical. Embedded real-time systems, distributed computing systems, robotic systems of control for technical and industrial processes, networks, and integrated networks are examples of "cyber-physical systems" that came before them [19] (Fig. 2).

2.2 CPS Layers and Components

The framework of CPS systems is made up of various layers and components that communicate with one another using various communication protocols and technologies [20].

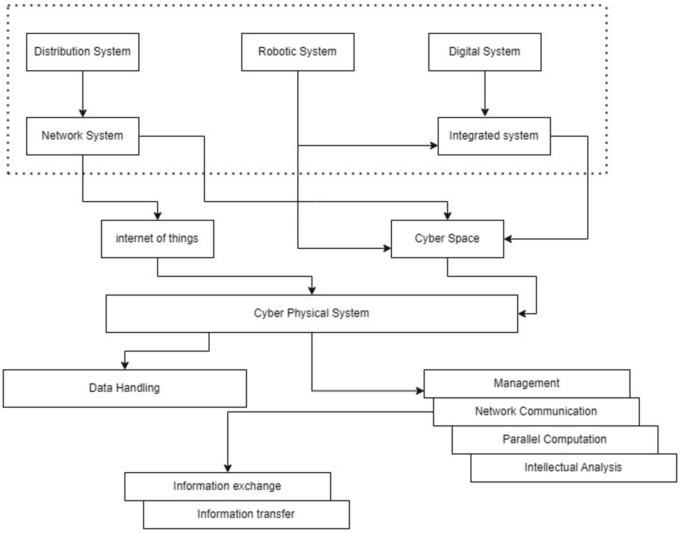


Fig. 2. The development of Cyber physical systems [19]

2.2.1 Layers of CPS

The three primary layers of the CPS architecture the transmission layer, perception layer, and application layer are shown and described in Table 2.

Table 2. CSP Layers

Layer Name	Objectives	Targets
Perception Layer	Data and information Collection	Confidentiality, Privacy, Authentication
Transmission Layer	Data and information Transmission	Confidentiality, Integrity, Authentication, Availability
Application Layer	Data and information Analysis and Decision making	Privacy, Security, Safety, Authentication

2.2.2 CPS Components

Components of the CPS are employed to control signals (Fig. 3) or to sense information [21]. Accordingly, the components of the CPS are divided into two groups: sensing components (SC), which gather and detect information, and controlling components (CC), which watch over and regulate signals.

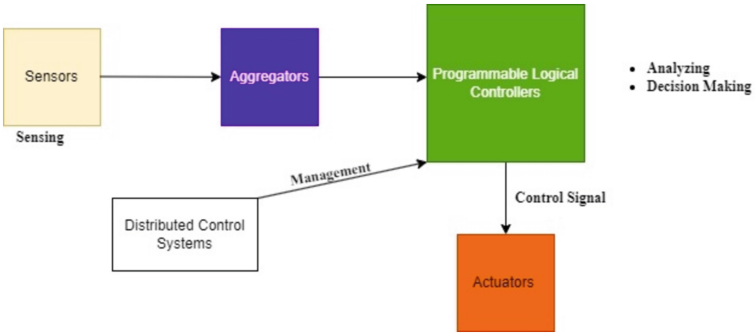


Fig. 3. CSP Components

Sensors that gather data and send it to aggregators make up sensing constituents, which are predominantly found at the perception layer. The actuators will then get this data and information for additional processing to ensure proper decision-making. The main CPS sensor components are listed below.

- Sensors
- Aggregators
- Actuators

In order to obtain greater stages of precision and safeguarding against nefarious attacks or accidents, primarily noise, interference, and signal jamming, controlling components are used to control signals. They play an important role in signal control, monitoring, and management. As a result, it has become crucial to use Programmable Logic Controllers and Distributed Control Systems (DCSs) and all of associated parts, including PAC [22], OT/IT [23], Server/Control Loop and (HMI)/(GUI) [24]. Following that, we outline the various control system types utilized in CPS systems:

- Programmable Logic Controllers (PLC)
- Distributed Control Systems (DCS)
- Remote Terminal Units (RTU)

2.2.3 Types of Models of CPS

Models of CPS fall under the following categories:

CPS Timed Actor: Geilen et al. [25] proposed a theory with a functional and classical modification that limits a specific behavioral set, increasing efficiency while lowering complexity. In fact, these time predictable models may more easily derive analytical bounds and are less prone to state expansion issues [26].

Event-Based CPS: In these kinds of models, actuation decisions cannot be made until an event has been sensed and detected by the appropriate CPS components. As a result of the various CPS actions, the non-deterministic system delay affects the individual component time restrictions which can be managed, according to Hu et al. in [27], by using an event based strategy that relies on CPS events.

Model of Lattice-Based: Events Pursuant to the type of event, as well as the event that have internal and external properties, the CPS events are depicted in. The combination of these events enables the definition of a spatio-temporal attribute of every specified event and the identification of all the observers.

CPS Model Based on Hybrid: The physical dynamical systems the discrete computing systems are the two separate interactive system types that make up hybrid CPSs, which are the heterogeneous systems [28].

2.3 Characteristics of Cyber Physical Systems

A system must possess a number of qualities in order to be classified as a CPS. The production processes can become more efficient and flexible when there is high autonomy and quick decision-making procedures, which are fundamental criteria [29]. Following are key characteristics of cyber physical system in Table 3.

Table 3. Characteristics of CPS

Characteristics	Description
Reliable	Consistent operation without failures
Stability	Consistent operations
Accurate	High precision data analysis
Efficiency	No waste operation
Communicative	Data connection and sharing with all systems
Scalability	On-demand system expansion
Autonomy	Decision-making capacities
Safe Trustworthy system	Avoiding accidents
Robustness	Tolerant to perturbations in the system

2.4 Design of CPS

The components of the CPSs are positioned at an advanced degree of collaboration than other information concepts [20].

2.4.1 Layers of Cyber Physical Systems

The primary layers can be described as under:

- First is physical layer, which consists of actual objects in the real world
- Secondly digital layer, which consists of algorithms for handling actual objects
- The interface that allows for the communication of the physical layers and the digital layers with people, which consists of control mechanisms and detectors
- The interface between the physical and digital layers with actual objects, which consists of augmented reality technologies.

The following levels of communication between cyber-physical system items exist [20] about which Fig. 4 displays a graphical perspective.

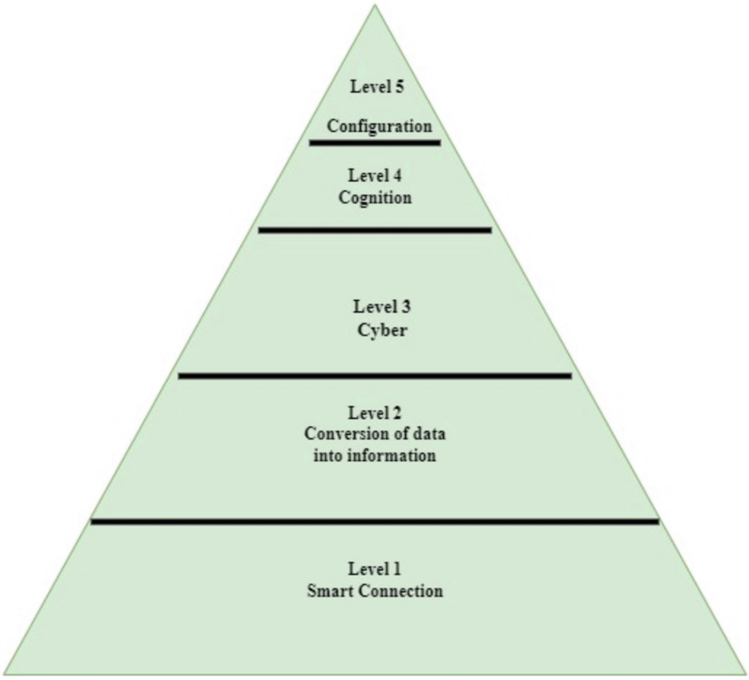


Fig. 4. Communication Levels of Cyber Physical Systems

3 Discussion

A CPS has various difficulties that aren't necessarily present in an embedded or traditional corporate information system [30]. The key challenges faced in most of the cyber physical systems are described in Table 4.

Different characteristics allow CPS to function in many domains related applications. Depending on the uses, there are many CPS kinds that work either self-sufficiently or cooperatively to provide services that are secure, trustworthy, dependable, efficient, agile, and affordable. Main applications are discussed in Table 5.

Table 4. Challenges of CPS

Challenge	*Description*
Data heterogeneity	Platforms must be capable to accommodate a wide range of unique uses and gadgets. Different protocols related to communication, including Bluetooth, RF, Zigbee, and infrared, are utilized by digital policies
Reliability	Due to the environmental impact of actuators, reliability and safety are fundamental considerations. Any CPS component failure can result in system degradation, which could seriously affect people's lives and their property
Data management	Big data from many linked devices must be stored, analyzed, processed, and displayed in real-time
Privacy	Since CPSs handle a lot of data, including private information about people's health, gender, and religion, significant privacy concerns are raised
Security	Since CPSs are built on heterogeneous applications and wireless communications, there are frequently serious security concerns. The issue of security is now a global one
Real-time	Because failures to take actions on time might result in permanent harm, CPSs must make sure they have the bandwidth or system capacity required to accomplish time-critical functions
Data Trustworthiness	The sensor modules in CPS are able to transfer only trustworthy data and reject the inaccurate or corrupted data before delivering it to the upstream nodes due to in-network data manipulation and coordination amongst sensors. As a result, the amount of data transmitted to the upstream component is greatly decreased [31]

Table 5. Applications of CPS

Application	Description
Smart Buildings	Smart or intelligent buildings, commonly referred to as green buildings, place a strong emphasis on sustainability and are outfitted with cutting-edge technology like 5G, cloud computing, the Internet of Things (IoT), edge computing, and artificial intelligence which renders them human- and energy-friendly [32]

(*continued*)

Table 5. (*continued*)

Application	Description
A Smart Grid and Smart Cities	A smart grid, often referred to as a smart energy grid, is divided into seven categories, including users, service providers, markets, procedures, generation in bulk, transmission, and then distribution, as defined by the National Institute of Standards and Technology (NIST) [33] As the name suggests, a smart city is an urban region that uses technology to become connected and adaptable in order to handle the environmental, social, and economic concerns of the twenty-first century and enrich the eminence of life for its occupants [34]
Intelligent Transportation Systems	Today, vehicles can avoid traffic jams, consume less land and energy, improve operating control, security and safety, act as distributed resources of energy to maintain a balance between supply of electricity and demand, lower costs (or increase benefits) for those who own them, and enhance environmental sustainability [35]
The Tele-Medical Systems	The Tele-medical systems are interconnected medical equipment systems that offer context aware, services relating to life critical situations in hospitals to provide patients with high-quality continuous care [36]. As a result, patients can now receive care both at home and in a hospital
Autonomous Robotic Systems	Unmanned ground-based vehicles (UGV) and unmanned aerial vehicles (UAV) are examples of autonomous robotic systems that are increasingly in demand as the CPS of the future. A UAV, also referred to as a drone, is a vehicle that can fly like a plane without a human pilot or other passengers. UGVs, are autonomous system of robots that fly over the land without a human pilot [37]
Smart Agricultural Systems	The population of the planet will surpass 9.0 billion people by 2050. Under the stringent constraints of scarce resources, unskilled labor, a lack of agricultural land, and climate change, it would be difficult to achieve the necessary level of agricultural output. One potential solution to this significant issue is precision agriculture, a clever CPS-based farming technique [38]
Industry 4.0	Industry 4.0 has already begun to take shape thanks to CPS's integration of cutting-edge functions through the IoT, cloud manufacturing, big data analytics, IoE, and the fog-based computing [39]

4 Conclusion

CPS will address various facets of social and economic life, have a significant impact, and drive the all-encompassing advancement of computer science as well as other disciplines. The development of CPS, however, also faces significant difficulties because to the limitations imposed by the theory and technology of computation, communications, and control that are already in use. Take the lead globally in CPS development thanks to a breakthrough in a crucial piece of CPS technology. CPSs combine physical and computational processes. CPSs have much higher economic potential than has been realized, and significant investments are being undertaken all around the world to further the technology. The capabilities, adaptability, scalability, resilience, safety, security, and usability of CPS will greatly outpace those of today's straightforward embedded systems. This work will support and provide new horizons for further research and the betterment in data protection cyber physical architecture. This will provide a better understanding and conducive decision support system for effective and efficient transmission of trustworthy data from upstream nodes.

New studies should definitely be done to emphasize and utilize the potential of CPS. A trustworthy and secure environment for technological growth could be created through CPS technology, but this will take time and much research. Future research should concentrate on creating standards and best practices for CPS implementation while addressing trustworthiness of data, reliability, scalability, standardization, integration, and complexity.

References

1. Serpanos, D.: The cyber-physical systems revolution. Computer **51**, 70–73 (2018)
2. Colombo, A.W., Karnouskos, S., Kaynak, O., Shi, Y., Yin, S.: Industrial cyberphysical systems: A backbone of the fourth industrial revolution. IEEE Ind. Electron. Mag. **11**, 6–16 (2017)
3. Cogliati, D., Falchetto, M., Pau, D., Roveri, M., Viscardi, G.: Intelligent cyber-physical systems for industry 4.0. In: 2018 First International Conference on Artificial Intelligence for Industries (AI4I), pp. 19–22. IEEE (2018)
4. Jamaludin, J., Rohani, J.M.: Cyber-physical system (cps): State of the art. In: 2018 International Conference on Computing, Electronic and Electrical Engineering (ICE Cube), pp. 1–5. IEEE (2018)
5. Kumar, R., Kumar, P., Tripathi, R., Gupta, G.P., Gadekallu, T.R., Srivastava, G.: SP2F: A secured privacy-preserving framework for smart agricultural Unmanned Aerial Vehicles. Comput. Netw. **187**, 107819 (2021)
6. Hai, T., et al.: DependData: Data collection dependability through three-layer decision-making in BSNs for healthcare monitoring. Information Fusion. **62**, 32–46 (2020)
7. Hao, L., Sun, B., Li, G., Guo, L.: The eco-driving considering coordinated control strategy for the intelligent electric vehicles. IEEE Access **9**, 10686–10698 (2021)
8. Wilhelm, J., Petzoldt, C., Beinke, T., Freitag, M.: Review of digital twin-based interaction in smart manufacturing: enabling cyber-physical systems for human-machine interaction. Int. J. Comput. Integr. Manuf. **34**, 1031–1048 (2021)
9. Zhang, X., et al.: Data-driven transportation network company vehicle scheduling with users' location differential privacy preservation. IEEE Transactions on Mobile Computing (2021)

10. Guddanti, K.P., Matavalam, A.R.R., Weng, Y.: PMU-based distributed non-iterative algorithm for real-time voltage stability monitoring. IEEE Transactions on Smart Grid. **11**, 5203–5215 (2020)
11. Tang, Y., Dananjayan, S., Hou, C., Guo, Q., Luo, S., He, Y.: A survey on the 5G network and its impact on agriculture: challenges and opportunities. Comput. Electron. Agric. **180**, 105895 (2021)
12. Pivoto, D.G., et al.: Cyber-physical systems architectures for industrial internet of things applications in Industry 4.0: A literature review. J. Manufact. Sys. **58**, 176–192 (2021)
13. Ning, Z., et al.: Mobile edge computing enabled 5G health monitoring for Internet of medical things: A decentralized game theoretic approach. IEEE J. Sel. Areas Commun. **39**, 463–478 (2020)
14. Wang, J., Wu, L., Wang, H., Choo, K.-K.R., He, D.: An efficient and privacy-preserving outsourced support vector machine training for internet of medical things. IEEE Internet Things J. **8**, 458–473 (2020)
15. Lee, E.A.: Computing foundations and practice for cyber-physical systems: a preliminary report. University of California, Berkeley, Tech. Rep. UCB/EECS-2007–72. 21 (2007)
16. Gonzalez, G.R., Organero, M.M., Kloos, C.D.: Early infrastructure of an internet of things in spaces for learning. In: 2008 eighth IEEE international conference on advanced learning technologies, pp. 381–383. IEEE (2008)
17. Hecklau, F., Orth, R., Kidschun, F., Kohl, H.: Human resources management: Meta-study-analysis of future competences in Industry 4.0. In: Proceedings of the International Conference on Intellectual Capital, Knowledge Management & Organizational Learning, pp. 163–174 (2017)
18. Plakhotnikov, D.P., Kotova, E.E.: Design and analysis of cyber-physical systems. In: 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), pp. 589–593. IEEE (2021)
19. Kudzh, S., Cvetkov, V.: YA. Setecentricheskoe upravlenie i kiberfizicheskie sistemy. Obrazovatel'nye resursy i tekhnologii 19 (2017)
20. Plakhotnikov, D., Kotova, E.: The use of artificial intelligence in cyber-physical systems. In: 2020 XXIII International Conference on Soft Computing and Measurements (SCM), pp. 238–241. IEEE (2020)
21. Yaacoub, J.-P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M.: Cyber-physical systems security: Limitations, issues and future trends. Microprocess. Microsyst. **77**, 103201 (2020)
22. Mazur, D.C., Quint, R.D., Centeno, V.A.: Time synchronization of automation controllers for power applications. In: 2012 IEEE Industry Applications Society Annual Meeting, pp. 1–8. IEEE (2012)
23. Morelli, U., Nicolodi, L., Ranise, S.: An open and flexible cybersecurity training laboratory in IT/OT Infrastructures. In: Computer Security: ESORICS 2019 International Workshops, IOSec, MSTEC, and FINSEC, Luxembourg City, Luxembourg, September 26–27, 2019, Revised Selected Papers 2, pp. 140–155. Springer (2020)
24. Ardanza, A., Moreno, A., Segura, Á., de la Cruz, M., Aguinaga, D.: Sustainable and flexible industrial human machine interfaces to support adaptable applications in the Industry 4.0 paradigm. Int. J. Prod. Res. **57**, 4045–4059 (2019)
25. Geilen, M., Tripakis, S., Wiggers, M.: The earlier the better: a theory of timed actor interfaces. In: Proceedings of the 14th international conference on Hybrid systems: computation and control, pp. 23–32 (2011)
26. Canedo, A., Schwarzenbach, E., Al Faruque, M.A.: Context-sensitive synthesis of executable functional models of cyber-physical systems. In: Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems, pp. 99–108 (2013)

27. Hu, F., et al.: Robust cyber–physical systems: Concept, models, and implementation. Futur. Gener. Comput. Syst. **56**, 449–475 (2016)
28. Yang, Y., Zhou, X.: Cyber-physical systems modeling based on extended hybrid automata. In: 2013 International Conference on Computational and Information Sciences, pp. 1871–1874. IEEE (2013)
29. Rojas, R.A., Rauch, E., Vidoni, R., Matt, D.T.: Enabling connectivity of cyber-physical production systems: a conceptual framework. Procedia Manufact. **11**, 822–829 (2017)
30. Alwan, A.A., Ciupala, M.A., Brimicombe, A.J., Ghorashi, S.A., Baravalle, A., Falcarin, P.: Data quality challenges in large-scale cyber-physical systems: A systematic review. Inf. Syst. **105**, 101951 (2022)
31. Rahman, H.U., Wang, G., Bhuiyan, M.Z.A., Chen, J.: In-network generalized trustworthy data collection for event detection in cyber-physical systems. Peer J. Comp. Sci. **7**, e504 (2021)
32. Li, P., Lu, Y., Yan, D., Xiao, J., Wu, H.: Scientometric mapping of smart building research: towards a framework of human-cyber-physical system (HCPS). Autom. Constr. **129**, 103776 (2021)
33. Abrahamsen, F.E., Ai, Y., Cheffena, M.: Communication technologies for smart grid: a comprehensive survey. Sensors **21**, 8087 (2021)
34. Habibzadeh, H., Nussbaum, B.H., Anjomshoa, F., Kantarci, B., Soyata, T.: A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. Sustain. Cities Soc. **50**, 101660 (2019)
35. Massar, M., et al.: Impacts of autonomous vehicles on greenhouse gas emissions—positive or negative? Int. J. Environm. Res. Pub. Health **18**, 5567 (2021)
36. Gupta, A., Singh, A.: A comprehensive survey on cyber-physical systems towards healthcare 4.0. SN Computer Science **4**, 199 (2023)
37. Asadi, K., et al.: An integrated UGV-UAV system for construction site data collection. Autom. Constr. **112**, 103068 (2020)
38. Torky, M., Hassanein, A.E.: Integrating blockchain and the internet of things in precision agriculture: Analysis, opportunities, and challenges. Comput. Electron. Agric. **178**, 105476 (2020)
39. Lee, J., Azamfar, M., Singh, J.: A blockchain enabled cyber-physical system architecture for Industry 4.0 manufacturing systems. Manufacturing letters **20**, 34–39 (2019)

Analysis of Device-To-Device Communication in Iot System

Usman Nawaz[1], Faisal Rehman[1,2(✉)], Kainat Azmat Ullah[1], Usman Ahmed Raza[3], Hanan Sharif[1], Furqan Rafique[1], Abid Ali[1], Masood Ashiq[1], and Junaid Iqbal[1]

[1] Department of Computer Science, Lahore Leads University, Lahore, Pakistan
Faisalrehman0003@gmail.com
[2] Department of Statistics and Data Science, University of Mianwali, Mianwali, Pakistan
[3] Faculty of Information Technology, University of Central Punjab, Lahore, Pakistan

Abstract. Peer-to-Peer communication is based on an important feature of communication which is Device-to-Device (D2D) communication. IoT is a computational device that is equipped with accurate identifiers and the capacity to speak data across a network without the assistance of a human. D2D communication is referred to as "Direct verbal exchange among the taking part gadgets without the use of the centralized infrastructure". This research study examines the advantages and barriers of D2D communication as a means of meeting the IoT's requirements. Many companies and quality management organizations have demonstrated a strong interest in implementing the D2D approach in wireless networks. The thought of working without the necessary control of centralized supervision and making Wi-Fi networks wider as well as energy saving can be made possible with D2D communication in IoT. These devices' technical limitations and the connection's support limitations provide an upward push to numerous problems that must be addressed. Some of the IoT studies Electricity production, connectivity, security, scenario technologies, and so forth are all issues. We cognizance's on troubles that in the IoT there is an influence in D2D communication surroundings. We also discovered some important stumbling blocks to the success of smart D2D speech communication in the Internet of Things. We talked about how to deal with these difficult situations. This research explains the idea of a tool to tool verbal exchange and IoT system and defines its predominant techniques and applications imparting a subsequent era therefore as procedure strategy to the demanding situations. To boost research and development in the domains IoT problems have been studied. Every cited research work's contribution and limitations are discussed as well as any potential problem statement and open rely.

Keywords: Device to Device communication · Internet of Things (IoT) · Wireless network resources

1 Introduction

Sending and receiving messages through language, expression, or some other medium is referred to as communication. The major feature of the Internet of Things (IoT) is device-to-device communication which is peer-to-peer communication. Working outcomes,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 108–127, 2025.
https://doi.org/10.1007/978-3-031-77620-5_8

enhanced efficiency, and resource utilization can be improved with the help of the D2D [1] communication approach. There are multiple wireless or wired methods for IoT-based networks but we lack in the field of communication between IoT devices while they are the primary client in IoT systems. Gadgets will autonomously communicate with each other without centralized power and pre-collect, distribute and save in a multi-tabbed manner. Facts may be transformed into intelligence as a way to facilitate the creation of a wise environment. The main benefit of IoT systems is that they can gather data in real-time. The collection of data in real-time and the speed of devices to manage the time-critical environment shows that the devices are more clever than our imaginations [2]. Furthermore, speaking devices should work under extraordinary requirements for connectivity will have a connection that comes and goes one another and would be limited in terms of resources in many cases. Such traits are there to create a slew of networking problems that typical routing techniques can't tackle. Mostly as a reason to gain a competitive advantage devices would need astute network parameters.

The communication network is required to meet the Internet of Things needs. Many companies and standards organizations have demonstrated a significant interest in implementing the D2D technique in wireless networks. People are becoming increasingly connected via the Internet, resulting in exponential development in the number of related gadgets. Several networks such as Bluetooth connectivity, Wi-Fi, RFID, ZigBee, etc. are used for short-range communication. They're made up of record-processing equipment. The method of creating, sharing, and altering content necessitates a connection between technologies, whether or not they require processing time. Some gadgets can be any type of devices or objects (for example, smartphones, sensors, electrical devices, autos, equipment for the house, or RFID tags) that are equipped with intelligent Skills in outcome, calculation, and public speeches. As a result, not only are the most effective persons interconnected, but so are the most effective gadgets. From this paradigm shift (IoT), the concept of the Internet of Things was born. The Internet of Elements (IoT) is an extraordinary extension of the current Internet that has evolved from an interconnected community of people to an interconnected community of gadgets. Therefore, humans can collect data from their environment, and these devices interact with the body's world through network protocols and standards.

The Internet of Things (IoT) along with machine and deep learning has emerged to be recent research area while talking about networks and networks security and various types of research have also been proposed in this domain, for instance [3–9].

The Internet of Things will make it possible to transform perception or information gathering into intelligent knowledge and successfully integrate intelligence into the surrounding environment. In addition, the Internet of Things will consist of billions of gadgets that can save their space, identity, and information over Wi-Fi connections. In 2003 when the world's population is estimated to exceed 6.3 billion and all 500 million of the simplest devices are connected to the internet. As a result, there was just one tool that was constant with each individual at the time. By 2010, the types of internet-related devices had increased to 12.5 billion and the population of the arena to 6.8 billion, making the number of related devices equal to one floor for the first time.

As a consequence, there was no Internet of Things in 2003 because there were several types of connected devices. After creating the first computer system for smartphones and

pill makers in 2003, the number of connected devices gradually increased. According to a recent prognosis, the number of connected devices would quadruple by 2013 when compared to the total number of people on the planet reaching. It is estimated that it will reach 25 billion in 2015 and the world population will reach 7.2 billion. It is also estimated that there will be around 50 billion connectable devices by 2020. The number of gadgets will eventually exceed the industry's population by four times. Improvements in the tools used to plan and control human physical activity daily could contribute to this expansion. Internet of Things devices, including private devices on the Internet of Things, are non-standard computing devices that can connect to the community wirelessly and have the ability, to tell the truth (IoT).

1.1 D2D Communication

Device-to-device communication is a cutting-edge data transmission method designed to boost network efficiency. D2D communication-capable devices can communicate with each other utilizing a secure transmission protocol similar to how they communicate with the base station in LTE -Direct. D2D communication networks are divided into two categories. (Fig. 1) is a stand-alone D2D verbal exchange in which devices converse with one another without the need for infrastructure.

Fig. 1. D2D Communication without Infrastructure [10]

In Fig. 2 there is an existing helping infrastructure, with network-assisted D2D communication. With the advancement in technology, the need for a D2D communication system is increasing. The communication between devices should be smooth, reliable, and time efficient, for the success of IoT in bigger societies.

1.2 D2d Communication Approach

In the Wi-Fi community, D2D stands for the location of the hobby because of several benefits. This strategy is ideal for reducing the stress on the network infrastructure caused by site traffic. Devices will communicate with one another via the D2D technique,

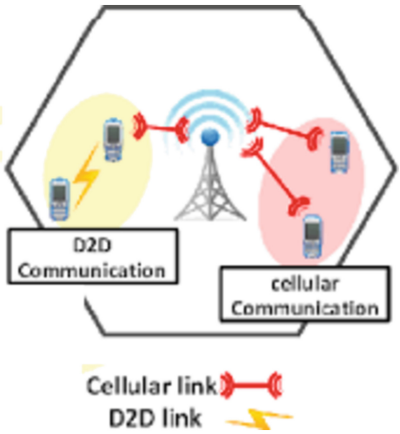


Fig. 2. D2D Communication with Infrastructure [10]

which eliminates the need for BS manipulation. It also converts -hop communications (through BS) into a single Hope spoken exchange. Figure 3 demonstrates immediate D2D communication in a phone link with standard cell communication. D2D generation is becoming increasingly significant to deliver improved facilities. For instance the event of an attack or tragedy or when internet work is unavailable or broken. D2D connectivity might reduce reliance on existing core infrastructure.d2d communique is primarily based on the mobile community and includes all three types of d2d communication. Essentially, D2D conversations can be classed as running in a certified or unauthorized band. The most extensively utilized wireless technologies are Wireless charging and Wi-Fi eras in the unlicensed spectrum for establishing tiny communities for information sharing.

Because it is publicly available it provides a vital platform for inventors. A comfortable network for quick-range communication can be created by commercial use of unlicensed spectrum, clinical or scientific services at any time and from any location. The community is constrained by its constraints due to the limited range of signals available. For a large community, many intermediate nodes are required, which results in higher bandwidth utilization or delay difficulties.

These gadgets are also susceptible to intervention. Once again, in the certified frequency band, the wireless community can transmit a density of 1000 samples and a distance hundreds of times greater than the communication system [11]. It will improve the communications variety, throughput, and performance. Security concerns may likely be alleviated, and the system will be less susceptible to outside intervention. Furthermore, the use of green resources and interference control are key subjects to consider when evaluating network performance. In an IoT environment established with D2d users, a connection between unregistered and allowed bands is essential.

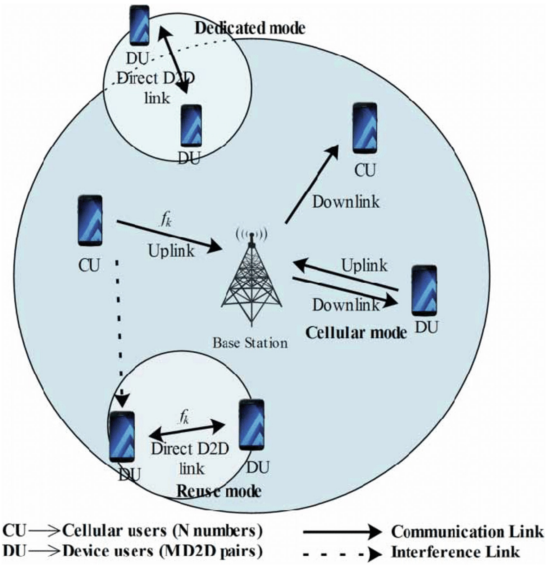


Fig. 3. D2D under laid using Wireless Connectivity and All Three D2D Communication Modes [1]

Cellular Mode
Devices speak in this mode as though they have been using a traditional cell telephone. The data is passed via the BS which serves as an intermediary point. From source to destination, a bridge connection is required (Uplink and downlink).

Dedicated Mode
A separate connection between the sender and receiver is formed under this state, allowing for an immediate spoken connection. There are no gaps between cellular and d2d voice communication.

Reuse Mode
In this method, D2D verbal interaction collaborates with cellular communication to share available resources. It allows you to repurpose a tunnel that is currently being used by mobile communication. This mode makes environmentally friendly usage with no trouble easily accessible communal sources. The main difficulties to overcome in the usable plan updated and intervention management are two reusable kinds of strategies.

1.3 Advantages of D2D Communication

- Increased efficiency in the community
- Less power usage and a longer battery life
- Controlling traffic loads efficiently
- Even in the absence of a community, a connection can be established.
- Extending the network without the need for expensive infrastructure like base stations is possible.

- Multiple applications of D2D communication.
- Public safety and security services
- Peer-to-peer communication [12] between machines
- Independent riding packages and vehicle-to-vehicle communication
- Offloading of cells (to WLAN community for quicker records transfer)
- Gaming and social networking in the neighborhood
- Content distribution, local advertising, and location-based services
- Emergency broadcast and warning message for a specific place

1.4 Types of D2D Connectivity Approach

The participation of cellular infrastructure in the setup of the direct connection, as well as the spectrum over which the direct speech exchange occurs, may be used to classifyd2d (direct-to-device) connectivity cooperation between wireless connections as managed by the users in self-organized D2D communication. This method works in the same way as unregistered radio is used in classic wireless communication. It identifies software when the mobile network isn't always available, and it's frequently motivated by its low interaction and straightforward maintenance (e.g. in case of an herbal catastrophe).In community-assisted D2D communication, on the other hand, the base station (BS) aids immediate facts dissemination via command communication and aid maintenance [13]. In this situation to limit the likelihood of interruption computer system may integrate any transmissions. One consequence of this cooperation is that it may necessitate a lot of signaling and utilization that is central. Multiple kinds of systems integration are also available that are expected such as the intention of striking a good balance of expense in terms of difficulty and transmission, as well as promised efficiency. As illustrated at some point within the investigation portion, d2d clients may be provided by the most effective network. They are in charge of their own operations and media sources after which they can plan. According to what Device - to - device users are accessing the range.

There are some main components that one needs.

- Sensor
- Gateway
- Connectivity
- Cloud
- Analytics
- User interface

Sensor

Sensors are the link between IoT devices and the outside world or people. It identifies changes and sends the data to the cloud for processing as the name implies. These sensors collect data from the environment constantly and send it to the next level. Sensors such as pressure sensors, temperature sensors, and light density detectors are examples.

Gateway

The gateway helps mobile data management and protocol layer transfer statistical information from one device to any other device. It interprets the device's community protocol

and provides encryption for information flowing into the community. It is like a layer between the cloud and the device that can clean up statistics of network attacks and illegal logins.

Connectivity
Statistical data collected by the sensor should be sent to the cloud for analysis. Information needs the Internet as a means of transferring facts from one device to any other device. Therefore, all IoT devices want to be connected to the Internet at all times. Wi-Fi, Bluetooth, WAN, satellite networks, and other networks make it easy to stay in touch. Statistics can be sent to the cloud via these networks.

Cloud
IoT systems generate large volumes of data from devices that must be properly managed to produce useful outputs. The IoT cloud is used to store so much data. It provides tools for data collection, processing, and storage. Data can be easily accessed and accessed from anywhere via the internet. It can also be used as an analysis tool. The IoT cloud is a complex network of high-performance servers that can rapidly process large amounts of data.

Analytics
The process of transforming raw data into something useful is called analysis. IoT analytics supports real-time analytics to capture changes and anomalies in real-time. The data is then converted into an easy-to-understand format for the end user. For the successful implementation of their ideas, users and businesses can use the reports to adapt trends, market predictions, and plans beforehand.

User Interface
The Internet of Things system has a visible and tangible user interface. It is the part where the machine communicates with the plug. Statistics can be provided in document format or in the form of actions such as alerting, or sending notifications. Also, the user can choose to perform some actions. It is very important to design a user-friendly interface that can be used without much effort or technical knowledge.

1.5 Characteristics of IOT

Connectivity
The primary purpose of the IoT is connectivity, which makes the devices send data and stay connected with other devices. Allows devices to connect to the network and collaborate on functions.

Intelligence
The Internet of Things system is preferred by the market because of its intelligence. The combination of algorithms and computers enables the device to detect processes in the environment and take appropriate actions. For example, the system is smart enough to detect a sudden temperature rise and trigger an oven alarm.

Expressing
The Internet of Things is about intelligent interaction with the outside world and people. This interaction is achieved through expression. Expression allows us to communicate the output to the real world, as well as the inputs of people and the environment.

Sensing
Sensitivity refers to being aware of the changes occurring in our environment. Sensor technology enables us to create an experience that reflects awareness of changes in the physical world and its inhabitants. This makes it easier for you to express yourself. This document records the introduction to the IoT system and provides a better understanding of the complex world around us.

Energy
Everything in this world is based on the use of force. The design of the Internet of Things structure is smart enough to synthesize and store energy from the outside world. It has also been developed to be strong enough to paint for a long time.

Security
The most important feature of any device is its safety and security. Nobody will utilize a device if it is vulnerable to cyber-attacks and unauthorized access. IoT systems deal with personal information [5], so it's a must that every safety level be met on this machine. All IoT structures are secure enough to handle personal information. Aside from that, the equipment required is substantial. IoT networks may also be vulnerable because device security is critical and crucial.

1.6 Problem Statement

The voice d2d era will play a key role in the Internet of Things (IoT). The incredible rapid improvement of operators' internal levels necessitates big adjustments to the Internet of Things tools' design, and community devices supply a set of processes to improve the element network. The system's physical restraint and the community's auxiliary restraint make for a difficult decision. The performance of language exchange will be greatly impacted by D2D pair interference, and the minimum distance requirement for D2D communication must assure SNR.

Research Objective
This research aims to study modern linguistic communication techniques and how we can follow these strategies to communicate in IoT. Our important goal is to provide readers with the latest cutting-edge material on the work (protocols and proposed solutions) done so far in d2d communication and uncover the issues that still need to be resolved.

1.7 Research Question

What is device-to-device communication and how does d2d communication work in IOT?

2 Literature Review

In this study [14] authors categorized the forms of interaction as well as the reasons for each form of oral exchange of information in IoT. In intra-domain networks, gadgets can also collect records through calls or record their kingdoms with each other. Across networks, devices can also communicate without or with manual intervention. Interacting with humans or issuing alarms for human decisions may require communication between devices through human intervention. Devices can also speak to perform actions or discover or find different devices without human intervention. Devices can communicate with humans without delay to bypass information about humans or immediately obtain information from humans to make decisions. Gadgets can also communicate with information garage agents to deliver captured statistics, update stored records, or retrieve saved records for computerized decision-making.

In this work [15] a complete end-to-end solution for each application is needed to be provided for the healthcare strategy to cover the technical details. From the standpoint of verbal communication technology, the survey looked at crucial application-specific criteria. Different approaches and protocols are provided in the studies which help to make these applications work, with the possible potential benefits and barriers of short and long-distance communication methods. Finally, the poll identified important open research challenges and difficulties, particularly those concerning the future healthcare structure, which would be driven by the Internet of Things. Optical sensors (blood sugar and strain, oxygen saturation, and other key symptoms), Environment (temperature, pressure, humidity measurement, etc.), accelerometer, magnetometer, and other sensors are all included in today's smartphones (which can be used as a framework coordinator or an important unit for personalized health monitoring) (for measuring speed, route, and gravity results). Additionally, the Smartphone's built-in bag (such as S-Health) can be utilized to save daily fitness music. The widespread usage of wearable auxiliary generation and the open supply of general-purpose systems, on the other hand, has issues with dependability, statistical privacy and security, and value effectiveness. In general, cutting-edge language exchange technology can meet the requirements of dependability, connectivity, factual cost, and delay for most practical situations, including infectious diseases, musculoskeletal, and neuromuscular disorders. Converged technologies may, however, be required to deliver smoking cessation solutions for expanding healthcare application.

This research [16] states that To promote a structure with controlled structural resistance. A device-to-instrument (d-d) negotiating mechanism is proposed in this study that allows green to react at the point of consumption. The proposed method creates a neighborhood voice exchange community and a negotiation algorithm between the smart grids connected to the IOT gadget that communicates along with the intelligent machine's base structure. In addition, a mesh network to enable a dynamic and responsive network system amongst IoT devices and configuration is used. As a result, the language exchange system ensured that the suggested set of d-d energy settlement rules is highly reliable. Each IOT tool will receive statistics on a specified amount of electricity consumption reduction from the smart meter and send a backup record of its preparedness to perform the required electricity diminution. The d-d interaction and IOT gadget selection rule set are dependent on the operational priority of the device, power requirement as well

as accessibility. Therefore, the proposed d-d trading algorithm guarantees a knowledge selection mode and reliable factual dialogue to promote green energy management.

In this work [17] one of the most advanced technologies for improving network performance is communication. Customers near the periphery or close to the insurance region can communicate through D2D linkages, allowing D2D communication to grow. Gadgets in the radio location are authorized to use D2D oral communication in the D2D communication device settings. When using a mobile network, however, several communication devices are not always in the same radio range. In this case, two communication parties exchange statistical data over a direct hyperlink without the need for any involvement from the cellular infrastructure, including the BS or both in the cellular mode.

Here, the two talking devices communicate utilizing mobile services and peer-to-peer transmission, as well as direct linkages between pals. It is possible to simulate and analyze D2D customer behavior, whether it be individual or collective, using a set of mathematical tools provided by the theory of many transmission systems. As a result, a new strategy is required in this location to address some issues connected to disconnection. These issues may need to be dealt with well in addition to bandwidth limits, high latency, and so on. Structure of the D2D type the peer must go through the peer discovery process before the device can begin D2D communication. For two capacity devices to create a connection for D2D discussions on the direct link, peer discovery is required.D2D candidates are a pair of devices that can discover each other during P2P discovery. From the discovery phase until the two devices begin to communicate this is the overall discovery process of D2D communication.

In this study [18] the reaction time of edge gadgets in an IoT system [5] is calculated by layout time. These partial devices continuously offer a flow of data to guarantee that real-time IoT units run smoothly. Facet devices, on the other hand, are prone to errors and must often address issues while attempting to maintain a decent level of vocal communication in the face of external interference. The absence of any conversation at the threshold tool level can cause the entire system to fail or deliver inaccurate information. Because IoT equipment contains a wide array of heterogeneous devices that's not easy to see all of these gadgets in one place or to look through the gadget logs to see if there's a problem with connectivity. As a result, a lightweight intelligent layer on the edge device, which may be modified according to internal changes, may be required to retain the maximum quality of first-class communication while being as close as feasible to the precise theoretical reaction time. Their proposed ASB can be implemented on IoT devices as a lightweight intelligence layer to track good communication and offer the next best exchange alternative to maintain a sufficiently high level of communication so that the device can communicate in real time.

In this work [19] in the IoT D2D newsletter they looked at the importance of security. Furthermore, we offer Secure Key Exchange with QR Code (SeKeQ), a single authentication mechanism that ensures automatic key assessment and uses the Diffie-Hellman key agreement with SHA-256 hash Key to validate personal identity. We used a test mattress and a gadget with a Wi-Fi-Direct connection interface to evaluate SeKeQ's performance. The results suggest that our concept can provide the necessary security aspects, such as crucial backup, data secrecy, and integrity. Furthermore, our approach

achieves the same level of security as MANA (Manual Authentication) and UMAC (Universal Hash Message Authentication Code), but with a 10x reduction in key computation and a smaller memory footprint. Currently, regardless of the tool's vicinity, all data traffic in a Wi-Fi cellular network creation must transit via a set of infrastructure. To minimize overburdening the infrastructure, it's ideal to allow direct device-to-device communication whenever possible. The problem of the radio access network load and intermediate network load will be discovered when the gadgets are close to each other.

This paper [20] is designed to increase the cumulative machine improvement system by determining the transmission rate of each d2d and mobile hyperlink.D2d customers considered three modes of communication: mobile mode, delivery function as well as reusable mode. Energy management and combined power management and connection allocation are two sub-problems of the optimization problem (Table 1).

Table 1. Analysis of Literature Review Regarding D2D Communication Systems in IoT

Sr. No.	Author	Year	Title	Objective	Tools or Techniques	Short Summary
1	F, Zenalden, et al. [17]	2020	Peer Selection in Device-to-Device Communication Based on Multi-Attribute Decision Making	When a user moves between multiple network spots, it tries to find and select the optimal peer to initialize a D2D connection	Using the Analytic Hierarchy Process and Hierarchical Adaptive [21] Weighting, the peer selection process makes decisions	When the network verified the D2D connection, better results were observed
2	S.Umrao et al. [22]		Device-to-Device Communication from Control and Frequency Perspective	Issues like interference, mode decision-making, supplemental distribution, and security can all be resolved via D2D communication's native support	Over the analysis technique in detail and ruled out any open research requirements	discussed the core D2D architecture, protocols, and associated procedures
3	Y. Haung et al. [23]	2016	Mode selection, resource allocation [24], and power control for D2D-enabled two-tier cellular network	Two-tier mobile network mode selection with d2d enabled, payload allocation, and intensity control	It is suggested to use geometric vertex search technology to boost overall performance and address the power distribution issue	The total cost of the system can be increased with the frequency-sharing technology

(*continued*)

Table 1. (*continued*)

Sr. No.	Author	Year	Title	Objective	Tools or Techniques	Short Summary
4	A. Sultana et al. [25]	**2017**	Efficient resource allocation in device-to-device communication using cognitive radio technology.“	Optimize the transmission cost of d2d users while limiting electricity costs, interference costs, and statistical charges	He proposed a subcarrier allocation scheme using cognitive radio networks and also developed a power allocation scheme	Determine the most suitable solution with less computational complexity to solve the nonlinear failure rule
5	M.Belleschi et al. [26]	2011	Performance analysis of a distributed resource allocation scheme for D2D communications	Distributed rule sets require minimal reporting overhead and reduced computational complexity	Combined mode transmission and resource allocation for d2d communication	A two-step method of low complexity is proposed and a d2d communication in mixed mode with a useful resource allocation method is proposed
6	Y. Zhang et al. [27]	2014	Social network aware device-to-device communication in wireless networks	Optimize the stream download process in d2d communication	Indian Buffet gained knowledge on modeling methods of online social networking. Chernoff’s limit is derived to assess the overall performance of the proposed algorithm	A weird social awareness method is proposed to optimize traffic offload for d2d communication
7	J. Liu et al. [28]	**2015**	A stochastic geometry analysis of D2D overlaying multi-channel downlink cellular networks	Improve insurance probability and cross-cost of multi-channel D2D mask	The random geometry method works on a complete cellular network based on d2d, which will improve the performance of community coverage	Enabling d2d links relies primarily on store connections, which can dramatically improve network assurance performance

(*continued*)

Table 1. (*continued*)

Sr. No.	Author	Year	Title	Objective	Tools or Techniques	Short Summary
8	Q. Ye et al. [29]	2014	Distributed resource allocation in device-to-device enhanced cellular networks	d2d distribution assistance distribution in the largest mobile networks	Provides useful resource locks and power allocation and abandons the idea of going out of the transmission relay to improve the performance of the d2d	Achieve big productivity gains with low overheads
9	M.Tehrani et al. [30]	2014	Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions	Discover cellular applications in D2D cellular communication	For d2d cellular communication, a code-based protocol is proposed, which uses a method entirely based on the hash and bloom clear characteristics	The proposed protocol dealt with an excessive density of devices and quickly absorbed a small number of radio resources
10	L. Wang et al. [31]	2015	Socially enabled wireless networks: Resource allocation via bipartite graph matching	Maximize the overall performance of the entire system	Used to match the Hungarian rule set. Optimize functionality by maximizing total registration costs	In the event of maximization of conventional performance indicators, taking into account power and quality of service constraints and taking into account aid sharing problems
11	Q. Duong et al. [32]	2014	Location-dependent resource allocation for mobile device-to-device communications	Research on the allocation of useful green resources for D2D communication in the cellular network	The total allocation of resources based on distance based on outage probability assessment	A resource allocation plan that is beneficial for interference detection is suggested to increase the efficiency of the spectrum

(*continued*)

Table 1. (*continued*)

Sr. No.	Author	Year	Title	Objective	Tools or Techniques	Short Summary
12	G. Yu et al. [11]	2014	Distributed resource allocation in device-to-device enhanced cellular networks	Selection of common mode and auxiliary distribution of d2d communication	For light and medium load scenarios, a set of low-complexity heuristic rules is proposed	To get the most out of the system as a whole, low-complexity algorithms are designed
13	Wang, F et al. [33]	2012	Energy-efficient radio resource and power allocation for device-to-device communication underlying cellular networks	The community management side chain communication scheme has a context-sensitive rule in place to ensure the effectiveness	Apply tool-to-device newsletters to decorate IOT products	A signaling system is employed to enable large-scale D2D communication and to configure linkages and cell links
14	D. Feng et al. [34]	2013	Device to Device communication underlying cellular networks	Maximize the overall productivity of the community	Maximize overall throughput when the device and cellular users pay attention to uplink control	With the help of the suggested plan, d2d began to load and enhanced the total network throughput
15	C. Xu et al. [35]	**2013**	Efficiency resource allocation for device-to-device underlay communication systems	Optimize the total cost of the machine by sharing useful resources in d2d and mobile mode	Public sale using the opposite iterative combination	Low complexity auxiliary distribution scheme is proposed to increase the total cost of the machine

3 Materials and Methods

The generation of PCs has been with us because in the middle of 20thCentury has laid its foundation despite all the technical obstacles. The foundation for the idea of conversation from system to device (M2M) which progressively evolved collectively with connectivity improvements the answers initiated the concept of the Internet of Things as we understand it today. Factor Network (IoT) [36] is a system of virtual tools, machines, objects, or people connected by specific identifiers and can transmit statistics and percentages within the community without the need for people or persons with pc interactions. The Internet of Things has several goals to create intelligent Humans and also groups of people who live in situations that are conducive to learning. Entire cultures could be capable of maintaining a more intelligent and calm state. As grandiose as it

could appear, the Internet of Things (IoT) [37] has indeed proven its worth emerged as a regular aspect of our lives and certainly finds its way there and do it. With something in consideration, let's take a look at the equipment that powers the global IoT and allows it to move spherically.

3.1 Research Methodology

IoT gadgets are composed of multiple additives, which interact with each other. It gives a conceptual model of the components that make up a typical IoT device, such as the relationship between the main IoT ideas. The user can be a human character or a software agent with a goal. Things are discrete and recognizable parts of the physical environment, and users may be interested in accomplishing their goals. Things can be any physical entity, including people, cars, animals, or computers.

The interaction between users and issues in the Internet of Things is mediated through services, which constitute the interface between consumers and Internet of Things devices. Services are associated with virtual entities, that is, virtual diagrams of physical entities. Components can be represented in a virtual world by digital entities. Different types of numerical representations of factors can be used, such as gadgets, 3D models, avatars, or perhaps social community bills. Some virtual entities can also interact with different digital entities to meet their purposes.

A key element of the Internet of Things is that the adjustment of the problem location and its corresponding virtual entities need to be synchronized. This is usually achieved by devices that are embedded, connected to, or placed in the vicinity of the factor. Filters, identifiers, and actuators are the three categories of gadgets that can be identified in theory. Sensors are used to rank the countries and locations where things are filtered. The sensor turns a mechanical, optical, magnetic, or thermal signal into a voltage and tip. These details can then be analyzed and used to create a description of the sport in question. The tag is a device that aids in the analysis procedure, which normally involves the use of a specialized sensor called a reader. Special documentation, including optics, such as barcodes and QR codes, can be handled by the identifying system, which is solely based on the frequency range. Actuators are employed to transform or influence things once more (Fig. 4).

3.2 Architecture of an IOT System

Companies and services that are one-of-a-kind outline, develop, and comprehend the structure of the Internet of Things in a unique way. Regardless of the application or business strategy, the underlying framework of IoT devices remains the same.

The four-layer version of the IoT devices' basic structure can be understood as

1) IoT devices and Gateway
2) Network of communication
3) Server or cloud
4) Programmed is the Internet of Things Utility Program.

Through IoT devices, data is generated, transported, processed, and transformed into meaningful insights (Fig. 5).

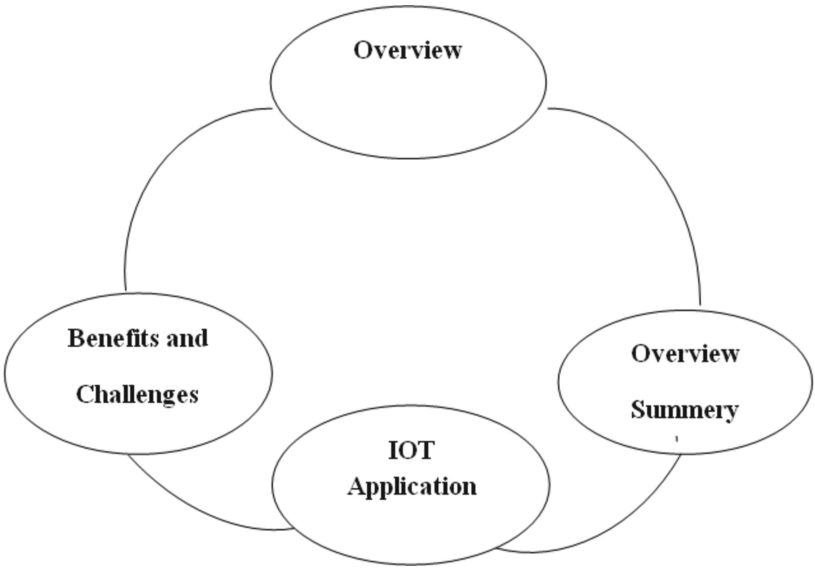


Fig. 4. Working mechanism of the proposed methodology

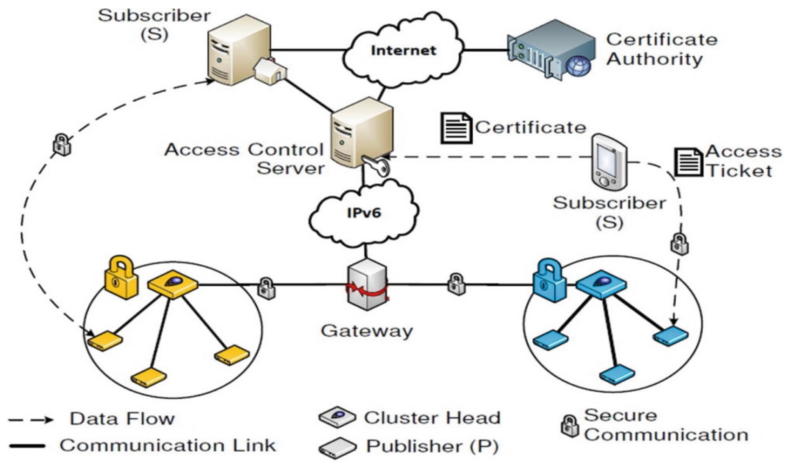


Fig. 5. Architecture of IOT System which describes the communication flow from the subscriber to the access control authority [38]

4 Discussion and Results

This chapter focuses on the analysis of empirical statistics gathered during the fieldwork phase of the study. After completing the interviews and surveys, review the company's statistics data to verify that any questionnaires that are invalid or incorrect are removed by looking for samples of the respondents' responses and adding the finishing touches. The data analysis and interpretation will be finished soon, and the research goals will

be revealed. The empirical portion of this thesis focuses on device-to-device verbal communication, sequencing, blessings, and challenging scenarios, applications, issues, and safety, all of which are based only on IoT devices. Community social networks, on the other hand, have gotten a lot of attention from scholars in recent years. Cluster and alliance creation are the two main solutions recommended for resolving the privacy issue in this situation. In general, D2D communication [39] uses one-hop routing; however, in some instances (public safety, insurance growth, content distribution, and so on), multi-hop routing may be used. There is virtually little research on routing components in D2D communications in the literature. A lot of work needs to be done in terms of security factors, particularly to combat security issues associated with a lack of trust authorization. On the one hand, it's the topology's dynamic nature; on the other, it's to safeguard customers' security and privacy so that they can be observed. Without authorization, a large amount of sensitive data goes through a single node.

The Internet of Things is a concept that has yet to be fully realized, despite extensive research. Many off-the-shelf products rely on effective ways to meet demand. The installation of the Internet of Things is surely progressing with the technology supplied here. RFID allows gadgets to be automatically identified without the need for costly manual intervention. IPv6 enables IP processing to be offered for all projects. The Internet of Things is a forward-thinking and innovative concept that is now gaining traction. The concept of connecting everything and everything at all times is incredibly appealing. Its actual implementation is tough to assume, therefore overcoming these problems may require a significant amount of responsibility. There may be demanding scale requirements in terms of IP addressability, privacy, protection, and information control and analysis.

5 Conclusion

The Internet of Things needs to connect something, anytime, anywhere, build a bridge, and connect some real worlds with virtual worlds. Intelligent vehicles have autonomous functions under proper cooperation. Evolving equipment and new applications require wireless networks to deliver higher data costs, more powerful capacities, lower latency, and a better service experience. The d2d dialogue method meets these requirements but faces many difficult situations. The goal is to highlight the capabilities of the d2d method in improving the IoT environment. Also, it has an advertising value capable to causes an impact on the economy in the future and the domain. D2D conversation and IoT have performed a brilliant position in developing and improving the networks this paper intends to study both technologies in the past, cutting-edge, and predicted destiny based totally on the preview studies and demonstrate the venture. IoT expanding to plenty of industries and offerings together with enterprise and healthcare safety will keep being extra vital to shield touchy records and devices in opposition to harm. IoT has many advantages however is developing at a fast pace and some devices are stuck with old protection leaving them susceptible to assault and being restrained via way of the gadget's processing & energy consumption barriers. For a better, reliable, and user-friendly environment, D2D oral communication is becoming an important part of the IoT system that is growing rapidly. The most favorable paradigm for the future

communication of devices is D2D conversation. We provided a comparative evaluation of the IoT society with supportive arguments from the conventional systems. This study highlights the usage, benefits, and challenges of the entire convergence of IoT.

References

1. Pawar, P., Trivedi, A.: Device-to-device communication based IoT system: benefits and challenges. IETE Tech. Rev. (Institution Electron. Telecommun. Eng. India) **36**(4), 362–374 (2019). https://doi.org/10.1080/02564602.2018.1476191
2. Chen, Y.S., Hong, J.S.: Intelligent device-to-device communication in the internet of things. IEEE Syst. J. **7**(1), 77–91 (2014)
3. Ashraf, S., Rehman, F., Sharif, H., Kirn, H., Arshad, H.: Fake reviews classification using deep learning. 2023 Int. Multi-disciplinary Conf. Emerg. Res. Trends (2023). https://doi.org/10.1109/IMCERT57083.2023.10075156
4. Safdar, M.F., Sharif, H., Rehman, F., Bilal, Z., Ahmad, S.: A Review of Recent Advances in Deep Learning for Object Detection (2023). https://doi.org/10.1109/ICONICS56716.2022.10100486
5. Khalid, M.H., et al.: A Brief Overview of Deep Learning Approaches for IoT Security (2023). https://doi.org/10.1109/iCoMET57998.2023.10099306
6. Hassan, A., et al.: Performance Enhancement in Agriculture Sector Based on Image Processing (2022). https://doi.org/10.1109/ICONICS56716.2022.10100392
7. Manan, I., Rehman, F., Sharif, H., Riaz, N., Atif, M.: Quantum Computing and Machine Learning Algorithms - A Review (2023). https://doi.org/10.1109/ICONICS56716.2022.10100452
8. Sarfraz, N., Rehman, F., Sharif, H., Akram, S., Mughal, B.H.: Efficient Energy Storage Systems Management in Power Plants with Artificial Intelligence and Price Control (2022). https://doi.org/10.1109/ICONICS56716.2022.10100617
9. Riaz, N., Shah, S.I.A., Rehman, F., Gilani, S.O., Emad-udin: An Approach to Measure Functional Parameters for Ball-Screw Drives, 398–408 (2020). https://doi.org/10.1007/978-981-15-5232-8_34
10. Abualhaol, R.A.R.M.S.I.: Survey on device-to-device communications: challenges and design issues Publisher: IEEE (2014). https://doi.org/10.1109/NEWCAS.2014.6934057
11. Feng, D., Lu, L., Yi, Y.W., Li, G.Y., Feng, G., Li, S.: Device-to-device communications underlaying cellular networks. IEEE Trans. Commun. **61**(8), 3541–3551 (2013). https://doi.org/10.1109/TCOMM.2013.071013.120787
12. Wang, H., Wang, R., Yan, J., Wu, D., Zhang, C.: Socially aware D2D cooperative communications for enhancing Internet of Things application. EURASIP J. Wireless Commun. Netw. **2018** (2018). https://doi.org/10.1186/s13638-018-1127-0
13. Jameel, F., Hamid, Z., Jabeen, F., Zeadally, S., Javed, M.A.: A survey of device-to-device communications: Research issues and challenges. IEEE Commun. Surv. Tutorials **20**(3), 2133–2168 (2018). https://doi.org/10.1109/COMST.2018.2828120
14. Hussain, A., Manikanthan, S.V., Padmapriya, T., Nagalingam, M.: Genetic algorithm based adaptive offloading for improving IoT device communication efficiency. Wirel. Networks **26**(4), 2329–2338 (2020). https://doi.org/10.1007/s11276-019-02121-4
15. Alam, M.M., Malik, H., Khan, M.I., Pardy, T., Kuusik, A., Le Moullec, Y.: A survey on the roles of communication technologies in IoT-Based personalized healthcare applications. IEEE Access **6**, 36611–36631 (2018). https://doi.org/10.1109/ACCESS.2018.2853148
16. Simulink, M.: Electronics and electrical engineering Elektronika ir elektros inžinerija **10**, 1–6 (2018)

17. Zenalden, F., Hassan, S., Habbal, A.: Peer selection in device-to-device communication based on multi-attribute decision making. 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 570–574 (2020). https://doi.org/10.1109/ICIoT48696.2020.9089605
18. Sudharsan, B., Breslin, J.G., Ali, M.I.: Adaptive strategy to improve the quality of communication for IoT edge devices. IEEE World Forum Internet Things, WF-IoT 2020 - Symp. Proc. (2020). https://doi.org/10.1109/WF-IoT48130.2020.9221276
19. Belghazi, Z., Benamar, N., Addaim, A., Kerrache, C.A.: Secure Wifi-Direct using key exchange for IoT device-to-device communications in a smart environment. Futur. Internet **11**(12) (2019). https://doi.org/10.3390/fi11120251
20. Xiang, X., Liu, W., Xiong, N.N., Song, H., Liu, A., Wang, T.: Duty cycle adaptive adjustment based device to device (D2D) communication scheme for WSNs. IEEE Access **6**, 76339–76373 (2018). https://doi.org/10.1109/ACCESS.2018.2882918
21. Xiang, X., Liu, W., Xiong, N.N., Song, H., Liu, A., Wang, T.: Duty Cycle Adaptive Adjustment Based Device to Device (D2D) Communication Scheme for WSNs Publisher: IEEE (2018). https://doi.org/10.1109/ACCESS.2018.2882918
22. "No Title", https://doi.org/10.1109/TCOMM.2014.2386874
23. "Mode selection, resource allocation, and power control for D2D-enabled two-tier cellular network. https://doi.org/10.1109/TCOMM.2016.2580153
24. Cheng, P., Deng, L., Yu, H., Xu, Y., Wang, H.: Resource allocation for cognitive networks with D2D communication: An evolutionary approach (2012). https://doi.org/10.1109/WCNC.2012.6214252
25. "Efficient resource allocation in device-to-device communication using cognitive radio technology". https://doi.org/10.1109/TVT.2017.2743058
26. Belleschi, M., Fodor, G., Abrardo, A.: Performance analysis of a distributed resource allocation scheme for D2D communications Publisher: IEEE (2011). https://doi.org/10.1109/GLOCOMW.2011.6162471
27. Zhang, Y., Pan, E., Song, L., Saad, W., Dawy, Z., Han, Z.: Social network aware device-to-device communication in wireless networks. IEEE Trans. Wirel. Commun. **14**(1), 177–190 (2015). https://doi.org/10.1109/TWC.2014.2334661
28. "No Title", https://doi.org/10.1109/INFOCOM.2015.7218366
29. Ye, Q., Al.-Shalash, M., Caramanis, C., Andrews, J.G.: Distributed Resource Allocation in Device-to-Device Enhanced Cellular Networks Publisher: IEEE (2015). https://doi.org/10.1109/TCOMM.2014.2386874
30. Tehrani, M., Uysal, M., Yanikomeroglu, H.: Device-to-device communication in 5G cellular networks: Challenges, solutions, and future directions. IEEE Commun. Mag. **52**(5), 86–92 (2014). https://doi.org/10.1109/MCOM.2014.6815897
31. Wang, L., Wu, H., Wang, W., Chen, K.C.: Socially enabled wireless networks: Resource allocation via bipartite graph matching. IEEE Commun. Mag. **53**(10), 128–135 (2015). https://doi.org/10.1109/MCOM.2015.7295474
32. Botsov, M., Klügel, M., Kellerer, W., Fertl, P.: Location dependent resource allocation for mobile device-to-device communications. IEEE Wirel. Commun. Netw. Conf. WCNC, no. April 2014, pp. 1679–1684 (2016). https://doi.org/10.1109/WCNC.2014.6952482
33. Wang, F., et al.: Energy-efficient radio resource and power allocation for device-to-device communication underlaying cellular networks Publisher: IEEE (2013). https://doi.org/10.1109/WCSP.2012.6543016
34. Feng, D., Lu, L., Yuan-Wu, Y., Li, G.Y., Feng, G., Li, S.: Device-to-device communications underlaying cellular networks (2013). https://doi.org/10.1109/TCOMM.2013.071013.120787
35. Xu, C., et al.: Efficiency Resource Allocation for Device-to-Device Underlay Communication Systems: A Reverse Iterative Combinatorial Auction Based Approach. https://doi.org/10.1109/JSAC.2013.SUP.0513031

36. Zhang, S.S.P.: Improving Quality of Data: IoT Data Aggregation Using Device to Device Communications Publisher: IEEE (2018). https://doi.org/10.1109/ACCESS.2018.2878640
37. Xia, W., Shao, S., Sun, J.: Relay selection strategy for device-to-device communication (2013). https://doi.org/10.1049/cp.2013.0065
38. Ray, P.P.: A survey on Internet of Things architectures (2018). https://doi.org/10.1016/j.jksuci.2016.10.003
39. Chen, J., Liu, C., Li, S., Li, H., Li, X.: A Categorized Resource Sharing Mechanism for Device-to-Device Communications in Cellular Networks (2016). https://doi.org/10.1155/2016/5894752

Extending WSN Lifetime with Cluster Head Election

Noroze Fatima, Danish Shehzad, Ali Imran, Ahsan, and M. Arif(✉)

Superior University, Lahore, Pakistan
{danish.shehzad,arif}@superior.edu.pk

Abstract. Several problems with wireless sensor networks exist now, including, energy efficiency (WSN). Since the sensor networks are battery-powered, they expire after a certain amount of time. Therefore, improving data dissipation in an energy-efficient manner will continue to be difficult in order to prolong the lifespan of sensor devices. The life duration of WSNs could be improved or extended using the clustering method, which has already been proven. In the clustering model, the cluster head selection (CH) in each cluster is considered as the efficient method for energy-efficient routing, which lowers transmission delay in WSN. The selection of the best CH that enables prompt network service was the key issue, similarly. Further study has been done so far on finding a solution to this problem that takes various requirements into consideration. This study makes an effort to create an optimal clustering model with the best CH selection by taking four key factors into account: energy, latency, distance, and security. In this article, we examine some basic concepts surrounding the clustering procedure in WSNs and give a comparison survey of several clustering procedures.

Keywords: Power efficient · wireless sensor networks · cluster heads · delay

1 Introduction

The sensors of a wireless sensor network are arranged in a sensor field to track and measure certain environmental traits and gather information about those events. The sensors are tiny devices with constrained battery life, memory, computational capacity, low data rates, limited processing bandwidth, and irregular network performance and other resources [1]. Despite their limitations, the sensors can provide us a fairly accurate picture of the field being detected when they are spread out widely.

1.1 Wireless Sensors Network

The wireless network sensors are wired and wireless networks were unable to cover the same geographic area as WSN. Once deployed in the field, they may be continuously watched after or may be left unattended in a variety of conditions [2]. The potential of the WSN will be used to offer effective and affordable solutions to a variety of issues. To deal with the sensor restrictions, it is required to put in place processes or practices.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 128–140, 2025.
https://doi.org/10.1007/978-3-031-77620-5_9

Using clustering techniques in WSN can help address some of those limitations by enabling the processes of the sensors, grouping them into clusters, and assigning specific responsibilities to the sensor in the clusters before transferring the information to higher levels.

Applications that need to scale the number of nodes to hundreds or thousands benefit most from clustering. In this context, scalability emphasizes the necessity for data aggregation, effective resource usage, and load balancing [1]. Additionally When communicating with the base station, a number of routing protocols have the potential to use clustering to create a hierarchical structure and lower the path cost (Fig. 1).

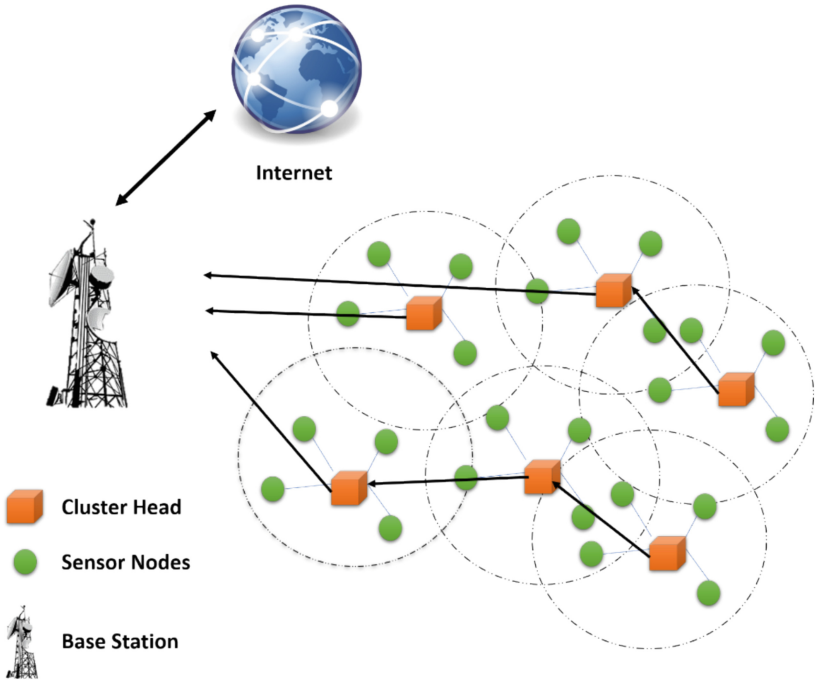


Fig. 1. Network architecture for wireless sensors

The three primary WSN components that can be divided when working with clusters are sensor nodes (SNs), base stations (BSs), and cluster heads (CH). To view the surroundings and gather data, the network's sensors, or SNs, are organized in a set. The primary responsibility of an SN in a sensor field is to recognize events, process nearby data right away, and then broadcast the outcomes. The three primary WSN components that can be divided when working with clusters are sensor nodes (SNs), base stations (BSs), and cluster heads (CH). To view the surroundings and gather data, the network's sensors, or SNs, are organized in a set. The primary responsibility of an SN in a sensor field is to recognize events, process nearby data right away, and then broadcast the outcomes. The BS is the location where data from the sensor nodes is processed before being made accessible to the end user. It is typically regarded as fixed and located a long

way from the sensor nodes. Between the SNs and the BS, the CH serves as a gateway. The cluster head's responsibility is to complete tasks that are common to all cluster nodes, like consolidating data before sending it to the BS [3]. While the BS acts as the sink for the cluster nodes, the CH acts as the sink for the cluster heads. By replicating the structure that was established between the sensor nodes, the sink, and the base station, the various layers of the hierarchical WSN are produced.

It is important to consider factors like cluster size and design, how to choose the cluster head, how to manage collisions between and within clusters, and energy-saving concerns while establishing a cluster. Due to the investigated efficiency of using a hierarchical communication strategy between the network piece show clustering works 'design is one of the most crucial challenges for the proper functioning of the WSN. We can distinguish three key stages in the clustering establishment process across all cluster-based protocols:

 Cluster head election; Cluster formation (set-up phase) Phase of data transmission.

Each of these stages can be implemented using a variety of strategies. One option is to employ Instead of employing a predetermined distribution of the SN and CH, a dynamic strategy was used for sensor placement and CH election (Fig. 2).

In various suggestions, the cluster heads are arranged in a hierarchy (Fig. 3) as done in (Bandyopadhyay & Coyle, 2003) and (Manjeshwar & Agarwal, 2001) to facilitate inter-cluster communication Multi-level hierarchies enable better energy allocation and overall energy use. Maintaining the hierarchy could be costly in large, dynamic networks where nodes disappear as soon as their energy supply runs out.

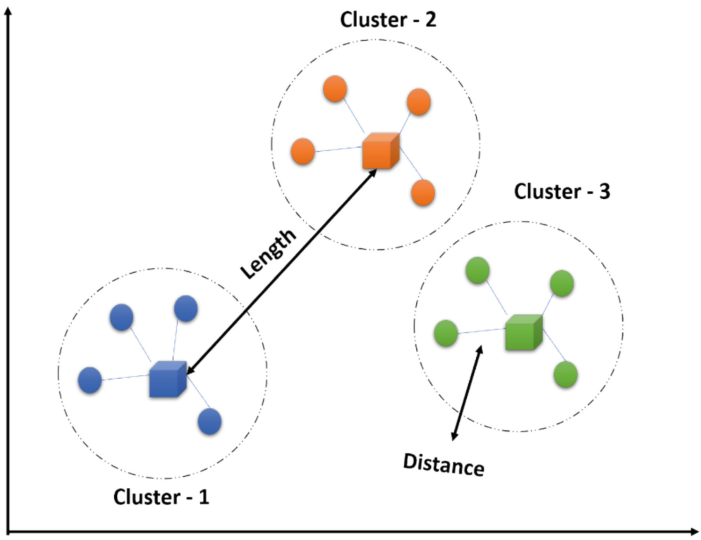


Fig. 2. Distance and length of cluster selections

One of the primary objectives of hierarchical organization in sensor networks is energy efficiency, which enables a longer network lifetime. A cluster head can combine and aggregate the data it receives before transmitting it to the base station. In extremely dense networks, it is possible to select a subset of nodes for low-power sleep mode operation without compromising connectivity or network coverage. An effective cluster head plan the states of its member nodes in this situation.

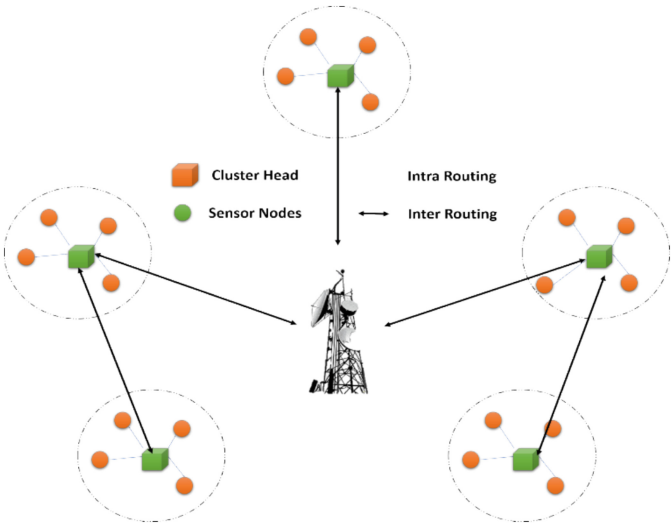


Fig. 3. Multi-hop inter-cluster communication

Furthermore, if a round-robin technique is a practice among the member nodes of the cluster, medium access collision can be avoided. Collisions may necessitate the retransmission of data by nodes, using up additional energy.

Balanced intra-cluster traffic leads to a severely skewed load distribution on cluster heads in terms of inter-cluster communication (Fig. 3). The farther the cluster head is from the base station, the more energy it uses, and the sooner it will expire in singlehop communication where cluster heads use direct connection to connect to the base station. Even if multi-hop inter-cluster communication is used, the so-called hot spot problem still exists since nodes adjacent to the base station have to deal with larger traffic loads. Many-to-one traffic theory that distinguishes WSN is to blame for this. Nodes close to a hot spot lose energy more quickly and die significantly more quickly than cluster heads farther away. This might cause significant connection (network partition).

Since LEACH is totally distributed, substantial network understanding is not required. Large area networks cannot use it since it creates a one-hop intra-cluster and inter-cluster topology. It is expected that cluster heads have a long communication range and can directly communicate with the sink. Due to the fact that the cluster heads are ordinary sensors and the sink is frequently positioned far away, this assumption is not always accurate. Additionally, the additional cost created by the ads phase at the start of each round by dynamic clustering may reduce the energy gain. LEACH cluster head

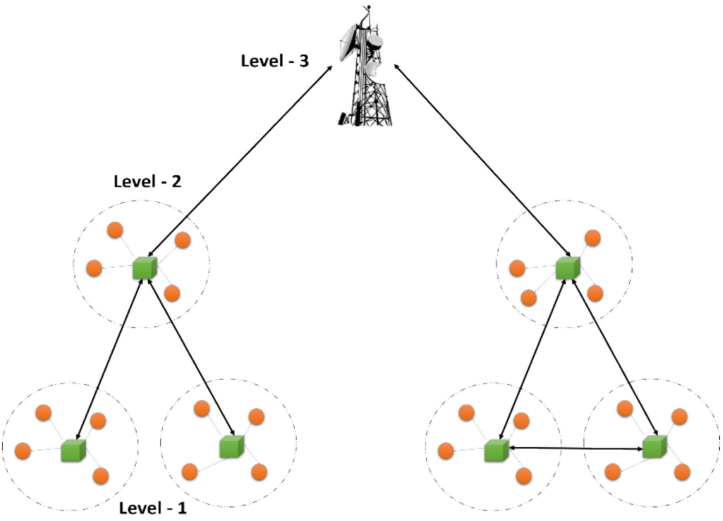


Fig. 4. Three level hierarchy of cluster head with base station

rotation assumes a homogeneous network and is unable to guarantee actual loadbalancing in the case of nodes with varied initial amounts of energy since the choice to elect a cluster head is probabilistic and does not take energy taken into consideration. A node with extremely low energy will prematurely perish after serving as the cluster head nodes with higher energy for the same number of rounds. This can have an impact on connectivity and network coverage (Fig. 4).

2 Literature Review

Various clustering procedures were compared in a survey by Arboleda et al. [1]. The survey's authors briefly studied WSNs' proactive and reactive algorithms, LEACHbased protocols, as well as some fundamental clustering concepts like cluster structure, cluster kinds, and clustering advantages. The key differences between these protocols were evaluated, and examples of contemporary applications for them were provided.

The currently employed clustering methods for WSNs were reviewed. by Kumarawadu et al. [4] And categorized according to the cluster formation characteristics and CH election criteria. According the authors of the survey looked at the major design challenges and discussed performance issues related to clustering protocols in addition to classifying identity-based clustering algorithms, neighborhood information-based clustering algorithms, probabilistic clustering algorithms, and biologically inspired clustering algorithms (Table 1).

Deosarkar et al. [5] Focuses on analyzing different clustering schemes' CH selection processes using the categories of deterministic scheme, adaptive scheme, and mixed metric scheme. The costs of CH selection were examined for cluster formation, CH distribution, and cluster creation. The need for a clustering technique that is more reliable, expandable, and energy-efficient for data collection in WSNs was also raised.

Table 1. Cluster head selection techniques and limitations

Protocols	Features	Limitations
MEACM	superior performance by reducing the sensor node's energy usage increases the number of dead sensor nodes, throughput, and network lifetime	Simulation is preferred to real-time experiments. Requires that the scalability of sensor nodes within each cluster be taken into account
ACOPSO	a smaller packet size increases the network's lifespan effective energy conservation	Defining the basic design parameters is crucial cannot specify the scattering difficulties
DCT- CDA	increases network lifetime boosts the stability of the network	Security must be taken into account
GWO	improved network throughput and lifespan energy usage made simple	Uncertain acquisition procedure MAC and network layer consideration must be combined
WOA-C	increases network longevity Improving scalability	Network performance should be enhanced. There is no consensus on the properties of Cluster Heads
GECR	improved network lifecycle optimum use of energy	The focus of upcoming research is on validating and utilizing the proper metaheuristic algorithms. It is unclear which option is best
Load balanceing protocol	enhanced network throughput, stability, and packet drop rate	Consideration should be given to energy harvesting schemes, and network longevity needs to be further improved
RE attempt	improved network throughput and lifespan energy usage made simple	Plans to concentrate on crosslayer design procedures MAC and network layer consideration must be combined
K-means	maximum output reduction in energy consumption	Finding the ideal solution in a fair amount of time is challenging
FCM	Maximizes energy	Information loss is a possibility
DBSCAN	According to belong-to, do not belong to, and ambiguity, it classified the cluster. Become more energy efficient	Less limitations are taken into account
LEACH	It gauges how long the sensor nodes will last. Reduce inter-cluster distance	The importance of packet routing

Jiang et al. [6] Presented a classification of the three primary benefits of clustering approaches for WSNs, including greater scalability, lower overheads, and easier maintenance. Using a total of eight clustering attributes, WSN clustering techniques. Additionally, the authors examined six well-known WSN clustering methods, including LEACH, PEGASIS, HEED, EEUC, and etc., as well as numerous features, and compared these WSN clustering techniques.

In the survey described in [7] the workings of different clustering protocols were discussed, and the advantages and disadvantages of each of these approaches were summarized. There are only seven popular clustering algorithms for WSNs, such as LEACH, TL-LEACH, EECS, TEEN, and APTEEN. [8]were chosen by the survey's authors. The survey also contrasted the energy usage and network longevity of these clustering techniques.

Boyinbode et al. [7]. Published a survey on WSN clustering methods. After exploring the major challenges for clustering algorithms, nine well-known clustering algorithms for WSNs, including LEACH, TL-LEACH, EECS, HEED, and EEUC, were briefly summarized in the survey. The authors further contrasted various clustering techniques based on variables such as residual energy, uniformity of CH distribution, cluster size, delay, hop distance, and cluster generation methods.

In [9], the parameters utilized for CH selection, the presence of a centralized control during clustering, and hops between nodes and CH in intra-cluster communication are simply three simple categorization criteria that the authors used to define the clustering architecture in WSNs [10]. The survey also emphasized the difficulties associated with clustering WSNs and briefly described a few clustering routing strategies.

Reduced frequent remote transmission is important to increase network lifetime due to the limited energy of the sensor nodes [11]. Therefore, direct contact between nodes and base stations is discouraged. The network nodes can be organised into a number of clusters, and each cluster can choose a cluster head who is in responsible of transmitting data from the entire cluster to the base station. In order to save energy, just a few number of nodes are needed to transmit data over long distances, and other nodes will handle short-distance transmission.

We provide an enhanced LEACH-based inter-cluster multi-hop routing mechanism. in [12]. Remaining energy and the distance between the node and the base station are assumed to have an impact on the threshold function of cluster head election, and the multi-hop routing transmission technique is employed for inter-cluster communication [13, 14]. Proposes a distributed unbalanced clustering routing method for WSNs. The time broadcast method chooses the cluster heads, and the cluster head can transmit data to the base station in line with social welfare to reduce the quantity of control message exchange. Function. In [15] In order to limit the amount of data transmitted by the node, the compressed sensing method is created. The redundant data is then reduced using data gathered from the cluster head. A multi-level heterogeneous network topology control algorithm is created using a technique for creating a reverse connected dominating set tree. In [16] to improve the network topology. Two different types of cluster head election probability are proposed to build bio-level heterogeneous clusters in wireless sensor networks (WSNs) in [17], which presents a stable election procedure for clustered heterogeneous wireless sensor networks (SEP) [18]. It can delay the initial node's demise;

however, it is not applicable in a heterogeneous WSN system. For heterogeneous networks, a distributed clustering algorithm is put forth in [19]. Since each sensor's initial energy varies, the competition among nodes for the position of cluster head is diverse. Additionally, the likelihood will change when a node's residual energy changes over time.

3 Proposed Solution

Data collection requires the use of a routing system that is energy-efficient. The significance and capacities of each sensor node are identical. This highlights the necessity to increase the sensor nodes' and the sensor network's lifetime. The PE-LEACH Protocol's stated goals are to decrease energy usage and improve network lifespans. The Gaussian distribution model in this case effectively covers the sensor network region. In addition,

Fig. 5. Proposed technique for cluster head selection

node aggregation makes use of the conditional probability theorem. Figure 2 illustrates the PE-LEACH Protocol's flow. Assume there is a base station and N nodes in a sensor network. Over a region, BS is split up. Both the base station's location and the sensor nodes' positions are known in advance. Let's have a look at a 2D network (Fig. 5).

Cluster formation in sensor networks is strongly influenced by the latency to receive a neighbor node message and the remaining energy. The process is divided into rounds, with each round beginning with the search for the optimum CH. How the cluster is formed is determined by the following processes.

3.1 Step 1: Initialization and Information Retrieval About Neighbors

The neighbor node information is found by broadcasting beacon signals throughout the network [20, 21]. First, we must specify the region we want to include in our clustering. Define two numbers, xa and xb, for the area determination, where xa and xb are $ 0, 1, 2, 3, etc. and xa and xb initially equal 0. In the finite range, there are n nodes total, but there is initially no lovely node. Every node has an energy of Eo, and a data package has a size of k. The data will be sent for sorting following the initialization process [22].

3.2 Step 2: Implement a Sorting Algorithm

The sorting approach is applied to get a list of all data package (k) within a certain hop distance. Ordered in decreasing priority is the list. [23]. The weight (w) is calculated of nodes in the finite filed and bases on the plot graph and their positions. The weight will be calculated as

$$Weight = (x - node(1) \cdot x)^2 + (y - node(1) \cdot y)^2$$

The coordinates of that node are represented by x and y in the above equation, and (I) represents the energy of the system with many sensor nodes [24].

3.3 Step 3: Candidate for Cluster

When a node's two-hop neighbor is not enclosed, examine each stage 2 member individually and select any one of them as a candidate for the cluster [25, 26]. These simplifications form the basis of the computations: Assume that there is a lengthy intra cluster transmission stage. Since inter cluster transmission is long enough and all data nodes can send data to their CH, all CH with data can transfer their data to the BS [27]. The suggested PE-LEACH Protocol's Fig. 2 Flow and data aggregation must be carried out by the CH. There we have three cluster head selection techniques. The weight (w) determines the cluster head based on the Light(l) and the distance(d) in the finite field [28]. The random clustering performs in the first stage and determine the cluster head randomly then every other node wait for the approval to join the sink.

$$E_o > E_{present}$$

The system waits for the ever node to join and then the cluster selection process complete. Finally, the sorting procedure is carried out using the adjacent nodes' remaining energy [29] (Fig. 6).

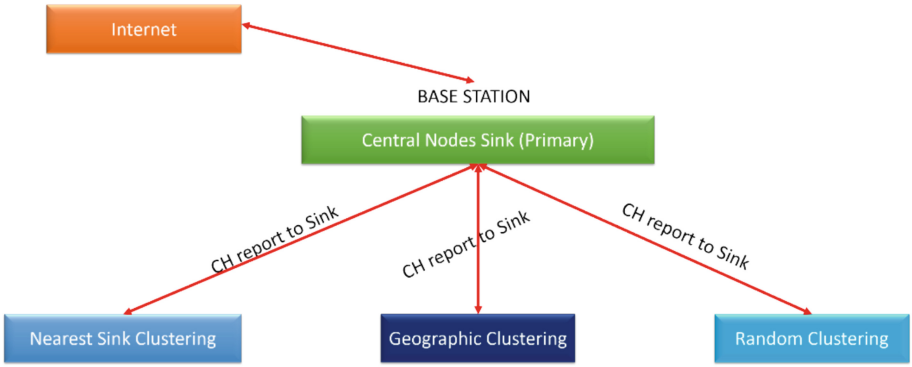


Fig. 6. Cluster head selection techniques

4 Results and Discussion

The proposed method has been implemented using MATLAB, and the outcomes have been contrasted with those of the protocols CRPD, LEACH, and MODLEACH. In comparison to CRPD, the adoption of EEMCS has improved energy utilization by 20–30%, and it is more stable than LEACH and MODLEACH in large-scale networks. Furthermore, the network lifetime of CRPD [30], MODLEACH, and LEACH is 62%, 58%, and 46%, respectively, compared to 77% for EEMCS on 150 nodes in a 50 50 m^2 region? Due to EEMCS's dynamic nature and very low energy consumption, nodes can remain in the network for a longer time [31]. In every situation, EEMCS has a higher throughput than the current protocols.

4.1 Advantages of a Strong CH Election

The selection of CH nodes in sensor networks can provide the following three benefits: Increasing the networks' longevity Heterogeneous networks are used [32].

1. **Data transmission.** Typically consumes a lot less energy than transmission in homogenous networks from the sensor node to the BS.
2. **Enhancing data.** It is commonly known that links typically have low forwarding reliability. With each hop, the packet delivery rate is significantly decreased.
3. **Decreasing latency.** Computational heterogeneity can reduce the latency in nearby nodes for data transmission.

4.2 Data Gathering Using Data Ensemble

When a cluster of nodes is replaced by a single node, the joint deployment of the network is not altered [33]. During node aggregation, the data ensemble process also takes place. It's essential to locate the macro node for data aggregation. The process now consists of two steps (Fig. 7):

- Path definition
- Pair of combinable nodes

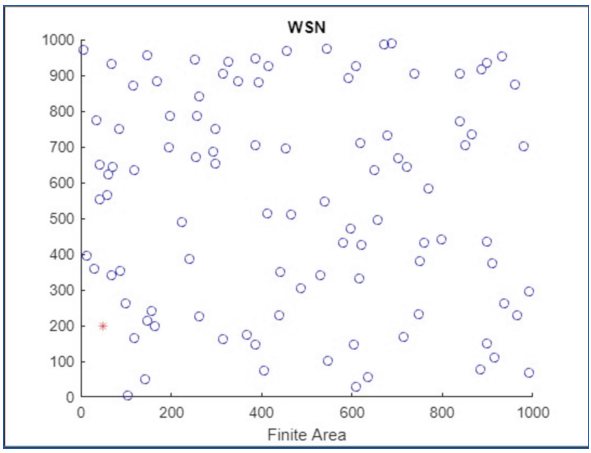


Fig. 7. Clusters in wireless sensor network

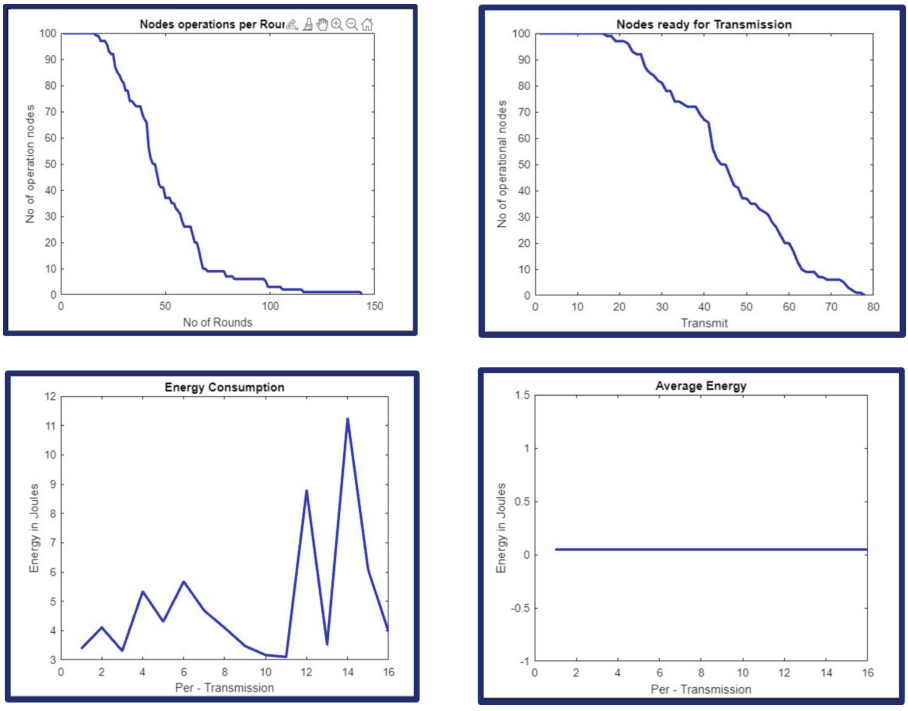


Fig. 8. Operations to perform rounds for transmission and energy

4.3 Power Efficient Data Routing

After gathering the data from various clusters, the CHs must give it to the BS [7]. The forwarding nodes are thus selected based on the nodes with the highest residual energy (Fig. 8).

5 Conclusion

An energy-efficient routing mechanism must be used for data collection each sensor node serves the same function and has the same skills. This highlights the necessity to increase the sensor nodes' and the sensor network's lifespan. The PE-LEACH Protocol's goals are to cut down on energy use and increase network lifespans. Here, the sensing network region is effectively covered by the Gaussian distribution model. In addition, the conditional probability theorem is used in node aggregation.

References

1. Arboleda, L.M.C., Nasser, N.: Comparison of clustering algorithms. IEEE, p. 6 (2006)
2. A. E. J. M. L. a. A. S. D. J. Dechene: A Survey of Clustering Algorithms for Wireless, p. 10 (2005). https://uwo.ca/
3. Goel, P., Goyal, E.A.:Clustering in Wireless Sensor Networks: Survey. IJARIIE-ISSN(O), p. 5 (2017)
4. Behera, T.M. Mohapatra, S.K., Samal, U.C., Khan, M.S., Daneshmand, M., Gandomi, A.H.: Residual Energy Based Cluster-head Selection. IEEE, p. 8 (2019)
5. Konde, S., Deosarkar, S.: IOT based WSN. In: ICCIP, p. 11 (2020)
6. Jiang, C., Yuan, D., Zhao, Y.: Towards Clustering Algorithms in Wireless Sensor. IEEE, p. 6 (2009)
7. Udit Sajjanhar, P.M.: Distributive Energy Efficient Adaptive Clustering Protocol for Wireless Sensor, p. 5. IEEE (2007)
8. Su, S., Zhao, S.: An optimal clustering mechanism based on FuzzyC. In: suscom, p. 17 (2017)
9. Xu, D., Gao, J.: Comparison Study to Hierarchical Routing Protocols, p. 6. Elsevier (2011)
10. Wu, W., Xiong, N., Wu, C.: Improved clustering algorithm WSN, p. 7. In: IET (2017)
11. Liu, X.: A survey on clustering routing protocols, p. 41. In: mdpi (2012)
12. Hu, J., Jin, Y., Dou, L:: a time-based cluster-head selection algorithm for LEACH, p. 5. IEEE (2008)
13. Yang, H.. Sikdar, B.: Optimal Cluster Head Selection in the LEACH Architecture, p. 8. IEEE (2007)
14. A. E. J. i. M. L. A. S. D. J. Dechene: A Survey of Clustering Algorithms for WSN, p. 9. In: UWO.ca (2015)
15. Haque, M., Ahmad, T., Imran, M.: Review of Hierarchical Routing Protocols, p. 10. Springer (2018)
16. Maimour, M., Zeghilet, H., Lepage, F.: Cluster-based Routing Protocols for Energy, p. 24. Intechopen (2009)
17. Katiyar, V., Chand, N., Soni, S.: Clustering algorithms for heterogeneous wireless sensor network: a survey. Int. J. Appl. Eng. Res. **2**, 745–754 (2010)
18. Behera, T.M., Mohapatra, S.K., Samal, U.C., Khan, M.S., Daneshmand, M., Gandomi. A.H.: Residual Energy Based Cluster-head Selection, p. 8. IEEE (2019)

19. Saini, N., Singh, J.: A Survey: Hierarchal Routing Protocol in Wireless Sensor, p. 8. ISSN (2014)
20. Jia, D., Zhu, H., Zou, S., Hu, P.: Dynamic cluster head selection method for wireless sensor, p. 9. IEEE (2015)
21. Singh, B., Lobiyal, D.K.: Energy-aware cluster head selection using packet retransmission in WSN. Elsevier, p. 6 (2012)
22. Sang, S.M., Kang, H.: Distance Based Thresholds for CH in WSN. IEEE, p. 4 (2012)
23. Arumugam, G.S., Ponnuchamy, T.: EE-LEACH: development of energy-efficient LEACH Protocol for data gathering in WSN. J. Wireless Com. Network **2015**, 76 (2015)
24. Xiu-wu, Y.U., Hao, Y.U., Yong, L., Xiao, R.: A clustering routing algorithm based on heterogeneous algorithm. Elsevier, p. 10 (2020)
25. Liang, Y., Yu, H.: Energy adaptive cluster-head selection for wireless sensor networks, p. 5. IEEE (2005)
26. Latiff, N.M.A., Tsimenidis, C.C., Sharif, B.S.: Energy-aware clustering for wireless sensor networks, p. 5. IEEE (2018)
27. Xiangning, F., Yulin, S.: Improvement on LEACH protocol of wireless sensor network, p. 5. IEEE (2007)
28. Liu, X., Wu, J.: A method for energy balance and data transmission. In: MDPI, p. 14 (2019)
29. Yong, Z., Pei, Q.: A energy-efficient clustering routing algorithm. Elsevier, p. 7 (2012)
30. Yin, Y., Shi, J., Li, Y., Zhang, P.: Cluster head selection using analytical hierarchy process, p. 5. IEEE (2017)
31. Thein, M.C.M., Thein, T.: An Energy Efficient Cluster-Head Selection for Wireless Sensor Networks, p. 5. IEEE (2010)
32. Zeng, M., Huang, X., Zheng, B., Fan, X.-X.: A heterogeneous energy wireless sensor network, p. 12. Hindawi (2019)
33. Behera, T.M., Samal, U.C., Mohapatra, S.K.: Energy-efficient modified LEACH protocol, p. 6. IETDL (2018)
34. Boyinbode, O., Le, H., Mbogho, A., Takizawa, M., Poliah, R.: A survey on clustering algorithms for wireless sensor networks. In: NBiS, p. 7 (2010)

Automatic HTP Assessment for Schizophrenic Patients Using Machine Learning

Muhammad Zubair, Samra Kyinat, and Sohail Masood(✉)

Superior University Lahore, Lahore, Pakistan
sohailmasood@superior.edu.pk

Abstract. The present study aimed at automated personality of schizophrenic patient by using House Tree Person technique. In order to do the assessment, the sample of 70 schizophrenic indoor patients was selected through purposive sampling technique (N = 70). HTP was administer in order to gather data on the personality characteristic of schizophrenic patients. Then HTP was manually interpreted in order to train the model about the features of the drawing in HTP and the interpretation of the drawing as well as considering post interrogative questions. After that the data on HTP was entered with the help of feature extraction technique and available output was used in order to train the model for automatic assessment of the personality. In this way the specific personality characteristics were identified on the basis of categories of the vulnerability and existence of the disorder i.e. severity of the problem.

Keywords: Machine learning · Personality · Assessment · House · Tree · Person

1 Introduction

Automated machine learning is defined as the automated ML or auto ML. It is the method of computerizing the time-consuming, iterative tasks of machine learning model progression. It permits data scientists, analysts, and developers to build ML models with high scale, efficiency, and productivity all while supporting model's quality. Machine learning is a subfield of artificial intelligence (AI) [1].

The aim of machine learning usually is to recognize the arrangement, construction and structure of data and fit that data into models that can be easily understood and utilized by people. Although ML is a field of computer science but it is somehow different from ordinary computational approaches [2].

Machine learning has achieved progress in the field of medical and mental health. Barbara Engelhardt, a computer scientist at Princeton University worked in the field of medicine, was developing statistical tools that look for out expected natural patterns in order to plot out the genome's real [3]. The other achievement of machine learning technology is being used to determine the mass and site of crater impacts on the moon [4].

As disused the progress of machine learning, it can also be applicable in the field of mind sciences and also in psychology or clinical psychology. The increasing number

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 141–148, 2025.
https://doi.org/10.1007/978-3-031-77620-5_10

of advancement in the role of technology in the assessment of human behaviors and personality raised several question about how to analyze and interpret results that are got from the assessment [5].

In the field of clinical psychology the psychologist focuses on assessment and treatment of mental health problems. Personality assessment is the important modality of assessment. Personality assessment is the measurement of personal qualities and characteristics that render person life in a scale [6]. Personality assessment can be done through projective and objective techniques. House Tree Person was the projective technique developed by John Buck in 1947 and then revised in 1948, 1949 and then 1992.It was originally developed as outgrowth of good enough scale* used to access the intellectual functioning [3].

HTP was designed to aid mental health professionals in getting information regarding individual's sensitivity, maturity, flexibility, efficacy and degree of personality integration. The purpose of developing the concept of HTP was the idea that creativity represents a stream of flow onto graphic art [7].

HTP is used with combination with other projective measurement tools usually given first as ice berg. HTP was developed for the individuals above 3 years of age and at the time of development it was created for non-English in order to get respond in to an ambiguous stimulus [3].

Although people have unique personality traits and characteristics that make them differ to each other but there are also group of people who can share somehow similar characteristics, so these certain characteristics are key point on which one can get information that these people have specific problem in their lives. Same is the true with schizophrenic patients [6].

Schizophrenia is a psychotic disorder in which individual lost contact with reality and also had poor orientation. Schizophrenia is a serious mental illness. It is the chronic mental illness that affects the way person thinks, feel and, behave. The patients with schizophrenia experience hallucination, delusions and disorganize speech and behavior. The hallucination is the sensory experience of something having that is not actually present in real situation and it is only experienced by the patient e.g. seeing things or persons, hearing voices etc. The delusions are the false and firm believes that are difficult to shatter e.g. someone will give me poison, someone is in love with me, I am prophet etc. HTP is the important technique give us information about detail personality characteristics of schizophrenic patients [7].

The interpretation of the HTP techniques is subjective analysis of the drawing in order to get information about the individuals personality. This test is used by clinical psychologist, occupational therapist counselling psychologist with adherence of multiple personality tests series and intelligence tests [8].

In the process of test administration, the examinee is instructed to draw house, tree and person as accurately as possible the separate side or separate sheet of paper. Alog with making a drawing z a series of questions are asked to the examinee. These questions are called post interrogative questions. In the present study the schizophrenic patients were instructed to draw HTP and then post interrogative questions are asked.

2 Methodology

The study was based on deep learning model. The study was conducted to measure the personality of schizophrenics by using House Tree Person technique based on deep learning strategy. The study was attempted in order to assess personality characteristics that schizophrenic patients were having.In order to do so HTP was administered to the patients and the data was converted in form of machine learning.

2.1 House Tree Person Technique

House tree person technique commonly known as HTP was personality assessment tool based on assessment of House tree and person drawing [9]. It was developed by Buck and used to identify hidden personality characteristics and needs of individual. House tree person technique was also useful in identification of schizophrenic patients [10]. The usefulness of the test was said to because of drawing is the powerful medium to identify emotions [11]. The study was based on deep learning model. The study was conducted to measure the personality of schizophrenics by using House Tree Person technique based on deep learning strategy. The study was attempted in order to assess personality characteristics that schizophrenic patients were having.In order to do so HTP was administered to the patients and the data was converted in form of machine learning.

2.2 Sample

For the purpose of data collection, the samples of 70 indoor schizophrenic patients between the ages of 20 to 60 years were selected through purposive sampling technique. In order to collect data for the study, the sample was selected from males and female wards of Fountain House Lahore. HTP, a projective test of personality measurement was used.

2.3 Procedure

In order to carrying out research Sample of 70 indoor schizophrenic patients between the ages of 20 to 60 years were selected. The sample included 35 males and 35 female patients. The sample was selected through purposive sampling technique. In order to collect data for the study, the sample was selected from males and female wards of Fountain House Lahore. Formal permission was taken from concerned authorities of Fountain House Lahore. After taking permission from authority researcher approached to patients and informed consent was taken. Patients were given paper and pencils and asked to draw a picture of a House, A tree and a Person. Along with this patient's demographics were also used. After getting manual pictures designed by HTP, data was stored by making mobile application. In concerned mobile application developed for the purpose of data entry and analysis there were three sheets were available and after entering demographic information the clinical practitioners entered all the responses that got from the picture. It was done and entered according to pre made categories about picture. For example, size of the house, if this is cloudy tree, the gender of the person in

drawing etc. Then data taken from the patients (males, females) was entered separately on the basis of requirement of the drawing of house, tree and person based on data base. At after entering the data, the model would be trained by using existing data to analyze the further drawings of HTP by diverse population of schizophrenia (Tables 1, 2, 3 and 4).

Table 1 .

Client Information				House							
id	Name	age	gender	h_size	h_lines	h_roof	h_windows_doors	h_chimney_smoke	h_pathways	h_shading	h_house_shape
1	Sohail Basit	49	Male	2	3	3	2	2	3	1	1
2	Kashif	42	Male	1	2	3	2	2	3	1	1
3	Zahid mehmood	46	Male	1	2	2	3	2	3	1	2
4	Basit	30	Male	1	3	1	1	2	3	1	1
5	Majid Saleem	30	Male	1	3	2	3	2	3	2	3
6	Mohadisa	31	Female	2	1	2	1	2	2	1	1
7	Rana Imtiaz	56	Male	1	2	1	2	2	2	1	1

Table 2 .

Person											
p_size	p_head	p_hair	p_eyes	p_nose	p_ears	p_mouth	p_teeth	p_arms	p_legs_and_feet	p_shading	p_insufficient_
1	2	4	4	1	1	3	2	1	1	1	2
1	4	4	4	1	1	3	1	2	3	2	1
3	4	4	4	2	2	3	1	1	1	2	2
2	3	4	5	1	2	1	1	6	1	1	1
2	4	4	5	1	3	2	1	2	1	1	2
2	1	4	4	1	1	1	1	2	1	2	1
1	1	4	4	1	1	4	1	2	3	1	1

Table 3 .

Tree						
t_branches	t_age_of_tree	t_trunk	t_leaves	t_roots	t_shading	t_tree_type
8	1	1	3	1	1	1
2	1	1	3	3	1	1
7	1	1	3	1	1	1
3	1	1	1	3	1	1
1	1	4	1	3	2	1
8	1	1	1	3	1	1
7	1	6	3	3	1	1

Table 4 .

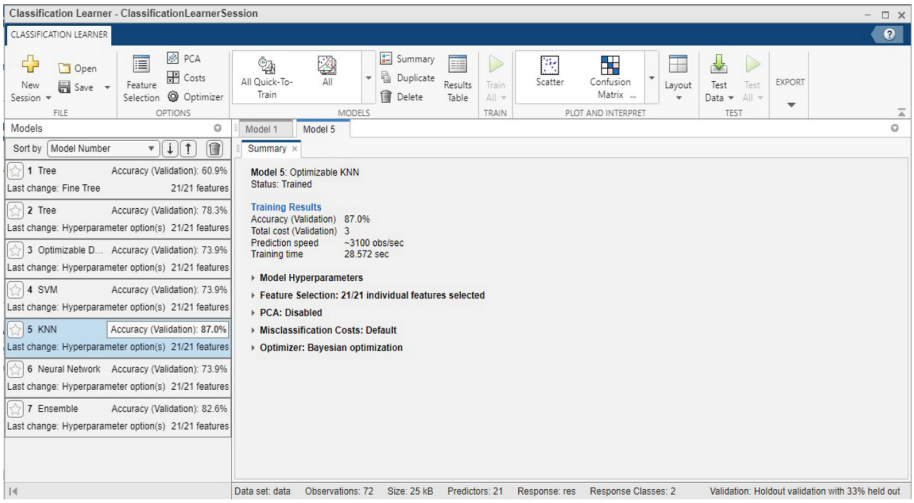
Assessment
Psychological Etiology of Schizophrenia
Schizophrenic Personality
Schizophrenic Personality
Schizophrenic Personality
Schizophrenic Personality
Schizophrenic Personality
Pronness to schizophrenia
Schizophrenic Personality

3 Results and Discussion

The present study aimed at automatic personality assessment of schizophrenic individuals using House Tree Person technique. House Tree Person technique is a personality measure that purports to measure the hidden characteristics of someone. Different aspects of personality are measured through this projective technique. In the process of HTP administration the test taker is asked to draw the picture of a Houser Tree and a person. Interpretation of drawings of house tree and person provide information about someone's cognitive emotional and social functioning. Initially the interpretation was done manually so in next steps the model would be trained on the basis of pilot study data. After manually interpreted, the researcher has done the development of android application in order to enter the input data that was gotten from the sample of the patient. The reason behind the development of application was to enter the features of HTP in the application.

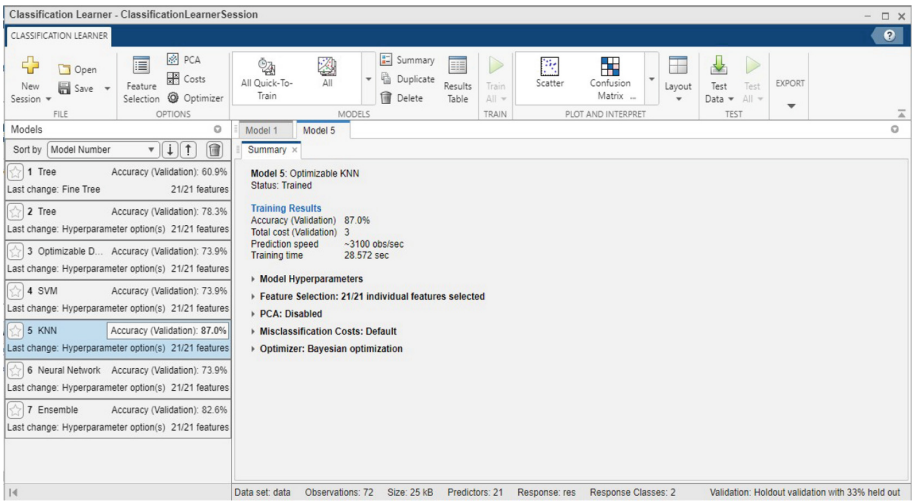
Following tables are shown in the result section.

Load data.csv in MATLAB and apply different classifiers and compare results.



The first objective of the study to assess the personality of schizophrenic patients through HTP. Basically HTP used to assess the personality characteristics of individual but researcher selected the sample of schizophrenic patients through purposive sampling technique in general population the personality tool application would be difficult due to limited time given to research slot and it will be difficult to apply the HTP and train the model (machine learning) for general population. For above explained reasons the researcher used harmonious sample of schizophrenic patients so in shorter period of time the machine would be trained to automatic interpretation of personality of on standardized sample. HTP was administered to schizophrenic patients equally divided in males and females. The researcher after proper training of HTP administration, administered the HTP on schizophrenic patients. Informed consent was formally taken by the institute from which data was collected. After successful administration of personality measure and the co researcher (trained clinical psychologist) interpreted the HTP with the help of standardized manual. Initially the interpretation was done manually so in next steps the model would be trained on the basis of pilot study data. After manually interpreted, the researcher has done the development of android application in order to enter the input data that was gotten from the sample of the patient. The reason behind the development of application was to enter the features of HTP in the application.

Load data.csv in MATLAB and apply different classifiers and compare results.



Choose best 2 classifiers KNN with Accuracy (Validation): **87.0%** and Ensemble with Accuracy (Validation): **82.6%**

4 Implication of the Study

The present study is the great contribution in the field of machine learning as well as in the field of clinical psychology. The present trained model would be helpful for fresh clinical psychologists and for who did not get proper training in the interpretation of HTP in order to assess accurately personality assessment of schizophrenics. In order to use goal-oriented treatment approach to schizophrenics, psychologists would get better understanding and interpretation on individual.

5 Limitation of the Study

- The sample was suboptimal in size and diversity due to short time span and logistic limitations.
- Due to short time span, model could be not trained on the data of general population so comparison of normal population and schizophrenics could not be made.
- The researcher could approach specific and limited population so many of the features of HTP characteristic were being ignored.
- There are many cultural variations in test were difficult to incorporate due to specific sample.

6 Recommendations

- The sample should be expanded to general population so findings would be generalizable to general population.
- The post interrogative questions should be also considered in future projects regarding automatic HTP assessment

References

1. What is automated machine learning (2012). retrieved from http.ibm.com
2. Pedamker, P.: Types of machine learning retrieved from Machine Learning Methods | Types of Classification in Machine Learning (educba.com) (n.d).
3. Wani, J., et al.: Machine learning and deep learning based computational techniques in automatic agricultural diseases detection: methodologies, applications, and challenges. Archiv. Comput. Methods Eng. (2021). https://doi.org/10.1007/s11831-021-09588-5
4. House tree person:A personality technique (2016). House, Tree, Person (HTP): A Personality Test – Exploring your mind
5. Theoder, T.: House tree person personality test retrieved from The House-Person-Tree Personality Test – Practical Psychology (practicalpie.com) (2022)
6. Lutkevich, B.: automated machine learning (AutoML) (2022). https://www.techtarget.com/
7. Khan, W., et al.: Deception in the eyes of deceiver: a computer vision and machine learning based automated deception detection. J. elseviori. Expert Syst. Appl. (2021)
8. Stachl, C.: Personality research and assessment in the era of machine learning European. J. Personal. **34**, 613–631 (2020). https://doi.org/10.1002/per.2257
9. Bhatti, I.: Interpretation of House Tree Person.International Islamic university, Islamabad (n.d)
10. Sarason, G.: personality assessment (n.d). https://www.britannica.com/science/personality-assessment
11. Stricker, G.: Projective Methods in Psychology (2001). https://www.sciencedirect.com

Deep-Learning Based Multi-Modalities Fusion for the Detection of Brain-Related Diseases: A Review

Syed Muhammad Ali Imran(✉), Muhammad Arif, Arfan Jaffar, Hafiz Muhammad Tayyab Khushi, and Abida Hussain

Faculty of CS&IT, Superior University, Lahore 54000, Pakistan
phcs-s21-006@superior.edu.pk

Abstract. Accidental brain injuries are the major cause of haemorrhages, which can be difficult to detect due to the similar intensity and disorientation of brain-related diseases like haemorrhages. Computer-assisted disease diagnosis (CAD) has the potential to detect and identify brain-related diseases. Computed tomography and magnetic resonant imaging-like modalities are sensitive to haemorrhage detection, and a novel study has revealed complexity in the modulation of vascular and bone haemorrhage. Because of the vast amount of medical images generated each day, the discipline of medical imaging is focused on inventing equipment to aid medical professionals. Because of distortions and extraneous information, brain imaging might be difficult to diagnose bleeding spots in the brain haemorrhage. A deep learning strategy under AI that can efficiently diagnose and detect brain-related diseases with multi-modality fusion, as opposed to the traditional method, which is tedious and time-consuming. The analysis of brain hemorrhage using DL is indispensable to help medical professionals address these illnesses. These concerns must be identified for medical diagnosis, treatment, and research. This paper describes the previously published review papers in brain-related disease diagnosis, AI approaches, multi- modality, challenges, and future work.

Keywords: Brain Diseases · Multi-modality Fusion · Image Segmentation

1 Introduction

Now day's research in medical imaging is drawing the attention of researchers to develop a device that can assist medical professionals because large numbers of medical images are being generated every day in different cases. In addition, due to the process of imaging and use of different devices, there are high chances of getting distortions and unwanted information. As a result, it is hard to analyze and observe tiny important information in the images to diagnose the hemorrhage. Therefore, this paper focuses on developing new approaches for analyzing Brain images by identifying bleeding and calcification in brain images. The study on the identification of calcification and Brain Hemorrhage is useful for several real-world applications, such as medical diagnosis, treatment, research, and

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 149–170, 2025.
https://doi.org/10.1007/978-3-031-77620-5_11

education. In addition, the automatic extraction of vital information that represents real causes from images facilitates physicians to diagnose specific abnormalities or diseases [1] caused by risks and accidents. A CT scan image of a brain blood clot, calcification, and haemorrhage is shown in Fig. 1.

Automobile accidents tremendously influence daily life, resulting in head traumas such as skull fractures and brain damage, among other things. Many people disregard safety standards. For example, riding a motorbike without a helmet. The machine learning applications in brain haemorrhage research are particularly difficult since it requires the acquisition of patient data from computed tomography (CT) scan pictures [2]. Every year, roughly seven million people worldwide encounter brain injuries as a result of car accidents, falls, attacks, brain disorders, or blood vessel bursting. Out of those, accident is the main cause of Brain injuries, especially in big cities. This is because of overwhelming vehicles driving on roads at high speed; heavy traffic due to congested roads may cause some accidents. This results in brain damage which may press the soft tissues against the bone of the hard skull. Therefore, blood bleeding from nerves may pour into the brain area. This causes swelling and inflation which in turn affect other parts of the brain. The basic problem is identifying hemorrhage having the same intensity and it may create confusion in diagnosing. Haemorrhage bleeding shows bright spots on the CT scan images, creating intra- observer variability in results. Due to the frequent use of brain CT and similar imaging patterns, it may be overlooked or confused with intra-axial or extra-axial hemorrhages. Computed tomography is very sensitive for the localization and detection of intracranial calcification [3]. Recent research has revealed an unanticipated level of intricacy in the regulation of vascular and bone haemorrhage.

There is another issue of blood clot detection before hemorrhage. The ability to perceive the shape of hemorrhagic blood clots on brain CT images is dependent on basic characteristics like density, volume, location, and interactions with the adjacent tissues, as well as technical parameters like scanning angles, slice thickness, intensity and homogeneity, irregular borders, and most severe tissue contrast, among others, which can cause significant difficulties in identification from brain CT scans. [4]. Different tissues, depending on their grey level, can provide a plethora of information to help clinicians make medical diagnoses if processed properly [5]. In summary, there is a necessity to analyses Brain Hemorrhage to help medical professionals some extent to solve the above-mentioned issues.

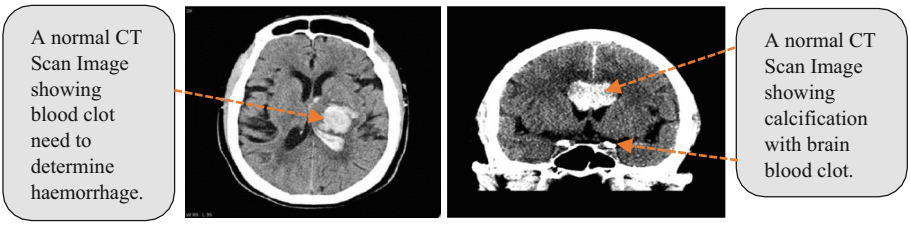


Fig. 1. A CT scan image of a brain blood clot showing calcification and haemorrhage.

Hence, this paper reviews some previous research focusing on analyzing and identifying Brain Hemorrhage. There are many diseases due to brain hemorrhage that are given below. (1) Stroke, is a type of disease that occurs due to loss of brain sensation when there is no proper blood supply to the brain [4]. (2) Brain disorders, is kind of disorder due to disability of the brain. (3) Calcification, a type of disease that develops as a result of calcium salt deposition in deteriorated necrotic tissue and in local lesions, foreign substances or an increase in calcified substances may be present. There is calcium, phosphorus, silicon, potassium, magnesium, and zinc. Apart from these three main diseases, we can also see noise introduced by the CT scanning and hard bone while scanning that are: (4) Streaks artifacts, which may exist due to hard material like bone while scanning, such as noise, unwanted information, etc. (5) Low contrast, which may exist due to poor quality machine or aged machine. As a result, there are chances of losing information about important tissues [4]. These artifacts make the problem of identifying the brain hemorrhage more complex and challenging [6]. Intracranial haemorrhage is divided into four categories: epidural haemorrhage, subdural haemorrhage, subarachnoid haemorrhage, and intraparenchymal haemorrhage [7]. Each form of bleeding is caused by a different etiology, and the clinical symptoms, prognosis, and consequences vary [8]. The bleeding pattern, calcification pattern, and blood clot of the brain tumor is presented in Fig. 2 and 3. This paper presents a unique region-based segmentation strategy for increasing the accuracy and efficiency of CT- automated 3D image processing in brain injury analysis in prior research articles in a single paper.

Diseases that impact the central or peripheral nervous systems are referred to as neurological and mental ailments. Because of the intricacy of the neurological system, there are several probable causes and manifestations of brain sickness. Physical trauma, illness, and a variety of environmental factors can all contribute to the onset and development of brain illnesses [9]. Multiple sclerosis (MS) [10], Alzheimer's disease (AD) [11], Parkinson's disease (PD) [12], traumatic brain injury [13], cerebral palsy [14], amyotrophic lateral sclerosis (ALS) [15], autism spectrum disorder (ASD) [16], and epileptic seizures [17, 18] are some of the most serious brain disorders.

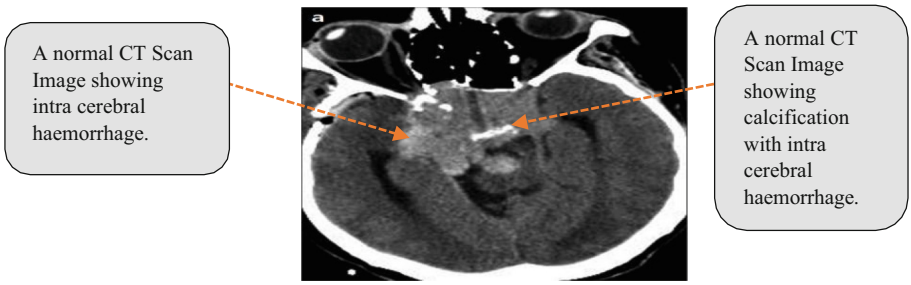


Fig. 2. A CT scan image showing intra-cerebral haemorrhage in the brain.

H. Lee et al. presented the construction of an intelligible deep-learning structure that identifies and classifies five forms of intracranial haemorrhage (ICH) using unenhanced head CT data. The system includes a focus map and an estimation basis developed from data used for training to improve accuracy. This algorithm building method can help with

the development of deep-learning algorithms for several medical applications [19]. J. Napier et al. developed a CAD system that incorporates a basic classification algorithm that identifies recent bleedings and separates intra-axial and extra-axial haemorrhages, as well as the subarachnoid haemorrhage (SAH). Among the procedures employed are noise elimination methods, morphological processes, and segmentation techniques [20]. P. Kaur et al. discuss diagnostic MRI systems that involve the enhancement of segmentation and classification processes using image processing filtering techniques. The implementation of the suggested strategies is evaluated using a mumulti-supportector algorithm that distinguishes between brain disease and MRI images [19].

M. Monteiro et al. used expert manual segmentations to train and validate an initial CNN (dataset 1). This CNN was used to segment a fresh dataset of scans automatically, which was then manually rectified (dataset 2). They trained a final CNN for multi-class, voxel-wise lesion-type segmentation using a subset of images from this dataset. The performance of lesion volume quantification, progression, recognition, and classification was evaluated [24]. J. Y. Lee et al. used the method for detecting intracranial haemorrhage (ICH) and classifying its subtypes without using the CNN. Regarding ICH localization, CT scans were segmented into ten sections based on intracranial height. This study found that the suggested technique can significantly minimize the time it takes to diagnose ICH in a real emergency while maintaining fairly high diagnostic performance [20]. O. Karadima et al. reported preliminary validation by the experiment of a microwave tomography (MWT) prototype for brain stroke identification and classification that used the distorted born iterative approach and the two-step iterative shrinkage thresholding (DBIM-TwIST) algorithm. Furthermore, the prototype can distinguish between haemorrhagic and ischemic strokes based on dielectric property estimation [26]. In his study, B. Sohani et al. presented an evaluation of alternative artifact elimination approaches for ultra-wideband Microwave Imaging (MWI) to estimate and calculate current approaches in a real-world context utilizing measurements with an MWI device. The MWI device captures dispersed signals in a multi-bistatic manner and applies an imaging approach based on the Huygens principle. To compare the object removal approaches, an "ideal/reference" image is used. Furthermore, artifact removal processes are quantified using quantities taken with an MWI device [21]. In his paper, S. P. Singh et al. presents a method for normalizing 3D volumetric scans utilizing an intensity profile from the training data. This aids the CNN by boosting contrast in the scan's abnormal region of interest. They contrast the suggested approach to a baseline, two variants of the 3D VGGNet topologies, and ResNet, and find that the proposed method considerably improves classification performance. The proposed method can detect anomalies in a variety of organs [28]. V. Poornachander et al. and Mehendale, et al. suggested that it is possible to transfer information from nature photography to medical image classification. Furthermore, our findings suggest that the proposed modified "AlexNet-SVM" model may be utilized to identify brain bleeding using an overall neural network constructed from scratch, as well as the original AlexNet [22, 23].

D. Venugopal et al. study's findings demonstrated that the proposed FFEDL-ICH model can outperform existing models, with a significant performance improvement. The researcher suggests that future studies increase the performance of the FFEDL-ICH model using learning rate scheduling strategies for DNN [7]. Brain Haemorrhage

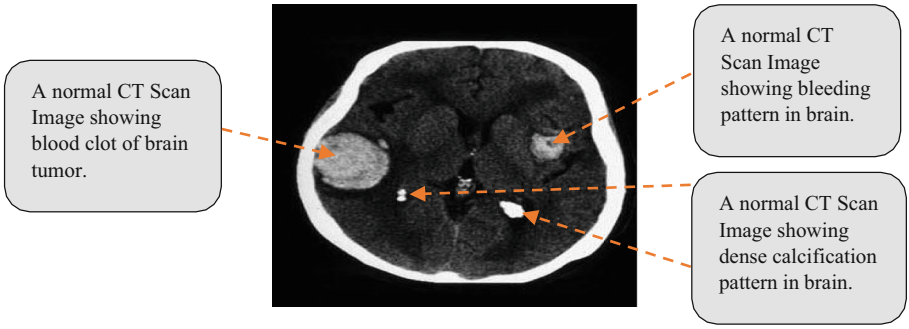


Fig. 3. A CT scan image showing bleeding pattern, calcification pattern, and blood clot of tumor in bthe rain.

Segmentation Using Adaptive Slices was proposed by Dawood et al. Based on the SLIC Algorithm for segmenting brain injury. It is challenging to create a highly efficient super-pixel technique that keeps a strategic distance from segmentation and limited clusters of pixels about intensity boundaries [24]. Raghavendra, U., et al. used non-linear characteristics in conjunction with a probabilistic neural network classifier and computed tomography (CT) images to construct one such model for assessing intra-cerebral haemorrhage. In distinguishing between normal and hemorrhagic individuals, our model attained a maximum curacy [25]. B. A. Mohammed et al. proposed a hybrid technology system that based o GoogLeNet, ResNet-50, and AlexNet models, the extents of which are decreased by a principal component analysis (PCA) technique and then integrated with the GLCM and LBP algorithms. All of the anticipated technologies shown capable results in CT image identification for the quick recognition of cerebral haemorrhages [26]. P. Liu et al. suggested a classifier for ICH subtypes that may be applied to CT images. To categories ICH subcategorize CNN-RNN architecture was used. In the CNN module, which tackles the issue of inadequate feature differentiation in prior techniques [37], the problem is examined from a fine-grained viewpoint. P. Rani et al. designed CNN models to automate the method for early diagnosis by classifying CT scan brain images as normal (no bleeding) or abnormal (with haemorrhage) using ResNet50 and DenseNet21 model. DenseNet121 model The denseNet121 both models in terms of class prediction [27].

1.1 Motivation

The motivation behind the fusion multimodalities method for haemorrhage detection is to improve the accuracy and robustness of medical imaging diagnosis of haemorrhagic stroke, which is a leading global cause of death and disability. Haemorrhagic by bleeding in the brain due to ruptured blood vessels, and early and accurate detection is critical for timely intervention and improved patient outcomes. The fusion multimodalities method for haemorrhage detection is motivated by the need for more accurate and robust diagnosis of haemorrhagic stroke, which is a significant cause of demise and disability globally. The technique leverages each modality's capabilities while overcoming its limits, with the potential to improve patient outcomes and revolutionize medical imaging.

1.2 Scope

Fusion multimodality techniques for bleeding identification have shown enormous promise in terms of improving medical diagnosis accuracy and efficiency. Data from various imaging modalities, including as computed tomography (CT) and magnetic resonance imaging (MRI), are combined in these treatments to provide a more complete view of the patient's condition. These techniques have a wide range of applications since they can be employed in a variety of medical settings, including emergency rooms, intensive care units, and radiology departments. The goal of this study is to provide a detailed scientific description of brain haemorrhage segmentation approaches based on deep learning. They can detect haemorrhages in the cerebral brain, abdomen, and other regions of the human anatomy, as well as follow how the problem develops over time.

The potential of fusion multimodality approaches to reduce false positives and false negatives can result in more precise diagnoses and improved treatment results. They can also assist medical practitioners in making more informed judgments regarding the best course of therapy, such as if surgery is required or if the patient may be treated with medicines. In short, fusion multimodality approaches for haemorrhage identification offer tremendous potential for increasing the accuracy and efficiency of medical diagnosis, and their application is anticipated to grow as more powerful imaging techniques become accessible.

1.3 Research Area

Traditional medical imaging technologies include magnetic resonance imaging (MRI), computed tomography (CT), and positron emission tomography (PET) scans, which provide further information regarding the location, extent, and severity of bleeding. Yet, each modality has limits, and integrating them can improve the analysis's accuracy and dependability. By merging the complementing information offered by each mode, fusion multimodalities best features of each modality while addressing their limitations. The fusion can be performed at different levels, such as the input- layer/pixel-level, layer/feature level, decision level, to create a more comprehensive and accurate representation of the human anatomy and function [28–30]. Deep-learning models used in the fusion multimodalities technique has shown promising results in haemorrhage detection, with high precision and sensitivity in detecting and localizing haemorrhage. The method has the potential to transform the field of medical imaging and improve patient outcomes by enabling earlier and more accurate diagnosis and treatment [31].

The current paper provides a comprehensive review of previous available research on the use of DL techniques and neuroimaging multimodalities for diagnosing brain diseases like haemorrhage. In Sect. 2, computer aided diagnosis for brain haemorrhage like diseases are discussed using different AI, ML Dl and multimodalities fusion methods. Section 3 specifically focuses on the discussion and analysis of relevant review papers that have been published on this topic. In the last, conclusion and future work is described.

2 Computer Assisted Disease Diagnosis (CAD) for Medical Imaging

Computer assisted diagnosis (CAD) systems can help with the early detection of haemorrhage. CAD provides doctors with quick and reliable results with higher accuracy, allowing them to make improved treatment formation and deliberate decisions [32]. By systematizing the routine scanning of CT scans with slight or no human intrusion, the triage workflow can also be reduced and optimized. The part that follows discusses existing works on bleeding detection using CAD. Many semi- automatic and automated methods for detecting ICH from CT images have been developed. CAD techniques for hemorrhage diagnosis involve the use of algorithms and machine learning models to analyze medical images and identify the presence of hemorrhage. Some of the commonly used CAD techniques for hemorrhage diagnosis include: (1) Convolutional Neural Networks (CNNs): [33] CNNs are a sort of deep learning system that can automatically extract data from medical images and classify them into different categories, including hemorrhage. (2) Support Vector Machines (SVMs): [34] SVMs are a sort of supervised machine learning procedure which can classify medical images as either normal or abnormal, with hemorrhage falling under the latter category. (3) Random Forests (RFs): [35] RFs are an collective learning method that can combine multiple decision trees to classify medical images accurately.

Several studies have been conducted on the use of CAD for hemorrhage diagnosis, with promising results. For instance, a study by Kumar et al. [36] used the suggest unsupervised learning which is entropy based and automatic segment the intracranial brain haemorrhage using CT medical images. Further, Using medial brain scans images, Phan et al. [37] suggested a method for analyzing brain haemorrhage locations. They use HU values to discover haemorrhage locations and to calculate the draining period of haemorrhages. It is beneficial for assisting clinicians in providing suitable therapy. Their investigational consequences reveal that the best precision of brain haemorrhage recognition and categorization obtains the maximum accuracy. Nag et al. [38] used an auto-encoder and the Chan Vese model to identify haemorrhagic areas in 48 CT images. Foo et al. [39] created a CAD system that identified acute ICH in 108 CT volumes by employing repeated thresholding and symmetry detection.

Despite the promising results reported in the research data, CAD for hemorrhage diagnosis still faces some challenges and limitations. The one of the major issues is the lack of diverse and representative data sets. Most of the available data sets are limited in size and are not diverse enough to reflect the variations in hemorrhage appearances across different patients. Another limitation is the interpretability of the models. Most deep learning models, such as CNNs, are black boxes, making it difficult to understand how they arrive at their decisions. In short, CAD for hemorrhage diagnosis has the potential to revolutionize the way hemorrhagic stroke is diagnosed and treated. However, there is still a need for more research to address the challenges and limitations facing CAD for hemorrhage diagnosis. With more diverse and representative data sets and improved interpretability of the models, CAD for hemorrhage diagnosis can significantly improve patient outcomes.

2.1 Different AI, ML, and DL Methods for Medical Imaging Analysis

Artificial Intelligence techniques can be categorized into two types, machine learning (ML), and deep learning (DL) methods, according to recent studies [40]. ML is a subset of AI That allows systems to acquire knowledge from data, discover patterns, and make judgments through little explicit coding. However, evaluating and selecting ML algorithms for disease diagnosis is a challenging and time-consuming task [40]. Two review papers have been published in this field, Meher et al. [41] and Osama S., et al. [42]. The process of image fusion, its utilization in healthcare, and its advantages and disadvantages were examined. Meher et al. [41] also looked into using AI-based ways to combine MRI, PET, and CT medical images. In the meantime, Osama S., et al. [42] published a review paper on data fusion strategies for detecting brain illnesses. They investigated the significant obstacles of detecting brain illnesses and assessed several image fusion approaches, fusion levels, multi-scale decomposition methods, and their benefits and shortcomings.

Deep learning (DL) models may spontaneously optimize and build robust representations from raw data, making them more resistant to natural data changes [40]. DL model performance generally improves as training data quantity increases, and they can learn from un-structured data, potentially allowing the usage of multiple data types without labelling. Zhou et al. [43] presented DL-based multimodal medical picture segmentation methodologies, discussing and comparing several DL architectures and fusion procedures. They also suggested future study directions. DL techniques can be used for diagnosis of brain diseases, and the use of image fusion techniques can improve the accuracy of such diagnoses.

Convolutional Neural Networks A decade ago, CNNs ushered in a machine learning revolution, ushering in the domain today famous as deep learning. The idea of training convolutional filters, on the other hand, is not new, having been proposed earlier in [137–139]. Nonetheless, their first major appearance is often considered as the AlexNet, [44] significantly improved the standard for images classification tasks. CNNs are too effective learners, and they are employed in a wide range of applications, including image enhancement and medical diagnostics. At the moment, a few renowned network topologies, such as VGG [55] and ResNet [55], are widely used, and designing the CNN design from fresh is uncommon; also, these networks are deliberated as baselines in the model development process. CNNs aren't just for jobs that require a 2D image-like pattern in the data underneath. A prominent variation for medical diagnosis is 3D CNN, which is suited for 3D data that includes MRI brain scans. 3D CNNs function by accounting for spatial information in all directions; nevertheless, they are more difficult to train and involve significantly more data and processing resources [45]. CNN's capacity to autonomously acquire and extract characteristics from images without the need for traditional feature engineering is one of its greatest benefits. This means that the CNN can automatically identify and extract important patterns, textures, and shapes from the input image, which are then used to make accurate predictions or classifications.

Another great feature of CNN is its ability to handle spatial invariance, meaning that it can recognize the same object regardless of its position, orientation, or scale in the input image. This is accomplished by employing convolutional layers, which add filters to the source image in order to recognize particular characteristics, and pooling

layers, which down-sample the feature maps to reduce their dimensionality and make them more robust to variations in the input.

Many pre-trained models have been produced in recent years to assist the application of deep learning to various tasks. Pre-trained models are trained on a big dataset and can then be fine-tuned on a reduced dataset to improve performance [45]. The U-Net [46] model is one sort of pre-trained model that has gained prominence in recent years. The U-Net model is a fully convolutional neural network that was designed to segment medical images. It is made up of an encoder and a decoder network that are linked together using skip connections so as to maintain the spatial information of input image. The U-Net model has demonstrated promising results in image segmentation tasks such as biological image segmentation and semantic segmentation. The Generative Adversarial Network (GAN) [47] model is another sort of deep learning model that has grown in popularity in recent years. The GAN model is built using two neural networks: a generator network that produces new data samples and a discriminator network that attempts to distinguish between produced and genuine data samples. The GAN model has been utilized to perform a variety of tasks such as image synthesis, style transfer, and super-resolution.

Another prominent form of deep learning model for image segmentation is Fully Convolutional Networks (FCN) [48]. FCN models are completely convolutional, which means they can take any size picture as input and output the same size segmentation map. FCN models have produced encouraging results in a variety of picture segmentation tasks, including semantic, instance, and panoptic segmentation. Another form of deep learning model utilized for unsupervised learning problems is the auto-encoder model [45]. An auto-encoder model consists of two networks: an encoder network that transfers the data being input to a reduce-dimensional implicit space, and a decoder network that recreates the actual input from the latent space illustration. Image de-noising, data compression, and anomaly detection have all been done using auto-encoder models. Lastly, Recurrent Neural Network (RNN) [45] models are a sort of deep learning model utilized for sequence data, such as time series data, speech recognition, and natural language processing applications. RNN models contain a feedback loop that allows them to capture temporal dependencies in the input data. Long Short-Term Memory (LSTM) [45] and Gated Recurrent Unit (GRU) [45] are common RNN variations that have been utilized for a variety of applications such as machine translation, speech recognition, and sentiment analysis.

To summarize, deep learning models have revolutionized many fields, and pre-trained models such as U-Net, GAN, FCN, auto-encoder, and RNN models have grown in popularity in recent years because to their excellent performance and ability to generalize to new tasks.

2.2 Multimodalities Fusion Analysis for Medical Imaging

The section discusses the importance of neuroimaging in diagnosing and identifying brain diseases. There are two categories of neuroimaging modalities: structural and functional [49]. Structural modalities are used to show the material composition of the brain and identify neurological illnesses that cause structural alterations in the brain, whereas functional modalities assess the brain's behavior, and growth while completing certain

tasks. The most important neuroimaging modalities are listed along with their advantages and disadvantages. Some known structural modalities are Structured MRI (sMRI), Computed Tomography (CT), and diffusion tensor imaging DTI. And functional modalities are magnetoencephalography (MEG) functional magnetic resonant imaging (fPET), Positron emission tomography (PET), and single-photon emission computed tomography (SPECT) [50]. However, it is important to note that no neuroimaging modality is flawless and that there are alternatives for identifying brain diseases.

CT (Computed Tomography) uses X-rays to produce comprehensive images of the brain's internal structure. It is primarily used to diagnose and monitor neurological conditions, such as strokes, traumatic brain injury, and tumors [51]. PET (Positron Emission Tomography) is a functional imaging technique that measures the metabolic activity of brain cells. It involves injecting a radioactive tracer into the patient's bloodstream, which is then detected by a scanner that produces images of the brain's function. PET is typically utilized to diagnose and maintain conditions like epilepsy, Alzheimer's disease, and brain tumors [52]. SPECT (Single Photon Emission Computed Tomography) is another functional imaging technique that uses radioactive tracers to create images of the brain's blood flow. SPECT can detect changes in blood flow that may be indicative of brain disorders such as stroke, epilepsy, and Alzheimer's disease [53]. MRI (Magnetic Resonance Imaging) is a non-invasive technique that generates images of the brain's structure and function using a strong magnetic field and radio waves. It is highly sensitive and can provide detailed images of the brain's soft tissue, making it a useful tool in diagnosing and monitoring neurological conditions such as multiple sclerosis, brain tumors, and Parkinson's disease [54]. Each of these imaging techniques has its advantages and disadvantages, and they are often used in combination with each other to provide a comprehensive understanding of brain organization and function.

The combination of several neuroimaging modalities is a relatively new method to identifying brain illnesses. Surgeons have just begun combining multiple neuroimaging techniques to diagnose brain illnesses. Typically, a structural modality like sMRI is paired with a functional modality like PET [65]. Integrating a structural modality like sMRI with a functional modality like PET may enhance each other and provide an improved understanding of the brain's anatomy, physiology, and disease. The advantage of this fusion technique is that it allows the merging of high-resolution structural images obtained from CT and/or MRI with high-temporal resolution images from PET or SPECT, resulting in a spatiotemporal resolution fusion image [55, 56]. This approach has the potential to enhance the accuracy of diagnosis and improve patient outcomes. The challenges in image fusion for brain disease diagnosis are because of alterations in brightness, resolution, noise presence, multiple modalities, limited images, increased costs, and computational complexity [57]. However, recent research has focused on using AI techniques to overcome these challenges and achieve diagnosis based on multimodality neuroimaging.

Image fusion can be carried out at three levels: the input level (which is also called the pixel-level), the layer level (also recognized as feature level), and the decision level [28–30]. The data is directly merged into the original image or the image's multi- resolution modifications at the input level [39]. The features taken from the image are merged at the layer level since features are more meaningful than pixels [40]. Finally, the results of

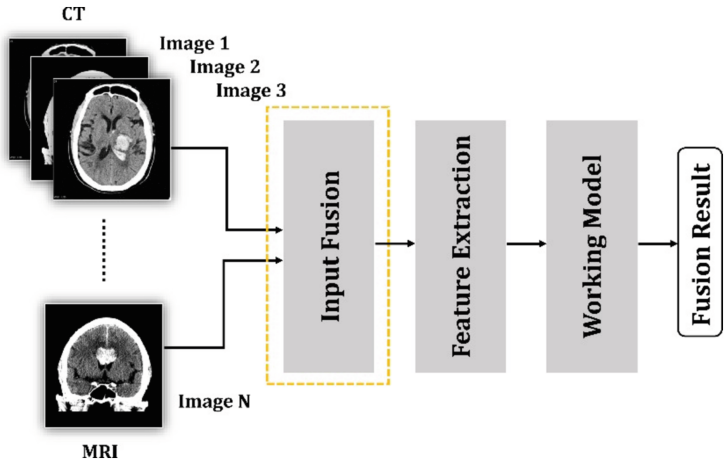


Fig. 4. Schematic diagram of Input/pixel level image fusion

various DL algorithms are combined at the decision level to arrive at the end result. In this procedure, each image undergoes processing independently, and the outcome is delivered to the final classifiers for fusion [41]. All the level of fusion of multimodality images is a technique used to combine diverse types of medical images, such as magnetic resonance imaging (MRI), computed tomography (CT), and positron emission tomography (PET) scans (described in Sect. 2.1). The purpose of the fusion is to create a more comprehensive and accurate representation of the anatomy and function of the human body.

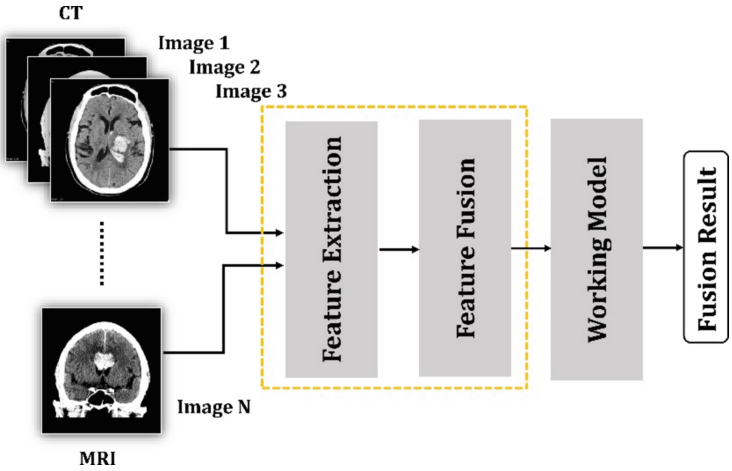


Fig. 5. Schematic diagram of layer/feature level image fusion

In input-layer fusion, the individual images are first pre-processed to ensure they are of similar size, resolution, and orientation. The images are then aligned using image registration techniques to ensure they are in the same anatomical space. The next step

is to combine the images by fusing the pixel-level information from each modality in a single image [28]. The fusion is typically performed in the input layer of a deep learning model, which enables the model to learn the significant features from the multimodality images simultaneously. The fused image is then passed through the network, where the features are extracted, and the final prediction is made as shown in Fig. 4. In feature/layer-level fusion [29] can be performed at diverse layers of the deep learning model, such as the early or intermediate layers. In early fusion, the features from each modality are combined at the input layer of the model. In contrast, in intermediate fusion, the features are combined at a later stage of the model, after they have been learned by the model as described in Fig. 5. The decision-level fusion [30] involves combining the outputs of multiple deep learning models that are trained on each modality image independently, shown in Fig. 6. The outputs are then combined using decision-making strategies, such as voting or averaging, to make a concluding prediction. The hybrid-level fusion [58] combines the strengths of feature/layer-level and decision-level fusion techniques. The features information from each modality are extracted at diverse layers of the deep learning model, and the fused features are then combined at the decision level.

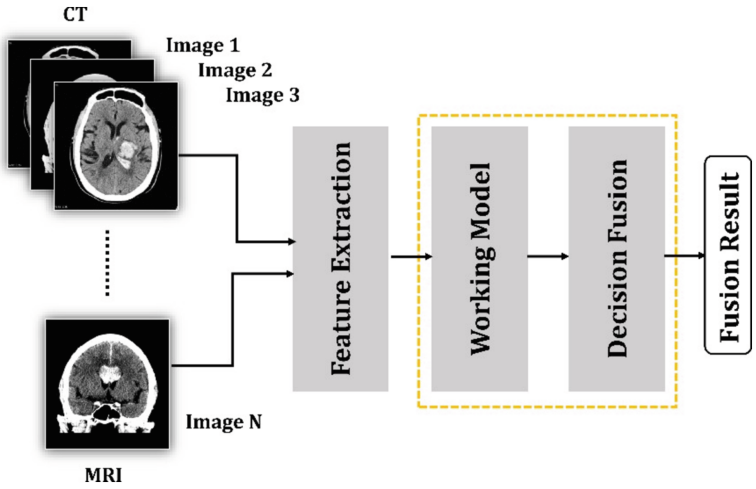


Fig. 6. Schematic diagram of decision level image fusion

3 Discussion and Comparative Analysis

This section described various review papers published between years 2018 to 2023. Which focuses on the identification of brain diseases using AI methods and neuroimaging modalities fusion. The Table 1 summarizes these review papers and includes their approaches, publication year, artificial intelligence methods, multi- modalities used, and the references. The focus of this study is on detection of brain disease through modalities fusion based on CT/MRI data and ML or DL models. The paper describes the novelties of the current study. The study also explores papers that combine different fusion levels to improve performance and these are reported in Table 1.

Table 1. Summary of research for haemorrhage detection in multi-modality fusion published in previously available papers.

Approach	Method	Modalities	Year	Ref.
fusion technique for medical analysis	ML	MRI, CT	2018	[59]
Multi-Modality fusion based Image Segmentation using DL Models	DL	CT, MRI, PET	2019	[60]
Diverse Multi-modal Image Fusion	ML	CT, MRI, PET	2019	[61]
Wavelet Models based image fusion	ML	MRI, CT	2019	[62]
Multi-Model based Medical Image Fusion	ML	CT, MRI, PET, SPECT	2019	[63]
Multi-modal Analysis by DL on Medical Images	DL	MRI, CT, PET	2019	[64]
Medical Image Fusion on region-based Methods	ML	MRI, CT	2019	[41]
Medical Image based Fusion provides the current solution	ML	MRI, CT, PET, SPECT	2020	[42]
Multi-modality based fusion in Medical Images	ML	MRI, CT, PET	2020	[43]
Fusion on Medical Image	ML and DL	Ultrasound, MRI, CT, PET	2020	[57]
Multi-modal Data Fusion Improvements	ML	CT, SPECT, PET, MRI,	2020	[65]
DL Methods based Multi-modal Data Fusion	DL	Different types of Modalities	2020	[66]
Multi-modal Medical Image based Fusion Methods	ML and DL	MRI, CT, PET, SPECT	2020	[67]
Different Image based Fusion Methods	ML	MRI, CT	2020	[68]
DL Models for Medical Image Fusion with electronic medical records	DL	Medical Imaging with HER	2020	[69]
Medical Image based Fusion Methods	ML	CT, MRI, PET, Echo	2021	[70]
Performance Metrics based Several Fusion Algorithms	ML	MRI, CT, PET	2021	[71]

(*continued*)

Table 1. (*continued*)

Approach	Method	Modalities	Year	Ref.
Medical Image Multi-modal Fusion Medicine Review	ML and DL	MRI, CT, PET, SPECT	2021	[72]
Numerous Multi-modal Fusion Techniques	ML and DL	MRI, CT, PET, SPECT, Ultrasound, X-Rays	2021	[73]
Sparse Representation-Based Medical Image Fusion	ML	MRI, CT, SPECT	2021	[74]
Deep Learning based Image Fusion	DL	Different types of Modalities	2021	[75]
Medical Image based Fusion	ML and DL	Different types of Modalities	2021	[76]
Multi-modality Image based Fusion	ML	CT, MRI, PET, SPECT	2021	[77]
Fusion in medical images	-	Different types of Modalities	2022	[78]
Medical Image Multi-modal based Fusion	-	Different types of Modalities	2022	[79]
Multi-modal Fusion, Non-image Data and Prognosis	ML and DL	Image and Non- Image data	2022	[31]
Non-traditional multi-modality fusion	DL	Different types of Modalities	2023	[80]
Multi-modality phenotype method	DL	fMRI, sMRI	2023	[81]
Modality feature fusion based disease prognosis	ML	MRI, PET, DTI	2023	[82]
Multi-modality approaches	ML and DL	MRI, DTI, PET	2023	[83]
Multi-modality image fusion	ML and DL	CT, MRI	2023	[84]

From the above studies, it is determined that by through machine learning and deep learning models for the identification of medical brain images using multimodality fusion is much more efficient rather than any single modality. The latest studies shows up to the mark performances but still there is a room to improve their work which is discussed in future work section. Although, there are some limitation and challenges faced by different physicians and medical experts for identification of any disease.

4 Challenges

Multimodality fusion employing deep learning algorithms for brain illness diagnosis raises substantial challenges and issues like datasets, data labeling, data privacy, lack of standards of data collection, modalities and multimodalities fusion, class imbalance, and

deep learning. The integration of several data modalities, such as medical images, clinical data, and genetic information, poses a substantial risk to patient. All these challenges are described below.

The requirement to combine and evaluate massive and complicated datasets from diverse sources is one of the primary problems in data fusion for the identification of brain illnesses utilizing DL approaches [85]. This necessitates the creation of sophisticated algorithms and tools for data pre-processing, feature extraction, and fusion. Another issue is a lack of standards in data collecting and labeling, which can lead to data discrepancies and inaccuracies. This can have an impact on the performance of DL models and make it difficult to compare and validate results across research [85]. The difficulty is the scarcity of large and diverse labeled datasets for multimodal brain illness diagnosis. To achieve acceptable performance, DL models for multimodal fusion frequently require huge volumes of labeled data, however getting such data is problematic due to ethical and privacy considerations in the medical profession. To use labeled datasets and generalize to new domains, methodologies for transfer learning and domain adaptation must be developed. Additionally, significant amounts of labelled data are frequently required by DL models for brain illness diagnosis [86], which can be difficult to get in the medical profession due to ethical and privacy considerations. This can limit the models' generalizability and applicability. Furthermore, interpretability and openness in DL models are required, particularly in the medical industry where decisions might have a major impact on patient outcomes. This necessitates the development of ways for explaining DL models' decisions and ensuring that they are congruent with clinical knowledge and guidelines.

There are various hurdles to multimodality fusion for the diagnosis of brain disorders employing DL methods. One of the most difficult issues is integrating heterogeneous data from many modalities, including as MRI, PET, and EEG [87]. Although the various modalities give complementary information, they also inject tremendous variety and complexity into the data. This necessitates the creation of powerful multimodal data fusion and analysis techniques and frameworks. Another challenge is selecting the most informative features from each modality and combining them into a uniform representation that represents the underlying patterns and relationships in the data. This necessitates the development of feature selection and extraction methods capable of dealing with multimodal data's high complexity and variability. Likewise, interpreting and explaining multimodal DL models for brain illness diagnosis is a difficulty [88]. The integration of many modalities, as well as the complexity of DL models, might make it challenging to understand how decisions are made and verify that they are by clinical knowledge and guidelines.

Keeping patient data secret and secure is one of the most difficult challenges. Medical records contain sensitive information, such as personal and medical information, which must be kept secure. Data breaches can have serious ramifications for healthcare businesses, including identity theft and reputational damage [89]. Data exchange and collaboration across healthcare organizations are another difficulty. In many circumstances, healthcare companies will need to share patient data to increase diagnosis accuracy and design more effective treatment strategies. But, if not managed properly, data sharing might offer privacy problems. Many ways can be taken to overcome these

difficulties. To begin, the use of encryption and access limits can aid in the security of patient data. This can include data encryption in transit and at rest, as well as role-based access controls to edge data access to just approved individuals. Second, to ensure that patient data remains private, privacy-preserving machine learning techniques can be deployed [90]. These methods entail training machine learning models on encrypted data, ensuring that sensitive patient data is not disclosed to third parties. Finally, while designing data-sharing rules and processes, healthcare companies can use privacy-by-design principles [91]. This entails incorporating privacy in all stages of the data-sharing process, such as data collection, processing, and storage.

Class imbalance is a critical difficulty in multimodality fusion for deep learning-based diagnosis of brain disorders. Class imbalance describes circumstances in which the sample distribution across multiple classes is extremely skewed, i.e., one class contains significantly fewer samples than the others [86]. The prevalence of brain disorders, such as Alzheimer's or Parkinson's disease, is generally low, resulting in a class imbalance problem. Class imbalance can have a detrimental impact on deep learning model performance since they tend to favor the majority class, resulting in worse accuracy for the minority class [86]. In the case of brain illnesses, this could imply that the deep learning model will have difficulties effectively detecting and diagnosing the disease, perhaps resulting in significant implications for the patient.

5 Conclusion

Every year, millions of people worldwide experience brain injuries as a result of car accident, falls, attacks, brain disorders, or blood vessel bursting. Out of those, the accident is the main cause of Brain injuries, especially in big cities. This results in brain damage which may press the soft tissues against the bone of the hard skull. Therefore, blood bleeding from nerves may pour into the brain area. This causes swelling and inflation which in turn affect other parts of the brain. The basic problem is identifying hemorrhage having the same intensity and it may create confusion in diagnosing. Haemorrhage bleeding shows bright spots on the CT scan images, creating intra observer variability in results. Due to the frequent use of brain CT and similar imaging patterns, it may be overlooked or confused with intra-axial or extra-axial hemorrhages.

Computed tomography (CT) and magnetic resonant imaging (MRI) are very sensitive for localization and detection of haemorrhage i.e. epidural hemorrhage, subdural hemorrhage, subarachnoid hemorrhage, and intraparenchymal hemorrhage [3]. Recent research has revealed an unanticipated level of intricacy in the regulation of vascular and bone haemorrhage using different multimodality fusion methods. Fusion multimodality methods for haemorrhage detection have significant potential for improving the accuracy and efficiency of medical diagnosis, and their scope is likely to continue expanding as more advanced imaging technologies become available.

6 Future Work

There are various possibilities for future research in computer-assisted disease diagnosis (CAD) for brain images, especially in datasets, data augmentation, deep learning approaches, and class imbalance fuzzy deep learning. These are some possible directions:

The availability of big and diverse datasets is critical for CAD system development and training. Researchers might concentrate on building larger databases with more diverse types of medical brain imaging, as well as assuring ethnic variety. Another possibility for improvement is data augmentation strategies, which can help to expand a dataset's size and improve the generalizability of a CAD system. Researchers should look into novel data augmentation techniques like generative adversarial networks (GANs), which can create realistic medical brain images.

Moreover, Deep learning algorithms have proven to be extremely effective in medical brain imaging modality fusions, although there is always potential for improvement. To improve the accuracy and robustness of DL models, researchers could investigate alternative designs and optimization techniques for CAD and multi-modality fusion like CT, MRI, and PET etc. In medical image databases, another thing that can need improvement is class imbalance. It is a typical issue, with some classes having considerably fewer examples than others. Methods for resolving class imbalance, such as over-sampling, under-sampling, or applying expense learning algorithms, could be investigated by researchers. In last, Fuzzy deep learning is a new method that blends deep learning and fuzzy logic. This method could be useful for computer-assisted disease diagnosis systems since it can aid with uncertainty and inaccuracy in medical brain image interpretation.

References

1. Gonçalves, F.G., Caschera, L., Teixeira, S.R., et al.: Intracranial calcifications in childhood: part 1. Pediatr. Radiol. **50**, 1424–1447 (2020)
2. Torad, M.A., Salam, M.A.: Smart helmet using internet of things. Int. J. Reconfigurable Embed. Syst. **10**, 90 (2021)
3. Shao, M., Zhang, W., Niu, Z., et al.: Computed tomography characteristics of adrenal ganglioneuroma: a retrospective analysis of 30 pathologically-confirmed cases. J. Int. Med. Res. **48**, 0300060520945510 (2020)
4. Chen, H., Khan, S., Kou, B., et al.: A smart machine learning model for the detection of brain hemorrhage diagnosis based internet of things in smart cities. Complexity **2020**, 1–10 (2020). https://doi.org/10.1155/2020/3047869
5. Hema Rajini, N., Bhavani, R.: Automatic classification of computed tomography brain images using ANN, k-NN and SVM. AI Soc. **29**, 97–102 (2014)
6. Rava, R.A., Seymour, S.E., LaQue, M.E., et al.: Assessment of an artificial intelligence algorithm for detection of intracranial hemorrhage. World Neurosurg **150**, e209–e217 (2021)
7. Venugopal, D., Jayasankar, T., Sikkandar, M.Y., et al.: A novel deep neural network for intracranial haemorrhage detection and classification. Comput Mater Contin **68**, 2877–2893 (2021)
8. Burduja, M., Ionescu, R.T., Verga, N.: Accurate and efficient intracranial hemorrhage detection and subtype classification in 3D CT scans with convolutional and long short-term memory neural networks. Sensors **20**, 5611 (2020)
9. Deuschl, G., Beghi, E., Fazekas, F., et al.: The burden of neurological diseases in Europe: an analysis for the Global Burden of Disease Study 2017. Lancet Publ. Health **5**, e551–e567 (2020)
10. Shoeibi, A., Khodatars, M., Jafari, M., et al.: Applications of deep learning techniques for automated multiple sclerosis detection using magnetic resonance imaging: a review. Comput. Biol. Med. **136**, 104697 (2021)

11. Ebrahimighahnavieh, M.A., Luo, S., Chiong, R.: Deep learning to detect Alzheimer's disease from neuroimaging: a systematic literature review. Comput. Methods Programs Biomed. **187**, 105242 (2020)
12. Khachnaoui, H., Mabrouk, R., Khlifa, N.: Machine learning and deep learning for clinical data and PET/SPECT imaging in Parkinson's disease: a review. IET Image Process **14**, 4013–4026 (2020)
13. Silverberg, N.D., Duhaime, A.-C., Iaccarino, M.A.: Mild traumatic brain injury in 2019–2020. JAMA **323**, 177–178 (2020)
14. Zhang, J.: Multivariate analysis and machine learning in cerebral palsy research. Front. Neurol. **8**, 715 (2017)
15. Hardiman, O.: Major advances in amyotrophic lateral sclerosis in 2020. Lancet Neurol. **20**, 14–15 (2021)
16. Khodatars, M., Shoeibi, A., Sadeghi, D., et al.: Deep learning for neuroimaging- based diagnosis and rehabilitation of autism spectrum disorder: a review. Comput. Biol. Med. **139**, 104949 (2021)
17. Miri, M., Amini, Z., Rabbani, H., Kafieh, R.: A comprehensive study of retinal vessel classification methods in fundus images. J. Med. Signals Sens. **7**, 59 (2017)
18. Shoeibi, A., Ghassemi, N., Khodatars, M., et al.: Detection of epileptic seizures on EEG signals using ANFIS classifier, autoencoders and fuzzy entropies. Biomed. Signal Process. Control **73**, 103417 (2022)
19. Kaur, P., Singh, G., Kaur, P.: Classification and validation of MRI brain tumor using optimised machine learning approach. In: Kumar, A., Paprzycki, M., Gunjan, V.K. (eds.) ICDSMLA 2019. LNEE, vol. 601, pp. 172–189. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-1420-3_19
20. Lee, J.Y., Kim, J.S., Kim, T.Y., Kim, Y.S.: Detection and classification of intracranial haemorrhage on CT images using a novel deep-learning algorithm. Sci. Rep. **10**, 20546 (2020)
21. Sohani, B., Puttock, J., Khalesi, B., et al.: Developing artefact removal algorithms to process data from a microwave imaging device for haemorrhagic stroke detection. Sensors **20**, 5545 (2020)
22. Poornachander, V.: Application of profound training in neuroradiology: the classification of brain haemorrhage through transfer learning. J. Innov. Dev. Pharm. Tech. Sci. JIDPTS 4 (2021)
23. Mehendale, D., Gupta, P., Rajadhyaksha, N., et al.: A Graphical Approach For Brain Haemorrhage Segmentation. ArXiv Prepr ArXiv220206876 (2022)
24. Dawod, A.Y., Phaphuangwittayaku, A., Ying, F., Angkurawaranon, S.: Adaptive slices in brain haemorrhage segmentation based on the SLIC algorithm. Eng. Lett. **29** (2021)
25. Raghavendra, U., Pham, T.-H., Gudigar, A., et al.: Novel and accurate non-linear index for the automated detection of haemorrhagic brain stroke using CT images. Complex Intell. Syst. **7**, 929–940 (2021)
26. Mohammed, B.A., Senan, E.M., Al-Mekhlafi, Z.G., et al.: Multi-method diagnosis of CT images for rapid detection of intracranial hemorrhages based on deep and hybrid learning. Electronics **11**, 2460 (2022)
27. Rani, P., Mohan, M.: A tenable approach to detect brain Haemorrhage using deep learning. In: 2022 4th International Conference on Circuits, Control, Communication and Computing (I4C). IEEE, pp. 198–201 (2022)
28. Ashok Kumar, B., Sivaranjani, A., Senthilrani, S., Senthil Murugan, A.: A Study on Various Medical Imaging Modalities and Image Fusion Methods. In: Artificial Intelligence on Medical Data: Proceedings of International Symposium, ISCMM 2021, pp 111– 126. Springer (2022)
29. Gaw, N., Yousefi, S., Gahrooei, M.R.: Multimodal data fusion for systems improvement: a review. IISE Trans **54**, 1098–1116 (2022)

30. Wang, S., Celebi, M.E., Zhang, Y.-D., et al.: Advances in data preprocessing for biomedical data fusion: an overview of the methods, challenges, and prospects. Inf. Fusion **76**, 376–421 (2021)
31. Cui, C., Yang, H., Wang, Y., et al.: Deep multimodal fusion of image and non-image data in disease diagnosis and prognosis: a review. Prog. Biomed. Eng. **5**(2), 022001 (2023)
32. Khan, M.A., Sarfraz, M.S., Alhaisoni, M., et al.: StomachNet: optimal deep learning features fusion for stomach abnormalities classification. IEEE Access **8**, 197969–197981 (2020)
33. Yu, H., Yang, L.T., Zhang, Q., et al.: Convolutional neural networks for medical image analysis: state-of-the-art, comparisons, improvement and perspectives. Neurocomputing **444**, 92–110 (2021)
34. Razzak, M.I., Naz, S., Zaib, A.: Deep learning for medical image processing: Overview, challenges and the future. In: Dey, N., Ashour, A.S., Borra, S. (eds.) Classification in BioApps. LNCVB, vol. 26, pp. 323–350. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-65981-7_12
35. Konukoglu, E., Glocker, B.: Random forests in medical image computing. In: Handbook of medical image computing and computer assisted intervention, pp. 457–480. Elsevier (2020). https://doi.org/10.1016/B978-0-12-816176-0.00024-7
36. Kumar, I., Bhatt, C., Singh, K.U.: Entropy based automatic unsupervised brain intracranial hemorrhage segmentation using CT images. J. King Saud. Univ.-Comput. Inf. Sci. **34**, 2589–2600 (2022)
37. Phan, A.-C., Vo, V.-Q., Phan, T.-C.: A Hounsfield value-based approach for automatic recognition of brain haemorrhage. J. Inf. Telecommun. **3**, 196–209 (2019)
38. Nag, M.K., Chatterjee, S., Sadhu, A.K., et al.: Computer-assisted delineation of hematoma from CT volume using autoencoder and Chan Vese model. Int. J. Comput. Assist. Radiol. Surg. **14**, 259–269 (2019)
39. Foo, Y.H., Wong, J.H.D., Azman, R.R., et al.: Identification of acute intracranial bleed on computed tomography using computer aided detection. J. Phys.: Conf. Ser. **1497**(1), 012019 (2020)
40. Shoeibi, A., Sadeghi, D., Moridian, P., et al.: Automatic diagnosis of schizophrenia in EEG signals using CNN-LSTM models. Front. Neuroinform. **15**, 777977 (2021). https://doi.org/10.3389/fninf.2021.777977
41. Meher, B., Agrawal, S., Panda, R., Abraham, A.: A survey on region based image fusion methods. Inf. Fusion **48**, 119–132 (2019)
42. Faragallah, O.S., El-Hoseny, H., El-Shafai, W., et al.: A comprehensive survey analysis for present solutions of medical image fusion and future directions. IEEE Access **9**, 11358–11371 (2020)
43. Yadav, S.P., Yadav, S.: Image fusion using hybrid methods in multimodality medical images. Med. Biol. Eng. Comput. **58**, 669–687 (2020)
44. Janiesch, C., Zschech, P., Heinrich, K.: Machine learning and deep learning. Electron. Mark. **31**, 685–695 (2021)
45. Ikechukwu, A.V., Murali, S., Deepu, R., Shivamurthy, R.: ResNet-50 vs VGG-19 vs training from scratch: a comparative analysis of the segmentation and classification of Pneumonia from chest X-ray images. Glob. Transit. Proc. **2**, 375–381 (2021)
46. Ronneberger, O., Fischer, P., Brox, T.: U-net: convolutional networks for biomedical image segmentation. In: Navab, N., Hornegger, J., Wells, W.M., Frangi, A.F. (eds.) Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015: 18th International Conference, Munich, Germany, 5–9 October 2015, Proceedings, Part III, pp. 234–241. Springer International Publishing, Cham (2015). https://doi.org/10.1007/978-3-319-24574-4_28
47. Creswell, A., White, T., Dumoulin, V., et al.: Generative adversarial networks: an overview. IEEE Signal Process. Mag. **35**, 53–65 (2018)

48. Wang, J., Song, L., Li, Z., et al.: End-to-end object detection with fully convolutional network. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, pp 15849–15858 (2021)
49. Khan, P., Kader, M.F., Islam, S.R., et al.: Machine learning and deep learning approaches for brain disease diagnosis: principles and recent advances. IEEE Access **9**, 37622–37655 (2021)
50. Zhang, L., Wang, M., Liu, M., Zhang, D.: A survey on deep learning for neuroimaging-based brain disorder analysis. Front. Neurosci. **14**, 779 (2020)
51. Songul Meltem, C., Turkmenoglu, O.N., Tanik, C., et al.: Computerized tomography- guided stereotactic biopsy of intracranial lesions: report of 500 consecutive cases. Turk. Neurosurg. **27**, 395–400 (2017)
52. Adebimpe, A., Bertolero, M., Dolui, S., et al.: ASLPrep: a platform for processing of arterial spin labeled MRI and quantification of regional brain perfusion. Nat. Methods **19**, 683–686 (2022)
53. L'Heureux, F., Baril, A.-A., Gagnon, K., et al.: Longitudinal changes in regional cerebral blood flow in late middle-aged and older adults with treated and untreated obstructive sleep apnea. Hum. Brain Mapp. **42**, 3429–3439 (2021)
54. Pflüger, I., Wald, T., Isensee, F., et al.: Automated detection and quantification of brain metastases on clinical MRI data using artificial neural networks. Neuro-Oncol. Adv. **4**, vdac138 (2022)
55. Liu, L., Kurgan, L., Wu, F.-X., Wang, J.: Attention convolutional neural network for accurate segmentation and quantification of lesions in ischemic stroke disease. Med. Image Anal. **65**, 101791 (2020)
56. Venugopalan, J., Tong, L., Hassanzadeh, H.R., Wang, M.D.: Multimodal deep learning models for early detection of Alzheimer's disease stage. Sci. Rep. **11**, 3254 (2021)
57. Li, C., Zhu, A.: Application of image fusion in diagnosis and treatment of liver cancer. Appl. Sci. **10**, 1171 (2020)
58. Jo Dolz, C., Desrosiers, IB Ayed.: IVD-Net: Intervertebral disc localization and segmentation in MRI with a multi-modal UNet. In: Zheng, G., Belavy, D., Cai, Y., Li, S. (eds.) Computational Methods and Clinical Applications for Spine Imaging: 5th International Workshop and Challenge, CSI 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 16, 2018, Revised Selected Papers, pp. 130–143. Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-030-13736-6_11
59. George, N., Saju, K.: Study on Image Fusion Techniques Applicable to Medical Diagnosis. In: 2018 International Conference on Emerging Trends and Innovations In Engineering And Technological Research (ICETIETR), pp. 1–5. IEEE (2018)
60. Zhou, T., Ruan, S., Canu, S.: A review: deep learning for medical image segmentation using multi-modality fusion. Array **3**, 100004 (2019)
61. Dolly, J.M,. Nisa, A.: A survey on different multimodal medical image fusion techniques and methods. In: 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), pp 1–5. IEEE (2019)
62. Yadav, S.P., Yadav, S.: Fusion of medical images using a wavelet methodology: a survey. IEIE Trans. Smart Process. Comput. **8**, 265–271 (2019)
63. Polinati, S., Dhuli, R.: A review on multi-model medical image fusion. In: 2019 International Conference on Communication and Signal Processing (ICCSP), pp. 554– 558. IEEE (2019)
64. Yan, X.: Deep learning in multimodal medical image analysis. In: Wang, H., Siuly, S., Zhou, R., Martin-Sanchez, F., Zhang, Y., Huang, Z. (eds.) HIS 2019. LNCS, vol. 11837, pp. 193–200. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-32962-4_18
65. Zhang, Y.-D., Dong, Z., Wang, S.-H., et al.: Advances in multimodal data fusion in neuroimaging: overview, challenges, and novel orientation. Inf. Fusion **64**, 149–187 (2020)
66. Gao, J., Li, P., Chen, Z., Zhang, J.: A survey on deep learning for multimodal data fusion. Neural Comput. **32**, 829–864 (2020)

67. Huang, B., Yang, F., Yin, M., et al.: A review of multimodal medical image fusion techniques. Comput. Math. Methods Med. **2020**, 1–16 (2020). https://doi.org/10.1155/2020/8279342
68. Elmasry, S.A., Awad, W.A., Abd El-hafeez, S.A.: Review of different image fusion techniques: comparative study. In: Ghalwash, A.Z., El Khameesy, N., Magdi, D.A., Joshi, A. (eds.) Internet of Things—Applications and Future. LNNS, vol. 114, pp. 41–51. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3075-3_3
69. Huang, S.-C., Pareek, A., Seyyedi, S., et al.: Fusion of medical imaging and electronic health records using deep learning: a systematic review and implementation guidelines. NPJ Digit. Med. **3**, 136 (2020)
70. Chauhan, K., Chauhan, R.K., Saini, A.: Medical image fusion methods: Review and application in cardiac diagnosis. In: Image Processing for Automated Diagnosis of Cardiac Diseases, pp. 195–215. Elsevier (2021). https://doi.org/10.1016/B978-0-323-85064-3.00004-2
71. Singh, S., Mittal, N., Singh, H.: Review of various image fusion algorithms and image fusion performance metric. Arch. Comput. Methods Eng. **28**, 3645–3659 (2021)
72. Hermessi, H., Mourali, O., Zagrouba, E.: Multimodal medical image fusion review: theoretical background and recent advances. Signal Process. **183**, 108036 (2021)
73. Kumar, K.V., Sathish, A.: A comparative study of various multimodal medical image fusion techniques–a review. In: 2021 Seventh International conference on Bio Signals, Images, and Instrumentation (ICBSII). IEEE, pp 1–6 (2021)
74. Liu, Y., Chen, X., Liu, A., et al.: Recent advances in sparse representation based medical image fusion. IEEE Instrum. Meas. Mag. **24**, 45–53 (2021)
75. Zhang, H., Xu, H., Tian, X., et al.: Image fusion meets deep learning: a survey and perspective. Inf Fusion **76**, 323–336 (2021)
76. Kaur, H., Koundal, D., Kadyan, V.: Image fusion techniques: a survey. Arch Comput Methods Eng **28**, 4425–4447 (2021)
77. Tawfik, N., Elnemr, H.A., Fakhr, M., et al.: Survey study of multimodality medical image fusion methods. Multimed. Tools Appl. **80**, 6369–6396 (2021)
78. Nazari, E., Biviji, R., Roshandel, D., et al.: Decision fusion in healthcare and medicine: a narrative review. mHealth **8**, 8–8 (2022)
79. Azam, M.A., Khan, K.B., Salahuddin, S., et al.: A review on multimodal medical image fusion: compendious analysis of medical modalities, multimodal databases, fusion techniques and quality metrics. Comput. Biol. Med. **144**, 105253 (2022)
80. Diwakar, M., Singh, P., Ravi, V., Maurya, A.: A non-conventional review on multi-modality-based medical image fusion. Diagnostics **13**, 820 (2023)
81. Zhang, L., Pang, M., Liu, X.., et al.: Incorporating multi-stage diagnosis status to mine associations between genetic risk variants and the multi-modality phenotype network in major depressive disorder. Front. Psychiatry **14** (2023)
82. Mishra, S., Dutta, M.: Modality feature fusion based Alzheimer's disease prognosis. Optik **272**, 170347 (2023)
83. Shukla, A., Tiwari, R., Tiwari, S.: Review on Alzheimer disease detection methods: automatic pipelines and machine learning techniques. Science **5**, 13 (2023)
84. El-Shafai, W., Aly, R., Taha, T.E.-S., El-Samie, F.E.A.: CNN: a tool to fuse multi- modality medical images. J. Opt. 1–15 (2023)
85. Buduma, N., Buduma, N., Papa, J.: Fundamentals of deep learning. O'Reilly Media, Inc. (2022)
86. Johnson, J.M., Khoshgoftaar, T.M.: Survey on deep learning with class imbalance. J. Big Data **6**, 1–54 (2019)
87. Panigrahy, C., Seal, A., Mahato, N.K.: MRI and SPECT image fusion using a weighted parameter adaptive dual channel PCNN. IEEE Signal Process. Lett. **27**, 690–694 (2020)
88. Perez, J., Mazo, C., Trujillo, M., Herrera, A.: MRI and CT fusion in stereotactic electroencephalography: a literature review. Appl. Sci. **11**, 5524 (2021)

89. Javan, A.A.K., Jafari, M., Shoeibi, A., et al.: Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems. Sensors **21**, 3925 (2021)
90. Kekha Javan, A.A., Shoeibi, A., Zare, A., et al.: Design of Adaptive-Robust Controller for multi-state synchronization of chaotic systems with unknown and time-varying delays and its application in secure communication. Sensors **21**, 254 (2021)
91. Kaissis, G.A., Makowski, M.R., Rückert, D., Braren, R.F.: Secure, privacy-preserving and federated machine learning in medical imaging. Nat. Mach. Intell. **2**, 305–311 (2020)

Human Activity Recognition Using Transformer Model

Hafiz Yasir Ghafoor, Muhammad Izhar, Muhammad Zubair, Mian Abid, and Rashid Jahangir(✉)

Superior Univeristy, Lahore, Pakistan
rashidjahangir@cuivehari.edu.pk

Abstract. Human activity recognition has become a popular research topic in recent years, due to its many practical applications in areas such as smart homes, healthcare, robotics and sports. Researchers are interested in developing systems that can identify user activities from raw data with minimal resource usage. Deep learning is a promising technology for analyzing large datasets quickly and efficiently. However, previous methods that relied solely on smartphone accelerometers were limited in their ability to recognize complex, real-time human activities. In this study, we propose a transformer model that is trained on input datasets to extract low-level, high-level, and complex features and classify human activities. We use three publicly available datasets (UCI-HAR, WISDM, and MHealth) to test the system. Despite limited hardware resources, our proposed system performs well and provides satisfactory activity identification.

Keywords: Human Activity Recognition (HAR) · Transformer Model · Smartphone Sensors · Wearable

1 Introduction

Human Activity Recognition (HAR) has turned to a distinguished research field in ubiquitous computing due to its amazing contributions [8, 9, 12]. To get information about peoples' behavior researchers are using these systems as a medium [11]. A lot of research areas are getting benefits of HAR including smart home, health care, robotics, elderly care, pets, arts and entertainment, gesture and poster analysis, smart surveillance and sports [29] as shown in Fig. 1. Activities of daily living especially of elder people Monitoring in real time is a critical issue in intelligent healthcare system [5]. By utilising wearable and mobile sensors can clearly improve these issues [5]. The use of HAR in ubiquitous computing environments has gained a lot of attention as a way to better understand people's daily interactions and behaviours [19].

In recent years, a number of distinguished activities [17, 20] were considered for HAR such as walking, running, jumping, upstairs, downstairs, cooking etc.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 171–190, 2025.
https://doi.org/10.1007/978-3-031-77620-5_12

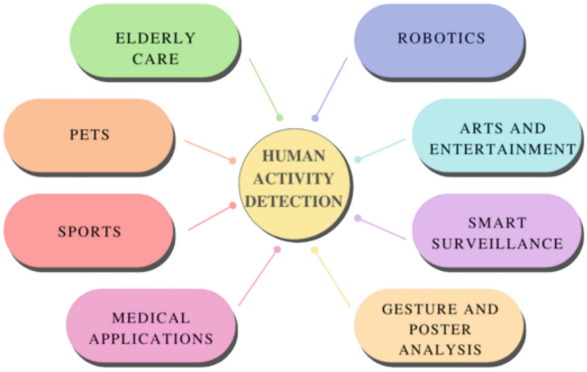


Fig. 1. Applications of human activity recognition system

With respect to the complexity and duration, these activities are categorized into three key groups. These are short activities, simple activities, and complex activities [7]. Firstly, the short activities are those activities having very short duration such as from stand to sit. Secondly, basic activities are bit complex than short activities like reading and walking [7]. Finally the complex activities essentially combines progressions of fundamental tasks and contacting with various things and people. Partying or attending joint formal meetings are examples of such activities [1].

Nowadays, internal and external sensing are the primary methods used for HAR [26]. In the first mode, devices such as cameras are installed on specified fixed positions. The inference of actions is totally based on the user's contact with these devices. There are some shortcomings of this method. Firstly, the action cannot be detected if the user is outside the sensor's range or the subject is free to move about the area. Secondly, the environment is complex and dynamic like the background, daylight and weather. These environmental factors make identification more challenging. Thirdly, Video sensors maintenance and installation entails high charges. Lastly, computationally expensive and complex video processing technology make this systems less practical. These limitations do not apply to wearable sensors for HAR. In external sensing, a device such as an inertial sensor are placed on human's body to detect motion. Among these two methods, researchers prefer to use wearable sensors having advantages such as being easily portable, relatively low energy usage, lightweight in nature, mountable at different locations [26].

The strategies based on wearable inertial sensors demand additional sensing components, though. Particularly when used for long-term surveillance, these are obtrusive for people [3]. With the advancement of smartphone technology, these devices are now strong sensor platforms as well as communication devices.

Fig. 2. Deep learning process for human activity recognition

[15]. Other than accelerometer, gyroscope and magnetometer a large number of sensors are embedded in smartphones. Smartphone can be a good candidate for HAR as it is extensively use of smartphone in our daily life and non-intrusive nature, they [15]. A single sensor data is not sufficient [24] for accurate HAR so the multiple sensors data can be fused to get more accurate results.

Given the growing importance of HAR for navigation performance, various learning-based approaches to reasoning about inertial sensory data have been proposed. In earlier approaches classical machine learning based methods were applied [22]. The classical ML model is given in Fig. 2. From raw data hand crafted features were generated with classical methods including decision tree and support vector machine [21, 23]. Recently feed forward networks and long short term memory models were proposed [24, 25]. These models removed features extraction overhead and improved accuracy. Readers who are interested can get detailed surveys outlining classic and deep learning methods for HAR [13, 18–20]. Recurrent neural networks, convolutional neural networks, temporal convolutional networks, variational autoencoders, and stacked autoencoders are a few examples of the different deep learning methodologies that are reviewed.

Deep learning is a type of machine learning algorithm that is based on artificial neural networks. It uses multiple layers of neurons to process data and create predictions or decisions about the data. In the case of human activity recognition, deep learning models can be used to classify and categorize human activities based on a large set of data points as shown in Fig. 2. The most prominent method in current research is features level fusion. This method at an early stage makes use of the correlation between the modalities. Further-more, this method uses only one classifier to make the training process efficient. However, in diffrent modalities the data recording speed and format is different, this leads to time synchronisation problem at feature level fusion [28]. Decision level fusion is another widely employed fusion technique. This technique's key benefit is

that it enables us to openly analyse each modality, considerably reducing the possibility of one modality dominating the others. Furthermore, In terms of modality decision level fusion offers scalability [4] because addition of new modality is comparatively easy. The use of more than one classifier is the considerable issue in features level fusion. It makes the process lengthy and inefficient. To make up for feature level and choice level fusion's flaws The use of hybrid multi-modal fusion has been tested by researchers [23]. However, no study provided an ultimate solution.

Transformers [31] are proposed in this work for learning, using inertial sensors for HAR problems. For sequence analysis transformer utilize attention-based encoder-decoder architecture. Attention module [32] learn to integrate entire sequence information. Transformers provide position- and context-aware representations by stacking attentional layers that scan the sequence. This approach has been demonstrated to perform better than recurrent neural networks and LSTMs for a variety of sequence-based issues in computer vision and natural language understanding [31,33–36]. In summary, the main contributions of the paper are as follows:

- An approach for retrieving prominent and resilient HAR characteristics is proposed.
- A cross-corpus model with effective performance is proposed.
- To achieve recognition of different classes of HAR this study will develop new transformer based method.
- Unlike earlier research, this application will minimize user end high performance computing issues by utilizing cloud based high-performance parallel computing of graphics processing unit (GPU).

The remainder of the essay is structured as follows: The proposed Transformer-based architecture for categorization using inertial data is described in Section II. While Section IV discusses the findings, Section III reviews the datasets used in this study. Finally, Section V presents the study's findings.

2 Literature Review

Many different applications, including as smart health services and smart home applications, can benefit from HAR. Numerous sensors, including cameras, wearable sensors, telephones, radio frequency (RF) sensors (WiFi, RFID), and LED light sensors, have been used to detect human movement. As a result of the rapid expansion of wireless sensor networks, a sizable amount of data has been gathered for the detection of human behaviours with various types of sensors.

Traditional shallow learning methods like support vector machines and random forests necessitate additional manual labour and can produce noisy features. Additionally, manual feature engineering will inevitably miss implicit features because it requires export expertise. Deep learning has recently experienced significant success in a number of difficult study areas, including picture identification and natural language processing. Deep learning's main benefit is the automatic generation of discriminative features from enormous amounts of data.

[14] proposed smartphone based HAR system that is based on two inertial sensors including accelerometer and gyroscope. Furthermore, very common statistical features namely mean, median and autoregressive coefficient were utilized. To strengthen

these features kernel principal component analysis and linear discriminant analysis were applied. Further to train this model features were fed to Deep Belief Network (DBN). The outcome was evaluated and compared with very common machine learning algorithms such as Support Vector Machine (SVM) and Artificial Neural Networks (ANN) where the proposed method outperformed and attained 95.85% accuracy and 89.61% mean recognition rate.

To competes with previously developed deep neural network (DNN) architectures that rely on manually engineered features, this study [22] introduced an activity recognition architecture that is based on holistic deep swdxlearning, a convolutional neural network-long short-term memory network (CNN-LSTM). This architecture not only decreased model complexity while effectively eliminating the need for complex feature engineering but also increased the prediction performance of human actions from raw data. This network is large in both time and space. On the UCI HAR dataset, the proposed architecture obtained 92% accuracy while on the iSPL dataset, it reached 100% accuracy.

To address the issue of consistent computation times under real-time node processing constraint on smartphones and a wearable sensor platform this study [25] introduced a deep learning methodology that integrates features learnt from inertial sensor data with complementary information from a set of shallow features. Prior to delivering the data to the deep learning framework, the proposed method for real-time on-node computation is optimised via spectral domain preprocessing. We used five openly accessible datasets, including ActiveMiles, WISDM v1.1, WISDMV2.0, Daphnet FoG, and Skoda databases. The proposed method was compared to state-of-the-art techniques using activity datasets from the real world and the lab. Our results beat competing methods, including the two methods used in our combined pipeline, demonstrating the validity of the concept on a variety of datasets, including those involving human activities.

This study [30] presented a semi-supervised deep learning framework for more accurate HAR, which efficiently examines data from sensors with weak labelling and trains the classifier learning model. Moreover, an intelligent auto-labeling scheme based on Deep Q-Network (DQN) to effectively address the problem of ineffectively labeled sample is Designed using a newly developed distant reward rule that can improve learning efficiency in IoT contexts. A multi-sensor based data fusion method is then developed to coherently fuse context sensor data, personal profile data, and onbody sensor data. Finally, a classification technique based on Long Short Term Memory (LSTM) was suggested in order to fine-grained patterns based on the high-level properties contextually recovered from sequential motion data. The suggested technique is then tested and evaluated using data from the real world to confirm its efficacy and usefulness.

wan et al [26] examined the benefits and drawbacks of the five algorithms CNN, LSTM, BLSTM, MLP, and SVM for identifying human behaviour and compared with propsed method. For HAR, an inertial accelerometer-based architecture for smartphones was created. The smartphone takes sensory data while the participants go about their daily lives, isolates the high-efficiency features from the original data, and then uses numerous three-axis accelerometers to record the user's physical behaviour. The data was first preprocessed by nor-malisation, segmentation, and denoising in order to extract the useful feature vectors. Furthermore, for HAR at real time a CNN based classification

method was proposed that used CNN for local feature extraction. Finally, SVM, LSTM, BLSTM, CNN and MLP were employed on the Pamap2 and UCI datasets. We explore how the proposed method outperforms the others on two large public datasets.

Three novel deep multilevel multimodal (M2) fusion frameworks have been proposed to increase the HAR's accuracy when using inertial and depth sensors [2] in order to take advantage of diverse fusion tactics at various levels and to fully utilise multilevel fusion. At the time of input, the inertial sensor data and depth data were converted into signal images and sequential front view images, respectively. Each input modality, including depth and inertial, is further rendered multimodal by employing convolution with the Prewitt filter. CNN may extract new supplementary and discriminative characteristics because to "modality inside modality". CNN was used to extract low-level, high-level, and complicated features from input images created using various modalities. For the suggested framework, all of the extracted complementary and discriminative traits were combined. A multi-class Support Vector Machine (SVM) received the newly created feature vector as input. Three freely available multimodal HAR datasets were used to evaluate the proposed frameworks: the UTD Multimodal Human Action Dataset (MHAD), UTDMHAD Kinect V2 and Berkeley MHAD. Experiment findings demonstrate that the proposed fusion frameworks outperform existing ones.

To address the crucial issues involved in developing an activity detection system based on sensors that works on and near a lossy medium, such as the human body, in order to achieve a trade-off between computing complexity, accuracy power usage and cost. This study [13] developed a magnetic induction based wireless system for HAR to address these issues. ML techniques were integrated with magnetic induction to detect. to detect a variety of human movements the magnetic induction system is integrated with ML techniques . The proposed system was evaluated using This approach is successfully evaluated using deep recurrent neural networks, laboratory measurements and synthesized datasets. [27] offered a technique for identifying people's intricate, in-home activities utilising wearable multimodal sensing and simply Bluetooth beacons as infrastructure. In particular, author designed a context-based activity classifier based on body multipositional wearables and hybrid multimodal sensors. Experimental results of 19 in-home activities expressed that the proposed scheme provides on average more than 80 percent accuracy of classifying.

[24] proposed multi-sensor fusion method to inegrate the results of different motion sensors. The most efficient machine learning methods like logistic regression, decision tree, and k-Nearest Neighbors were used. For compact features representation co-relation based features selection and bio inspired featured selection methods were applied. To reduce the impact of class imbalance synthetic oversampling minority (SMOT) was applied. For evaluation purpose two publically available datasets were used. The performance results shows that this improved 3

This article [24] proposes a method to integrate the predictions of various motion sensors in order to boost HAR in health monitoring systems employing mobile and wearable sensors. A number of adaptable and dynamic human activity detection systems were created using computationally effective classification approaches as decision trees, logistic regression, and k-Nearest Neighbours. We looked into a hybrid bio-inspired evolutionary search algorithm and a correlation-based feature selection strategy in order to produce compact feature vector representation, and we assessed the effects of both techniques on the feature vectors that were gathered from each unique sensor modality. Furthermore, Synthetic Over-sampling Minority Techniques (SMOTE) were used to lessen the effects of class inequality. The performance outcomes achieved utilising two openly accessible datasets demonstrated a considerable increase over baseline methods in the detection of certain activity details and a decreased mistake rate.

This research introduced an online independent support vector machine (OISVM), which uses a small quantity of data from the hidden location to update the SVM algorithm's parameters in real-time [10]. In terms of subject variations, placement and orientation its a robust HAR system. This is based on online support vector machine (OSVM), principal component analysis (CT-PCA) and coordinate transformation. To overcome the effect of orientation variations the proposed CT-PCA played major role. The suggested approach also demonstrates the success of this plan with regard to placement and subject changes. The experimental findings show how well this OISVM algorithm handles placement and subject differences.

[21] This study proposed deep recurrent neural networks for building recognition models to capture long-range dependencies in variable-length input sequences. LSTM deep recurrent neural networks was applied to present unidirectional, bidirectional, and cascaded architecture. Experimental results showed that this study outperformed in terms of accuracy as compare to SVM and KNN.

[3] proposed wrapper and filter based hybrid method for features selection. For better and desired activity recognition, sequential floating forward search was applied. For training and testing purpose Features are then fed to a multiclass SVM to create nonlinear classifiers by adopting the kernel trick. The proposed method was tested with bench mark datsets. The suggested approach effectively identifies activities while utilising minimal hardware resources.

[18] proposed 1D-CNN architecture based HAR detection framework. This framework was validated using UTD-MHAD dataset. This study addressed two major issues of HAR such as high level activity recognition and reduction of computational cost to configure in embedded devices. The proposed architecture achieved 84% accuracy that is higher than the baseline study.

Using inertial sensor signals, which have a wide range of real-world applications in areas like sports analysis and human-machine interactions, we address human action recognition in this work. In order to achieve this, we suggest a 1D-CNN architecture centered brand-new learning framework. Further, this was evaluated and obtained excellent results on the freely accessible UTD-MHAD dataset. Additionally, the suggested approach offers some solutions to two of the biggest problems action recognition algorithms now face, namely (1) the decrease of their computing cost and (2) the identification of high-level activities in order to make them usable by embedded devices. The accuracy,

clarity, and hardware compatibility of the proposed solution will need to be improved in further studies, therefore this research also looks at the tractability of the features across the proposed framework in terms of time and length.

To develop a device free activity recognition system this study [16] proposed EI, a deep-learning based framework that can overcome the environment and subject specific information that is hidden in activity data. Furthermore, With the help of this framework, data on various subjects in various environments is shared in a way that is independent of the environment or the subject. Fot the evaluation purpose this study performed in-depth tests using ultrasound, visible light, WiFi and 60 GHz mmWave on four separate test beds for device-free activity identification. The experimental findings prove the suggested EI framework's higher efficacy and generalizability.

3 Proposed Method for HAR

This section demonstrates the details of research methodology used for HAR from smartphone sensors. Transformers Models are a type of deep learning models that are based on the self-attention mechanism, which was first introduced in the paper "Attention Is All You Need" by Ashish Vaswani et al. Transformers are used to process natural language for tasks such as machine translation, text summarization, question answering, and more. Transformers can encode a sentence into a fixed-length vector and then decode it into a different language or summarize it. The proposed method is evaluated using UCI-HAR, WISDM and PAMAP2 Dataset. The complete and high level elaboration of proposed method is shown in fig. Spyder (Python 3.9.12 64-bit) was used on laptop having 44 GB RAM, Intel(R) Core (TM) i5-3320 M CPU with windows 10 operating system for experimental purpose. The proposed method is described in detail in the following subsections.

3.1 Preprocessing

The raw data gathered by motion sensors needs to be pre-processed in the following ways in order to feed the suggested network with a certain data dimension and increase the model's accuracy.

The sensors worn by the individuals are wireless, and the datasets indicated above are accurate. As a result, some data may be lost while being collected. In order to address this issue, the missing values in this study were filled using the linear interpolation approach.

To avoid training bias as data is collected from channels directly, data normalization is necessary between 0 and 1 as shown in given equation: Xi = Xi - Ximin/Ximax - Ximin (i = 1,2,...n) where n denotes the number of channels, and xi max, xi min are the maximum and minimum values of the i - thchannel, respectively.

Data segmentation In this study for HAR an end to end model was implemented. The model received the data sequence as input. Raw sensor data were used to create this sequence. Throughout the data collection process, the data were continuously captured. The motion sensor data was segmented using a sliding window with a 50.

3.2 Datasets

In this study three publicly available datasets were employed. The are UCIHAR, WISDM and MHealth. Detail is given below:

3.2.1 UCI-HAR Dataset

UCI-HAR Dataset [3]: This dataset is publicly available in UCI repository for activity recognition. Thirty participents were participated in data collection experiment. The smartphone was wore around waist and each participant performed six activities including walking, walking upstairs, walking downstairs, laying, sitting and standing. Data was collected using gyroscope and accelerometer signals by setting sampling rate 50 Hz. Nine time series features were considered such as total acceleration, gyroscope signals and body acceleration. The window size was 2.56 with almost 50% overlap in a total 10,299 number of samples. For training purpose 21 volunteers and for test purpose 9 volunteer parcipated. There are 7352 samples in the training and 2947 samples in the test set.

3.2.2 WISDM Dataset

This Dataset [23] was released by Fordham University's Wireless Sensor Data Mining team. Thirtysix people participated in in data collection experiment and collected six different activities including sitting, walking, upstairs, downstairs, jogging and standing. Accelerometer was used to collect data at 20 Hz sampling rate. The dataset's values were normalised so that they fall between 0 and 1 (Fig. 3).

Fig. 3. Illustrates three different activities performed by three different subjects at lying down, cycling and waist bends forward positions. The Shimmer2[BUR10] wearable was employed by using elastic strap.

3.2.3 MHEALTH Dataset

This dataset was collected by Rafael Garcia, Alejandro Saez and Oresti Banos and can be freely downloadable from UCI Machine Learning Repository [6]. It contains vital signs and body motion recordings of 12 participants having diverse profile [6]. These individuals engaged in 12 exercises, including sitting motionless, lying down, walking, climbing stairs, bending forward at the waist, raising their arms in front of them, cycling, jogging, and jumping forward and backward. To measure the participants s rate of turn, magnetic field and acceleration was calculated. Accelerometer, magnetometer and gyroscope sensors were placed on body. For the recordings Shimmer2 [BUR10] wearable sensors were used.

3.3 Features Extraction

Table 1.

3.4 Class Imbalance Overcoming

This section presents the impact of over-sampling the minority class activities on proposed methods. Class imbalance occurs when the classes in a dataset are unequally distributed. Class imbalance is very common in medical diagnosis fraud detection and in activity detection. In datasets employed in this study walking and running have higher occurrences as compare to other activities. This can lead to problems when training machine learning models because a large proportion of the data will be from one class, resulting in skewed results. To address this issue, the SMOTE (Synthetic Minority Oversampling Technique) can be used to create synthetic data points for the minority class in order to balance the dataset. This study over-sampled the training data to improve the data distribution of these minority activities. We resampled the dataset once using percentage value equal to 100 and nearest neighbour equal to 5. Tables 8 and 9 shows the performance results of resampled datasets.

In SMOTE, the minority class is oversampled by creating "synthetic" examples that are combinations of existing examples from the minority class. The idea is to increase the number of examples in the minority class by generating new data points that are similar to existing data points in the minority class. The algorithm works by selecting a random example from the minority class and then generating a new data point that is a randomly chosen combination of features from the selected example and one of its closest neighbors. This process is repeated until the desired number of synthetic examples has been generated. SMOTE can be used to overcome class imbalance in datasets and help machine learning models to learn more effective decision boundaries. By creating synthetic examples for the minority class, the dataset is more balanced and the model is less likely to be biased towards the majority class.

By applying the SMOTE algorithm, we observed a marginal increase in performance on the training data. The use of SMOTE algorithms makes the system more efficient by 97.17% F-measure, 97.18% recall, 97.89% accuracy and 98.44% AUC. Moreover, the changes in sensors placement gave the similar improvements. This demonstrates how SMOTE algorithms have benefited the activity detection system [6]. When the SMOTE

Table 1. Datasets Details

	UCI-HAR	WISDM	MHEALTH
Sensors	gyroscpe and accelerometer	Accelerometer	accelerometer, magnetometer, gyroscopes
Placement Positions	wore around waist	Smartphone	smartphone
Performed Physical Activities	walking, moving from one level to another, lying, sitting, and standing	sitting, walking, upstairs, downstairs. Jogging and standing	Walking, climbing stairs, bending forward at the waist, raising the arms in front of you, cycling, jogging, running, jumping forward and backward, etc.
Number of Total Activities	6	6	12
Number of Total Participants	30	36	9
Sampling Rate	50 Hz	20 Hz	100 Hz
Total No of features			52
Window Type and Size	2.56	-	-

technique was used in Dataset 2 to boost the data distribution among activity classes, the performances of feature-level fusion and multi-view stacking ensemble also improved. In multi-view stacking methods, the highest accuracies of 99.18%, 99.13%, and 99.05% were shown utilising the ankle placement in three multi-view stacking experiments.

3.5 Transformer Model

The transformer model was initially created to be used for machine-level translation. With its efficient performance this model replaced Recurrent Neural Network (RNN) and became popular in Natural Language Processing (NLP). The self-attention mechanism, a separate internal attention mechanism used by the transformer model, prevents processing of any sort of recurrence. For a given data linear transformation applies to generate significant features.

It consists of two components: an encoder and a decoder. The encoder encodes a sequence of words into a sequence of vectors, while the decoder decodes the vector sequence into a sequence of words. Encoder encodes feature vectors into X = (x1, . . . , xT) and decoder decodes encoded feature illustrations into W = wm = (w1, . . . , wM). The transformer uses attention mechanisms to learn the relationship between words in the input and output sequences. It does not need to iterate over each word in

the sequence. The transformer model is autoregressive, meaning that each stage receives as input the output of the stage before it, and each block includes several self-attention layers connected to one another. Encoder and decoder blocks operated separately.

Traditional speech recognition models employed attention mechanisms comprised of simple encoder and decoder blocks. In this traditional model sensor data is converted into alternative signal then the decoder decode it further. The significant part of signal is highlighted using attention mechanism. The transformer model differs from all of these conventional models in that it includes many encoders and decoders, as well as internal self-attention mechanisms in each block that are linked together.

As per studies six layers of coders are piled from top to bottom in each encoder of transformer model. Each encoder have different number of coder layers and each coder have same structure. In a given block coder structure is same but weight can be different. Frequency coefficients or convolutional neural networks are frequently used to extract features for the encoder of the transformer model. Each encoder in a series completes a similar task, extracts features, converts them into an alternative signal, and feeds altered vectors to the following encoder via a basic artificial neural network. Finally, the last encoder transmit the transformed vector to decoder.

The decoder and encoder blocks have same number of layers arranged in a sequence. Same like encoder decoder also have two layered architecture. First layer transform feature vectors into vector from the given input. These encoded vectors are supplied to the subsidiary encoder via the second layer. There is an additional attention layer in decoder to highlight the significant part of signal. Prior data is used by attention layer to predict the given signal. The same process is used for each word of the statement before the second layer outputs the posterior probabilities of the decoded words or characters.

The self-attention mechanism is a key component of the transformer model. It allows the model to learn contextual relationships between words in a sentence, leading to improved performance. Self-attention works by allowing the model to attend to a specific token or phrase in a sentence, allowing it to better understand the context of that phrase or token. This mechanism helps the model learn to better capture long-range dependencies, which are important for understanding the meaning of a sentence.

The self-attention mechanism in the Transformer model allows it to automatically learn a representation of a sentence by attending to different parts of the sentence at the same time. In the Transformer, the self-attention mechanism is implemented through a Multi-Head Attention (MHA) layer, which is composed of multiple attention heads (e1, $\cdots$, eH). The MHA layer takes three inputs: the query (Q), key (K) and value (V) vectors, which are generated from the input and the Transformer's internal parameters. The self-attention mechanism is then applied to these vectors, and the outputs of the different heads are combined using a matrix W to generate a single output vector. This output vector is then used as an input to the Transformer's other layers, allowing it to generate a representation of the input sentence.

4 Experiments

This study employed three different publicly available datasets. The data was split into 80-20 ratio. The 80% feature set was applied for training of transformer model and remaining 20% feature set was applied for test purpose. Scientific research proposed that 70–80% use of data for training purpose and rest 0f 20–30% for test purpose produce excellent results. This split method produce accurate and genuine results and avoid over estimation. The proposed model produced 100% accuracy in training phase for all three datasets. This model reduced the loss and enhance the accuracy for all three datasets that shows the effectiveness and significance of proposed model.

4.1 Experimental Setup I

Table 2.

UCI-HAR Dataset			
Activities	Precision	Recall	F1-Score
1	0.97	0.99	0.95
2	0.92	0.99	0.95
3	0.95	0.99	0.97
4	0.88	0.98	0.93
5	0.89	0.94	0.93
6	0.98	0.97	0.97

Table 2. WISDM dataset

Performance of Proposed HAR Model			
Activities	Precision	Recall	F1-Score
Downstairs	0.84	0.90	0.87
Jogging	0.97	0.99	0.98
Sitting	0.99	0.98	0.98
Standing	0.97	0.98	0.98
Upstairs	0.91	0.81	0.86
Walking	0.98	0.99	0.98

4.2 Experimental Setup II

Figs. 4 and 5.

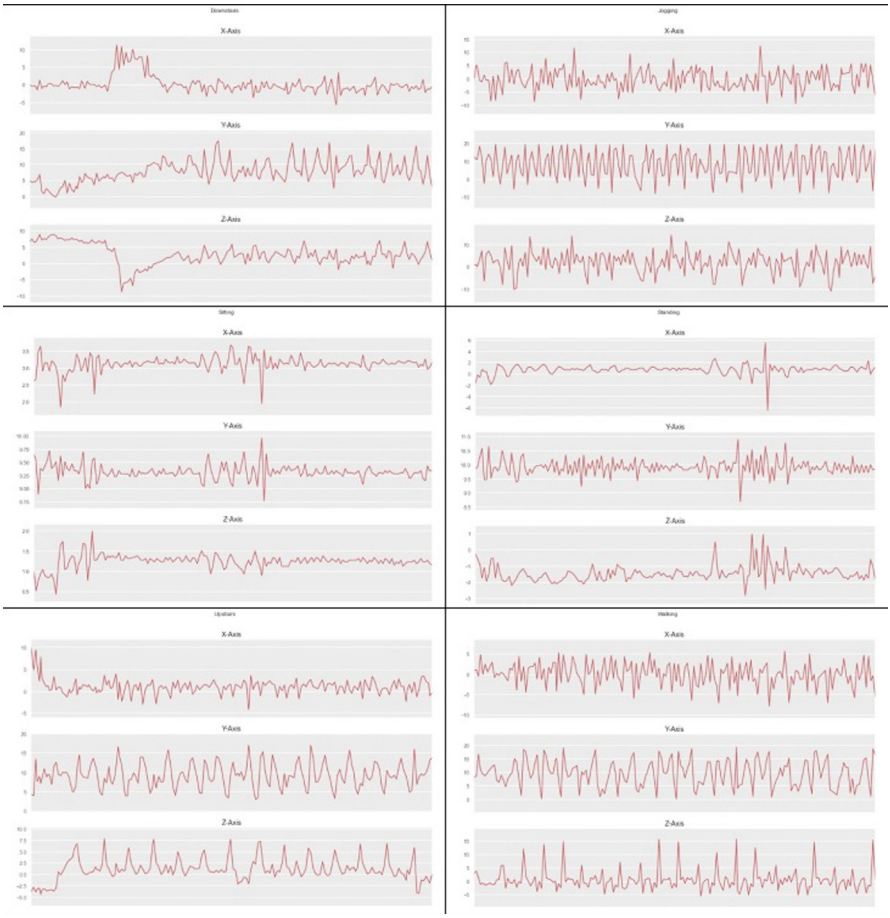


Fig. 4. Training of WISDM Dataset

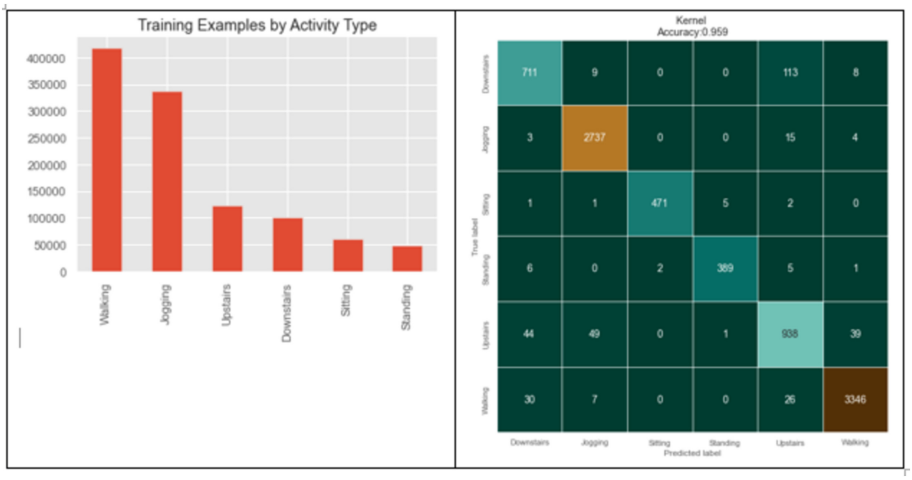


Fig. 5. Training Sample and Confusion matrix of WISDM Dataset

4.3 Experimental Setup III

MHealth Dataset			
Activities	Precision	Recall	F1-Score
0	0.87	0.39	0.54
1	0.86	0.99	0.92
2	0.92	0.99	0.95
3	0.95	0.99	0.97
4	0.88	0.99	0.93
5	0.89	0.94	0.92
6	0.97	0.97	0.97
7	0.97	0.99	0.98
8	0.99	0.93	0.96
9	0.99	0.99	0.99
10	0.99	0.83	0.90
11	0.84	0.99	0.91
12	0.90	0.98	0.93

5 Evaluation Metrics

Accuracy, F1-score, precision, and recall were the four evaluation measures we used to assess and compare the performance of the HAR model. For the evaluation of various HAR classification and associated systems, these evaluation measures have been

commonly used 40]. The confusion matrix of each prediction was used to calculate the performance of each emotion class. A confusion matrix is a table that shows false negatives (FN), false positives (FP), and true negatives (TN), true positives (TP), depending on how effectively the classifier predicts (Fig. 6 and Table 3).

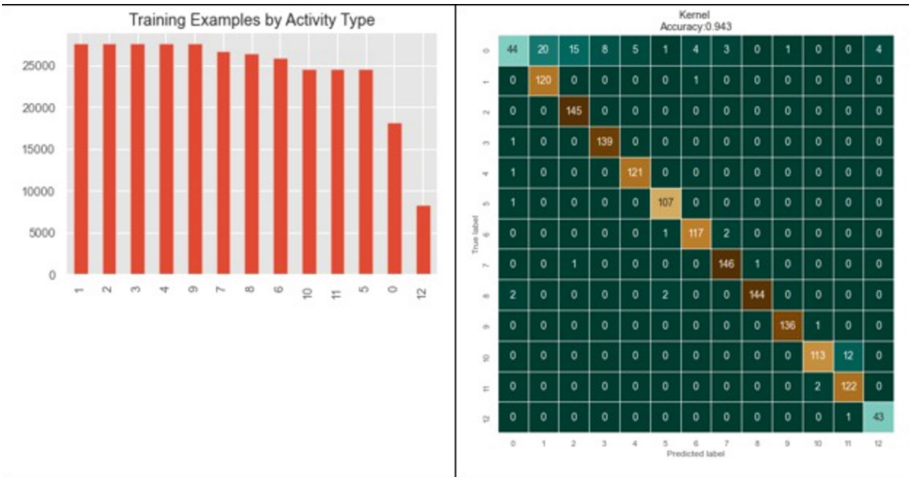


Fig. 6. Training Sample and Confusion matrix of MHEALTH Dataset

Table 3. Evaluation Metrics

Confusion Matrix		
	Actual Instances FP	TN
Predicted Instances		
Yes	TP	FN
No	FP	TN

5.1 Accuracy

Accuracy means to find the correctly predicted values out of total no of values. Higher the value of accuracy means model is working efficiently. Accuracy = True Positive/(True Positive+True Negative)*100 where N is the total no of values.

5.2 Recall

A recall can be computed as the ratio of true positive values and the total number of true positive instances and false negative instances. It demonstrates how comprehensive the classification model is.

Recall= TruePositives/(TruePositives + FalseNegatives)

5.3 Precision

Precision is computed as the ratio of true positive instances instances and the total number of true positive instances and false negative instances. It demonstrates the model's factualness.

Precision= TruePositives/(TruePositives + FalsePositives)

5.4 F1-Score

When dataset is imbalance to determine class-wise accuracy F1-score is generally employed. The weighted harmonic mean of recall and precision is defined as the F1-score. F1 Score= (2*((precision*recall)/(precision+recall)))

6 Experiments

In experimental phase this study used three publicaly available datasets for HAR. For the evaluation of HAR models percentage split technique was applied where the 20% of dataset was used for test and remaining 80% was used for training of CNN model. According to scientific studies [43], the best performance is obtained when 20–30% of the dataset is used for testing and the remainder 70–80% for training. Within the model. A genuine accuracy was produced by this split method and there is no report of overestimated accuracy. 100% accuracy was achieved for the training of all datasets except UCI-Har where 98% was achieved. This study proposes CNN models, which show the significance and efficacy of the suggested method for all four databases by increasing accuracy and reducing loss for both training and testing samples. Model Prediction Performance

7 Discussion

For experiments three publicly available datasets including UCI-HAR, WISDM and MHEALTH were employed. All these datasets considered all the common activities that a user perform in his daily life. It should be highlighted that the database employed for this work does not have an evenly distributed number of samples for training and testing different activities. There are some activities that employ a lot of samples, while there are others which use very few samples. In order to determine whether the performance of the models discussed above would match expectations, this study conducted a number of experiments to carefully assess their performance. The experimental results are illustrated in section 5. This section presents the theoretical analysis of HAR techniques employed in this study. The findings show that the suggested method in combination with the transformer model can reach accuracy greater than 98%. The recommended features with an 80-20% training to testing ratio offered the highest level of accuracy, as seen by the results (Table 4).

Table 4. Evaluation Metrics

Metric	Description	Formula
Accuracy	The amount of accurately labelled data is its accuracy. It determines all properly known occurrences	$Accuracy = ((TP + TN))/((TN + TP + F$
Precision	It measures the proportion of accurate positive guesses to all positive guesses. It reduces errors made while speculating on positive labels	$Precision = TP/(FP + TP)$
Recall	It is the proportion of overall positive labels to accurate positive guesses. True positive rate (TPR) is another name for it	Recall=TP/(FN+TP)
F1-Score	The harmonic mean of precision and recall is used to calculate the F1-Score, a metric for test accuracy. When there are only two possible outcomes (true or false) in a binary classification task, it is used to assess a model's accuracy	F1-Score = 2 * (precision * recall)/(precision + recall)

8 Conclusion

The suggested solution uses smartphone accelerometer and gyroscope data to precisely identify human activities. A CNN model is trained on an augmented dataset to improve performance after it is used to recognise activities from the sensor data using a transformer model. By introducing random noise and shifts to the original data, the augmented dataset is produced. On three publicly accessible datasets, including UCI-HAR, WISDM, and MHealth, the model's performance is assessed. The findings show that in terms of precision, recall, and F1-Score, the suggested system performs better than the state-of-the-art techniques. With an accuracy of over 97% across all datasets, the system is capable of identifying a wide range of actions, including walking, running, jumping, sitting, and standing.

References

1. Aggarwal, J.K., Ryoo, M.S.: Human activity analysis: a review. Acm Computing Surveys (Csur) **43**(3), 1–43 (2011)
2. Ahmad, Z., Khan, N.: Human action recognition using deep multilevel multimodal (M2) fusion of depth and inertial sensors. IEEE Sensors Journal **20**(3), 1445–1455 (2019)
3. Ahmed, N., Rafiq, J.I., Islam, M.R.: Enhanced human activity recognition based on smartphone sensor data using hybrid feature selection model. Sensors **20**(1), 317 (2020)
4. Atrey, P.K., Kankanhalli, M.S., Oommen, J.B.: Goal-oriented optimal subset selection of correlated multimedia streams. ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM) **3**(1), 2–es (2007)

5. Avci, A., Bosch, S., Marin-Perianu, M., Marin-Perianu, R., Havinga, P.: Activity recognition using inertial sensing for healthcare, wellbeing and sports applications: A survey. In: 23th International conference on architecture of computing systems 2010, 1–10. VDE (2010)
6. Banos, O., et al.: mhealthdroid: a novel framework for agile development of mobile health applications. In: International workshop on ambient assisted living, pp. 91–98. Springer (2014)
7. Bao, L., Intille, S.S.: Activity recognition from user-annotated acceleration data. In: International conference on pervasive computing, pp. 1–17. Springer (2004)
8. Campbell, A., Choudhury, T.: From smart to cognitive phones. IEEE Pervasive Comput. **11**(3), 7–11 (2012)
9. Chen, Y., Shen, C.: Performance analysis of smartphone-sensor behavior for human activity recognition. Ieee Access **5**, 3095–3110 (2017)
10. Chen, Z., Zhu, Q., Soh, Y.C., Zhang, L.: Robust human activity recognition using smartphone sensors via ct-pca and online svm. IEEE Transactions on Industrial Informatics **13**(6), 3070–3080 (2017)
11. Clarkson, B.P.: Life patterns: structure from wearable sensors. PhD thesis, Massachusetts Institute of Technology (2002)
12. Cornacchia, M., Ozcan, K., Zheng, Y., Velipasalar, S.: A survey on activity detection and classification using wearable sensors. IEEE Sensors Journal **17**(2), 386–403 (2016)
13. Golestani, N., Moghaddam, M.: Human activity recognition using magnetic induction-based motion signals and deep recurrent neural networks. Nat. Commun. **11**(1), 1–11 (2020)
14. Hassan, M.M., Uddin, M.Z., Mohamed, A., Almogren, A.: A robust human activity recognition system using smartphone sensors and deep learning. Future Generation Computer Systems **81**, 307–313 (2018)
15. Hong, J.-H., Ramos, J., Dey, A.K.: Toward personalized activity recognition systems with a semipopulation approach. IEEE Transactions on Human-Machine Systems **46**(1), 101–112 (2015)
16. Jiang, W., et al.: Towards environment independent device free human activity recognition. In: Proceedings of the 24th annual international conference on mobile computing and networking, pp. 289–304 (2018)
17. Lara, O.D., Labrador, M.A.: A survey on human activity recognition using wearable sensors. IEEE Communications Surveys & Tutorials **15**(3), 1192–1209 (2012)
18. Lemieux, N., Noumeir, R.: A hierarchical learning approach for human action recognition. Sensors **20**(17), 4946 (2020)
19. Lin, W., Sun, M.-T., Poovandran, R., Zhang, Z.: Human activity recognition for video surveillance. In: 2008 IEEE international symposium on circuits and systems, pp. 2737–2740. IEEE (2008)
20. Mannini, A., Sabatini, A.M.: Machine learning methods for classifying human physical activity from on-body accelerometers. Sensors **10**(2), 1154–1175 (2010)
21. Murad, A., Pyun, J.-Y.: Deep recurrent neural networks for human activity recognition. Sensors **17**(11), 2556 (2017)
22. Mutegeki, R., Han, D.S.: A cnn-lstm approach to human activity recognition. In: 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), pp. 362–366. IEEE (2020)
23. Ni, J., Ma, X., Xu, L., Wang, J.: An image recognition method based on multiple bp neural networks fusion. In: International Conference on Information Acquisition, 2004. Proceedings, pp. 323–326. IEEE (2004)
24. Nweke, H.F., Teh, Y.W., Mujtaba, G., Alo, U.R., Al-garadi, M.A.: Multi-sensor fusion based on multiple classifier systems for human activity identification. Human-centric Computing and Information Sciences **9**(1), 1–44 (2019)

25. Ravi, D., Wong, C., Lo, B., Yang, G.-Z.: A deep learning approach to on-node sensor data analytics for mobile or wearable devices. IEEE J. Biomed. Health Inform. **21**(1), 56–64 (2016)
26. Wan, S., Qi, L., Xiaolong, X., Tong, C., Zonghua, G.: Deep learning models for real-time human activity recognition with smartphones. Mobile Networks and Applications **25**(2), 743–755 (2020)
27. Wang, L., Gu, T., Tao, X., Chen, H., Lu, J.: Recognizing multi-user activities using wearable sensors in a smart home. Pervasive Mob. Comput. **7**(3), 287–298. Elsevier (2011)
28. Wu, Z., Cai, L., Meng, H.: Multi-level fusion of audio and visual features for speaker identification. In: International Conference on Biometrics, pp. 493–499. Springer (2006)
29. Yadav, S.K., Tiwari, K., Pandey, H.M., Akbar, S.A.: A review of multimodal human activity recognition with special emphasis on classification, applications, challenges and future directions. Knowledge-Based Systems **223**, 106970 (2021)
30. Zhou, X., et al.: Deep-learning-enhanced human activity recognition for internet of healthcare things. IEEE Internet of Things Journal **7**(7), 6429–6438 (2020)

Usability Impact of Conversational Chatbot

Maryam Rasheed[1], Muhammad Waseem Iqbal[2(✉)], Anam Fatima[1], Maryam Saleem[1], Sohail Masood Bhatti[1], and Muhammad Junaid Ahsan[1]

[1] Department of Computer Science, Superior University Lahore, Lahore 54000, Pakistan
{sohailmasood,MSCS-f20-039}@superior.edu.pk
[2] Department of Software Engineering, Superior University Lahore, Lahore 54000, Pakistan
Waseem.iqbal@superior.edu.pk

Abstract. The resurgence of the chatbot has been facilitated by recent developments in machine learning. Recently, chatbot technology has been more widely available on the web and on mobile devices. According to recent statistics, 57% of businesses have already used or plan to execute a chatbot in the close to future. As a result, chatbots will be crucial in a future powered by AI. The goal of chatbots, which can be text-based computer systems, is to mimic human communication skills. In numerous industries, including customer service, e-coaching, and entertainment, they are spreading like wildfire. The effectiveness of these virtual agents cannot yet be evaluated in a consistent manner. As an alternative, a variety of individuals and groups have developed their guiding principles, either exclusively for their chatbot project or with some inspiration from other groups. In this paper, we explore the trends and evaluation techniques currently in use for chatbots. We investigate chatbot evaluation techniques and rank them in accordance with the ISO 9214 usability characteristics of efficiency, effectiveness and satisfaction. After that, we examine the techniques applied in the literature between 1970 and 2022 and contrast the outcomes. We find a clear trend toward examining the efficacy of chatbots in several recent studies, which is likely due to the growing popularity of task-based chatbots, which are increasingly being deployed in many business situations.

Keywords: text-based chatbot · systematic literature review · human-computer interaction

1 Introduction

1.1 Chatbots

A chatbot is essentially computer software that simulates and studies human interaction, enabling users to have conversations with digital gadgets that sound natural [1]. Chatbots can range from being as simple as one-line scripts that respond to straightforward questions to being as complex as virtual assistants that evolve in time to provide a growing number of specialized services as they collect and analyze more data [2]. Chatbots will make it simple for users to access the information they require by responding to

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 191–204, 2025.
https://doi.org/10.1007/978-3-031-77620-5_13

their text, audio, or both, queries and requests from users without the need for human assistance. Both household smart speakers and business messaging platforms employ chatbot technology today. The most sophisticated AI chatbots are frequently referred to as virtual assistants or virtual agents [3]. Text messages or voice assistants like Apple's Siri, Google Assistant, or Amazon's Alexa can be used to converse with them.

1.2 Types of Chatbots

The following are a few examples of popular chatbot types:

- **Scripted or quick reply chatbots**: Businesses can save up to $8 by using chatbot services, it has been found. They operate as a hierarchical decision tree and represent the most basic type of chatbot. These chatbots engage consumers in conversation by asking pre-written questions, which they continue to do until the user receives a response. The menu-based chatbot is similar to this one in that it asks users to choose alternatives from enabled organizations or menus in reorganization to better understand the user's wants.
- **Keyword recognition-based chatbots:** According to studies, businesses can save $8 per year by adopting chatbot services. These chatbots are a little more sophisticated; they try to decipher what the user is typing and reply with words taken from consumer feedback. This bot mixes artificial intelligence with user-customizable keywords to deliver pertinent answers. Regrettably, these chatbots have trouble handling commonly requested inquiries or overused jargon (Fig. 1).
- **Hybrid chatbots:** Companies have been shown to save an estimated $8 using chatbot services. The components of menu-based and keyword recognition-based chatbots are combined in these systems. Users have the option of having their questions answered directly or using the chatbot's menu if keyword detection is failed.
- **Contextual chatbots:** Companies have been shown to save an estimated $8 using chatbot services. These chatbots need to be more data-centric because they are more complicated than others. They evolve and get better over time by using the discussions and interactions that users have with them that are remembered by AI and ML. These bots don't rely on keywords; instead, they learn from and adapt to the questions and queries that they receive from users.
- **Voice-enabled chatbots:** The future of this technology is chatbots like this one. Users' speech is used as input by voice-enabled chatbots to generate unique thoughts or responses. These chatbots can be developed by programmers using text-to-speech and voice recognition APIs. Apple's Siri and Amazon Alexa are two examples [4].

1.3 Architecture and Working of Chatbots

To respond to user inquiries via text, graphics, and voice, a chatbot's design needs a candidate response generator and response selector.

The three methods of classification that chatbots employ are as follows:

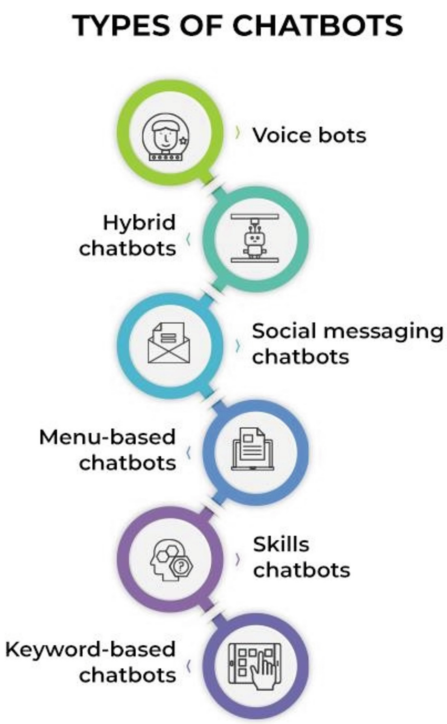


Fig. 1. Types of chatbots

1.3.1 Pattern Matches

Bots organize text using pattern matching, asking users for the appropriate response. A well-liked structured form of these Patterns is Artificial Intelligence Markup Language (AIML) (Fig. 2).

```
<aiml version="1.0"encoding="UTF-8"?>
        <category>
                <pattern> WHO INVENTED EMAIL</pattern>
                <template>according to google Ray Tomlinson invented email.</template>
        <category>


        <category>
                <pattern> DO YOU KNOW WHO * IS</pattern>
                <template>
                        <srai>WHO IS <stat/></srai>
                <template>
        </category>
</aiml>
```

Fig. 2. Simple pattern matching examples

Who was the person who created email the? Google claims that Ray Tomlinson invented email.

The chatbot can respond correctly because the person's name appears in the pertinent pattern. When faced with anything related to the correlation patterns, the chatbots react identically. But the same pattern places a limit on it. It can be advanced to a later stage with the use of algorithms.

For each sort of query, the database needs to have a notable pattern in order to deliver an appropriate answer. It creates a hierarchy with numerous pattern combinations. We employ methods to simplify the classifiers and produce a framework that makes more sense (Fig. 3)

1.3.2 Natural Language Understanding (NLU)

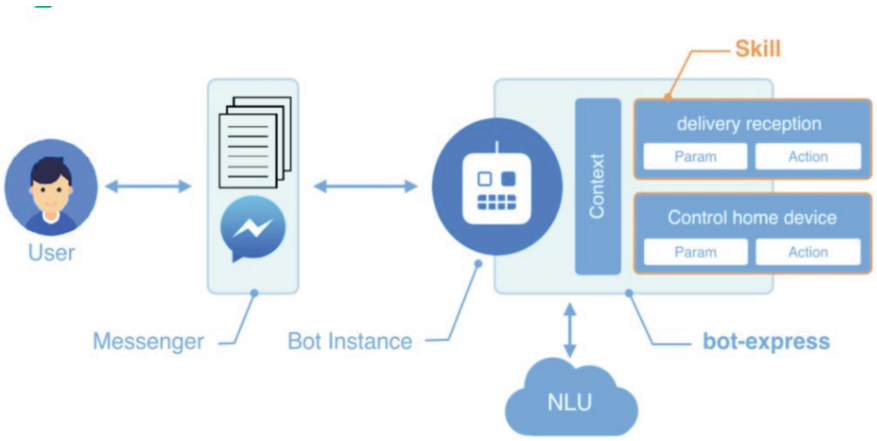


Fig. 3. Natural Language Understanding Structure

These 3 particular NLU principles are listed below.

Entities: In essence, your chatbot interprets this as an idea. For instance, your chatbot for e-commerce can have a payment system.

Context: A natural language understanding algorithm cannot analyse a sentence in the context of the user's text chat. This implies that it won't recall the question it asked if it gets an answer to a recent question it posed. As a result, each stage of the chat dialogue is saved separately. It is possible to utilisanalyzee banners like "Ordering Pizza." As an alternative, you might include other criteria, such as "Domino's: Restaurant." When provided context, you may easily make the connection between expectations and the requirement to comprehend the final question.

Expectations: A chatbot must fulfill these when a customer sends an inquiryare . Many inquiries might have the same answer. The objectives "I want to get a pair of white shoes" and "Do you already own white shoes? Whether you say, "I want to buy these," or "Show me a pair of white shoes," the response will be the same. As a result, the only command seen in every user's text entry is the distinct tag of white shoes.

1.3.3 Natural Language Processing (NLP)

Natural language processing is used by chatbots to transform a user's speech or text into structured data. The appropriate reaction is then selected utilising this knowledge. The following processes are part of natural language processing: The NLP divides a group of words into linguistically suitable tokens or bits, each of which fulfils a particular function in the application. This process is known as tokenization (Fig. 4).

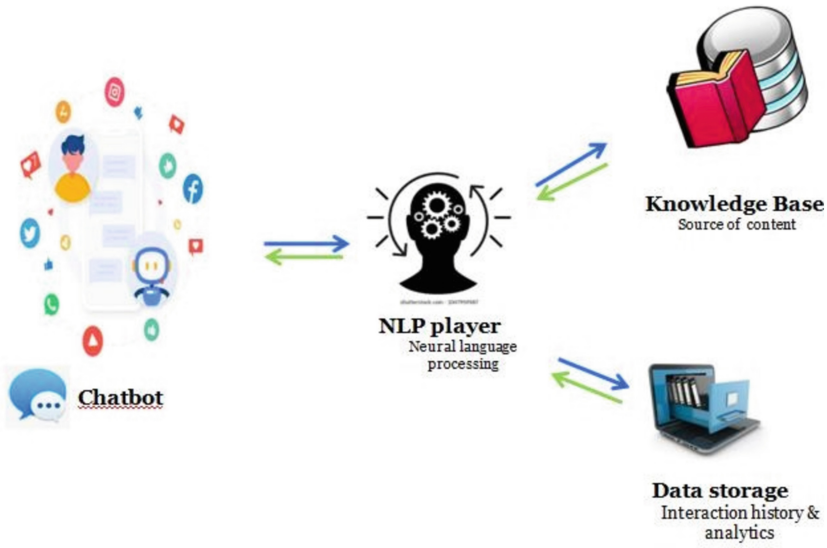


Fig. 4. Natural Language Processing Structure

Sentiment Analysis: When needed, after researching and understanding the user's experience, it will pass the query to a person.

Normalization: This tool analyses the text to find typographical and common spelling errors that could distort the user request's original intent.

Named Entity Recognition: Depending on the information required, a chatbot's programming searches for terms that program into different groups and sound related to the name of the invention in question, the user's address, or their name [5].

Dependency Parsing: To identify related sentences that the user has written, a chatbot searches the user's text for subjects, activities, objects, common phrases, and nouns.

2 Literature Review

The first chatbot, named ELIZA, was developed in 1966 [6]. In 1979, five psychiatrists employed PARRY to assess whether a patient was a computer program or a genuine schizophrenic patient [7, 8]. PARRY is viewed as a chatbot in general who has trouble understanding English and expressing emotions [9]. Jabberwacky, a chatbot that uses pattern-matching to respond to context-based questions [10, 11]. Jabberwackay can manage a small number of users, but it cannot answer quickly. ALICE (Artificial Linguistic

Internet Computer Entity), the first online chatbot inspired by ELIZA, was created in 1995 [13, 14] (Fig. 5).

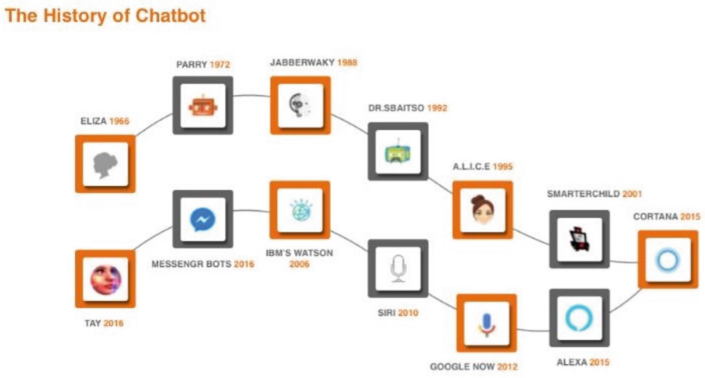


Fig. 5. History of Chatbot [14].

In 2010, Apple developed Siri (Siri), which helped personal assistants gain popularity [15, 16]. The voice-activated personal assistant Cortana was developed by Microsoft in 2014. In the same year, Amazon introduced Alexa, a speech assistant built into home entertainment and automation goods, making the Internet of Things more approachable for users [17]. Despite the information that personal voice assistants allow for voice communication with their users, errors commonly occur as a result of these assistants' inability to comprehend either the exact language used in oral speech by users or the general context of the conversation [18]. Intelligent personal voice assistants built into smart phones or specific home speaker system artificial intelligence chatbots. They could understand voice commands, speak in a computer voice, and manage tasks. Apple Siri, IBM Watson, Google Assistant, Microsoft Cortana, and Amazon Alexa are examples of virtual assistants.

Organizations like the Centers for Disease Control and Prevention (CDC) and the World Health Organization (WHO) have started using chatbots to spread knowledge, provide behaviour recommendations, and provide emotional support in the midst of the current coronavirus (COVID-19) outbreak. Thanks to the CDC, it now has a name. Chatbots are computer programmes that interact with users via text or voice in their own language. "Cortana" from Microsoft, "Alexa" from Amazon, and "Siri" from Apple are a few well-known examples [19]. They are frequently pre-installed on smartphones and smart speakers used at home. The use of chatbots for health-related tasks has significantly increased in recent years, from assisting professionals with clinical interviews and diagnosis to assisting patients in managing chronic diseases on their own. Despite being promising, chatbot use may have security risks. Chatbots have displayed a wide variety in their responses to inquiries about physical health, suicide, intimate relationship violence, substance abuse, and other delicate themes. In one study, 29% of chatbot responses to health-related questions had the potential to be hazardous, while 16% of

them had the potential to be fatal if used. The COVID-19 outbreak has made it clearer than ever before how useful chatbots could be in saving lives [19] (Fig. 6).

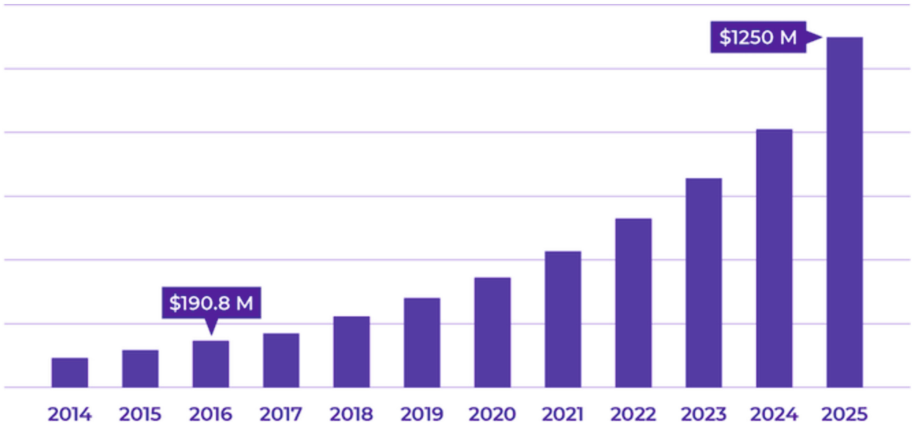


Fig. 6. Investment growing rate on chatbot [20].

By 2025, it is expected that the worldwide chatbot market would bring in $1250 million in revenue. Nearly one-quarter of small businesses utilis chine learning and artificial intelligence techniques, which are the foundation of certain chatbots, to enhance customer communication.

Some industries employ chatbots more frequently than others. For instance, in 2016, the finance and insurance industry's market for chatbots was estimated to be worth $190.8 million. This sum is anticipated utilize increase by 1,0000% to $9.83 billion by 2030.

3 Methodology

The evaluation techniques from 60 papers and articles regarding chatbots that were published between 2016 and 2022 were the main topic of this thesis. They come to several important findings, one of which is that the approaches frequently meet the requirements of ISO 9214, which defines usability as "the effectiveness, efficiency, and satisfaction with which individual users achieve specific goals in certain circumstances." The following explanations and interpretations were presented to these three groups. Whether it is through resistance to manipulation or unexpected input, successful function assignment, moderate degradation, or avoiding wrong utterances, chatbot efficacy is judged by how well they complete their tasks in relation to their goals. Effectiveness is composed of two distinct sub concepts.

The first is functionality, which encompasses qualities like precise linguistic precision, accurate speech synthesizing, correct command interpretation, all-around usability, and problem-solving on-the-fly. The capability to respond to specific inquiries, to be open to inspection, to make errors for added realism, and to pass (or fail) the Turing test is

Table 1. Overview of relatedworks.

Author	Contribution	Limitation
[21]	• Identifies the business ramifications of employing chatbots and discusses developments with regard to various various parties, such as consumers, as well as within the company (internal environment) • identifies areas and applications that need more study • Offers a thorough breakdown of the approaches applied to chatbot research in the context of business	• The study only included journal papers; conference proceedings were left out
[22]	• Without regard to topic or time constraints, offers a thorough overview of more than 30 years of expertise in AI development and marketing • The evolution of marketing and AI was examined with more objectivity	• There is no discussion of the varied effects of AI on marketing
[23]	Identifies the gaps in the literature and creates a comprehensive plan for further research • Identifies the literature gaps and establishes a thorough agenda for future study	• The assessment concentrates on applying AI to provide users with financial services
[24]	• Examines the role played by Chatbot in several business industry verticals during the past ten years	• The study only included search strings containing business terms
[25]	• Outlines the key issues with chatbots that have been overcome in the field of financial technology activities by mapping and classifying a few relevant publications	• The factors affecting the Chatbot are not included in the review

humanity's second goal. There are three distinct satisfaction subgroups. First, affect can be used to greet visitors and demonstrate personality, to give cues during conversations, to share emotional information, to show warmth and sincerity, to make work more interesting and exciting, or to recognize moods. Ethics and behavior cover things like honesty, paying attention to safety and social issues, being dependable, and being aware of trends. They also cover things like respecting, including, and maintaining the dignity of the users, as well as their ethics and cultural knowledge. In addition, accessibility examines if a goal can be behavior understood, whether a reaction to social cues is there, and whether a wider range of needs can be met.

Table 2. Chatbot Evaluation Methods in Relation to ISO 921

ISO	Effectiveness	Efficiency	Satisfaction
4.1	Performance	Functionality, Humanity	Affect, Ethics, Behaviour, Accessibility
4.2	Content eval.	Functional eval.	User satisfaction
4.3	IR perspective	Linguistic persp., AI perspective	User perspective
4.4	Conv. intelligence	Functionality	Chatb. interface, Chatb. personal.
4.5	Domain coverage	Coherence, Conv. breadth, Conv. depth	Conv. UX, Engagement

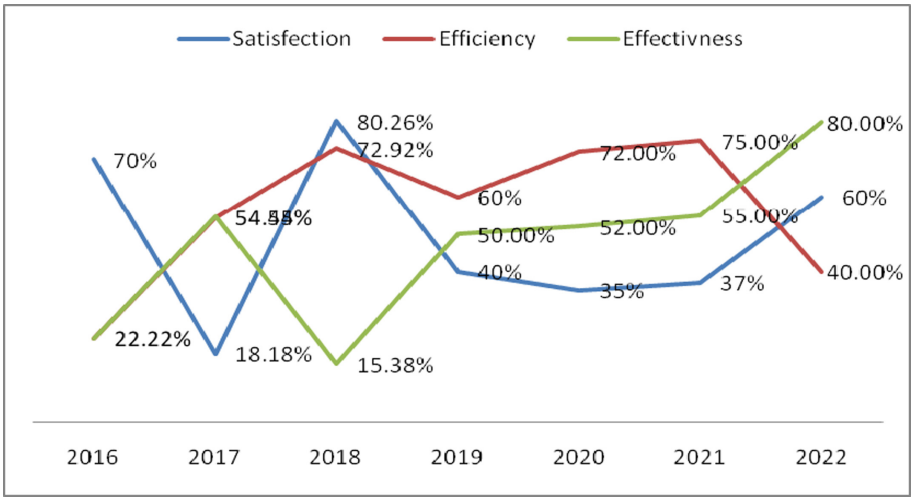
FFICIENCY		
Category	Quality Attribute	Reference
Performance	• Gracefully deteriorating • forcefulness to management • Robustness to unpredicted input • Avoid in appropriate utterance and be able to performd amage control • A useful location that offers people the proper channels for appreciation • Perform similarly to humans on a regular basis, yet they cannot entirely replace people • relating to a dialogue graph, and legal types • investigates how much humanlike cues are used • repetitive human being tasks the operations personnel • Chatbot application deployment platform privacy restriction • Exploratory technique research using an exploratory methodology • Inductive approach was used, where expert opinions were the basis for developing thematic patterns • Analysis of correlation for the automatic response service (ARS) (ANCOVA)	• Cohen&Lane(2016) • Thieltges(2016) • Kluwer(2021) • Morrisseyand Kirakowski(2017)
		• Staven(2017)
		• Mittal, A., Agrawal, A., Chouksey, A., Shriwas, R., & Agrawal, S. (2016) • Merisalo, S. (2018) • Morgan, J., Paiement, A., Seisenberger, M., Williams, J., & Wyner, A. (2018) • Araujo, T. (2018) • Brown-Pobee, J. P. Y. (2019) • As • Illescas-Manzano etal. (2021)
		• Stoeckli et al.(2020)
		• Nayak et al.(2021)
		• Hwang and Kim (2021)

These publications show that there are still differences between the various approaches to evaluate chatbots. However, it appears that Radziwill and Benton's conclusion that the evaluation methods typically fall within the three parameters of the ISO definition of usability is still valid. Therefore, for each of the five publications, we display in Table 1 the categories, viewpoints, and metrics related to the three ISO categories. As chatbots are often solely assessed based on the material they were designed for, these three categories emphasize evaluating the various areas of interest in chatbot research. Effectiveness relates to a more technical perspective, where the methodology underpinning the chatbot's operation is the primary focus of the evaluation and advancement occurs when the efficiency of the underlying algorithms is increased. Efficiency is more strongly related to the chatbot's stated purpose, or whether or not it succeeds in helping businesses, such as customer service, with the work it was designed to do. They can be judged in terms of the objectives they have set because they frequently recycle existing approaches instead than improve them. The measurement of client satisfaction is frequently entwined with these objectives. The objective could also be to deceive the user into believing they are a person. As previously indicated, a satisfaction evaluation typically reflects the aim to gauge user engagement in the chatbot or whether the contact was amicable. Although it has received less focus in recent studies, it is still crucial to advance the widespread use of chatbots in the future (Table 2)

4 Results and Discussion

We thoroughly examined recent research articles and technical reports to get a clear picture of how current research is assessing chatbots. We chose 60 of these articles and examined their evaluation procedures to determine the approaches they employed and which ISO 9214 category they most closely matched. Different approaches are more and less common. Of the 60 articles that were chosen, 20 (40.85%) utilized an evaluation strategy that was at least partially based on how effective their chatbot was, 35 (60.49%) on how efficient it was, and 30 (55.83%) on how satisfied users were with it. Although we see that Efficiency is the most common approach, it is not significantly more so than other methods—the mean of method adoption is 55%15.78%. Effectiveness-based methods are less common but yet not that much less than satisfaction-based methods, which are comparable. But these values change considerably over time.

We assessed nine pieces from 2016. Two-thirds of the papers surveyed that year used satisfaction-based evaluation methods, making them by far the most prevalent. Efficiency-based strategies were only included in 22.22 percent of the studies, whereas effectiveness-based methods were only present in one-third. Efficiency and Effectiveness tied for the top spot in 2017 with 9 papers, scoring 54.55% each, while Satisfaction dropped to just 18.18%. Only 15.38% of the 11 papers published in 2018 employed effectiveness-based assessment; instead, 80.26% used satisfaction-based approaches, and 72.92% used efficiency-based methods. 2019's 10 papers had a 60% efficiency check, a 50% effectiveness check, and a 40% satisfaction check. Out of 15 papers reviewed at the time of this study in 2020 and 2021, 75% rated efficiency, 55% rated satisfaction, and 35% rated effectiveness. Finally, out of 10 papers reviewed at the time of this study in 2020, 80% rated efficiency, 60% rated satisfaction, and 40% rated effectiveness.



We find that the most frequently used criterion for assessing chatbots is efficiency. This has been especially true in recent years since there appears to have been an increase in its popularity since the start of our study. Although the popularity of satisfaction varies greatly from year to year, it is still possible to identify some general trends. Effectiveness is a less used metric yet, perception of 2018, is largely consistent.

5 Conclusion

In this study, we examined many articles on chatbot evaluation methodology as well as 60 additional contemporary studies analyzing chatbots that were released between 2016 and 2020. We gathered a variety of perspectives on chatbot evaluation, reclassified them into groups that were consistent with the usability idea defined in ISO 9214, and clarified the meaning of each group. We then went back to the studies and separated their evaluation methodologies into three groups in order to detect recent trends in chatbot evaluation. Again, we discovered that efficiency-based chatbot evaluation methodologies are favored for the time period we are taking into consideration, with satisfaction-based methods coming in a close second. Every year, there were considerable differences in how these categories were distributed, with only Efficiency-based techniques clearly demonstrating a progression.

Additionally, we found that a small majority of studies only utilized one assessment technique to gratinate their chatbot, particularly when Effectiveness was the main topic of their investigation. The most common combination for articles that used two separate types of eval uation was Efficiency and Satisfaction. These findings led us to the conclusion that, perhaps due to the lack of a gold standard, there isn't a particular evaluation technique that appears to be more frequently in articles about chatbots. However, some approaches are more well-liked in certain fields and go well with certain types of research.

For instance, we wish to assess a task-based chatbot's capacity to do a particular task. Another illustration is research papers that try to improve natural language processing

methods and assess them using a chatbot. Since user satisfaction and task completion are less crucial in this situation, the evaluation is solely on effectiveness. The largest change we noticed was the growing popularity of efficiency evaluation methods. During the study period, the efficacy and satisfaction criteria were too erratic to allow for just any conclusions. One more thing I noticed is that a lot of publications don't seem to evaluate their chatbots at all; instead, they just present the work that has been done without putting it to the test.

References

1. Kim, S., Lee, J., Gweon, G.: Comparing data from chatbot and web surveys effects of platform and conversational style on survey response quality. Conf. Hum. Factors Comput. Syst. Proc. 1–12 (2019)
2. Kocabalil, A.B., Laranjo, L., Coiera, E.: Measuring user experience in conversational interfaces: a comparison of six questionnaires (2018)
3. López-Cózar, R., Callejas, Z., Espejo, G., Griol, D.: Enhancement of Conversational Agents by Means of Multimodal Interaction. Conversational Agents and Natural Language Interaction: Techniques and Effective Practices: Techniques and Effective Practices, pp. 223–252 (2011)
4. Dawson, J.: Visual attention during conversation: an investigation using real-world stimuli, Doctoral dissertation. University of Essex (2022)
5. https://www.crayondata.com/how-do-chatbots-work-an-overview-of-the-architecture-of-a-chatbot/
6. Lankton, N., McKnight, D. H., Michigan State University, Tripp, J., Baylor University: Technology, Humanness, and Trust: Rethinking Trust in Technology. Journal of the Association for Information Systems **16**(10), 880– 918 (2015). https://doi.org/10.17705/1jais.00411
7. Przegalinska, A., Ciechanowski, L., Stroz, A., Gloor, P., Mazurek, G.: In bot we trust: a new methodology of chatbot performance measures. Bus. Horiz. **62**(6), 785–797 (2019). https://doi.org/10.1016/j.bushor.2019.08.005
8. Colby, K.M., Hilf, F.D., Weber, S., Kraemer, H.C.: Turing-like indistinguishability tests for the validation of a computer simulation of paranoid processes. Artif. Intell. **3**, 199–221 (1972)
9. Jwala, K., Sirisha, G.N.V.G., Raju, G.P.: Developing a Chatbot using Machine Learning. International Journal of Recent Technology and Engineering (IJRTE) **8**(1S3), 89–92 (2019)
10. Wallace, R.S.: The anatomy of ALICE. In: Parsing the Turing Test, pp. 181–210. Springer, Dordrecht (2009)
11. Mikolov, T., Sutskever, I., Chen, K., Corrado, G.S., Dean, J.: Distributed representations of words and phrases and their compositionality. Advances in neural information processing systems, 26 (2013)
12. Bradeško, L., Mladenić, D.: A survey of chatbot systems through a loebner prize competition. In: Proceedings of Slovenian language technologies society eighth conference of language technologies, pp. 34–37. Institut Jožef Stefan, Ljubljana, Slovenia (2012)
13. Thakur, S.: Personalization for google now: user understanding and application to information recommendation and exploration. In: Proceedings of the 10th ACM Conference on Recommender Systems, p. 3 (2016)
14. Sabharwal, N., Barua, S., Anand, N., Aggarwal, P.: Building your first bot using Watson assistant. In: Developing cognitive bots using the IBM Watson engine, pp. 47–102. Apress, Berkeley, CA (2020)

15. Nobles, A.L., Leas, E.C., Caputi, T.L., Zhu, S.H., Strathdee, S.A., Ayers, J.W.: Responses to addiction help-seeking from Alexa, Siri, Google Assistant, Cortana, and Bixby intelligent virtual assistants. NPJ Digital Medicine **3**(1), 1–3 (2020)
16. Smith, J., et al.: Orthopaedic shoulder and elbow fellowship directors in the united states have substantial research output but lack diversity. Arthroscopy, Sports Medicine, and Rehabilitation (2022)
17. Chopra, S., Gianforte, R., Sholar, J.: Meet percy: The CS 221 teaching assistant chatbot. ACM Transactions on Graphics **1**(1), 1–8 (2016)
18. Miner, A.S., Laranjo, L., Kocaballi, A.B.: Chatbots in the fight against the COVID-19 pandemic. NPJ digital medicine **3**(1), 1–4 (2020)
19. Davenport, T., Guha, A., Grewal, D., Bressgott, T.: How artificial intelligence will change the future of marketing. J. Acad. Mark. Sci. **48**(1), 24–42 (2020)
20. Adamopoulou, E., Moussiades, L.: Chatbots: History, technology, and applications. Machine Learning with Applications **2**, 100006 (2020). https://doi.org/10.1016/j.mlwa.2020.100006
21. Miklosik, A., Evans, N., Qureshi, A.M.A.: The use of chatbots in digital business transformation: a systematic literature review. IEEE Access **9**, 106530–106539 (2021). https://doi.org/10.1109/ACCESS.2021.3100885
22. Vlačić, B., Corbo, L., et al.: The evolving role of artificial intelligence in marketing: Are view and research agenda. J. Busi. Res. **128**, 187–203 (2021). https://doi.org/10.1016/j.jbusres.2021.01.055
23. Hentzen, J.K., Hoffmann, A., Dolan, R., et al.: Artificial intelligence in customer-facing financial services: a systematic literature review and agenda for future research. Int. J. Bank Mark (2021). https://doi.org/10.1108/IJBM-09-2021-0417
24. Bavaresco, R., Silveira, D., Reis, E., et al.: Conversational agents in business: a systematic literature review and future research directions. Comput. Sci. Rev. 36 (2020)
25. Milian, E.Z., Spinola, M.M., Carvalho, M.M.: Fin techs: a literature review and research agenda. Electron Commer. Res. Appl. 34 (2019). https://doi.org/10.1016/j.el-erap.2019.100833
26. Hahm, Y., Kim, J., An, S., Lee, M., Choi, K.S.: Chatbot Who Wants to Learn the Knowledge: KB-Agent. Semdeep/NLIWoD@ ISWC, 4 (2018)
27. Kumar, V., Rajan, B., Venkatesan, R., Lecinski, J.: Understanding the role of artificial intelligence in personalized engagement marketing. Calif. Manage. Rev. **61**(4), 135–155 (2019)
28. De Cicco, R., e Silva, S.C., Alparone, F.R.: Millennials' attitude toward chatbots: an experimental study in a social relationship perspective. Int. J. Retail and Distribution Manage. **48**(11), 1213–1233 (2020)
29. Sanny, L., Susastra, A.C., Roberts, C., Yusramdaleni, R.: The analysis of customer satisfaction factors which influence chatbot acceptance in Indonesia. Management Science Letters **10**, 1225–1232 (2020)
30. Abd-Alrazaq, A.A., Alajlani, M., Alalwan, A.A., Bewick, B.M., Gardner, P., Househ, M.: An overview of the features of chatbots in mental health: a scoping review. Int. J. Med. Inform. **132**, 103978 (2019). https://doi.org/10.1016/j.ijmedinf.2019.103978
31. Oh, J., Jang, S., Kim, H., Kim, J.J.: Efficacy of mobile app-based interactive cognitive behavioral therapy using a chatbot for panic disorder. Int. J. Med. Inform. **140**, 104171 (2020). https://doi.org/10.1016/j.ijmedinf.2020.104171
32. Araujo, T.: Living up to the chatbot hype: the influence of anthropomorphic design cues and communicative agency framing on conversational agent and company perceptions. Comput. Hum. Behav. **85**, 183–189 (2018). https://doi.org/10.1016/j.chb.2018.03.051
33. Boecker, N., Borsci, S.: Usability of information-retrieval chatbots and the effects of avatars on trust (Bachelor's thesis). University of Twente, Netherlands (2019)

34. Zierau, N., Hausch, M., Bruhin, O., Söllner, M.: Towards developing trust supporting design features for AI-based Chatbots in customer service. International Conference on Information Systems (ICIS). Hyderabad, India (2020). https://www.alexandria.unisg.ch/261540/
35. Følstad, A., Skjuve, M.: Chatbots for customer service: user experience and motivation. Proceedings of the 1st International Conference on Conversational User Interfaces, 1–9 (2019). https://doi.org/10.1145/3342775.3342784
36. Illescas-Manzano, M.D., López, N.V., González, N.A., et al.: Implementation of chatbot in online commerce, and open innovation. J. Open Innovation: Technol. Mark Complexity **7**, 125 (2021). https://doi.org/10.3390/joitmc7020125
37. Stoeckli, E., Dremel, C., Uebernickel, F., et al.: How affordances of chatbots cross the chasm between social and traditional enterprise systems. Electron Mark **30**, 369–403 (2020). https://doi.org/10.1007/s12525-019-00359-6
38. Nayak, B., Bhattacharyya, S.S., Krishnamoorthy, B.: Explicating the role of emerging technologiesand firm capabilities towards attainment of competitive advantage in health insurance service firms. Technol. Forecast Soc. Change **170**, 120892 (2021). https://doi.org/10.1016/j.techfore.2021.120892
39. Hwang, S., Kim, J.: Toward a chatbot for financial sustainability. Sustainability **13**, 3173 (2021). https://doi.org/10.3390/su13063173
40. Kumar, V., Ramachandran, D., Kumar, B.: Influence of new-age technologies on marketing: a research agenda. Expert Syst. Appl. **125**, 864–877 (2021). https://doi.org/10.1016/j.jbusres.2020.01.007
41. Følstad, A., Taylor, C.: Investigating the user experience of customer service chatbot interaction:a framework for qualitative analysis of chatbot dialogues. Qual User Exper **6**, 1–17 (2021). https://doi.org/10.1007/s41233-021-00046-5
42. Rodríguez Cardona, D., Werth, O., Schönborn, S., et al.: A mixed methods analysis of the adoptionand diffusion of Chatbot Technology in the German insurance sector. Twenty-fifth Americas Conference on Information Systems. Cancun (2019)
43. Nguyen, D., Chiu, Y., Le, H., et al.: Determinants of continuance intention towards banks' chatbot services in Vietnam: a necessity for sustainable development. Sustainability **13**, 7625 (2021). https://doi.org/10.3390/su13147625

Securing Drug Supply Chain with Medledger: A Blockchain Solution to Counterfeit and Hoarding Challenges

M. Saad Bin Ilyas(✉), Imtiaz Ali Soomro, Iqra Tariq, and Muhammad Adil Butt

Department of Computer Science, The University of Chenab, Gujrat 50700, Pakistan
msaad@cs.uchenab.edu.pk

Abstract. One of the most serious dangers to the pharmaceutical sector is counterfeiting and hoarding of drugs during the manufacturing and supplying process. The world of online web-based pharmacies has made the medication supply chain process extremely convoluted and difficult to secure. This study presents a novel and state-of-the-art Medledger system based on blockchain that uses chain codes to develop the smart contracts. Our proposed system, Medledger, is a state-of-the-art traceability system based on blockchain technology that eliminates the need for a centralized trusted authority, intermediates, and transaction records. The system utilizes chain codes to develop smart contracts that manage the connection between the entities involved in the pharmaceutical supply chain. Through the use of sequence diagrams, our system ensures better traceability and transparency. Furthermore, all transactions and events are preserved on the blockchain's immutable Medledger permanently, which is connected to peer-to-peer decentralized file systems. Our study demonstrates that Medledger is effective in mitigating the risk of counterfeit and hoarded drugs in the pharmaceutical industry while increasing efficiency in the supply chain.

Keywords: Supply Chain · Pharmaceutical Industry · Traceability · Blockchain · Hoarding

1 Introduction

The pharmaceutical industry is a vital component of the healthcare sector, playing a critical role in providing essential medication to millions of people worldwide. However, the industry is plagued with numerous challenges, including the widespread problem of counterfeit drugs, which poses a significant threat to public health and safety [1, 2]. According to the World Health Organization (WHO), counterfeit drugs are estimated to account for up to 10% of the global drug market, representing a multi-billion-dollar industry [3]. Counterfeit drugs not only result in the loss of revenue for legitimate manufacturers, but they also jeopardize patient health by delivering substandard or ineffective products, leading to treatment failures, drug resistance, and even death [4].

In addition to counterfeiting, the pharmaceutical industry is also facing the challenge of drug hoarding, where individuals or organizations purchase large quantities of drugs

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 205–222, 2025.
https://doi.org/10.1007/978-3-031-77620-5_14

with the intent to resell them at inflated prices or withhold them from the market, creating artificial scarcity [5]. This practice leads to increased prices and limited access to essential medication, particularly in regions with inadequate healthcare infrastructure and limited resources. To address these challenges, there is a need for a drug traceability system that can provide end-to-end visibility of drugs as they move through the supply chain. Such a system can ensure that the drugs are genuine and have not been tampered with or diverted to illicit channels. It can also prevent hoarding by limiting the number of drugs that can be purchased by a single entity and ensure equitable distribution of medication to the patients who need it the most.

To achieve the proposed drug traceability system based on a Medledger, it is essential to understand the underlying technology and its capabilities. Blockchain technology is a distributed ledger system that provides a decentralized and immutable record of transactions [6]. It ensures data integrity and transparency by utilizing a consensus mechanism to validate transactions and secure them cryptographically [7]. The blockchain network consists of nodes that participate in the validation process, and each node maintains a copy of the ledger, ensuring that all participants have access to the same information. The use of blockchain technology in healthcare has gained significant attention due to its potential to address various challenges, including data privacy, interoperability, and security [8]. The technology has several features that make it suitable for drug traceability systems. These features include immutability, transparency, and tamper- evident records, which can help prevent fraud, diversion, and counterfeiting [9].

The proposed drug traceability system utilizes a Medledger, which is a blockchain-based platform designed specifically for the healthcare industry. The Medledger is a private blockchain that provides secure and efficient data sharing among healthcare stakeholders, including manufacturers, distributors, pharmacies, and patients. The system uses a unique identification code assigned to each drug, which is recorded on the Medledger and tracked as the drug moves through the supply chain. The use of a unique identification code enables end-to-end visibility of the drug, ensuring that it is genuine and has not been tampered. The system also incorporates smart contracts, which are self-executing agreements that can automatically verify the authenticity of drugs and prevent hoarding by limiting the number of drugs that can be purchased by a single entity. Smart contracts can be programmed to execute specific actions when predefined conditions are met, making them suitable for supply chain management applications [10]. In the proposed system, the smart contract limits the number of drugs that can be purchased by a single entity, preventing hoarding, and ensuring equitable distribution of medication.

The proposed drug traceability system can provide several benefits to the pharmaceutical industry, including improved patient safety, increased supply chain efficiency, and reduced costs associated with counterfeit drugs [11]. The system can also enable regulators to monitor and enforce compliance with regulations and standards, improving overall transparency in the drug supply chain [12]. In conclusion, the proposed drug traceability system based on a Medledger is a promising solution to the challenges of counterfeiting and hoarding in the pharmaceutical industry. The use of blockchain technology and smart contracts can provide secure and transparent tracking of drugs from the manufacturer to the end-user, ensuring that the drugs are genuine and have not been

tampered with. The system can also prevent hoarding by limiting the number of drugs that can be purchased by a single entity, ensuring equitable distribution of medication to the patients who need it the most. The implementation of this system would provide more secure and transparent drug supply chain that promotes public health and safety.

In this paper, we propose a drug traceability system based on a Medledger, which leverages blockchain technology to enable secure and transparent tracking of drugs from the manufacturer to the end-user. The proposed system utilizes a unique identification code assigned to each drug, which is recorded on the Medledger and tracked as the drug moves through the pharmaceutical supply chain (see Fig. 1). The system also incorporates smart contracts that can automatically verify the authenticity of drugs and prevent hoarding by tracking the number of drugs purchased by the single entity and the number of drugs sell by that entity. Moreover, the user can check the availability of the drug on the application provided to him. The results of this study will contribute in the development of a drug supply chain that ensures the availability of genuine drugs and promotes public health and safety.

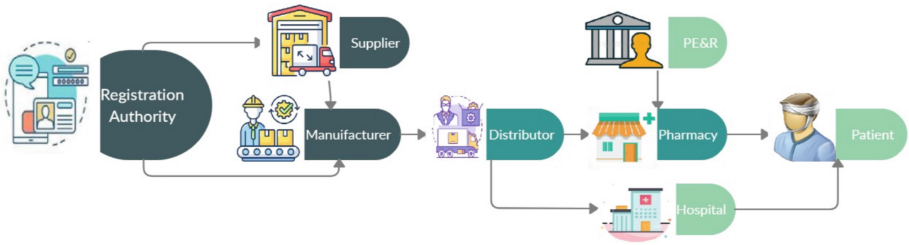


Fig. 1. Pharmaceutical Supply Chain

2 Literature Review

One of the main goals of the quality of life is believed to be access to high-quality healthcare. The rise in the creation, delivery, and distribution of fake medications across the pharmaceutical supply chain is one of the major problems. To help readers comprehend the need for the ongoing study, this section critically assesses and analyses the strategies and technology now employed in the pharmaceutical sector to combat the sale of fake medicines.

It should be noted in [13] that the emergence of technologies (such as big data analytics, blockchain, IoT, and artificial intelligence.) brings a possible assistance in improving real-time data flow in order to manage the ripple effect, severe resilience and disruptions. For hospitals, pharmacies and other healthcare companies to be efficiently and respond effectively to epidemic relief efforts, the authors of the paper [14] highlighted the prospects that the addition of blockchain technology with the idea of smart contracts offer up for them. In a similar line, smart contracts' features, which also enable automatic replies or warnings, may be used to track and monitor the development of epidemics like illnesses. Reference [15] did further proactive study to analyze serious supply chain

risks and the ripple impact by putting up a framework for supply chain digitization that includes the four crucial SC phases of preparation, manufacturing, sourcing, and logistics. Their research demonstrates the growing significance of cutting-edge technologies in responding to outbreak related distractions by improving supply chain operational flexibility, response traceability, real-time coordination, and the ability to reconfigure resources during the phases of recovery, leading to a robust and resilient supply chain.

An efficient way to automate the supply chain's operations was suggested in Reference [16], a blockchain network based on Ethereum with smart contracts, also known as crypto contracts, keeping all of a company's data. The whole company's data would be stored on this network. The solution that is being put up to enhance current practices of managing supply chains makes use of blockchain technology, the internet of things, and smart contracts by substituting the conventional contract for a smart contract. Studies also concentrate on specific sectors, such as the supply chain related to the food and the healthcare sector, where blockchain technology has the potential to ensure the traceability and tracking of pharmaceutical and food products. Recent times have seen a lot of discussion on this subject.

In this study, [17] provide a distinct authentication mechanism for IoT-based anti-counterfeit medication devices to verify the legitimacy of "unit dosage." A novel authentication protocol for IoT pharmaceutical anticounterfeiting is presented in this paper. The suggested procedure enables mobile evaluation of online drug dosage forms. The suggested strategy avoids drug fraud. The protocol provides a reliable and secure technique for mutual authentication between servers and NFC tags. To read and transfer stored data, the proposed protocol uses mobile NFC as an interface between the server and the NFC tag. The server verifies medicine dosage forms and responds to a mobile device with NFC capability. After the response from the server, the consumer can decide whether to purchase the medication. The suggested scheme's increased security characteristics make it ideal for anti-counterfeit pharmaceuticals.

In [18] author present a new authentication strategy for medicinal anti-counterfeiting system in the IoT context (dosage forms). The suggested technique uses NFC in a mobile context and enables efficient NFC update phase. The Real-Or-Random model establishes the proposed scheme's session key security. This protects against other, informal attacks. Furthermore, the proposed system is analogous in computation and transmission costs and delivers additional functionality capabilities. Overall, the suggested scheme's balance of security, added functionality, and efficiency makes it suitable for anti-counterfeiting medicinal dosage forms.

The author of [19] focuses on node reputation and data secrecy in decision-making. To ensure data integrity, his prototype employs a zero-knowledge protocol. It keeps track of each node's score, which depends on interactions, to gauge their dependability in reaching agreement. The suggested remedy enables open drug delivery. To ensure product integrity, prevent the use of fake medicines, and advance public health, pharmacies, hospitals, and governmental organizations can track their goods back to the source. Using API endpoints, professionals and consumers may validate medications. The ZKP proof established network-wide data consistency, and the system was created to guarantee availability, partition tolerance, and consistency, and based on CAP's theorem.

Trust-based decision-making is ensured by the Markov model scorekeeping. The prototype's examination reveals a reliable decision-making process that raises the secrecy, integrity, and availability of the system.

The author of [20] discusses the problems with product traceability in the pharmaceutical supply chain (PSC) and how blockchain technology can offer a provenance, track-and-trace solution to stop the sale of fake medicines. They recommend Besu and Hyperledger Fabric, which offer a shared, trusted, permissioned, and decentralized platform for storage and communications within the pharmaceutical supply chain. Additionally, they satisfy important requirements including scalability, accessibility, privacy, security, and transparency.

In order to create a smart healthcare ecosystem through a pharmaceutical supply chain, this research [21] focuses on improving conventional blockchain systems for IoT-based supply chain management. They discuss a blockchain-IoT supply chain management system to control fake medicines and keep an eye on temperature- sensitive medications. A blockchain system powered by IoT sensors keeps track of drugs as they move through the supply chain. System performance is enhanced by the Raft consensus process, and network scalability is enhanced by the Blockchain Distributed Network (BDN) with bloXroute servers. The performance and security of a scalable blockchain network are implemented and assessed by the author.

In this work [22], the author emphasizes the advantages of blockchain-supported e-commerce platforms in combating product counterfeiting by utilizing corporate profit-driven analytical models and Stackelberg equilibrium theory. They analyze the profitability of all actors in conventional and blockchain-supported supply chains in order to determine the benefits of blockchain. For both conventional and blockchain-supported supply chains, they developed enterprise profit-driven analytical models based on game theory, where the producer and retailer haggle according to Stackelberg equilibrium theory. To fight counterfeiting, they combined a platform with blockchain technology.

To combat fake pharmaceuticals in India, this article [23] suggests a blockchain-based electronic health network. It takes 11 decentralized computer nodes to simulate a blockchain. Blockchain is used in the proposed system to track medication logistics from manufacture to patient. If fake medication is introduced, it will be rapidly identified, and its supply will be stopped. The major metric for efficacy was throughput. However, there will be more nodes accessible to form agreement, which is necessary to make the system tamperproof. The proposed system is computationally expensive since the time to commit a transaction rises with the number of participating nodes in the network. Real-time smart smartphone applications. The system may be accessible by QR code scanning, but it cannot prevent unlicensed or fake drugs.

This section contains current blockchain and supply chain solutions, research, and studies, as well as their benefits. Many advantages exist beyond crypto currency and non-fungible tokens (NFT). Improved medicine supply chain traceability. The new proposed system utilizes blockchain [24], proving the government's recognition of the technology's merits. Pharmaceutical giants including Amgen, Sanofi, and Pfizer are looking into using blockchain to track drug trials and speed up drug development and delivery. Also, Coral Health and Patentor are looking towards letting patients control and view their data and keep track of their medication use [25, 26]. Other supply chains, such as

Walmart, are researching blockchain technology to improve transparency and speed up processing in their food supply chain. [27] proposes 'Gcoin' as a way to incorporate blockchain technology in Taiwanese pharmaceuticals. This article, on the other hand, restricts the degree of complexity the system's consensus features may provide. a second Ethereum-based private system for real-time remote monitoring of patients' health histories is being suggested. To ensure a products real supply history in the medication's distribution chain, both articles fail.

Context and consensus procedure are crucial factors in implementation selection. According to [28] private blockchains are more secure than public ones. Legitimate participants may now join the blockchain. [29] Presents PharmaCrypt, a private Ethereum blockchain technology. The method uses Amazon Web Services (AWS) and smart contracts to create and transfer goods. Modern supply chain systems may employ the software to scan barcodes to produce new assets with inimitable identifiers. Concerns about scalability and future development were raised. Private blockchains are not really decentralized because of network approval [30]. To maintain network integrity, incoming nodes must be confirmed (or, in this case, the genesis system).

Private vs. Public. Satoshi N. created the first PoW blockchain in 2009. It now builds immutable chains. Blockchain technologies are being developed for auditability and traceability. Consensus-based and hybrid blockchains are the most common. A closed blockchain network. Before a node may join a network, it must be approved by a group. In supply chain, finance, and retail. Public chains are suitable for cryptocurrency and e-voting. Like a private blockchain, a consortium chain is run by a group. It's a similar private blockchain. One or more nodes can modify the public blockchain. The public offers pseudo-anonymity. Simple and complete nodes. However, simple nodes cannot preserve or validate the ledger. In a PoW blockchain, customers are simple nodes. These nodes store the blockchain and validate each block. It is an invite-only network that requires authentication. However, only authorized users can access transactions in a private blockchain network [31]. They are used for digital signatures; identity verification and asymmetric keys identify it. Public blockchains allow anybody to join, validate blocks, and originate transactions [32].

NFT is popular because everyone may develop and agree on blocks. Public transaction verification (miners) is used in Bitcoin and Ethereum [33]. Blockchain miners demand a lot of processing power, making them expensive to set up and run. Market merchants build reputation and trust via long-term fair commerce [34]. The problem arises in a distributed ledger when nodes must trust each other's data. This is a random subset of the data needed from the verifier and proved. As part of the blockchain consensus system, all nodes participating in the process must concur on the associated block. The authors of [35, 36] propose a consensus-based reputation rating system for network nodes. The Markov model can assess a node's reliability [37]. It appears to contradict decentralization and creates a single point of failure because the authority is known to all network nodes.

The study effort presented in this paper began with a thorough examination of the available literature. Suggest using technology to improve supply chain management. DLT enhances operational efficiency and security. Byzantine fault-tolerant blockchain network allows full transparency of real-time transactions. Allows participants to track

data, resulting in patients receiving genuine products. Once the system has divided into groups with diverse replies, to reach a consensus they use the ZKP circuit computation and Markov models. The paper [38] proposes a transparent distribution method based on node reputation, security measures, and needs. Currently, drugs go from manufacturers through distributors, then to consumers. Wholesalers often order products from producers who ship them. This includes pharmacy, hospitals, and stores. These facilities then supply them to suppliers. Retailers rarely sell directly to consumers. What if the data on the centralized server is compromised later? What causes data loss? To prevent third-party or customer-issued counterfeit medicine, each entity's quantity and type must be constant. The prototype design in this study addresses these issues. RFID, barcode scanners, and holographic packaging are optional. Summary of the literature review is provided in Table 1.

Table 1. Summary of Literature Review

Reference	Technology Used	Advantages/Limitations
[13]	Digital twins' simulation	Enables data-driven optimization and visibility for supply chain management Limited empirical validation
[14]	Blockchain	Provides an overview of various blockchain applications Limited focus on specific applications
[16]	Blockchain, IoT	Enables full observability and transparency in supply chain management Limited empirical validation
[17]	NFC, IoT	Provides a lightweight authentication protocol for anti-counterfeiting. Limited to authentication
[18]	IoT, blockchain	Provides a secure authentication scheme for anti-counterfeiting. Limited empirical validation
[19]	Blockchain	Provides a secure distribution system to prevent counterfeiting. Limited empirical validation
[20]	Blockchain	Provides an overview of blockchain architectures for drug traceability Limited empirical validation
[21]	IoT, blockchain	Provides a secure system for temperature monitoring and anti-counterfeiting Limited empirical validation
[22]	Blockchain	Provides a secure e-commerce platform to prevent counterfeiting Limited empirical validation
[23]	Blockchain	Provides a secure system for e-health. Limited empirical validation

(*continued*)

Table 1. (*continued*)

Reference	Technology Used	Advantages/Limitations
[24]	Blockchain	Enhances the traceability of medicine supply chain, helps to detect counterfeit drugs Scalability and interoperability issues, lack of standardization
[25]	Blockchain	Decentralized digital currency, secure transactions. High energy consumption, scalability issues
[26]	RFID and Barcode	RFID has faster read rates and can capture data without line of sight, barcode is cheaper and more widely adopted RFID requires more investment; barcode has lower data density
[27]	RFID	Improved inventory management and supply chain visibility. High implementation costs, data security concerns
[28]	Various	Provides an overview of public health interventions against counterfeit drugs. Limited to a systematic review, does not offer a specific technological solution
[29]	Blockchain	Provides insights on how blockchain can be used in operations management. Focuses on theoretical aspects, does not present empirical evidence
[30]	Blockchain	Enhances supply chain transparency, reduces environmental impact. Limited to a conceptual framework, lack of empirical evidence
[31]	Blockchain	Secure automated patient monitoring, faster data access and analysis. Lack of scalability, limited to a proof-of-concept study
[32]	Blockchain	Provides an overview of different types of blockchains. Limited to a theoretical discussion, lacks empirical evidence
[33]	Blockchain	Offers a lightweight and efficient blockchain solution for healthcare applications Limited to a proof-of-concept study, needs further testing
[34]	Blockchain	Enhances data security and privacy for energy IoT applications. Limited to a proof-of-concept study, scalability issues
[35]	Blockchain	Offers insights on the opportunities and challenges of adopting blockchain in different sectors Limited to a literature review, lacks empirical evidence

3 Proposed Methodology

This research paper proposes the development of a secure system called "Medledger" using Hyperledger Fabric technology for drug traceability. The proposed methodology involves defining the requirements for the system, designing and developing it using Hyperledger Fabric, creating smart contracts for various processes related to drug traceability, implementing the system in a real-world scenario, and developing a process for requesting drugs using Medledger. By using a distributed ledger system, Medledger aims to improve drug traceability and ensure the authenticity of drugs throughout the supply chain. Overall, the proposed methodology provides a secure and transparent method for tracking medications from the manufacturer to the end-user.

3.1 Medledger: A Hyperledger Fabric-Based System for Drug Traceability

The construction and operation of our suggested innovatory drug traceability architecture based on Medledger will be discussed in details in this part in order to provide stakeholders of Pharmaceuticals Supply Chain (PSC) (see in Fig. 1) to trace, monitor, provenance, and verify their transactions. Blockchain technology we chose in our work is Hyperledger Fabric (HLF) because it eliminates the need for a centralized authority and provides interoperability, improved privacy, access control, scalability, and transaction efficiency over data related to the traceability of drugs, as well as a significant reduction in the time it takes to share, store, and alter transactions on the Blockchain network.

The HLF provides management service to ensure identity and maintains user identity and authenticates the participants registered in overall network to provide a trustworthy environment amongst untrusted participants. It provides the facility as a membership service provider that initiate rules and guidelines by which various PSC stakeholders are authenticated, governed, authorized, and verified to become part of the network associated with Blockchain and granted access to the Medledger for the purposes of ensuring privacy, confidentiality, and secrecy.

3.2 Fabric Deployment Approach for Hyperledger

Trace backward is the functional principles of our proposed drug traceability system, in which the we have the source of data related to the supplier (who provides raw material or ingredients to the manufacturer) and manufacturer (who make the drugs). In case of supplier active ingredients or raw material being supplied by the supplier to the manufacturer and on the other hand for manufacturer, the raw material or ingredients used in manufacturing of drugs that the manufacturer has ordered from supplier, history of the raw material used, manufactured drugs, location of drugs being transported to the hospitals or pharmacies, all are being traced on the Medledger. Track Forwarding, is used to track the current location of the medicine being supplied/transported in the PSL until it is hand over to the patient, pharmacy and hospital which we considered as end user.

The traceability of drugs was achieved by constructing a HLF network implemented through chain codes and all the peers or nodes connected with the Blockchain network

was agreed mutually. The cyber-physical properties of the network must be considered while building and organizing the Medledger system. Chain codes placed amongst stakeholders govern and regulate this transaction flow. It ensures the integrity, transparency, and quality of the procedure flow by allowing all participants to access transaction records at any time. To trace and monitor the transparency and authenticity of each medicine in the PSC, participating stakeholders build, implement, and initialize chain codes. At the Medledger, chain codes are used for the registration of pharmaceuticals and their raw material or ingredients, as well as their distribution and tracking information, as immutable, transparent, and timestamped blocks.

3.3 Contract for Registration of Drug Manufacturer

In our proposed system, to register newly drug manufacturer a Drug Manufacturer Contract (DMC) will be created and implemented between Manufacturer and Drug Registration Authority (DRA). In this process a certificate will be assigned to the newly registered drug manufacturer by the DRA after verifying the credentials of the manufacturer such as name, license number and location (see Fig. 2).

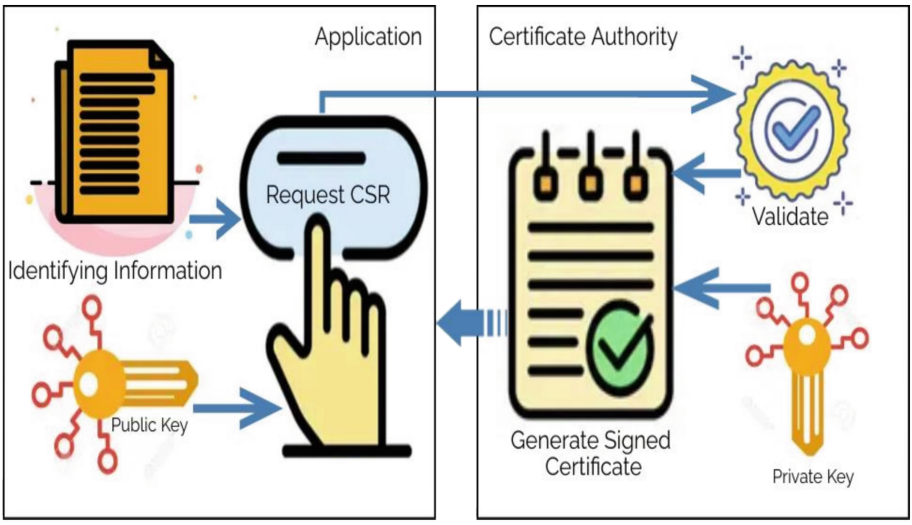


Fig. 2. Application for Registration from Drug Manufacturer to DRA

3.4 Contract for the Registration of Drug (CDR)

Contract for the Registration of Drug which has to be manufactured for the first time and the active ingredients or raw material being used for that drug, a Contract for Drug Registration (CDR) will be signed between the supplier of ingredients and raw material and the manufacturer of the drug (see Fig. 3). In this process step (1) is to register manufacturer under the contract signed between supplier and manufacturer.

After successful registration of manufacturer and verification by the supplier order would be placed in (2). In (3) order is verified by the control order and then request for generating tags (4) to the ordered material for tracking purpose. Tags published (5) would be placed on packages (6) and transported the raw material (7) to the requested supplier. After receiving the order manufacturer scan the tags (8) and after verification (9) that the required order has been received (10) as it is, the status will be updated as delivered (11) and payment (12) will be processed to the supplier. Record has been updated (13) after completing the whole process successfully.

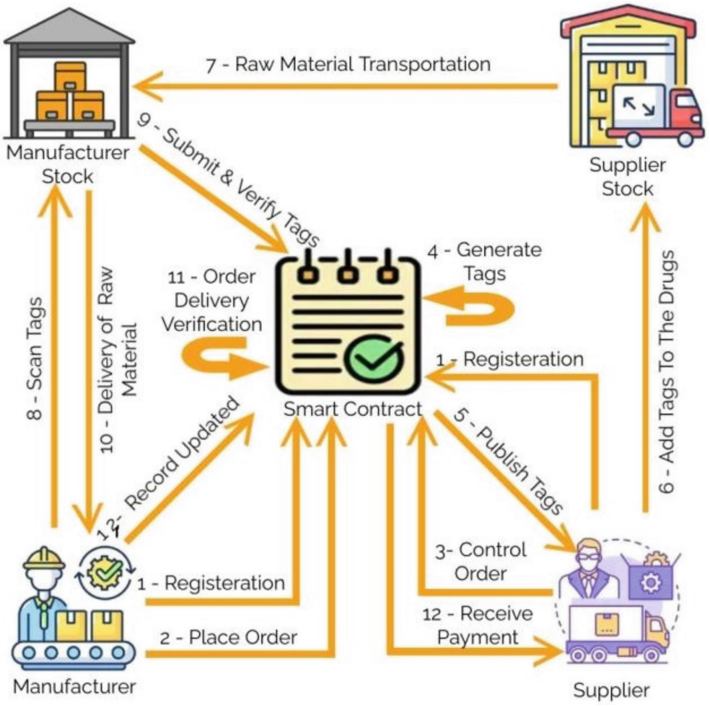


Fig. 3. Manufacturer and Supplier Contract

1. Registration	2. Place Order	3. Control Order	4. Generate Tags
5. Publish Tags	6. Add Tags to the Raw Material	7. Raw Material Transportation	8. Scan Tags
9. Verify Tags	10. Delivery of Raw Material	11.Delivery Verification	12. Payment Received
	13. Record Update		

3.5 Contract for Ordering of Drugs (COD)

When pharmacy or hospital required drugs for their stores, they will place order to the manufacturer, or the authorized distributor (see Fig. 4). In this process step (1) is to register pharmacy or hospital under the contract signed between manufacturer and hospital or pharmacy. After successful registration of hospital or pharmacy and verification by the manufacturer through DRA order would be placed in (2). In (3) order is verified by the control order and then request for generating tags (4) to the ordered material for tracking purpose. Tags published (5) would be placed on packages (6) and transported the drugs (7) to the requested hospital or pharmacy. After receiving the order hospital or pharmacy scan the tags (8) and after verification (9) that the required order has been received (10) as it is, the status will be updated as delivered (11) and if request came from patient, drug will be delivered to the patient either by the hospital or pharmacy (12). Record has been updated (13) after completing the whole process successfully and also updated to the DRA (14).

3.6 Medledger Medication Traceability System Implementation

The advantage of implementing our recommended HLF medication traceability system in the PSC is that it guarantees the accessibility of exact and irreversible information to all participants without the need for a centralized authority. Throughout the medication tracing process, patient or any other participant, end-user pharmacy or hospital may query about the source, history of a certain medicine using a specific drug ID. Participants in the Medledger have just the ability to save and change transaction data. It's also worth emphasizing that only legal, authorized, and transactions based on consensus will be added and updated to the Medledger. This part of paper describes how we implemented our proposed HLF-enabled pharmaceutical traceability system, which employs the fabrics execute-order-validate architecture to process and execute transactions across different blockchain network participants. In the proposed system, all transaction-related activities are continually recorded and saved. Events involving all stakeholders in the immutable Medledger on the blockchain, which is paired with a storage system that is decentralized to get maximal transparency and a storage capacity to keep considerable pharmaceutical data. All stakeholders in the supply chain system of pharma are identified first, then enrolled, and got registered in a P2P HLF blockchain network by the DRA. For registering the stakeholders, the chosen drug regulating agency that controls and monitors the HLF network will employ a registration mechanism in the chain code. It offers a permissioned network which will be a private that is only available to those who have joined up for it. The manufacturers, supplier, distributor, hospital, pharmacy, and patient will get themself registered by the relevant drug regulating agency. After the patient records have been registered, it will be verified by the drug regulatory authority (DRA) and assigned a unique ID.

1. Registration	2. Place Order	3. Control Order	4. Generate Tags
5. Publish Tags	6. Add Tags to the Drugs	7. Drugs Transportation	8. Scan Tags

(*continued*)

(*continued*)

1. Registration	2. Place Order	3. Control Order	4. Generate Tags
9. Verify Tags	10. Delivery of Drugs	11. Delivery Verification	12. Drug Delivery to patient
	13. Record Update	14. Updated Record to DRA	

This approach completes the registration procedure and prepares all participants to undertake network transactions. The likelihood of tampering with Medledger data is much reduced with this technique. In the suggested HLF system, the producer will register a drug and its components in the DRC contract. As part of the registration process, the pharmaceutical transaction proposal perform certain operations on chain code was generated and submitted to the Medledger. The endorsement policy of the fabric determines which peer nodes acts as endorsers and receive transaction proposal requests. The transaction payload, which comprises the list of activities to be done, the chain code identification, a random or counter number that the submitting user may use only once, and the transaction proposal identifier, is included in the drug registration proposal. This proposal of transaction will then be verified and confirmed keeping in view the endorsement policy formed by the fabric blockchain network's accessible and registered peer nodes. Endorsers function as a kind of peer node.

As stipulated in the endorsement policy, a predetermined number of endorsing peers will execute the drug registration transaction proposal. This record will be encrypted and saved with the endorsement peers digital signatures, resulting in an endorsement message. This endorsement includes information related to R.W. (readset and writeset) data, and also endorser I.D., transaction I.D., and signature of endorser. This approval will be sent back to the participant in reply to the request of transaction submitted by him. It's worth noting that the node of manufacturer will gather endorsements until the endorsement policy is met, and the transaction will not be committed to the Medledger until then. After everything has been verified and authenticated, a transaction proposal will be sent to the ordering node that is the part of the approval process of proposal.

The manufacturing node gathers all of the endorsements and publishes them to the ordering-service after receiving the enough response or acknowledgement from the nodes involves in endorsing during the request endorsement phase. The transaction response is made up of the transaction metadata, transaction payload, and a response of endorsements. Furthermore, ordering service groups together several similar transactions related to drug, including authorized transactions, into blocks. The ordering service then organizes all of the transactions for delivery, including their state dependencies.

3.7 Requesting Raw Material from Manufacturer

Manufacturer requests to the supplier for raw material or ingredients being used for the manufacturing of drug. Supplier checks/verifies the manufacturer through digital certificate provided by the DRA. After verification requests forwarded to the drug registration, checking officer who authorized the request after verifying that the requested drug is

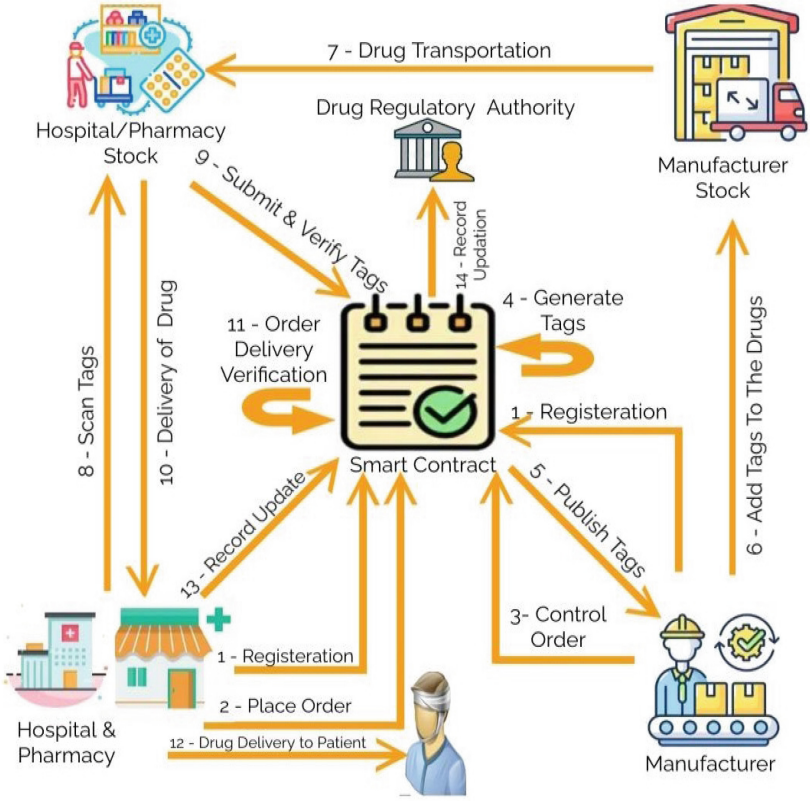


Fig. 4. Request of Drugs from Hospital or Pharmacy to the Manufacturers

registered or not and authorized limit of raw material being issued to the manufacturer (if the endorsing peer unable to endorse the request, then it will be considered as rejected).

After getting endorsed by endorsing peers the request will be forwarded to the ordering peer. Orderer node creates the block and forward it to the Committing node for validation and consensus purpose. Operational Manager acts as a committer and validate the transaction and broadcast the block to all the peers in the network as shown in the sequence diagram of manufacturer to supplier contract (see Fig. 5).

3.8 Requesting Drugs from Manufacturer

Hospital or pharmacy requests to the manufacturer for drugs required for their stores. Manufacturer checks/verifies the hospital or pharmacy through drug regulatory authority. After verification requests forwarded to the drug registration checking officer who authorized the request after verifying that the requested drug is registered or not and authorized quota of drug being issued to the hospital or pharmacy (if the endorsing peer unable to endorse the request, then it will be considered as rejected).

After getting endorsed by endorsing peers the request will be forwarded to the ordering peer. Orderer node creates the block and forward it to the Committing node for

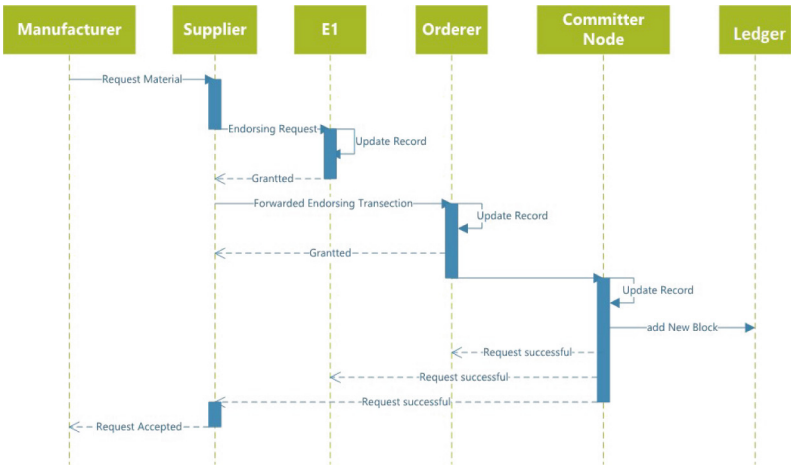


Fig. 5. Sequence Diagram for Requesting Raw Material from Manufacturer

validation and consensus purpose. Pharmacy manager acts as a committer and validate the transaction and broadcast the block to all the peers in the network as shown in the sequence diagram of manufacturer to hospital or pharmacy contract (see Fig. 6).

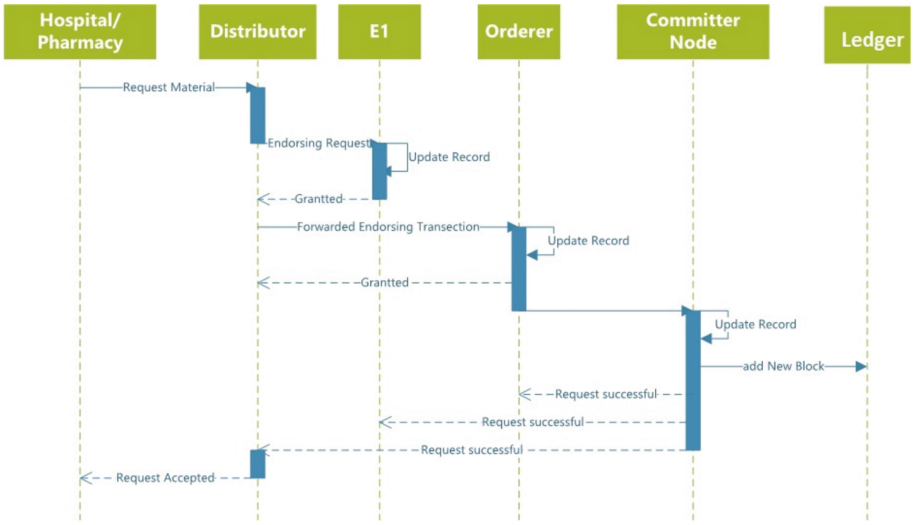


Fig. 6. Sequence Diagram for Requesting Drug from Manufacturer

3.9 Requesting Drugs from Hospital/Pharmacy

Patient can request drug through the application provided to him and gets the order from registered hospital or pharmacy on providing the prescription added by the doctor or

physicians (see Fig. 7). Upon successful authentication of patient record request will be approved and record about the quantity of medicine being delivered to the patient has been updated and forwarded to all the nodes connected in the network. Through this process we can control the hoarding of the drugs as well. All the updated record of drugs being delivered to the patients and the remaining stock of each drug has been maintained in the ledger. Anyone connected to the network can check the availability of the drug.

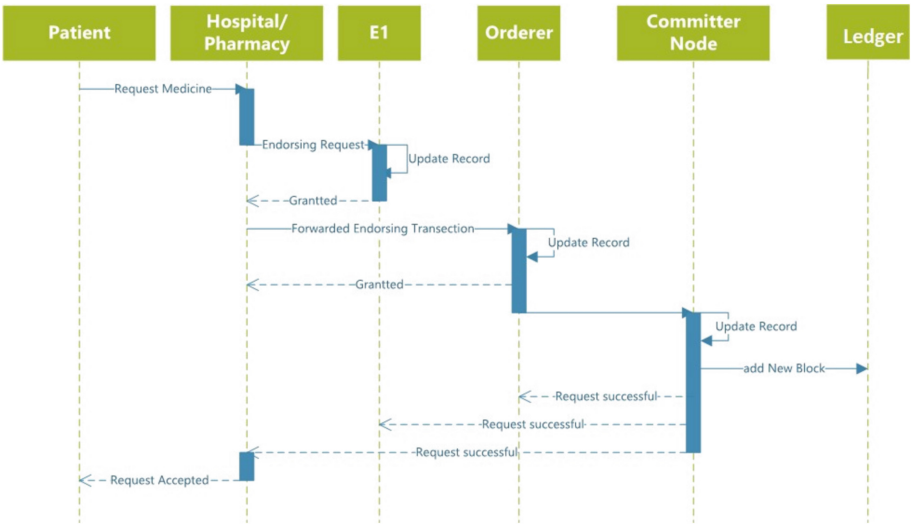


Fig. 7. Sequence Diagram for Requesting Drug from Hospital/Pharmacy

4 Conclusion

In pharmaceutical industry, blockchain technology used to reduce asymmetric information between investors and medicine manufacturers. It protects against hacks and cyber-attacks. The most important feature of blockchain technology is robust encryption, which offers virtual security in order to secure the data which is timestamped that cannot be manipulated or hacked. We suggested a Medledger architecture to handle medication traceability and hoarding concerns using blockchain technology in this study. Using chain codes, the system continuously archives and records activities and transactions involving all participants in the blockchain network. Collaboration amongst chain codes was used to complete the process of medication registration, transfer, and tracking. The Medledger system that has been suggested is completely decentralized. It offers a non-repudiation approach with authenticity and traceability to ensure that any problems in the pharmaceutical supply chain. All involved entities also use digital certificates to authenticate and identify themselves. Sequence diagrams and contracts, we presented explained all aspects of the procedure proposed, including its components that successfully mitigates the problem of counterfeit and hoarding in pharmaceutical

industry. The suggested system is built on decentralized blockchain technology, with all data being saved on the immutable Medledger. It's safe, transparent, and tamper-proof. HLF technology is still very much in early stages and faces several practical hurdles.

References

1. Drori, T., Salinas, E.A., Grigoryan, L.: The impact of counterfeit drugs on patients: a rapid review of the literature. Health Policy and Technol. **7**(3), 315–331 (2018). https://doi.org/10.1016/j.hlpt.2018.06.001
2. Sarwar, M., Syed-Abdul, S., Hafeez-Baig, A., Raza, S.: Counterfeit medicines: An updated review of its prevalence, health impact, and control. Front. Pharmacol. **10**, 1–20 (2019). https://doi.org/10.3389/fphar.2019.00001
3. World Health Organization: Substandard and Falsified Medical Products (2017). https://www.who.int/medicines/services/counterfeit/impact/Substandard_Falsified_En.pdf. Accessed: 25 Mar. 2023
4. Liu, Y., Chen, L., Liu, Y., Zhao, C.: MedLedger: a blockchain-based system for medical data sharing. IEEE Access **7**, 179653–179662 (2019). https://doi.org/10.1109/ACCESS.2019.2956398
5. Zaman, M.H., Hasan, M.T., Uddin, J.: The ethics of drug hoarding during COVID-19 pandemic. Health Policy and Technol. **9**(4), 489–491 (2020). https://doi.org/10.1016/j.hlpt.2020.08.003
6. Swan, M.: Blockchain: Blueprint for a new economy. O'Reilly Media, Inc. (2015)
7. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008). https://bitcoin.org/bitcoin.pdf. Accessed: 25 Mar. 2023
8. Yue, X., Wang, H., Jin, D., Li, M., Jiang, W.: Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. **42**(8), 1–8 (2018). https://doi.org/10.1007/s10916-018-0997
9. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: Architecture, consensus, and future trends. In: IEEE International Congress on Big Data, pp. 557–564 (2019). https://doi.org/10.1109/BigDataCongress.2019.00098
10. Christidis, K., Devetsikiotis, M.: Blockchains and smart contracts for the internet of things. IEEE Access **4**, 2292–2303 (2016). https://doi.org/10.1109/ACCESS.2016.2566339
11. Hernandez, J., Petrova, E., Fuster, B.: Blockchain technology in healthcare: a systematic review. Healthcare **8**(4), 425 (2020). https://doi.org/10.3390/healthcare8040425
12. Dhillon, G., Metcalf, D.: Blockchains and distributed ledgers in health and social care. BMJ Innovations **2**(1), 1–7 (2016). https://doi.org/10.1136/bmjinnov-2015-000075
13. Ivanov, D., Dolgui, A., Das, A., Sokolov, B.: Digital supply chain twins: managing the ripple effect, resilience, and disruption risks by data-driven optimization, simulation, and visibility. In: Handbook of ripple effects in the supply chain, pp. 309–332. Springer, Cham (2019)
14. Maesa, D.D.F., Mori, P.: Blockchain 3.0 applications survey. J. Parallel and Distrib. Comp. **138**, 99–114 (2020)
15. Ivanov, D., Dolgui, A., Sokolov, B.: The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int. J. Prod. Res. **57**(3), 829–846 (2019)
16. Naidu, V., Mudliar, K., Naik, A., Bhavathankar, P.: A fully observable supply chain management system using block chain and IOT. In: 2018 3rd International Conference for Convergence in Technology (I2CT), pp. 1–4. IEEE (2018)
17. Alzahrani, B.A., Mahmood, K., Kumari, S.: Lightweight authentication protocol for NFC based anti- counterfeiting system in IoT infrastructure. IEEE Access **8**, 76357–76367 (2020)

18. Wazid, M., Das, A.K., Khan, M.K., Al-Ghaiheb, A.A.D., Kumar, N., Vasilakos, A.V.: Secure authentication scheme for medicine anti-counterfeiting system in IoT environment. IEEE Internet Things J. **4**(5), 1634–1646 (2017)
19. Zoughalian, K., Marchang, J., Ghita, B.: A blockchain secured pharmaceutical distribution system to fight counterfeiting. Int. J. Environ. Res. Public Health **19**(7), 4091 (2022)
20. Uddin, M., Salah, K., Jayaraman, R., Pesic, S., Ellahham, S.: Blockchain for drug traceability: architectures and open challenges. Health Info. J. **27**(2), 14604582211011228 (2021)
21. Singh, R., Dwivedi, A.D., Srivastava, G.: Internet of things based blockchain for temperature monitoring and counterfeit pharmaceutical prevention. Sensors **20**(14), 3951 (2020)
22. Jiang, J., Chen, J.: Managing the product-counterfeiting problem with a blockchain-supported E-commerce platform. Sustainability **13**(11), 6016 (2021)
23. Pandey, P., Litoriya, R.: Securing e-health networks from counterfeit medicine penetration using blockchain. Wireless Pers. Commun. **117**(1), 7–25 (2021)
24. Kumar, R., Tripathi, R.: Traceability of counterfeit medicine supply chain through Blockchain. In: Book Traceability of counterfeit medicine supply chain through Blockchain, pp. 568–570. IEEE (2019)
25. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, p. 21260 (2008)
26. Groom, T., Barrios, D., George, K.: An In-Depth Analysis of RFID Versus Barcode Scanning for Tactile Learning. In: Book An In-Depth Analysis of RFID Versus Barcode Scanning for Tactile Learning, pp. 1–5. IEEE (2021)
27. Wu, N.-C., Nystrom, M., Lin, T.-R., Yu, H.-C.: Challenges to global RFID adoption. Technovation **26**(12), 1317–1323 (2006)
28. Hamilton, W.L., Doyle, C., Halliwell-Ewen, M., Lambert, G.: Public health interventions to protect against falsified medicines: a systematic review of international, national and local policies. Health Policy Plan. **31**(10), 1448–1466 (2016)
29. Babich, V., Hilary, G.: OM forum—distributed ledgers and operations: what operations management researchers should know about blockchain technology. Manuf. Serv. Oper. Manag. **22**(2), 223–240 (2020)
30. Park, A., Li, H.: The effect of blockchain technology on supply chain sustainability performances. Sustainability **13**(4), p. 1726 (2021)
31. Griggs, K.N., Ossipova, O., Kohlios, C.P., Baccarini, A.N., Howson, E.A., Hayajneh, T.: Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J. Med. Syst. **42**(7), 1–7 (2018)
32. Sharma, T.K.: Permissioned and permissionless blockchains: A comprehensive guide. Blockchain Certifications (2019)
33. Ismail, L., Materwala, H., Zeadally, S.: Lightweight blockchain for healthcare. IEEE Access **7**, 149935–149951 (2019)
34. Rui, H., Huan, L., Yang, H., YunHao, Z.: Research on secure transmission and storage of energy IoT information based on Blockchain. Peer-to-Peer Networking and Applications **13**(4), 1225–1235 (2020)
35. Akram, S.V., Malik, P.K., Singh, R., Anita, G., Tanwar, S.: Adoption of blockchain technology in various realms: Opportunities and challenges. Security and Privacy **3**(5), e109 (2020)
36. Wüst, K., Gervais, A.: Do you need a blockchain? In: Book Do you need a blockchain?, pp. 45–54. IEEE (2018)
37. Digiconomist, I.: Bitcoin Energy Consumption Index—Digiconomist. Digiconomist (2018)
38. Resnick, P., Zeckhauser, R.: Trust among strangers in Internet transactions: Empirical analysis of eBay's reputation system. The Economics of the Internet and E-commerce. Emerald Group Publishing Limited (2002)

Implementation of Authentic Resources for E-Learning in Education

Muhammad Yousaf Mushtaq[1], Hafiz Muhammad Irfan[2], Muhammad Ahmad Niaz[2], Muhammad Waseem Iqbal[1](✉), Anas Mazhar[2], Adnan Akhtar[2], and Amir Jamshaid[2]

[1] Department of Software Engineering, Superior University Lahore, Lahore 5400, Pakistan
waseem.iqbal@superior.edu.pk

[2] Department of Computer Science, The Islamia University, Bahawalpur, Bahawalnagar 62300, Pakistan
{ahmad.niaz,amir.jamshaid}@iub.edu.pk

Abstract. Students at all educational levels benefit from authentic learning, which helps them to connect the concepts they learn in the classroom and environments happening in the real world. Authentic learning is applied in schools. Elearning is an effective method of conveying knowledge both spoken and visually and has become more dominant in recent years. When conventional teaching methods are combined with online learning, an innovative and beneficial new educational model may be created for both the instructors and students. This research explores whether or not having experience in the real world may be helpful while learning in a virtual classroom environment. After the material has been presented to the participants using a prototype application, a survey questionnaire is used to evaluate the participants' knowledge levels. The variables included in the survey analyze the correlations between the ages of the respondents, the levels of education that they possess, and the knowledge that the respondents were able to recall and grasp. The results are consistent across all parameters, demonstrating that conventional training in a classroom setting and online courses have value in their respective fields.

Keywords: Teaching Methods · E-Learning · Higher Education · Authentic Learning

1 Introduction

Authentic learning is used in education and tuition techniques to help the students in connecting what they learn in the school to the problems, issues, and concepts they face in the real world. Several definitions of authentic learning are present in the literature. According to the definition provided by Hawland and her co-authors, genuine learning is defined as "learning that is seamlessly integrated or implanted into meaningful, 'real-world' situations" [1]. It is a truth universally understood that real-world experience may sometimes prove to be of far more value than theoretical understanding. According to the definition [2] provided by Revington, the phrase "authentic learning" alludes to

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 223–238, 2025.
https://doi.org/10.1007/978-3-031-77620-5_16

the idea of "real-life learning." This instructional methodology's pedagogical goal is to drive students to develop a product or service that holds value, which they can then transmit to a larger audience in the future. The target audience for this dissemination will be wider. According to Har [3] authentic learning requires students to take an active role in the problem-solving process of issues that are relevant to the actual world. Some of the authentic learning activities include role-playing, project-based learning, learning by doing, and problem-based learning. Authentic learning provides better learning opportunities, helps in a better understanding of a complex concept, prepares the learner for a better future, and blends learning and theories.

Learning that is both authentic and important requires the use of a wide variety of resources and approaches in order to be successful. The incorporation of examples drawn from real-world experiences is, in the opinion of a number of academics [4, 5], an essential component of an authentic educational experience. Authentic learning and a variety of teaching techniques were both integrated into a number of earlier researches [6–11]. Despite this reality, teachers still face a number of significant obstacles in their quest to integrate technology-based teaching aids into the classroom setting. E-learning takes an authentic approach, and an authentic learning environment encourages the development of unique approaches via the use of technologies made available by e-learning. Because of this, the full potential of elearning as an instructional medium may come one step closer to being realized. For the sake of this discussion, it is very necessary to articulate exactly what is meant when we talk about "e-learning." E-learning, also known as electronic learning is the exploitation of electronic technology to bridge the gap between traditional classroom instruction and self-directed learning, as described by Moreno and Mayer [12]. E-learning is also known as electronic learning.

The establishment of a teaching setting that faithfully replicates the real world serves as the essential structural underpinning for true educational practices. Recent breakthroughs in the field of education have led to the acknowledgment of educational practices that are ineffective and violate this basic concept. These approaches have been deemed to be in conflict with this ideal. It has been shown that the exploitation of technology breakthroughs such as visualization, simulation, and internet applications may help students more easily make the link between the theoretical information they gain in a classroom setting and its practical application in situations that occur in the real world. As a consequence of this, it is recommended that learning environments include real-world circumstances in order to improve the quality of the educational experience. This suggestion is backed by research from reputable sources [5]. In a variety of academic fields, including history [13], economics [14], and literature [15], and biology [16], research has shown that the deployment of genuine learning environments has resulted in favorable results as a result of the implementation of authentic learning environments. Students' skills in numerous areas, such as knowledge acquisition, collaborative problem-solving and effective communication, have the potential to be improved by the use of technology in educational contexts [17].

2 Structure

In recent years, there has been a dramatic rise in the amount of interest shown in e-learning by instructors and learners [18]. Arbaugh [19] contends that many of the components of e-learning (including students, instructors, courses, technology, system design, and the construction of an appropriate learning environment) align with the qualities of authentic learning. Both face-to-face and online education have been proven to benefit students' computer competence, ability to receive feedback, collaboration, adaptability, openness to new ideas, content quality, accessibility, and the development of higher-order thinking [20]. Online education has been demonstrated to be more cost-effective than face-to-face education. The study highlights the essential distinction between authentic learning and e-learning, suggesting that the former is a technique rather than a technology solution. The paper focuses on the critical contrast between genuine learning and e-learning.

Authentic learning, which focuses an emphasis on real-world solutions to challenging circumstances [5, 21] may be used to build workplace-relevant skills such as complex communication and higher-order thinking. This kind of learning allows for the development of workplace-relevant talents. The claims of [22] are in support of this, stating that "the ability to identify and solve problems using recognition and metacognition distinguishes those with skills that will help them advance in their careers from those with few opportunities for advancement," demonstrating the accuracy of the earlier made claims. Authentic learning opposes the idea that every problem can be solved by memorizing the right answers [5]. The authentic environment allows the students to learn in a situation closed to the one they face in a professional setting, making learners confident. One of the features of an authentic environment is to provide the learner with authentic activities [23].

Furthermore, it must be able to deliver multiple functions and diverse perceptions in studies [24]. Brown [25] mentions that the authentic learning environment encourages group work and concept exchange that enhances cognitive abilities. In an authentic learning environment, subject matter experts are responsible for sharing their views, methodology, and plans for future operations [26]. Another aspect that defines a classroom representative of the actual world is this. Students can build greater autonomy via instructional strategies such as scaffolding and fading the mentor's function in an atmosphere more authentically based on learning [27]. To validate the authentic learning in an educational setting, many educational psychologists and researchers have attempted to work on different criteria and ideas to date. Authors in [21] identified the availability of the authentic context as one of the most important criteria. Others have highlighted expert performance as the commonly used approach. Students can use online tools that allow them to assume the role of the teacher in organizing the classroom, learning methods and experiences, and how students receive a response in the classroom [28]. One of the other approaches to learning is collaboration. The author presents that students that work in a team can solve any problem more effectively as the discussion about the problem helps a lot in learning concepts [29].

Lee proposed an additional technical methodology for acquiring knowledge, referencing Vygotsky's assertion that the process of thought undergoes multiple transformations as it is translated into verbal communication. The spoken word is found to reveal both reality and form, while also exhibiting expressiveness in communication.

[30]. Practically put forward by Hoban and Ferry in their publication [31], presented a slow-motion animation as a tool, and selected a student to make comments about it. Afterwards, explaining the idea of the slow-motion video to other students, the selected student comprehends it first.

3 Literature Review

In literature, Herrington points out the importance of authentic learning in his book "A practical guide to authentic e-learning," by negating the objections against the authentic learning in higher education [32]. The author stated that the integration of authentic e-learning is accessible in higher education institutes that have already adapted the computer and web-based communication with students. The environment can improve student-learning conditions using the e-learning domain. However, the change will be gradual, and regular updates can be a long-lasting and sustainable authentic e-learning system. The idea is further enhanced by Chang and co-authors in their book on "Authentic learning through Advances in technology," with the development of newer and taskoriented devices, much better support for learning and transformation is expected [33]. It is postulated that with the initial slow pace of induction, the future students will be able to acquire things much quicker than generation. Although the speed in acquiring knowledge is necessary since, with the increasing volume of knowledge, there is a need for learning fast and learning in-depth. Authentic learning is also very crucial in developing innovative minds at the higher education level. Herrington [34] mentioned the effectiveness of technology in the field of higher education.

The research suggested that authentic learning can bring innovation in design and creation with its real-life learning opportunities. A supporting opinion is presented by Churchill [35], stating, "Technology amplifies our intellectual and physical capacity," presented a similar idea for a lower level of educational institutes. The author stressed the importance of technology at the secondary school level. However, the quantitative importance of authentic learning at the secondary school level was presented by Preus [36], stating an improvement in performance from 30 to 60 percentiles. There is also a need to not just focus on the authentic education mode of delivery, but the focus should also be on the valuation of knowledge, and that also needs to be authentic at all education levels. Investigators mark this method of learning as an authentic assessment [37]. So, combining the authentic mode of delivery and authentic assessment of knowledge fulfills the conditions for best practices [38, 39]. Academics have devoted significant time and energy to researching the relationship between digital technologies and practical experience. According to Bozalek, technological advancements correlate well with real education because they make it easier for individuals to work together and exchange ideas in fast-paced contexts. This, in turn, leads to more effective learning. The evolution of the educational system places a significant emphasis on the alignment of actual learning [40]. However, to fulfill the goals of this alignment, there is a need for a link between technology and education. The reason the current system is lagging this synergy because there is a need for collaborative efforts by specialists in technology and communication [41]. All of this, despite that authentic learning, is very appealing to those since it links the knowledge to real scenarios creating a better conceptual understanding and thereby

solving the problems [42]. By guiding students through a cognitive process that fosters their cognitive abilities, we can facilitate the cultivation of their problem-solving skills and enable them to attain a deeper understanding of the essence of authentic learning. According to source [43], students will be expected to engage in expert-level thinking as they tackle challenges that are grounded in real-world events. In order to achieve the aforementioned objective, it is imperative to allocate sufficient time and resources towards addressing prevailing issues and emerging challenges within the realm of higher education, as opposed to attending to trivial tasks [44]. In John Seeley and Allan Collins' opinion, authentic learning methods are "not just beneficial; they are crucial" [45]. Still, the problem existing in the current system is that despite knowing the importance of technology and authentic learning, students are deprived of an authentic environment because of the cost associated with it [46]. The old and lessen lightening syllabus makes the students follow lab guides making the slightest logical investigation. The exams are passed through cramming, while experimental testing is plagiarized, all to pass the system and get a job [47].

4 Methodology

The outcomes of the research are described via the use of quantitative analysis to acquire a comprehension of the concept of genuine learning and assessment of the responses received from the respondents. The researchers who were working in this facility made use of prototype software in order to replicate the circumstances that would be present outside of the laboratory. When formulating the survey questions, the prototype was used as a point of reference, and the questions were designed with the intention of symbolically representing the aforementioned real-world notion. The idea of "real learning" served as the drive for constructing and building the prototype, which put a considerable focus on utilizing concrete examples to transmit more general conceptualizations. The prototype was created and built with the intention of demonstrating how "real learning" might be achieved. After the addition of genuine particulars, studies were carried out to determine how well the prototype adhered to the constraints of the real world. These investigations were carried out to find out how well the prototype confirmed. The individuals who take part in the survey contribute their past knowledge as well as the experiences they have had to the total effort being made to address the present situation. In the survey, respondents are tested to see how well they recall the concepts introduced by the prototype and how successfully they can relay those ideas to others. A graphical representation of the concept will be generated by the computer based on the information that is provided. The information that is shown in the info graphics has been condensed and made more straightforward in order to make it easier for the reader to grasp the concepts that have been presented. After the user has completed the application's learning cycle, they are presented with a questionnaire to determine the extent to which they have benefited emotionally from their time spent using the program. They were developed by the use of the findings from the survey and the analysis to demonstrate that the prototype was successful. These four fundamental scientific areas served as the foundation for the creation of a prototype mobile application that is comprised of four displays. The educational material, the manner in which it was provided, and an analysis of the students'

recorded responses were the most important factors that needed to be taken into account throughout the process of developing the prototype. Initially, the idea for the prototype was being spoken about while it was being referred to as the "Egg Float Test."

The question "Does the user know the difference between a healthy chicken egg and a rotten chicken egg?" was placed on the first screen of the prototype. This was done so as to determine whether or not the user was familiar with the concept. The purpose of the concept was to assess the user's level of familiarity with the topic. The demonstrations that came before it included both visual and video representations of the abilities that were being shown. To raise people's knowledge of hydrogen, this concept was devised with the intention of creating similarities between the scientific study of gas and an issue that occurs in the real world. The second concept, which was used in the method of spreading information on hydrogen and was referred to as "Paper Bag Magic, "The prototype includes the "Save Green Vegetables" idea, which proposes to teach consumers about magnesium; the "Car Screens" concept, which intends to educate customers about carbon gas emissions; and both of these ideas' respective goals of educating customers about magnesium and about carbon gas emissions. The first endeavor tries to educate consumers about magnesium, while the second endeavor seeks to educate customers about the emissions of carbon dioxide and other greenhouse gases. The objective of providing information to customers is shared by both of these ideas. Following this, a poll was conducted in an effort to determine the level of comprehension shown by the respondents.

5 Feedback Survey Methodology

A study was conducted to investigate the effectiveness of an e-learning framework based on authentic learning. The research was conducted by selecting 98 students at random. Given the anticipated difficulty in obtaining data from the entire population of children, we opted to utilize a restricted sample size for our study. The study's participants exhibited a diverse range of academic levels, spanning from undergraduate students to Ph.D. candidates, as well as a wide range of ages. The age range of the participants spanned from 18 to 38 years old. Each individual received a participant information document. All survey participants comprehended and consented to the established terms and conditions. The fundamental aspect of the authentic learning approach involves imparting educational concepts through real-world illustrations. In this regard, a questionnaire was developed to scrutinize the users' pre-existing knowledge, comprehension level, and degree of assimilation of the concept introduced in the Authentic Lab. The centrality of authentic learning lies in the utilization of real-world contexts as exemplars for learning. During the initial phase, an examination was conducted on various concerns and subjects pertaining to practical learning.

- It is crucial to take into account the outcomes of continuous research endeavors pertaining to diverse scientific concepts.
- What was the student's evaluation of the usability?
- Has the fundamental idea of the experiment been comprehended? Either quantitative or qualitative metrics could be employed.

- Did the individual who responded encounter difficulty in comprehending the concept? Analysis can be classified into two categories: qualitative and quantitative.

The survey conducted in this study was comprised of 14 questions. The questions included in the survey are listed. As mentioned in the literature review, the authentic learning environment is based on real-world problems; all the items are constructed and framed on the same concept. All the survey questions utilized a 5-point Likert scale. We discussed four primary concepts while working within the constraints of this prototype. Table 1 displays the four scientific concepts that were used in the development of the prototype. These concepts correlate to the items on the list that span Questions 2 to 13.

Table 1. Question and concept sets description

Question No.	Concept Name	Concept Set
1	The Float Test	2,3,4
2	Paper Bag Magic	5,6,7
3	Save Green Vegetables	8,9,10
4	Car Screens/Shades	11,12,13

All the analysis is based on these four sets of questions. In each set of three questions framed the two that followed. The leading question in each set was taken to be the most important one. The third and fourth questions were developed as a direct result of the second. We made questions 6 and 7 for the sixth inquiry. We derived #9 and #10 from #8. In addition, the answers to question 11 were used to create questions 12 and 13. Some familiarity with the material was required to answer any of the crucial questions. The purpose of the research was to assess the prototype's user interface effectiveness. The two main types of questions that users want to have addressed are as follows: (a) "How easily have users understood the concept behind the scientific discussion for the question?" (b) "How well have users grasped the idea underlying the scientific discussion in response to question 2?" The same format was used for each question. Table 2 below displays the exact analytic order of the questions within each category. It also demonstrates the connections between the provided question banks and the core values of a true educational experience, which is a nice addition. Table 3 provides the Questions set with their Measuring Parameters.

6 Analysis of Data

Newman and his colleagues introduced a set of standards for authentic learning pedagogy and its evaluation. The previously mentioned requirements were evaluated with a focus on the analysis of advanced cognitive skills, the extent of knowledge acquisition, and the applicability of the subject matter to real-world contexts [48]. As per the authors' findings cited in references [5, 49], it is imperative to incorporate differentiators as a crucial component of the dynamic and genuine learning sphere. The differentiators

Table 2. Authentic Learning Attributes Description and Concept Sets

Set	Purpose of Provision	Comprehensiveness	Study Field	Potential Exploration
1	The individual was queried regarding their ability to differentiate between a viable egg and a spoiled one	To make the material easy to understand, it has been simplified	In this practical illustration, the subject matter is chemistry. The user gains knowledge of the physical and chemical characteristics of sulfur and hydrogen	The user was provided with a description of the concept and accompanying videos to enhance their understanding of the subject matter
2	The user was questioned about if they were aware of any quick methods for accelerating the ripening of fruits	To make the material easy to understand, it has been simplified	Chemistry is the subject matter of this collection. The user gains knowledge about carbon and hydrogen	The user was provided with a description of the concept and accompanying videos to enhance their understanding of the subject matter
3	I asked the user if they were familiar with any methods to prevent vegetables from turning green during the cooking process	To make the material easy to understand, it has been simplified	Chemistry is the area of study in this group. The user gains knowledge about magnesium's physicochemical characteristics	The user was presented with a comprehensive exposition of the concept, along with supplementary visual aids that served to enhance their understanding of the subject matter
4	The user was questioned regarding the rationale behind the integration of window shades and displays into automobiles	To make the material easy to understand, it has been simplified	The topic areas of biology and chemistry are covered throughout this set of textbooks. The user is provided with information on greenhouse gases	The user was presented with a comprehensive exposition of the concept, along with supplementary visual aids that served to enhance their understanding of the subject matter

can comprise unique communication, and they build an understanding of the concept. Based on the presented studies, two parameters were established to be researched in this study. These two parameters include perception and memory retention of concepts. Understanding of ideas is also considered a primary requirement of authentic learning by

Table 3. Measuring parameters of questions set

Measurements	Question No.
The concept Prior to understanding	2,5,8,11
The ease of understanding the concept of extent of via Authentic Lab	3,6,9,12
The concept of remembering the extent	4,7,10,13

researchers [28, 36, 46]. Also, remember plays a vital role in the retention of concepts to be used later in a problem-solving scenario. Table 4 provides the parameters considered and their corresponding questions added in the survey. In order to examine the data, we first counted how often each of the replies was provided, and then we calculated the percentages. The results of the Likert scale were put through an ANOVA and analyzed using the PROC GLM program in SAS 9.4 (SAS Institute, Cary, NC, USA) [47].

Table 4. Parameters and corresponding questions

Parameters	Corresponding Questions
The ease of understanding the extent of P1	Questions. 03
	Questions. 06
	Questions. 09
	Questions. 12
The numbering concept of the extent of P2	Questions. 04
	Questions. 07
	Questions. 10
	Questions. 13

An online survey was carried out to evaluate the success of an authentic learning-based e-learning framework. Out of the 98 students who took part in the survey, 9.18% (or 9 students) provided incomplete responses, while the remaining 90.82% (or 89 students) completed the survey in its entirety. The study required individuals within the age range of 18 to 38 years old, regardless of their educational background, which may include attainment of a bachelor's, master's, or doctorate degree. Error! The cited source could not be located. The reference source was not located, resulting in an error. This report presents a synopsis of the data pertaining to the ages and educational backgrounds of the participants (Figs. 1 and 2).

The majority of the people who took part in the study and said they had used an e-learning program in the past were between the ages of 23 and 27. In all, 44 people said that they had previous experience employing an e-learning tool, while just 12 respondents indicated that they lacked expertise with software of this kind. Individuals in this age range had the second-highest prevalence of past experience with e-learning, and they made up the demographic group with the second-highest prevalence overall. According

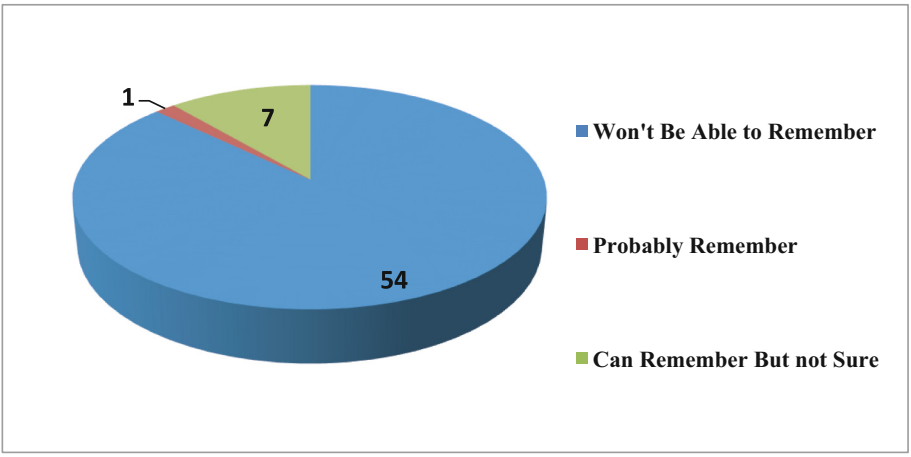


Fig. 1. Description of the Educational Level Respondents.

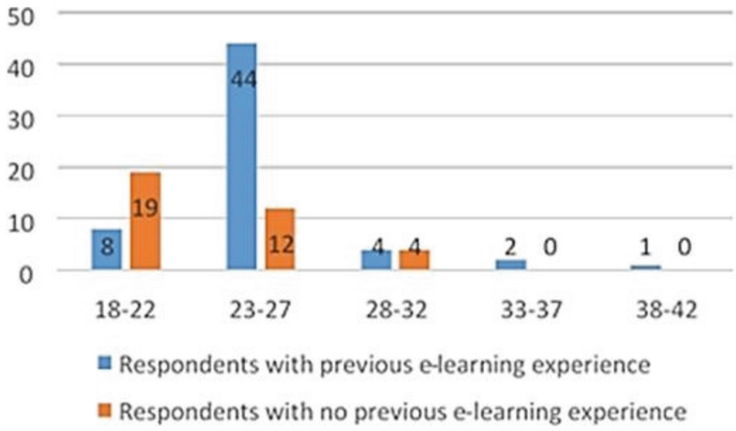


Fig. 2. Description of Respondents by Age Group Classification

to the educational backgrounds of the participants, as stated in Error!, a considerable number of persons who possessed previous exposure to elearning had successfully finished their undergraduate studies. This was the case for the majority of those individuals who had prior exposure to e-learning. The source of the information was not identified in the reference. The succeeding cohort, which included those who had advanced degrees and accounted for 11% of the overall sample, shown previous experience with e-learning.

7 The Concept of Ease of Understanding and Remembering

The report provides an illustration of the participants' previous educational backgrounds in relation to the topics addressed in the current laboratory prototype. The results indicate that a mere 25% of participants possessed antecedent comprehension of said concepts, while 73% of respondents lacked any previous familiarity. As per the provided data, a majority of 73% of the survey participants reported no prior usage of e-learning applications. Although the individual lacked pertinent experience, their comprehension level yielded favorable outcomes. The acquisition of the reference source posed difficulties, as indicated by 48% of the participants. Additionally, 31% of the respondents reported that comprehending the principles presented in the application was only somewhat challenging. A fundamental understanding of the concept is reported by 79% of the respondents. The third criterion of measurement pertains to the probability of retaining knowledge acquired through the Authentic Lab experience (Figs. 3–5).

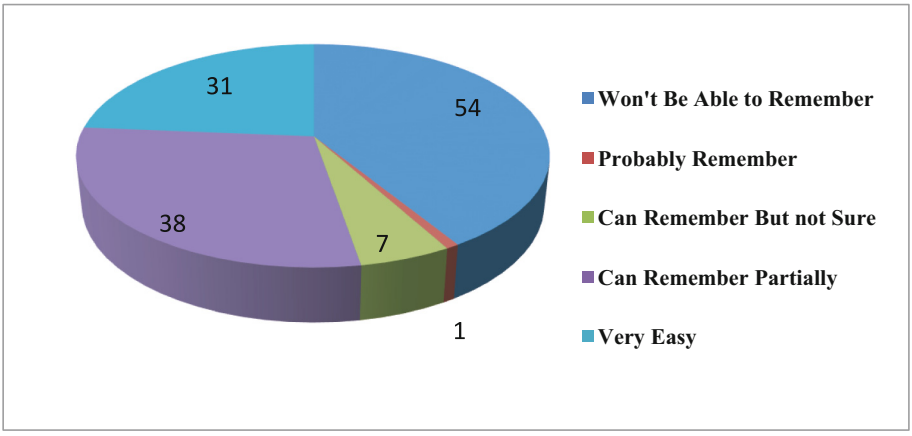


Fig. 3. Ease of Understanding the Concept of Percentage of Respondents

Participants in the usability testing of the prototype's prototype were asked to rate their "likelihood of remembering the concept," and the answers they provided varied greatly. On a scale of one to five, where one means "will not be able to remember at all" and five means "can remember partially," most respondents claimed they had positive responses. Every student accepted the concept to some extent, as shown by the fact that no student scored 1. 92 to 4 people comprehended the concept, with the first figure being the more typical result. This outcome is consistent with the study's objective: to speed up the learning process by imitating real-world circumstances in an environment created especially for that purpose. The following conclusions were established after thoroughly investigating the variables that affect qualities, including age, the breadth of prior experience, and educational background. We will review the first four subjects again and react to the poll questions in this part. The second question asked whether it was feasible to tell the difference between a fresh and ruined egg in case you missed it the first time. To ascertain the respondents' "likelihood to remember" and "ease of

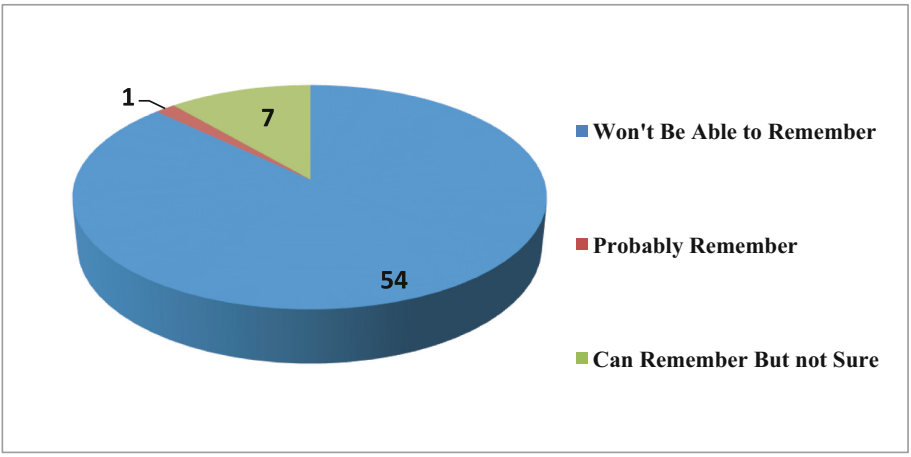


Fig. 4. Prior Experience of Respondents

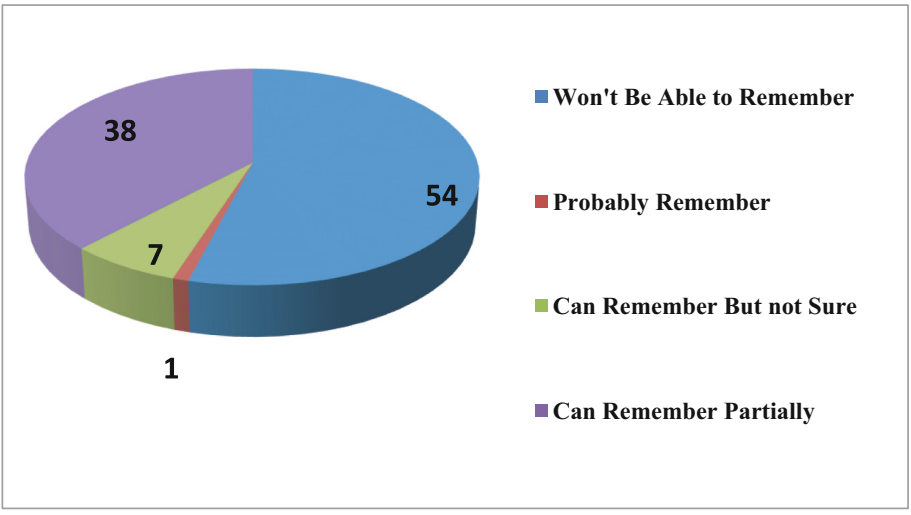


Fig. 5. To Remember the Concept of Percentage of Respondents on Likeliness

understanding" of the concepts contained in the thinking set, questions 3 and 4 asked about those concepts. Table 5 lists the concept set questions with compressed names that may be categorized under the "ease" and "remember" subcategories.

8 Discussion

An authentic learning environment will always include collaboration, real-world application, realworld applicability, in-depth inquiry, access to various sources and points of view, cumulative evaluation, and reflection. Only the qualities tested for in the Authentic

Lab, which was only meant to test a subset of the characteristics that were the focus of the investigation, were taken into account. This was because the Authentic Lab was created to test only those characteristics. In this part, we will discuss features such as the potential for exploration, the offers of purpose, and how we included these characteristics in the application prototype. Specifically, we will discuss the possibility of exploration and purpose offerings. According to the findings in Table 5, there was no discernible difference between the groups concerning the ease with which they learned about the topic or their capacity to remember the knowledge, regardless of whether the participants had prior experience. Once again, they provided comments that were in the high percentage range when asked how probable it was that they would recall the concepts. The data in Table 5 indicates how the software was developed to be user-friendly enough so that even inexperienced users could use it effectively.

Table 5. Analysis of results in comparison to Age, experience, and education

Main Effects	Egg		Fruit		Vegetable		Screens	
	Ease	Remember	Ease	Remember	Ease	Remember	Ease	Remember
Age								
18-22	3.53 ± 0.31	4.39 ± 0.24	3.94 ± 0.33	3.91 ± 0.29	4.51 ± 0.32	4.92 ± 0.28	4.43 ± 0.31	4.55 ± 0.25
23-27	3.76 ± 0.30	4.52 ± 0.23	3.94 ± 0.32	3.95 ± 0.28	4.55 ± 0.31	4.96 ± 0.27	4.31 ± 0.29	4.50 ± 0.24
28-32	4.40 ± 0.32	4.67 ± 0.25	3.95 ± 0.34	3.92 ± 0.31	4.22 ± 0.33	4.53 ± 0.29	4.12 ± 0.32	4.38 ± 0.26
33-37	4.19 ± 0.50	4.04 ± 0.40	3.43 ± 0.54	2.90 ± 0.48	3.91 ± 0.52	4.03 ± 0.46	4.32 ± 0.50	4.09 ± 0.40
P-Value	0.2040	0.3502	0.8325	0.2359	0.7504	0.3975	0.8373	0.8362
Experience								
May be	4.12 ± 0.55	4.49 ± 0.43	3.63 ± 0.59	2.74 ± 0.52	4.66 ± 0.57	5.06 ± 0.50	4.13 ± 0.55	3.98 ± 0.44
No	3.82 ± 0.16	4.36 ± 0.13	3.91 ± 0.18	4.18 ± 0.16	4.14 ± 0.17	4.51 ± 0.15	4.39 ± 0.16	4.65 ± 0.13
Yes	3.98 ± 0.16	4.36 ± 0.13	3.91 ± 0.18	4.08 ± 0.16	4.10 ± 0.17	4.26 ± 0.15	4.38 ± 0.16	4.51 ± 0.13
P-Value	0.4146	0.9560	0.5227	0.9463	0.2833	0.1386	0.2677	0.7407
Education								
Masters	3.95 ± 0.29	4.36 ± 0.23	3.91 ± 0.31	3.61 ± 0.28	4.18 ± 0.30	4.42 ± 0.27	4.05 ± 0.29	4.36 ± 0.23
PhD	3.68 ± 0.42	4.42 ± 0.33	3.97 ± 0.45	3.72 ± 0.40	4.79 ± 0.43	5.18 ± 0.38	4.81 ± 0.42	4.55 ± 0.34
Undergrad	4.29 ± 0.28	4.43 ± 0.22	3.55 ± 0.30	3.68 ± 0.27	3.92 ± 0.29	4.23 ± 0.26	4.03 ± 0.28	4.23 ± 0.22
P-Value	0.5939	0.9556	0.8925	0.0253	0.6181	0.1496	0.8888	0.2359

Regarding the investigated factors, there was not a discernible difference between the participants in terms of their ages, their levels of experience, or the degrees of education they held. Users rated each criterion based on how important it was to them using the Likert scale, which ranged from one to five points. All of the criteria received ratings that were greater than three, indicating that users had a positive response to the app and that it successfully conveyed knowledge in a manner that was congruent with the principles of authentic learning. Using this scale allowed for measuring the degree to which the research participants accepted the application.

The p-value in the above table signifies the statistical significance where a smaller (typically ≤ 0.05) value indicates a positive sign against the theory, while a more significant value indicates weak evidence against the theory. A marginal p-value leaves the decision on the decision-maker as to what the conclusion is. The data show that

recognizing the fruit idea produced a significant p-value in the education category. This specific investigation was the most difficult for all the participants, which may assist in explaining why it yielded such essential results. Having a higher level of education may make it simpler to rapidly understand and recall complicated concepts, which may help explain why the education category had a significant impact. The p-values of other attributes show a firm agreement with the hypothesis and signify the importance of e-learning in an authentic domain.

9 Conclusion

This study demonstrates how e-learning frameworks provide real-world ideas. Integrating concepts through the "use of real-world problems" is just one of the many characteristics of authentic learning. This is only one of these qualities. E-learning and sincerity contributed to the design and construction of the prototype, which encouraged the user to comprehend the concepts, permitted exploration, and displayed all of the relevant data. This was accomplished by simultaneously providing access to these features to the user. After participants evaluated the prototype, they were sent a web-based questionnaire. This form's foundation consisted of two essential requirements for all inquiries in the four distinct categories. These characteristics include the ease of understanding an idea (P1) and the likelihood that the ideas will be remembered (P2). Other variables, such as the respondent's age, degree of education, and prior exposure to e-learning programs, were evaluated alongside these parameters.

The data analysis demonstrated that both measures produced positive results compared to the specified criteria. After accounting for all variables, the results showed a modest variation. Age, prior experience, and educational level have little bearing on the perceived ease of comprehension and the likelihood of concept retention. This conclusion is bolstered by the fact that it is unquestionable, which provides more support.

References

1. Howland, J.L., Jonassen, D.H., Marra, R.M.: Meaningful Learning with Technology: Pearson New International Edition. Pearson Higher Ed. (2022)
2. Revington, S.: Authentic Learning - What is it? The Hong Kong Institute of Education. Retrieved, L. B. Har, Authentic learning (2022). http://authenticlearning.weebly.com/. Accessed 2 Jan 2022
3. Banas, J.R., York, C.S.: Authentic learning exercises as a means to influence preservice teachers' technology integration self-efficacy and intentions to integrate technology. Australasian J. Educ. Technol. **30**(6) (2020)
4. Lombardi, M.M.: Authentic learning for the 21st century: An overview. Educause Learning Initiative **1**(2020), 1–12 (2020)
5. Amory, A.: Instructivist ideology: education technology embracing the past? Interact. Learn. Environ. **20**(1), 41–55 (2019)
6. Diamond, S., Middleton, A., Mather, R.: A cross-faculty simulation model for authentic learning. Innov. Educ. Teach. Int. **48**(1), 25–35 (2011)
7. Herrington, J., Parker, J.: Emerging technologies as cognitive tools for authentic learning. Br. J. Edu. Technol. **44**(4), 607–615 (2019)

8. Herrington, J., Reeves, T.C., Oliver, R.: Authentic learning environments. In: Handbook of research on educational communications and technology, p. 401412. Springer (2018)
9. Pu, Y.H., Wu, T.T., Chiu, P.S., Huang, Y.M.: The design and implementation of authentic learning with mobile technology in vocational nursing practice course. Br. J. Edu. Technol. **47**(3), 494–509 (2016)
10. Tabuenca, B., Kalz, M., Ternier, S., Specht, M.: Mobile authoring of open educational resources for authentic learning scenarios. Univ. Access Inf. Soc. **15**(3), 329–343 (2016)
11. Moreno, R., Mayer, R.E.: Cognitive principles of multimedia learning: The role of modality and contiguity. J. Educ. Psychol. **91**(2), 358 (1999)
12. Glendinning, M.: Digging into history: Authentic learning through archeology. Hist. Teach. **38**(2), 209–223 (2005)
13. Parry, G., Reynoldson, C.: Creating an Authentic Learning Environment in Economics for MBA Studies. In: Authentic Learning Environments in Higher Education, pp. 76–87. IGI Global (2006)
14. Fitzsimmons, J.: Speaking snake: Authentic learning and the study of literature. In: Authentic learning environments in higher education, pp. 162–171. IGI Global (2006)
15. Koenders, A.: An authentic online learning environment in university introductory biology. In Authentic learning environments in higher education, pp. 48–60. IGI Global (2006)
16. Jonassen, D.H., Reeves, T.C., Hong, N., Harvey, D., Peters, K.: Concept mapping as cognitive learning and assessment tools. J. Interact. Learn. Res. **8**(3), 289 (1997)
17. Sun, P.-C., Tsai, R.J., Finger, G., Chen, Y.-Y., Yeh, D.: What drives a successful eLearning? an empirical investigation of the critical factors influencing learner satisfaction. Comput. Educ. **50**(4), 1183–1202 (2008)
18. Arbaugh, J.B.: Managing the online classroom: a study of technological and behavioral characteristics of web-based MBA courses. J. High Technol. Managem. Res. **13**(2), 203–223 (2002)
19. Thurmond, V.A., Wambach, K., Connors, H.R., Frey, B.B.: Evaluation of student satisfaction: determining the impact of a web-based environment by controlling for student characteristics. The American J. Dista. Educ. **16**(3), 169–190 (2002)
20. Herrington, J., Kervin, L.: Authentic learning supported by technology: ten suggestions and cases of integration in classrooms. Educ. Media Int. **44**(3), 219236 (2007)
21. Levy, F., Murnane, R.: How computerized work and globalization shape human skill demands. Harvard University, Department of Urban Studies and Planning, Cambridge, MA (2005)
22. Jonassen, D.H.: Interactive lesson designs: A taxonomy. Educ. Technol. **25**(6), 7–17 (1985)
23. Bransford, J., Sherwood, R., Hasselbring, T., Kinzer, C., Williams, S.: Anchored Instruction. Why we need it and how technology can help. In: Nix, D., Spiro, R. (eds.) Cognition, education, and multimedia: Exploring ideas in high technology. Lawrence Erlbaum Associates (1990)
24. Brown, A.L.: Design experiments: theoretical and methodological challenges in creating complex interventions in classroom settings. J. Learn. Sci. **2**(2), 141–178 (1992)
25. Lave, J., Wenger, E.: Situated learning: Legitimate peripheral participation. Cambridge University Press (1991)
26. Greenfield, P.M.: A theory of the teacher in the learning activities of everyday life. Everyday cognition: Its development in social context (1984)
27. Ferry, B., Kervin, L., Carrington, L.: ClassSim: an approach to educator development through a simulation. In: Virtual Learning Environments: Concepts, Methodologies, Tools and Applications, pp. 591–605. IGI Global (2012)
28. Rysavy, S.D.M., Sales, G.C.: Cooperative learning in computer-based instruction. Education Tech. Research Dev. **39**(2), 70–79 (1991)

29. Lee, S.J., Srinivasan, S., Trail, T., Lewis, D., Lopez, S.: Examining the relationship among student perception of support, course satisfaction, and learning outcomes in online learning. The Internet and Higher Education **14**(3), 158–163 (2011)
30. Hoban, G.: Teaching science concepts in higher education classes with slow motion animation. In: E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education, pp. 1641–1646. Association for the Advancement of Computing in Education (AACE) (2006)
31. Herrington, J., Reeves, T.C., Oliver, R.: A practical guide to authentic e-learning. Routledge (2009)
32. Chang, T.-W., Huang, R.: Authentic Learning Through Advances in Technologies. Springer (2018)
33. Herrington, J.: Authentic e-learning in higher education (2009)
34. Churchill, D.: Learning objects: an interactive representation and a mediating tool in a learning activity. Educ. Media Int. **42**(4), 333–349 (2005)
35. Preus, B.: Authentic instruction for 21st century learning: Higher order thinking in an inclusive school. American Secondary Education, pp. 59–79 (2012)
36. Wolf, D., Bixby, J., Glenn III, J., Gardner, H.: Chapter 2: To use their minds well: Investigating new forms of student assessment. Review of Research in Education **17**(1), 31–74 (1991)
37. Winardi, A.: Using multiple intelligences approach in designing classroom activities. Sino-US English Teaching **13**(3), 191–196 (2016)
38. Campbell, L., Campbell, B., Dickinson, D.: Teaching & Learning through Multiple Intelligences. ERIC (1996)
39. Bozalek, V., et al.: The use of emerging technologies for authentic learning: A South African study in higher education. Br. J. Edu. Technol. **44**(4), 629–638 (2013)
40. Herrington, J., Ostashewski, N., Reid, D., Flintoff, K.: Mobile technologies in teacher education: Preparing pre-service teachers and teacher educators for mobile learning. In: Successful teacher education, pp. 137–151. Brill Sense (2014)
41. Wilson, J., Schwier, R.: Authenticity in the process of learning about instructional design. Canadian Journal of Learning and Technology/La revue canadienne de l'apprentissage et de la technologie **35**(2) (2010)
42. Clinton, G., Rieber, L.P.: The studio experience at the University of Georgia: An example of constructionist learning for adults. Educ. Tech. Res. Dev. **58**(6), 755–780 (2010)
43. Herrington, A., Herrington, J.: What is an authentic learning environment? Authentic Learning Environments in Higher Education, 1 (2006)
44. Brown, J.S., Collins, A., Duguid, P.: Situated cognition and the culture of learning. Educ. Res. **18**(1), 32–42 (1989)
45. Quigley, C.: Expanding our view of authentic learning: bridging in and out-of-school experiences. Cult. Sci. Edu. **9**(1), 115–122 (2014)
46. Braund, M., Reiss, M.: Towards a more authentic science curriculum: The contribution of out-of-school learning. Int. J. Sci. Educ. **28**(12), 13731388 (2006)
47. Newmann, F.M.: Authentic pedagogy: Standards that boost student performance. Issues in Restructuring Schools (1995)

Securing Cyber-Physical Systems by Using Artificial Intelligence

Muhammad Umar, Majid Hussain(✉), Hina Zafar, and Amna Iqbal

The University of Faisalabad, Faisalabad, Pakistan
Hod.cs.ew@puf.edu.pk

Abstract. Security is a main issue in Cyber-Physical Systems. Experts emphasize that Intrusion detection is a critical task for ensuring the security of computer networks. Detecting suspicious activities and generating alerts when an intrusion is detected is crucial for system monitoring. Various solutions are presented in the literature for intrusion detection but many anomalies and breaches are still a Problem for experts to eliminate the intrusion risk in Cyber-physical systems (CPS). The proposed method investigates the application of data normalization, principal component analysis (PCA), and neural networks for detecting attacks on the KDD99 dataset. It is clearly observed that dimensionality reduction using PCA is effective for this dataset. Further Neural Network model is used as an attack detection module on the transformed data. The proposed method achieves high accuracy in detecting both known and unknown attacks while reducing false positives, consistent with prior research. The proposed solution has practical implications for enhancing intrusion detection systems' effectiveness and improving computer network security and increase the accuracy 97%.

Keywords: Cyber-physical systems (CPS) · cyberattacks · Artificial Intelligence (AI) · Machine Learning (ML) · Linear Discriminant Analysis (LDA) · Principal Component Analysis (PCA) · Artificial Neural Networks (ANN) · The Industrial Internet of Things (IIoT)

1 Introduction

Cyber-physical systems (CPS) have been used in a number of industries recently and have steadily gained popularity. System monitoring requires the detection of anomalous activities and the generation of alerts when an intrusion is identified [1, 2].

Cyber-physical systems commonly have three surfaces hardware, software, and network as collectively they make up the essential components of a CPS. The Industrial Internet of Things (IIoT) has classified Cyber-Physical Systems (CPS) as one of its major components, and Industry v4.0 is expected to heavily rely on them [3]. CPS makes it possible for real-time, accurate operation of smart applications and services. They are built on the fusion of cyber and physical systems, which instantly interchange different kinds of data and sensitive information [4]. The advancement of Cyber-Physical

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 239–248, 2025.
https://doi.org/10.1007/978-3-031-77620-5_17

Systems (CPS) is a collaborative effort among academic researchers and industry manufacturers. Researchers focusing on fundamental research and exploring new ideas, while manufacturers apply this knowledge to develop practical applications and products [5].

As Cyber-Physical Systems (CPSs) become more complex and interconnected, there is a growing concern for their cybersecurity, especially since these systems have been adopted across multiple critical infrastructure sectors. CPSs rely heavily on computer networks and control systems, making them vulnerable to potential breaches [6]. The interconnected nature of cyber and physical components means that cyber-attacks could cause physical harm or disruptions. As a result, CPSs are particularly susceptible to cyber-attacks and require robust security measures to ensure their integrity and reliability [7]. Conventional Intrusion detection and prevention systems (IDS/IPS) and access control alone are inadequate for identifying halt, or obstruct zero-day attacks as they are not stored in the security system's databases due to their unique nature. However, cyber security solutions that utilize artificial intelligence are capable of safeguarding CPSs from zero-day attacks [8].

Various industries, including manufacturing, transportation, energy, and healthcare, widely employ cyber-physical systems for their operations. As such, they are also a target for cyberattacks [9]. It is important to note that these are just some examples of attacks that can target CPS and that the nature and severity of attacks can vary depending on the specific system and its use case. As such, it is crucial for organizations to implement robust cybersecurity measures and regularly update and test their systems to ensure their resilience against cyberattacks [10].

Collaboration between various AI and ML technologies is imperative for the mitigation of zero-day attacks, in addition to the participation of security experts [11]. The aim of collaborating between humans and machines is to reduce the occurrence of false convictions, and as such, human decision-making can enhance the detection mechanism. Ad hoc networks or the Internet are employed to exchange communication and control signals among various components of Cyber-Physical Systems (CPS). This renders the system vulnerable to network-based attacks that can have severe consequences both in cyberspace and the physical world [12]. All components of the CPS can be targeted in cyber-attacks that can lead to structural malfunctions and disruption of physical processes. Traditional machine-learning approaches are utilized to detect such attacks, but they face difficulties in assessing them when networks are complex and information about the system is limited [13]. To address this challenge, artificial intelligence techniques can significantly improve the effectiveness of neural networks by using multiple layers to move from simple to complex characteristics. Despite several successful implementations, training-based methodologies have shown limitations due to the diverse nature of physical processes [14]. In this regard, the ANN approach is proposed to overcome these limitations and achieve high detection accuracy of cyberattacks with minimal model errors.

Feature selection is a crucial aspect of machine learning that seeks to identify and select the most relevant features that contribute to a model's ability to make accurate predictions. In machine learning, the ultimate objective is to develop models that can generalize well to new data. Feature selection plays a crucial role in achieving this goal. Improved understanding of data feature extraction also provides researchers with insights into the data's underlying structure, allowing them to better comprehend the relationships between the features and the target variable [15].

The main purpose of performing feature selection is to mitigate the problems of overfitting and underfitting in the model. Overfitting arises when the model is overly complex and captures the noise in the data, resulting in poor performance on new data. Underfitting, on the other hand, arises when the model is too simple and fails to capture the underlying patterns in the data, resulting in inadequate performance [16]. A commonly utilized approach in machine learning for feature extraction is Principal Component Analysis (PCA). Regarding the KDD99 dataset, PCA helped us to identify the most important features for intrusion detection. PCA is a data transformation technique that converts the initial dataset into a group of principal components that are uncorrelated and arranged by the level of variance they account for in the data. By retaining the essential information, the dimensionality of the dataset is reduced through the use of PCA. The process of PCA includes standardization, covariance matrix computation, Eigendecomposition, selection of principal components, and transformation. The most important principal components, determined by the largest eigenvalues, are selected. The original data is then transformed into the new space defined by these principal components. PCA has the potential to enhance the performance of machine learning models and expedite the training process for intrusion detection by reducing the dataset's dimensionality while maintaining its essential information [17]. ANN is used as an attack detection module, Artificial Neural Networks helped to classify network traffic data into normal or anomalous traffic. In the context of the KDD99 dataset, ANN learns patterns in the data to differentiate between normal and malicious traffic. The process involves data preprocessing, model training on a labeled dataset, model evaluation on a separate dataset, and model optimization by adjusting hyperparameters. Neural network-based detection improves the accuracy and speed of attack detection compared to traditional rule-based methods. It can detect attacks that may not be caught by rule-based systems by learning patterns in the data.

2 Related Work

Various studies have been conducted to detect cyber risks in commercial cyber-physical systems (CPSs) using Deep Learning (DL) and Machine Learning (ML) methods [18]. Deep Fed, a distributed machine learning method that utilizes a deep neural network with a gated recurrent unit to detect cyber risks in Cyber-Physical Systems [19]. Another study utilized deep convolutional neural networks to identify distributed denialof-service attacks, while a different one presented a DL-driven methodology for examining the literature on cyber breaches in CPS systems [20]. Additionally, studies have examined techniques for DL-based anomaly detection, identifying IoT dangers in CPS, and using unsupervised methods for detecting cyber-attacks in CPSs [21]. Some studies have also

focused on the security of healthcare systems and the integration of cyberphysical systems [22]. Overall, these studies reveal the risks associated with CPSs and the potential of ML and DL methods in detecting and mitigating cyber threats to CPSs [23].

Cyberattacks have become a growing concern in the modern era, with various parties, including individuals, companies, and even independent states, perpetrating them for different purposes [24]. The objectives of cyberattacks can vary, ranging from infecting malware on a single personal computer to launching an attack on an entire nation's critical infrastructure. The susceptibility of Cyber-Physical Systems (CPS) to various types of cyberattacks without any clear signs of failure exacerbates concerns about maintaining control [25]. The persistence of cyberattacks on CPS, which exhibit no indication of success, represents a significant threat to the organization. If the program's dynamics are not safeguarded by hardware or software, hackers are granted unrestricted freedom to cause any form of disruption they desire [26]. The challenges of controlling compromised systems are particularly significant in the context of power systems [27]. CPS can face both cyber and physical attacks, where the latter can manifest in different forms like attacking the infrastructure or manipulating measurements [28]. In order to distinguish more severe intrusions from minor data breaches, legal experts seek to restrict the term "hacking" to cases where the physical structure of a building or equipment is damaged. [29].

3 Methodology

KDD99 dataset is use as the primary source of data. Data from the CPS database is carried out as the initial step, followed by data normalization to address errors and remove duplicate entries. The feature extraction stage employs the Principal Component Analysis (PCA) technique to obtain relevant characteristics of the preprocessed data. As a technique of increasing the effectiveness of the intrusion detection system, In the optimization procedure, we used an Artificial Neural Network (ANN), serving as an attack detection module. In addition, we applied data normalization as a data preprocessing step to ensure that the data is on a common scale and reduce the impact of outliers on the PCA and neural network algorithms. Specifically, To scale the data into the range [0,1], we employed the Min-Max normalization technique. This allowed us to achieve better results with our PCA and Neural Network models (Fig. 1).

There are 22 different types of attacks represented by 41 features in the KDD99 dataset. But it is unclear whether the goal of the attacker was to gain full access or just temporary access. Table 1 presents and discusses the suggested dataset.

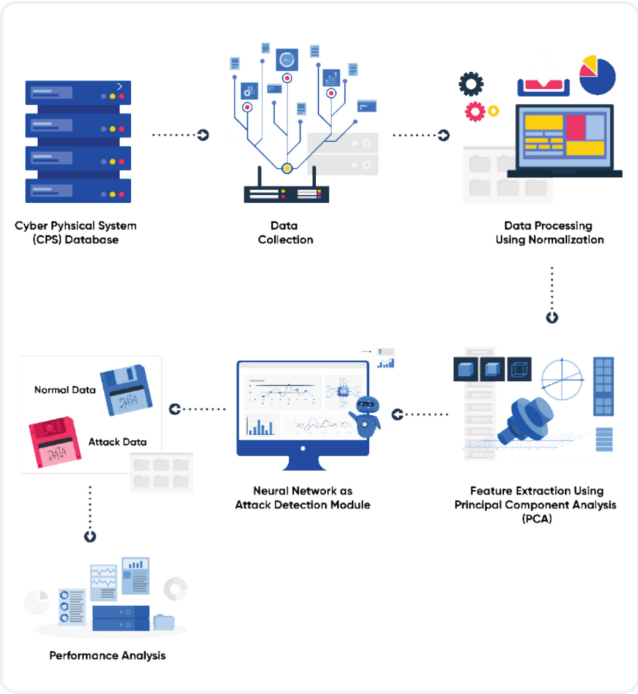


Fig. 1. The diagram depicts the recommended methodology.

3.1 Data Preprocessing and Normalization

The KDD99 dataset is pre-processed and normalized before applying PCA. The preprocessing step involves removing duplicates and handling missing values in the dataset. In the pre-processing step, we removed duplicates and handled missing values in the dataset [34]. we applied data normalization as a data pre-processing step to ensure that the data is on a common scale and reduce the impact of outliers on the PCA and neural network algorithms. Specifically, we scaled the data into the range [0, 1] using the Min-Max normalization method. This allowed us to achieve better results with our PCA and Neural Network models.

3.2 Feature Extraction Using (Principal Component Analysis) PCA

In order to reduce the dimensionality of high-dimensional data, PCA is employed for feature extraction, which involves identifying the linear combinations of original features that explain the greatest amount of variance in the data. The retained primary components are employed as input features for the neural network-based attack detection module, reducing computational complexity and overfitting potential. Examining the scree plot determines the number of primary components to keep. This improves the performance of the attack detection by lowering the amount of input characteristics in the module.

- Normalize feature data

- Apply PCA to extract principal components
- Select the desired number of components based on the variance explained

PCA aims to identify linear combinations of the original features that account for the maximum possible variance in the data. This approach helps to minimize the computational complexity of the model and reduce the risk of overfitting. The number of principal components to be retained is determined based on an analysis of the scree plot, with priority given to those that account for the greatest amount of variance in the data. The retained principal components are then utilized as input features for the neural network-based attack detection module. Through this process, PCA is leveraged for feature extraction in order to improve the performance of the attack detection module by reducing the number of input features for the neural network.

3.3 Attack Detection

Initially, the neural network's architecture is established, specifying the number of layers, the number of neurons per layer, and the activation functions employed. Next, the model is compiled with an appropriate loss function and optimizer, which will be used to update the neural network's weights during training. After compilation, the simulation is prepared on PCA-transformed Practice data using techniques like dropout regularization to prevent overfitting. Finally, the model's performance is evaluated on PCAtransformed testing data using Metrics like ROC AUC, F1-score, recall, accuracy, and precision. By following these steps, a robust neural network-based attack detection module can be developed for the KDD99 dataset, which can significantly improve the efficiency and effectiveness of network security operations.

- Define the architecture of the Neural Network
- Compile the model using a suitable loss function and optimizer
- Use the PCA for best feature selection
- Assess the model's performance on the testing data that has been transformed using PCA.

Analytical model of proposed framework for Securing Cyber-Physical Systems by Using Artificial Intelligence

```
Start: KDD99 dataset, Parameters

BDTbest_nn <- InitializeNeuralNetwork(Parameters);
BDTbest <- EvaluateCost(BDTbest_nn, KDD99 dataset);

        while (not StopCondition): for x
            in range(Parameters.W):
            Ti_nn <- GenerateNewNetwork(BDTbest_nn, Parameters);
            Ti_cost <- EvaluateCost(Ti_nn, KDD99 dataset);
                if (Ti_cost <= BDTbest): BDTbest_nn <-
                Ti_nn
                    BDTbest <- Ti_cost

UpdateWeights(BDTbest_nn, Ti_nn, Parameters);
DecayWeights(BDTbest_nn, Parameters);
DecayLearningRate(Parameters);

return BDTbest

//Preprocess the data features, labels <-
SeparateFeaturesAndLabels(KDD99)
X_train, X_test, y_train, y_test <- TrainTestSplit(features, labels)

//Perform PCA
X_train, X_test <- NormalizeData(X_train, X_test)
pca <- PCA(n_components=n)
X_train_pca <- pca.fit_transform(X_train)
X_test_pca <- pca.transform(X_test)

//Train the Neural Network model
<- Sequential()
model.add(Dense(units=n1, activation='relu', input_dim=n))
model.add(Dense(units=n2, activation='relu')) model.add(Dense(units=1,
activation='sigmoid')) model.compile(loss='binary_crossentropy', optimizer='adam',
metrics=['accuracy']) model.fit(X_train_pca, y_train, epochs=epochs,
batch_size=batch_size, validation_data=(X_test_pca, y_test))
score <- model.evaluate(X_test_pca, y_test, verbose=0)
```

Artificial Neural Network (ANN) is applied for attack detection module. Based on research findings, it can be concluded that Neural Networks are a powerful approach for intrusion detection in the KDD99 dataset. Their ability to effectively handle large datasets, robustness to noise, and adaptability to various data types make them a superior choice compared to other techniques in most scenarios [36]. Moreover, their automatic feature extraction capability and ability to provide interpretable results enhance the interpretability and usability of the attack detection module. Therefore, we use Neural Networks as a preferable option for designing effective intrusion detection systems for the KDD99 dataset. The following steps applied for model training

1. Divide the dataset into two parts: training and testing.

2. Preprocess training and test data by using the same method:
   a. Apply one-hot encoding to the categorical features.
   b. Normalize the continuous features to have zero mean and unit variance.
3. Create a neural network model with the specified architecture and parameters:
   a. Initialize the weights and biases of each layer randomly.
   b. Choose a loss function and optimization algorithm.
4. Train the neural network:
   a. For each epoch, iterate over each batch of the training set:
      i. Forward propagate the input through the network to compute the predicted output. ii. Calculate the difference between the projected and actual output. iii. Compute the gradients by back-propagating the loss through the network. iv. Use the optimization algorithm to update the weights and biases based on the gradients.
   b. Calculate the accuracy and loss of the model that has been trained on the test dataset.
5. Save the trained model for future use.
6. Return the trained neural network model.

4 Results

Performance of a proposed system to identify cyber-attacks by considering various attack factors and comparing it to existing methods, such as isolation forest, Kullback– Leibler distance, and Blockchain. The proposed approach for cyber attack detection in CPS is based on neural networks, with key parameters for assessing the system's accuracy including the recognition threshold, rate of true positive (RTP), and rate of false positive (RFP). Based on analysis, our proposed approach is more effective in achieving our objective of 97% accuracy.

Table 1. Comparison between existing and proposed Techniques (PT) Accuracy

	Isolation Forest	KLD [2]	Block Chain	Neural Network(PT)
Accuracy	45%	10%	59%	97%

5 Discussion

Proposed Solution: used normalization, PCA, and neural networks for attack detection on the KDD99 dataset. Normalization improved accuracy by scaling features, while PCA identified key characteristics and reduced dataset dimensionality [40]. Neural Network accurately detected attacks and outperformed other methods in literature. Findings are generalizable but may have limitations in other contexts, highlighting importance of normalization and PCA for improving model accuracy in attack detection.

Emphasizes the potential of neural networks and the need for effective pre-processing steps to enhance network security.

6 Conclusion

Proposed Research, explored the use of normalization, PCA, and neural networks for attack detection on the KDD99 dataset. The proposed approach achieved high accuracy for known and unknown attacks while reducing false positives. Normalizing the data and using PCA reduced computational complexity and overfitting. The neural networkbased attack detection module achieved high accuracy by identifying the principal components with the highest variance in the data. Future work can focus on testing the approach on other datasets and exploring other machine-learning algorithms for attack detection.

References

1. Yaacoub, J.P.A., Salman, O., Noura, H.N., Kaaniche, N., Chehab, A., Malli, M.: Cyber-physical systems security: Limitations, issues and future trends. Microprocess. Microsyst. **77**, 103201 (2020)
2. Almajed, R., Ibrahim, A., Abualkishik, A.Z., Mourad, N., Almansour, F.A.: Using machine learning algorithm for detection of cyber-attacks in cyber physical systems. Periodicals of Eng. Natur. Sci. **10**(3), 261–275 (2022)
3. Munir, K., Faisal, M., Khan, M.A., Naeem, M.A.: Cyber-physical systems security challenges and solutions in industry 4.0: A review. IEEE Access **9**, 58076–58102 (2021). https://doi.org/10.1109/ACCESS.2021.3079984
4. Feng, L., Zhao, H.: Cyber-physical systems security and privacy: State of the art and future directions. IEEE Trans. Industr. Inf. **16**(6), 4138–4146 (2020)
5. Kang, J., Gao, R.X.: Cyber-physical systems: A new frontier. J. Manuf. Syst. **37**, 517–527 (2015). https://doi.org/10.1016/j.jmsy.2015.06.001
6. Huang, L., Xiong, N.: Cybersecurity in cyber-physical systems. IEEE Trans. Industr. Inf. **17**(1), 250–259 (2021). https://doi.org/10.1109/TII.2020.2979319
7. Luo, L., Hu, Y., Lu, R., Chen, J.: Cybersecurity for cyber-physical systems: research challenges and opportunities. IEEE Network **34**(2), 180–186 (2020)
8. Kaspersky, M., Maghamez, R., Dehghantanha, A.: Zero-day vulnerability detection in cyber-physical systems: a systematic mapping study. Comput. Secur. **100**, 102–121 (2020)
9. Nutaro, J.J.: Cyber-physical systems and cybersecurity: a review. IEEE Trans. Industr. Inf. **14**(5), 2216–2224 (2018). https://doi.org/10.1109/TII.2017.2785584
10. Giraldo, J.A., Morales, J.A., Sánchez, Á., Villa, J.: Cybersecurity of cyber-physical systems: a review of the state of the art. Electronics **10**(8), 937 (2021)
11. Liao, Y., Xue, Y., Wang, X., Zhang, Y., Chen, H.: Collaborative defense for mitigating zero-day attacks using multi-AI and multi-ML technologies. IEEE Access **9**, 128686–128698 (2021). https://doi.org/10.1109/ACCESS.2021.3110077
12. Roy, S., Saxena, A., Hasan, M.A.: Human-machine collaboration for CyberPhysical security. IEEE Secur. Priv. **17**(1), 36–44 (2019). https://doi.org/10.1109/MSEC.2018.2872659
13. Alawadh, M.H., Almutairi, A., Alaqeel, A., Alaboud, A.: Cybersecurity challenges and solutions for cyber-physical systems: a review. IEEE Access **9**, 33583–33609 (2021)
14. Nikolopoulos, D.S., Loukas, G., Oikonomou, G.: Cybersecurity for industrial control systems: a survey. IEEE Communications Surveys & Tutorials **19**(2), 1090–1112 (2017). https://doi.org/10.1109/comst.2016.2634486
15. Peng, H., Long, F., Ding, C.: Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy. IEEE Trans. Pattern Anal. Mach. Intell. **27**(8), 1226–1238 (2005)

16. Yang, Y., Pedersen, J.O.: A comparative study on feature selection in text categorization. In: ICML, Vol. 97, pp. 412–420 (1997)
17. Huang, Z., Lu, W.: Research on intrusion detection technology based on PCA and SVM. Int. J. Online and Biomed. Eng. (iJOE) **15**(4), 114–126 (2019). https://doi.org/10.3991/ijoe.v15i04.10036
18. Chuang, H.Y., Hui, K.M.K., Li, V.O.K.: Deep learning-based cyber risk assessment for cyber-physical systems. IEEE Trans. Industr. Inf. **17**(8), 5857–5865 (2021). https://doi.org/10.1109/TII.2021.3089388
19. Alsheikh, M., Lin, S., Awwal, A.S., Zheng, H., Wang, Y.: DeepFed: distributed deep learning for cyber threat detection in IoT-enabled cyber-physical systems. IEEE Trans. Industr. Inf. **15**(10), 5677–5686 (2019). https://doi.org/10.1109/TII.2019.2929712
20. Wang, B., Lu, Z., Li, X.: A DDoS attack detection model based on deep convolutional neural networks. In: Proceedings of the International Conference on Information Networking (ICOIN) (2017). https://doi.org/10.1109/ICOIN.2017.7899496
21. IEEE Transactions on Industrial Informatics: Detection in Cyber-Physical Systems **15**(1), 91–99 (2019). https://doi.org/10.1109/TII.2018.2829539
22. Zhang, H., Chen, Q., Zhao, D., Gao, Z.: An unsupervised learning approach for detecting cyber attacks in cyber-physical systems. IEEE Trans. Industr. Inf. **14**(8), 3576–3585 (2018). https://doi.org/10.1109/TII.2018.2818898
23. Al-Eroud, R., Almiani, M., Alfarasani, I., Alabdulqader, M., Kim, H.: Machine learning for cybersecurity: trends, challenges, and future directions. IEEE Access **9**, 114935–114955 (2021). https://doi.org/10.1109/ACCESS.2021.3102835
24. Sarma, A.D., Rahman, A.K.M.M., Zhu, Y.: A survey of cyber attacks and their impact on enterprises. IEEE Commun. Surv. Tutor. **21**(1), 760–795 (2019). https://doi.org/10.1109/COMST.2018.2877455
25. Qadir, M.A., Khan, A.R., Javaid, N.: A review of cyber threats and defensive techniques in cyber-physical systems. IEEE Access **7**, 73095–73112 (2019)
26. Liu, Y., Jin, X.: A framework for cyber-physical system security: from network security to system security. IEEE Trans. Industr. Inf. **15**(4), 1919–1927 (2019). https://doi.org/10.1109/TII.2019.2891293
27. Li, Y., Chen, S., Shahidehpour, M., Zhang, J.: Cybersecurity challenges and opportunities in power systems. IEEE Transactions on Smart Grid **10**(2), 1341–1342 (2019). https://doi.org/10.1109/TSG.2018.2888929
28. Choo, K.K.R., Liu, C.C.: Cyber-physical security challenges in smart cities: a review. Sustain. Cities Soc. **51**, 101748 (2019). https://doi.org/10.1016/j.scs.2019.101748
29. Watterson, A.: The meaning of hacking in public and private law. SCRIPTed **14**(1), 6–28 (2017). https://doi.org/10.2966/scrip.140117.6

An Efficient Implementation of an IoT-Based Smart Home Security System

Zainab[1], Hamayun Khan[2], Irfan Ud Din[2(✉)], Muhammad Imran Tariq[2], Aleena Khalid[2], and Amna Naz[2]

[1] NCBA&E (WCC), Lahore 05309, Punjab, Pakistan
[2] Department of Computer Science, The Superior University, Lahore, Pakistan
irfan@superior.edu.pk

Abstract. The increasing number of home invasions and thefts has led to the need for effective home security systems. Commonly used security systems are limited in their capabilities and require manual intervention. With the advent of IoT, it is possible now to create a smart security system for homes that is automated and capable of detecting and alerting owners about any unusual activities. This research paper presents the design and implementation of an IoT-based smart home security system with enhanced capabilities. The system proposed in this paper includes a network of sensors and cameras that are connected to a central hub. The system can detect and respond to various security threats, such as suspicious intrusion, fire, and gas leakage, and can notify owners or authorized persons through their smartphones. The paper describes the system's architecture and the hardware and software components used in its implementation. It also discusses the communication protocols such as Wi-Fi and Bluetooth and algorithms which are used for data analysis and decision-making. The system's performance is evaluated through simulation and experimentation, and the results show that the system is effective in detecting and responding to security threats. This research paper provides insights into the design and implementation of an IoT-based smart home security system that can enhance the security of homes and provide owners of the home with peace of mind. The system's modular design and scalability make it suitable for use in various home sizes and configurations. The system's potential for integration with other smart home devices and services further enhances its capabilities. The system can be accessed remotely through a mobile application, providing real-time updates on security threats and allowing users to take immediate action.

Keywords: IoT · smart home · security sensors · cameras · automation · intrusion detection · fire detection · gas detection · data analysis · decision making · communication protocols · and smartphone notifications

1 Introduction

The emergence of the Internet of Things (IoT) has brought a revolution in the way we interact with the digital world, enabling a more connected and automated lifestyle. Smart homes are a new generation of homes that are equipped with various IoT devices

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 249–259, 2025.
https://doi.org/10.1007/978-3-031-77620-5_18

that allow for automation, convenience, and ease of use. With the rise of IoT devices, smart homes are becoming increasingly popular, offering a range of features such as home automation, energy management, and security. However, the increasing use of IoT devices in smart homes has also led to an increase in security concerns. Hackers and cybercriminals can easily gain access to these devices, allowing them to control their home and gain access to sensitive information. In recent years, the Internet of Things has revolutionized the way we interact with technology. With the proliferation of smart devices and sensors, it is now possible to create intelligent systems that can automate various tasks and improve our quality of life. One area where IoT can make a significant impact is smart home security [1] (Fig. 1).

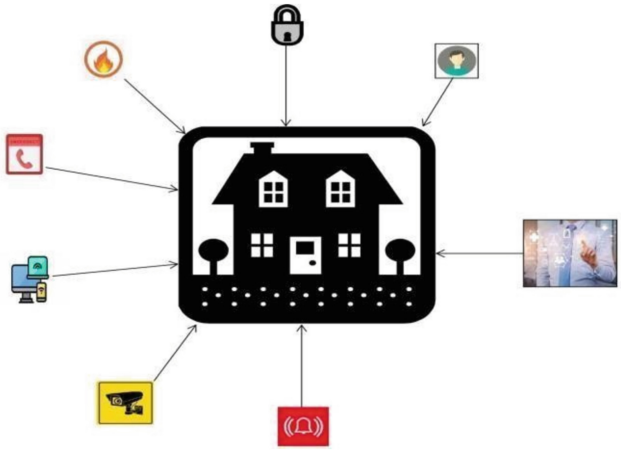


Fig. 1. IoT-based smart home security system [2]

The traditional home security systems that rely on motion sensors and alarms are often limited in their capabilities. They require manual intervention and can generate false alarms, which can be annoying and disruptive. With the advent of IoT, it is now possible to create a smart home security system that is more sophisticated, automated, and effective [3].

In this paper, researcher presents the design and implementation of an IoT-based smart home security system that is effective for even large areas and has enhanced capabilities to eliminate false alarms. The proposed system is designed to detect and respond to various security threats, such as intrusions, fire, and gas leakage, in an automated manner. The system is based on a network of sensors and cameras that are connected to a central hub. The hub is responsible for analyzing the data collected by the sensors and cameras and making decisions based on predefined rules and algorithms [4].

The proposed system has several advantages over traditional security systems. Firstly, it is more automated, which means that it can detect and respond to security threats without requiring any manual interaction. This reduces the risk of false alarms and ensures that owners of the home are notified only when there is a genuine security threat. Secondly, the system is more sophisticated, which means that it can detect a

wider range of security threats, including those that are not related to intrusion, such as fire and gas leakage. Finally, the system is more convenient, as owners of the home can be notified of security threats through the pop-up notification on their smartphones, which means that they can take immediate action such as an emergency call to mitigate the threat [5] (Fig. 2).

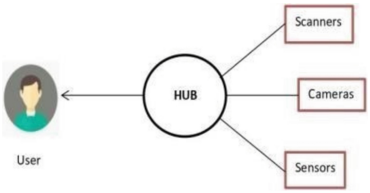


Fig. 2. Architecture of proposed security system [6]

The rest of the paper is organized as follows. In Sect. 2, we describe the architecture of the proposed system and the hardware and software components used in its implementation. In Sect. 3, we discuss the communication protocols used by the system, and in Sect. 4, we describe the machine learning algorithms used for data analysis and decision-making. In Sect. 5, we evaluate the system's performance through simulation and experimentation. Thus, this paper provides valuable insights for researchers, engineers, and practitioners working in the field of smart home security systems and IoT technology [7].

2 Literature Review

Home security systems have been around for decades, and they have evolved significantly over the years. The earliest security systems were based on simple alarms that would sound when a door or window was opened. However, these systems were limited in their capabilities and could be easily bypassed by intruders. In response to these limitations, security systems were upgraded to include motion sensors, which could detect movement within the house and trigger an alarm. While motion sensors improved the effectiveness of security systems, they still had several limitations. For instance, they could generate false alarms when pets or other small animals moved around the house. Additionally, they could not detect other security threats, such as fire or gas leakage. To address these limitations, researchers and engineers have been exploring the use of IoT in home security systems [8].

The use of IoT in home security systems has several advantages. Firstly, IoT-enabled security systems can be more automated, which means that they can detect and respond to security threats without requiring any manual intervention. This reduces the risk of false alarms and ensures that owners of the home are notified only when there is a genuine security threat. Secondly, IoT-enabled security systems can be more sophisticated, which means that they can detect a wider range of security threats, including those that are not related to intrusions, such as fire and gas leakage [9]. Finally, IoT-enabled security systems can be more convenient, as owners of the home can be notified of security

threats through their smartphones, which means that they can take immediate action to mitigate the threat.

Several researchers have explored the use of various sensors and devices to develop smart home security systems. Proposed an IoT-based smart home security system using Adriano, which integrates several sensors and sends notifications to a user's smartphone in case of security breaches. Similarly designed and implemented a smart home security system using ZigBee and IoT, which detects and alerts homeowners in case of a break-in or other security breaches [10]. The integration of cloud computing and artificial intelligence (AI) has also been explored in developing smart home security systems. Proposed a smart home automation and security system based on IoT and cloud computing, which allows remote monitoring and control of home appliances and security devices [11]. In [12] developed a smart home security system using AI algorithms to detect and prevent security threats in real time. He proposed a combination of sensors and cameras to detect security threats. The system was designed to be scalable and could be customized to meet the needs of different owners of the home. Moreover, the use of Raspberry Pi as a central hub for IoT-based smart home security systems has also been investigated. In [13] developed an IoT- based smart home automation and security system using Raspberry Pi, which integrates various sensors and devices and sends alerts to a user's smartphone in case of security breaches. A smart home security system using Raspberry Pi and an Android application, which allows users to monitor and control home appliances and security devices from their smartphones [14].

In summary, the use of IoT in home security systems has the potential to revolutionize the way we secure our homes. By leveraging the power of sensors, cameras, and machine learning algorithms, IoT- enabled security systems can be more effective, automated, and convenient than traditional security systems. The proposed system in this paper builds on previous work in this field and aims to provide a scalable and effective solution for securing homes using IoT [15].

3 Methodology

The proposed IoT-based smart home security system consists of hardwares that are placed in different areas of homes where security is needed, and software components for connection. The hardware components include motion sensors, door and window sensors, smoke detectors, gas detectors, cameras for face recognition, scanners for suspicious weapons, and a central hub while the software components include communication protocols, data analysis algorithms, and decision-making algorithms.

The cameras or scanners are used to provide visual information about security threats. The sensors and cameras are connected to a central hub, Cameras can scan, and communication protocols will transmit the information to the hub. The central hub is equipped with a microcontroller, which is responsible for analyzing and processing the data collected by the sensors and cameras and making decisions based on predefined rules and algorithms. The microcontroller is also responsible for communicating with the sensors and cameras using various communication protocols, such as Bluetooth and Wi-Fi.

The data collected by the sensors and cameras are analyzed using data analysis algorithms, which are designed to detect patterns and anomalies in the data. The data

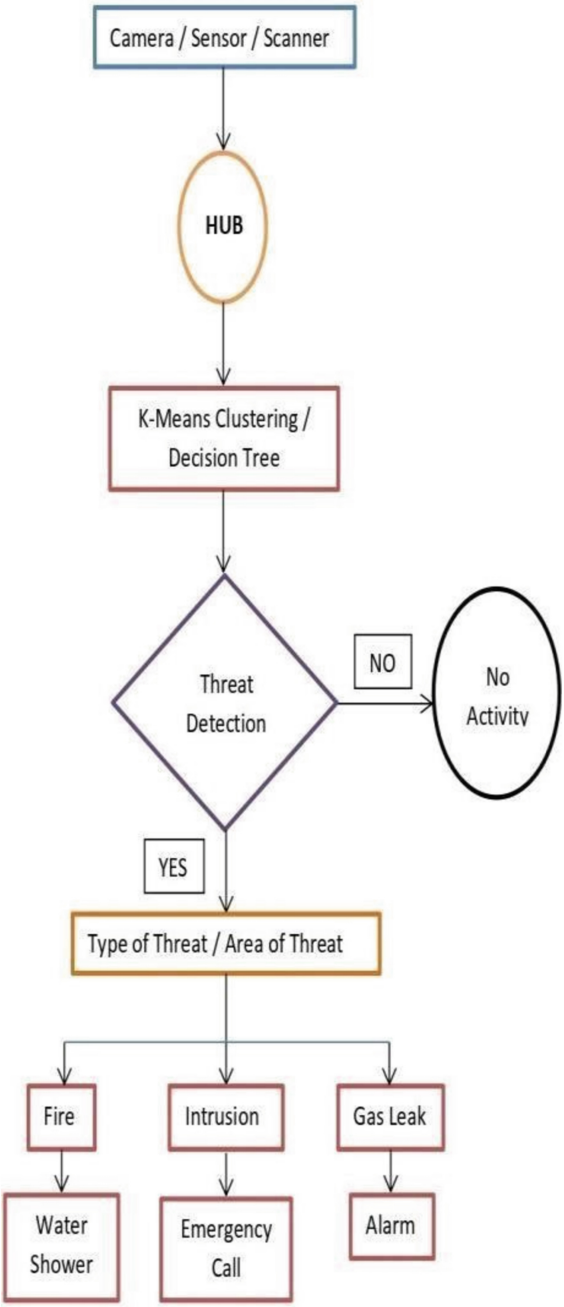


Fig. 3. Flow chart of an overview of the working of the proposed system.

analysis algorithms used in the proposed system include machine learning algorithms that are k-means clustering algorithms, capable of learning from the data and improving their accuracy over time. Furthermore, for decision-making, the decision tree algorithm is used to identify precise and actual threats. Once a threat is detected, the system sends an alert to the user's mobile application and even the system can call an emergency number automatically using authorized access to the owner's smartphone in case of an intrusion. If the detected threat is fire, the system is capable of automatic initiation of water showers. Similarly, if there is smoke the system may start the exhaust automatically (Fig. 3).

4 Algorithm

K-means clustering is an unsupervised machine learning algorithm that can be used to analyze data collected by various sensors such as motion sensors, door and window sensors, and security cameras, to detect anomalies or suspicious behavior. K-means clustering can be used to identify patterns of behavior that deviate from normal usage patterns. For example, if a home is typically empty during the daytime but suddenly has a high level of activity during working hours, with unfamiliar faces, this could be an indication of an intruder. The algorithm can be used to group data points into clusters based on their similarity, and then identify clusters that deviate from the normal usage pattern.

Once the clusters are generated, the decision tree algorithm uses them to analyze the results. For example, you might create a decision tree to identify the factors that lead to a particular cluster, such as time of day, user activity, or sensor readings. The combination of k-means and decision tree algorithms can be a powerful tool for analyzing and improving smart home security. By clustering data and analyzing the results with a decision tree, if a particular cluster has a high level of activity during the daytime when the home is typically empty, the system will send an alert to the user's mobile application indicating suspicious behavior (Fig. 4).

The K-means clustering algorithm and decision tree algorithm are responsible for making decisions about how to respond to the security threats detected by the sensors and cameras. The algorithms are based on predefined rules, which consider the type of security threat, the location of the threat, and the severity of the threat. These algorithms can trigger various actions, such as sounding an alarm, notifying the homeowner through their smartphone, or contacting emergency services.

To evaluate the performance of the proposed system, we conducted experiments using a prototype of the system. The simulations were conducted using a software simulator, which allowed us to test the system under different scenarios and conditions. The experiments were conducted in a controlled environment, where we tested the system's ability to detect and respond to various security threats.

In summary, the methodology used in this paper involved designing and implementing a hardware and software system that uses sensors, cameras, communication protocols, data analysis algorithms, and decision-making algorithms to detect and respond to various security threats in a smart home environment. The performance of the system was evaluated through simulations and experiments, which allowed us to test the system under different scenarios and conditions.

Creation of K-Means class:

```
class KM:
    def init (s ,k = 0, max_iter = n):
            s.k = k
            s.max_iter = max_iter
```

Implementing the similarity function:

```
def euclidDistance(s, x, y):
    return(np.sqrt(np.sum(np.square(x - y),axis = 1)))
```

Fitting the data:

```
def fit(s,data):
    s.centroids = []

        for i in range(s.k):
            s.centroids.append(data.iloc[i].to_nu
        mpy())
            s.classes = {}

for cluster in range(s.k):
    s.classes[cluster] = []

        for point in range(l(data)):

         distances = s.euclidDistance(s.centroids,
         data.iloc[point].to_numpy())classification =
         np.argmin(distances)
         s.classes[classification].append(data.iloc[point])

previous = np.array(s.centroids)



for classification in s.classes:
    s.centroids[classification] = np.average(s.classes[classification], axis = 0)

optimal = True
curr = np.array(s.centroids)


if np.sum((curr - previous)/previous * 100.0) > 0.0001:
    optimal = False
```

Fig. 4. Algorithm for Decision making and clustering data analysis

```
if optimal:
Break

def fit(s, data):
s.centroids = []

  for i in range(s.k):
    s.centroids.append(data.iloc[i].to_numpy())

      for itr in range(s.max_iter):
      s.classes = {}

              for cluster in range(s.k):
              s.classes[cluster] =[]

       for point in range(l(data)):
            distances = s.euclidDistance(s.centroids, data.iloc[point].to_numpy())
            classification = np.argmin(distances)s.classes[classification].append(data.iloc[point])

  previous = np.array(s.centroids)

  for classification in s.classes:

              s.centroids[classification] = np.average(s.classes[classification], axis = 0)
              optimal = True
              curr = np.array(s.centroids)

  if np.sum((curr - previous)/previous * 100.0) >
        0.0001:optimal = False
        data.head()

clf =KM()
```

Fig. 4. (*continued*)

5 Results

The proposed IoT-based smart home security system was designed and implemented using various hardware and software components, as described in the methodology section. The system was evaluated through simulations and experiments, which allowed us to test the system's ability to detect and respond to various security threats.

The simulations were conducted using a software simulator, which allowed us to test the system under different scenarios and conditions. The simulations showed that the system was capable of detecting and responding to various security threats, such as intrusion, fire, and gas leakage, with a high degree of accuracy. The simulations also showed that the system was able to differentiate between genuine security threats and false alarms, which is an important feature of any security system (Table 1).

Table 1. Record of Experiments on the Proposed System

Threats	Alarm in Home	Alarm on owner's phone	Emergency Call	Water Shower
Fire in Lobby	✔	✔	✔	✔
Gas in Kitchen	✔	✔	×	×
Intrusion through main Gate	✔	✔	✔	×
Intrusion through window	✔	✔	✔	×
Animals/Pets movement	×	×	×	×

The experiments were conducted in a controlled environment, where we tested the system's ability to detect and respond to various security threats in real time. The experiments showed that the system was able to detect and respond to security threats in a timely and efficient manner. For instance, when a fire was detected by the smoke sensor, the system immediately sounded an alarm and sent a notification to the homeowner's smartphone. The experiments also showed that the decision-making algorithms were able to make intelligent decisions about how to respond to security threats, based on predefined rules and algorithms.

One of the key advantages of the proposed system is its ability to provide owners of the home with realtime notifications about security threats through their smartphones. This allows owners of the home to take immediate action to mitigate the security threat, such as contacting emergency services or notifying neighbors. The system's ability to differentiate between genuine security threats and false alarms also reduces the risk of owners of the home becoming complacent about security threats, which can lead to a false sense of security.

Another advantage of the proposed system is its scalability. The system can be customized to meet the needs of different owners of the home, depending on the size and layout of their homes, as well as their specific security requirements. This makes the system suitable for a wide range of applications, from small apartments to large houses.

Overall, the results of the simulations and experiments demonstrate that the proposed IoT-based smart home security system is an effective and efficient solution for securing homes using IoT. The system's ability to detect and respond to various security threats in real-time, its scalability, and its ability to provide owners of the home with real-time notifications about security threats make it a valuable tool for ensuring the safety and security of homes.

6 Conclusion

In this paper, we presented the design and implementation of an IoT-based smart home security system. The system uses sensors, cameras, communication protocols, K-means algorithms, and decision tree algorithms to detect and respond to various security threats

in a smart home environment. The system was evaluated through simulations and experiments, which showed that it could detect and respond to security threats in a timely and efficient manner.

One of the key advantages of the proposed system is its ability to provide owners of the home with real- time notifications about security threats through their smartphones. This allows owners of the home to take immediate action to mitigate the security threat and ensure the safety and security of their homes.

The system's ability to differentiate between genuine security threats and false alarms also reduces the risk of owners of the home becoming complacent about security threats.

Another advantage of the proposed system is its scalability. The system can be customized to meet the needs of different owners of the home, depending on the size and layout of their homes, as well as their specific security requirements. This makes the system suitable for a wide range of applications, from small apartments to large houses.

Overall, the proposed IoT-based smart home security system is an effective and efficient solution for securing homes using IoT. The system's ability to detect and respond to various security threats in real- time, its scalability, and its ability to provide owners of the home with real-time notifications about security threats make it a valuable tool for ensuring the safety and security of homes. Future work can include expanding the capabilities of the system to include more advanced features, such as voice recognition, to further enhance the system's ability to detect and respond to security threats.

References

1. Bellini, P., Nesi, P., Pantaleo, G.: IoT-enabled smart cities: a review of concepts, frameworks and key technologies. Appl. Sci. **12**(3), 1607 (2022)
2. Lulla, G., Kumar, A., Pole, G., Deshmukh, G.: IoT based Smart Security and Surveillance System. 2021 International Conference on Emerging Smart Computing and Informatics (ESCI), pp. 385–390. Pune, India (2021). https://doi.org/10.1109/ESCI50559.2021.9396843
3. Mishra, S., Tyagi, A.K.: The role of machine learning techniques in internet of things-based cloud applications. Artificial Intelligence-based Internet of Things Systems, 105–135 (2022)
4. Zhang, H., Chen, Y., Lu, W., Jiang, Z.: An IoT-based smart home security system using dynamic resource allocation. In: Proceedings of the 2019 IEEE 6th International Conference on Industrial Engineering and Applications, pp. 147–151 (2019)
5. Tahsien, S.M., Karimipour, H., Spachos, P.: Machine learning based solutions for security of Internet of Things (IoT): A survey. J. Netw. Comp. Appl. **161**, 102630 (2020)
6. Mohanta, B.K., Jena, D., Satapathy, U., Patnaik, S.: Survey on IoT security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet of Things **11**, 100227 (2020)
7. Al Turjman, F., Zahmatkesh, H., Shahroze, R.: An overview of security and privacy in smart cities' IoT communications. Transactions on Emerging Telecommunications Technologies **33**(3), e3677 (2022)
8. Pande, V., Choudhary, S.S.: Design and implementation of a smart home security system based on IoT and raspberry Pi. 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI). Tirunelveli, India (2019)
9. Imran, A.R., Hasan, N.U., Khan, N.A.U.: Design and Implementation of IoT-Based Home Automation System. 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE). Cox's Bazar, Bangladesh (2019)

10. Aziz, M.A., Bhuiyan, A.H., Hasan, M.M.: Smart home automation and security system using arduino and IoT. 2019 6th International Conference on Advances in Electrical Engineering (ICAEE). Dhaka, Bangladesh (2019)
11. Islam, M.M., Islam, S., Faruque, S.H.: Smart home automation and security system based on IoT and cloud computing. 2019 4th International Conference on Electrical and Electronics Engineering (ICEEE). Dhaka, Bangladesh (2019)
12. Ali, M.Y., Kabir, M.H., Islam, M.A.: Design and Implementation of an IoT-Based Smart Home Security System with Image Processing, 2019 IEEE Region 10 Symposium (TENSYMP). Kuala Lumpur, Malaysia (2019)
13. Ahmed, S.M., Choudhury, A.S.: Design and Implementation of an IoT-Based Smart Home Automation and Security System Using Raspberry Pi. 2019 22nd International Conference on Computer and Information Technology (ICCIT). Dhaka, Bangladesh (2019)
14. Sultana, S., Saha, S.S.: IoT-based smart home security system with fire detection and alerting. 2019 5th International Conference on Electrical, Computer and Communication Engineering (ECCE). Cox's Bazar, Bangladesh (2019)
15. Zhang, Z., Liu, Y., Wang, Y.: An IoT-based smart home monitoring system with face recognition. In: Proceedings of the 2018 IEEE International Conference on Systems, Man, and Cybernetics, pp. 1664–1669 (2018)
16. Bao, C., Li, L., Li, Q.: Design and implementation of a smart home security system based on internet of things. In: Proceedings of the 2018 IEEE 3rd Advanced Guizani Information Technology, Electronic and Automation Control Conference, pp. 1682–1685 (2018)
17. Song, W., Jiang, C., Ma, Z.: An IoT-based smart home system for elderly care. In: Proceedings of the 2018 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference, pp. 327–330 (2018)
18. Zhang, C., Wang, H., Wu, Y., Li, Z.: An IoT-based intelligent system for smart home. In: Proceedings of the 2018 IEEE 3rd International Conference on Electronic Information Technology and Intellectualization, pp. 229–233 (2018)
19. Li, H., Li, Z., Li, Z., Wang, C.: Design and implementation of a smart home security system based on IoT. 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM). Bangkok, Thailand (2018)
20. Bonomi, S., Milito, R., Zhu, J., Addepalli, S.: Fog computing and its role in the internet of things. In: Proceedings of the First Edition of the MCC Workshop on Mobile Cloud Computing, pp. 13–16 (2012)
21. Kaliyamurthi, H.K.S., Kumaravel, K.S.: IoT-based smart home security system using raspberry Pi. 2018 International Conference on Inventive Communication and Computational Technologies (ICICCT). Coimbatore, India (2018)

Access and Secure Patient Medical Records Using Blockchain Technology Based Framework: A Review

Attique Ur Rehman[1(✉)], Muhammad Haseeb Zafar[2], and Muhammad Aslam[2]

[1] Department of Computer Science, Lahore Garrison University, Lahore, Pakistan
attique.rehman@lgu.edu.pk
[2] Department of Computer Science, Superior University, Gold Campus, Lahore, Pakistan

Abstract. Blockchain technology has key role in electronic health record systems for storing, accessing and securing patient medical records. Patient medical information is being stored like personal bio, diagnosis, treatments etc. in electronic health records systems whenever he visits to any health sector. This information is very sensitive and private and it has been remaining a big challenge to access and secure patient medical records in a decentralized manner. Blockchain has become very important for its use in storing, accessing and managing patient medical records in a very secure and decentralized manner. In this paper, a systematic literature review has been done to review blockchain architecture for electronic health records system to store, access and secure patient medical records. The main objective of this paper is to highlight the use of blockchain in accessing and securing patient medical records. Moreover, some blockchain based electronic health records systems has been presented to secure the patient medical records. Lastly some challenges and gaps in using blockchain based medical health records systems has been presented.

Keywords: Electronic health records · Blockchain · Patient medical records

1 Introduction

The eHealth technologies are becoming very important for exchanging real time data of patients across the globe [1]. This Patient medical records are very important information that is being used by many health care providers and research institutes [2]. The different institutions are using the technology to save and secure the patient information but the patient private data security is the main issue [3]. The data for patients like personal information, diagnosis, treatments, symptoms, region etc. is growing with the passage of time. Patient medical record systems that store and manage patient data are being used by different institutions and it is becoming an important technology [4]. There are many stakeholders that are involved in managing and accessing the patient data. But it has come with many challenges like data insecurity, accessibility [5]. Patient need to visit different hospitals, clinics or any health care system for medical diagnosis, treatments etc., in such cases patient data sharing is important for better treatment and

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 260–270, 2025.
https://doi.org/10.1007/978-3-031-77620-5_19

medications [4]. Patient does not have access to their records. Patient data can be shared with unauthorized person or data can be stolen due to these technologies.

Blockchain technology is becoming more important these days because it provides many featured like decentralized, immutability and security of data [1]. Blockchain technology is being used in electronic health record system that helps to share the data of patient among many stakeholders. Thorough blockchain technology, patient can control the data who can access or not. It provides security to data by using its advanced algorithms [6].

In this paper, we have presented that how block chain technologies help to improve the patient data accessibility, security in electronic health records system. We have described the architecture of block chain to understand its working and how it can help to improve the current patient records system. The challenges and gaps in using blockchain has been also presented in this article.

In the next session 2, we have mentioned related work, Sect. 3 we have defined our research methodology, in 4 section we have done assessment of our research questions and Sect. 5 and 6 contains discussion and conclusion. Respectively.

2 Related Work

The patient information is highly sensitive and private that is being shared with the multiple stakeholders. The challenge is to secure the information by using some emerging technologies such as block chain that is quite considerable due to its highly secured hashing algorithms. A survey has been done on the use of block chain in healthcare that discuss accessibility, security and privacy challenges in electronic health records [2]. However, the challenges in using blockchain based record systems has not been discussed. The role of block chain technology has been discussed in telehealth and tele medicine [7]. But the blockchain architecture has not been presented for managing patient records. A systematic literature review of block chain for electronic health records system has been done in [6] that focus on the security and privacy challenges. However, the security architecture has not been discussed. The use of information in health care by using block chain technology has been discussed in [8]. They have discussed the challenges that effects the transition of patient information. A systematic review has been done on using of blockchain applications in health sector. But the blockchain architecture has not been presented.

Our novelty in this paper is that we have focused on role of blockchain in patient medical records in sense of storing, sharing of data. Our study focuses on security of patient data by using the block chain. We have discussed challenges and gaps of blockchain based electronic health records in this paper.

3 Research Methodology

A systematic literature view method has been selected for this paper to review the use of block technologies framework to ensure the availability and security of patient records. The objectives of this review to provide an overview that how block chain methods are helping to improve the accessibility, security of patient records in a system. We have

used the proposed method by Kai Petersen [9]. We have followed the steps as mentioned in Fig. 1.

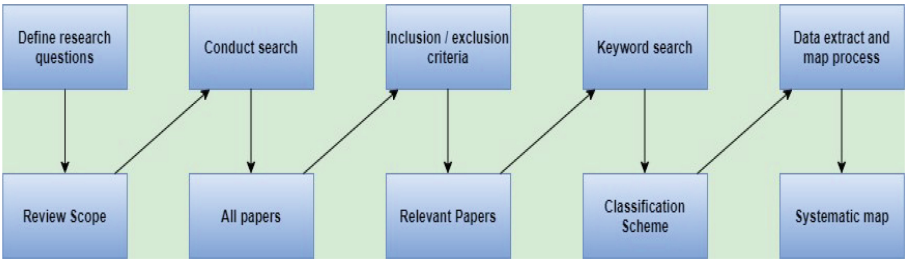


Fig. 1. Steps to conducting a systematic review.

3.1 Research Objectives

The objectives of this research are:

RO1. The main focus is to highlight the use of block chain methods in accessing, securing managing patient medical records.
RO2. Improving the security of patient medical records while using block chain.
RO3. Explore challenges and gaps in using blockchain based electronic health record systems.

3.2 Research Question

The important thing in systematic literature view defining the research questions. After reading detailed literature review, we have defined the following questions as in Table 1.

Table 1. Research Questions.

Q. No	Questions	Motivation
Q1	Why decentralized blockchain patient record system is better than centralized patient record systems?	Role of block chain-based health record systems
Q2	How block chain will ensure that patient records are secure and traceable?	Explore the important characteristics of smart contracts in block chain
Q3	What are the challenges and gaps in using blockchain based electronic health record?	Describe the challenges in using blockchain for electronic health record

These question enables us to review the challenges and gaps in using blockchain for patient health records.

3.3 Conducting Search

This is the second step of systematic literature view to search the papers related to research topic. The search string has been identified to collect the articles using different repositories. The papers are searched from different databases that are Springer Link, IEEE Xplore, Science Direct and ACM digital library. Following combination has been used to define the search string on Table 2.

$$\forall \text{ Primary} \wedge \text{Secondary} \vee \forall \text{ Additional}$$

Table 2. Search Strategy.

Database	Search String
Springer Link	("Patient Medical Records" OR "Electronic medical record" OR "Patient data") AND ("Blockchain" OR "Blockchain technology" OR "Blockchain security") AND ("ehealth" OR "telehealth" OR "healthcare") Publication Year: Year 2018–2020
IEEE Xplore	("Patient Medical Records" OR "Electronic medical record" OR "Patient data") AND ("Blockchain" OR "Blockchain technology" OR "Blockchain security") AND ("ehealth" OR "telehealth" OR "healthcare") Publication Year: Year 2018–2020
Science Direct	("Patient Medical Records" OR "Electronic medical record" OR "Patient data") AND ("Blockchain" OR "Blockchain technology" OR "Blockchain security") AND ("ehealth" OR "telehealth" OR "healthcare") Publication Year: Year 2018–2020
ACM digital library	("Patient Medical Records" OR "Electronic medical record" OR "Patient data") AND ("Blockchain" OR "Blockchain technology" OR "Blockchain security") AND ("ehealth" OR "telehealth" OR "healthcare") Publication Year: Year 2018–2020

3.4 Inclusion and Exclusion Criteria

We have included papers that were:

- Related to the search string
- Papers that are published from 2018–2020
- That contains block chain techniques
- Related to patient medical records We have excluded following articles:
- The titles were not matched with the blockchain and patient medical records
- Books
- Without abstract
- Does not contains blockchain solutions.

3.5 Search and Results and Collection

The initial results retrieved was 2447 against the search string on for databases. The results of the search and selection of research papers are shown in Table 4. The papers were included or excluded based on titles. We examined the titles of all papers and the results was 314. Many papers were not related to the topic so we exclude those. After applying inclusion and exclusion criteria, we selected 18 papers for this research paper.

3.6 Key Wording

In this, we have done key wording process on the base of abstracts. We have used the process defined by Petersen [9].

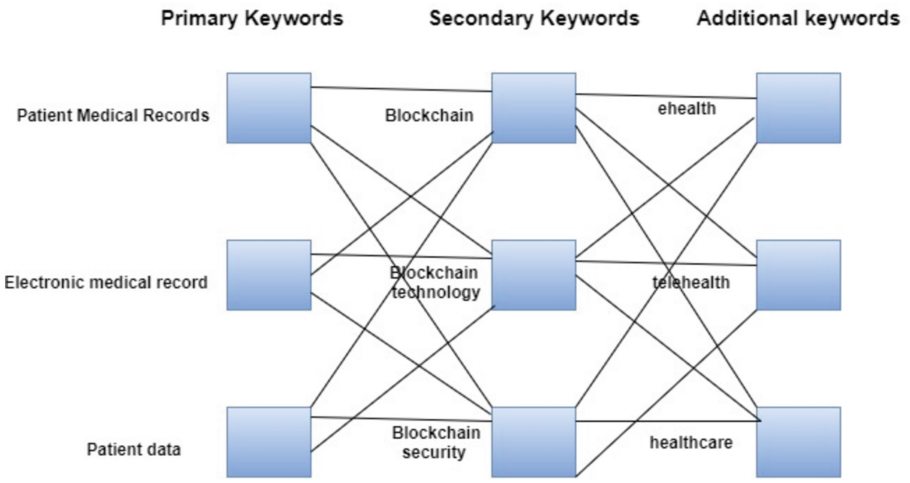


Fig. 2. Search string key wording.

We have examined the abstracts and basic concepts of contribution related to the topic. Keywords has been identified as primary, secondary and additional as in Fig. 2.

3.7 Quality Assessment

The quality assessment criteria have been identified to check or asses the quality of selected papers. We have defined some questions to score the paper quality as in Table 3.

3.8 Data Extraction and Classification

This process has been done to get the possible answers of the questions that are already defined in Table 1. All information related to address the questions are retrieved in this step. This also includes title of paper, author's and journal information. The initial search retrieved 2447 and then we applied screening on it by removing the duplications and by

Table 3. Criteria for Quality Assessment.

Criteria	Ranking	Score
The papers provide a clear solution or contribution for role of blockchain in managing patient medical records	Yes No	1 0
The methods for using block chain were clearly explained	Yes No	1 0
Databases ranking Journals/Conference	Q1 Q2 Q3 Core A Core B Core C	2.5 2 1.5 2 1.5 1

looking the tiles and the result was 314. Then the second phase of screening was done based on abstracts of the papers and the result was 52. The final selected articles for this paper are 18. Table 4 shows the selection process from different scientific databases.

Table 4. Criteria for Quality Assessment.

Sr	Process	Criteria Used	ACM Digital library	Springer	Science direct	IEEE explore	Total results
1	General Search	By keywords	981	759	568	139	2447
2	First round of screening	Removed based on titles	59	211	21	23	314
3	Second round of screening	Abstracts	13	24	11	4	52
4	Final selection	Entire article	3	7	4	4	18

4 Assessment of Research Questions

Q1. Why decentralized blockchain patient record system is better than centralized patient record systems?

The patient data may have compromised when using the centralized health record systems. As blockchain is peer to peer and decentralized technology so it has an important role in electronic health records. Many techniques are being used to make the data more secure and traceable. Through blockchain, an access is given to patients to control their medical records on one place and provide security [10]. As blockchain main features include shared, immutable and transparency for all the transactions, so this enables the stakeholder to provides opportunity to use EMR systems based on blockchain [11].

The smart contracts ensure the security of data in a blockchain based system. Consensus algorithms have been imposed to verify and secure the records in a system. Block chain methods helps us [12]. The patient data cannot be accessed by unauthorized entities. Any change or malicious attack can be tracked or traceable using the block chain-based health records systems. Patient will have control on its own data. The security can be managed and tracking of data sharing is possible.

Decentralization feature provide decentralized system, means there will be no central entity. So, all entities in blockchain will have equal rights to read/write data [13]. Every block has the previous block hash value, so if any block data is changed, then the hash values of each block will be recalculated and that node will be invalid [14]. The private information of entities is being encrypted and open to all, so those who have permission will query the data and have access to the information.

Q2. How block chain will ensure that patient records are secure and traceable?

Patient information privacy may compromise if the data is leaked in electronic health record systems. Block chain provides us secure, immutable and transparency by implementing its techniques in health records systems [11]. In Fig. 3 a blockchain based system has been defined and its process by [15]. The process is simply described. All the participants register through application and ask service provider for the certificate. The service provider will issue the certificate and will assign a key along with the ID. The transactions sent to EHR ledger. The providers can access only those records that have been allowed to them. When an record is updated it is distributed to all the participants over the blockchain so ever node has same copy of data every time so it is not possible to alter or delete the data. Each transaction has previous hash value along with the timestamp so history is being recorded. It makes the system more secure [15].

Another blockchain based system has been proposed by [16].

MedChain: (A blockchain based health record system) [16] Eman-Yasser proposed a block chain based for managing patient records system that is called MedChain. The main purpose of this system is to enable security, effectiveness for the records. It keeps the privacy of patient on priority. The smart contracts have been employed in this system for the transactions and access control to health records. For security purpose the encryption methodology has been adopted. They have employed hashing algorithm SHA-256 to ensure the data security and integrity. When a record is saved in electoric health system, Medchain keeps the hash value of that record. This encrypted value will be sent to authorized person to access the data. This has value is unique so it makes sure that no one can change or alter the data. To make sure security, MedChain stores the hash value,

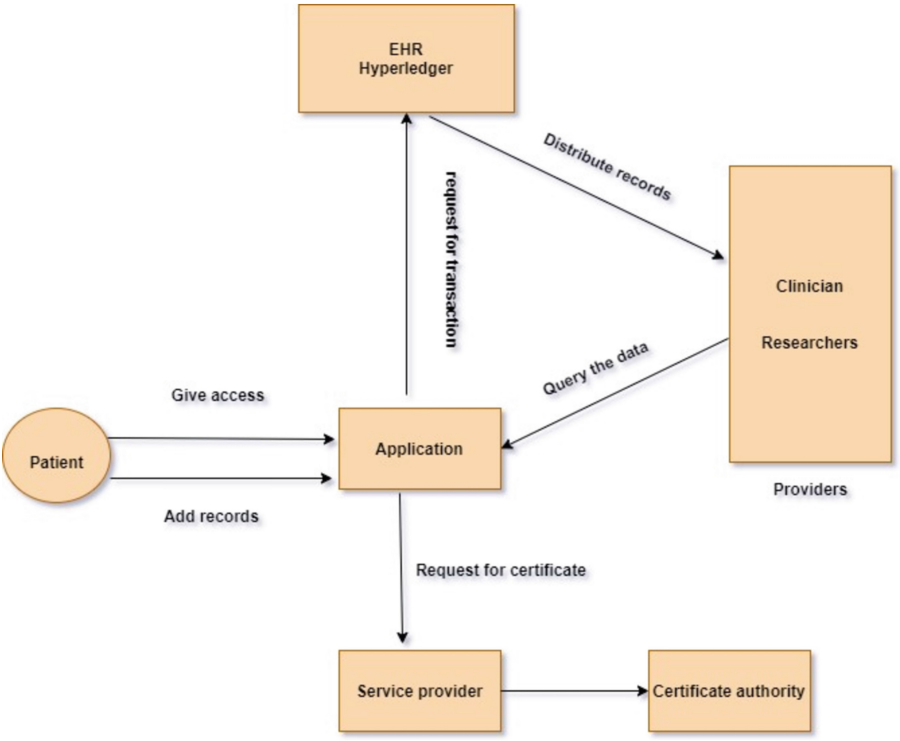


Fig. 3. Blockchain based HER system.

key and record in different locations. To maintain the privacy, the smart contracts have been used in this system. For the validation of new blocks or records, Proof of Authority algorithm has been used to verify the new records [8] Proof of Authority Algorithm helps us to create an authority in a block chain that will have access to add the data and will ensure the security of data [13]. Re-Encryption technique helps to encrypt the messages or data in that way that allow the other entity to decrypt this message with the use of its private key. Smart Contracts enables to ensure that authorized transaction have been done [17]. It monitors all the transactions in the chain [18]. These are the set of functions that executes when certain conditions are fulfilled.

Above all protocols helps to make the patient records storing, sharing and accessibility in a decentralized manner. All have its own unique function to enhance the data security and assures the privacy of patient private information.

Another keyless signature framework has been proposed by [14] to ensure the data security of health records. It uses the hash function to secure the data.

Q3. What are the challenges and gaps in using blockchain based electronic health record?

Blockchain comes with a massive benefits and opportunities but it still has some challenges and issues when applying it in managing patient medical records [19].

4.1 Scalability

One of the challenges is storage capacity. There is lot of patient data that needs to be stored on the blockchain including personal information, diagnosis, treatments that may contains lots of images as well. Data is becoming large every day and it has no limit. This will increase the size of the database that may lower the process of accessing or searching the data. So, we need a scalability solution for a blockchain [5].

4.2 Standards

The standardization for the blockchain is still a challenge. Standards for every industry has not been identified yet. There is lack of knowledge about the type of data and its accessibility. There is need to define the standard of information sharing, format of data, size evaluation in blockchain for health care applications [19].

4.3 Transformation

Many health care sectors are using the blockchain applications for patient records management but still there is challenge to motivate the clinical persons to use the blockchain rather than paper work or centralized applications [7]. The old systems are being used over the years and it is very difficult to transform them on a blockchain. There will be need of more expertise and knowledge to store and access the data through blockchain based health records applications.

5 Discussion

We have done systematic literature to provide the detailed discussion that how blockchain based electronic health records systems can help in accessing and securing patient medical records. A model has been proposed in Fig. 4 to sum up the results of this article.

Proposed model for electronic health record. This model is using two blockchain schemes, one is private blockchain and other is consortium blockchain. The private block saves all the data of patient medical records and the consortium chain contains indexes of the private records. The data will store on different nodes. When a user request for a data, the identity of user is checked through different algorithms techniques. After the user verification, the requested information is sent to the user. For security purpose, all record and patient identity is encrypted with the public key. This makes the data more secure in a blockchain/

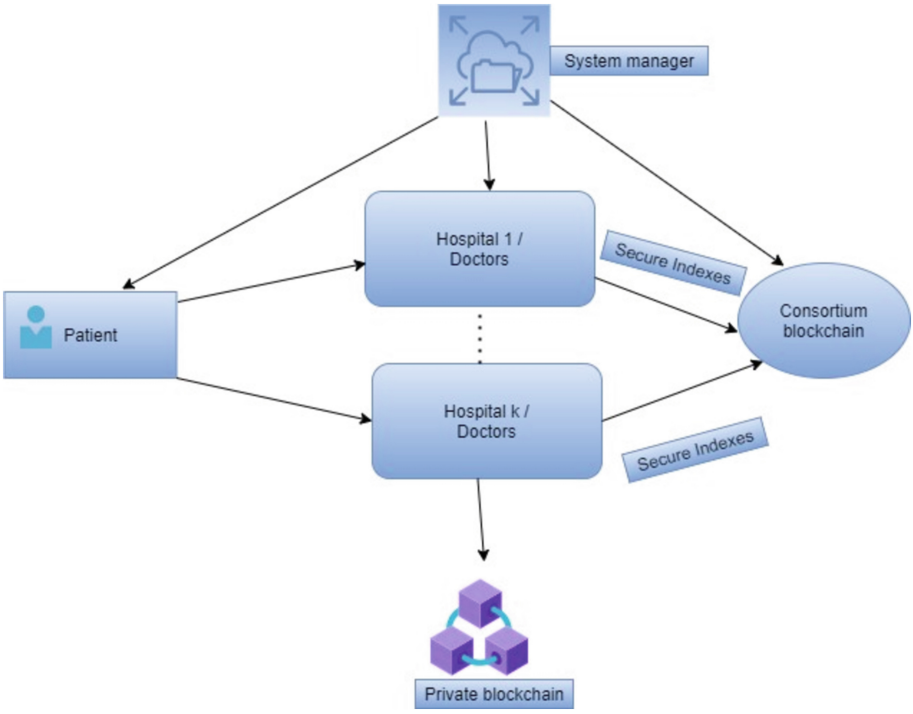


Fig. 4. Proposed Model for Electronic health record.

6 Conclusion

In this paper, a systematic literature review has been done to identify the use of blockchain in storing, accessing and securing patient medical records. This study has been conducted by selecting 18 articles and we have gone through all the process of systematics literature review. Since patient private information cannot be compromised in the sense of security and privacy. So, there was a need of to highlight the important features of blockchain that are being used in storing, sharing and accessing patient information. We have reviewed some blockchain featured that can be implemented to make the patient data secure and stored in decentralized manner so it can be access by authorized users easily. We have reviewed different block chain-based patient records systems that are using different algorithms to make the data secure and accessible to all authorized entities. We have also discussed challenges and gaps in using blockchain applications in health care system. We have concluded that using blockchain based systems for managing patient medical records make these records easily accessible, traceable and secure.

References

1. Alonso, S.G., Arambarri, J., López-Coronado, M., de la Torre Díez, I.: Proposing new blockchain challenges in eHealth. J. Med. Syst. **43**(3), 64 (2019). https://doi.org/10.1007/s10916-019-1195-7

2. Sookhak, M., Jabbarpour, M.R., Safa, N.S., Yu, F.R.: Blockchain and smart contract for access control in healthcare: a survey, issues and challenges, and open issues. J. Netw. Comput. Appl. **178**, 102950 (2021). https://doi.org/10.1016/j.jnca.2020.102950
3. Fan, K., Wang, S., Ren, Y., Li, H., Yang, Y.: MedBlock: efficient and secure medical data sharing via Blockchain. J. Med. Syst. **42**(8), 136 (2018). https://doi.org/10.1007/s10916-018-0993-7
4. Vistro, D.M., Rehman, A.U., Farooq, M.S., Abid, A., Idrees, M.: A literature review on security issues in cloud computing: opportunities and challenges. J. Crit. Rev. **7**(10), 1446–1455 (2020)
5. Khan, N.S., Abid, A., Abid, K., Farooq, U., Farooq, M.S., Jameel, H.: Speak Pakistan: challenges in developing Pakistan sign language using information technology. South Asian Stud. **30**(2) (2020).
6. Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.-K.R.: Applications of blockchain in ensuring the security and privacy of electronic health record systems: a survey. Comput. Secur. **97**, 101966 (2020). https://doi.org/10.1016/j.cose.2020.101966
7. Ahmad, R.W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., Omar, M.: The role of blockchain technology in telehealth and telemedicine. Int. J. Med. Inform. **148**, 104399 (2021). https://doi.org/10.1016/j.ijmedinf.2021.104399
8. Gordon, W.J., Catalini, C.: Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput. Struct. Biotechnol. J. **16**, 224–230 (2018). https://doi.org/10.1016/j.csbj.2018.06.003
9. Petersen, K., Feldt, R., Mujtaba, S., Mattsson, M.: Systematic mapping studies in software engineering. In: 12th International Conference on Evaluation and Assessment in Software Engineering (EASE), vol. 12, pp. 1–10 (2008)
10. Vistro, D.M., Rehman, A.U., Farooq, M.S., Abid, A., Idrees, M.: A survey on cloud computing security with cross platform. J. Crit. Rev. **7**(10), 1439–1445 (2020)
11. Dubovitskaya, A., Xu, Z.. Ryu, S., Schumacher, M.. Wang, F.: Secure and trustable electronic medical records sharing using blockchain. In: AMIA ... Annu. Symp. Proceedings. AMIA Symposium, vol. 2017, pp. 650–659 (2018). https://pubmed.ncbi.nlm.nih.gov/29854130
12. Liu, X., Wang, Z., Jin, C., Li, F., Li, G.: A blockchain-based medical data sharing and protection scheme. IEEE Access **7**, 118943–118953 (2019)
13. Belotti, M., Bozic, N., Pujolle, G., Secci, S.: A vademecum on blockchain technologies: when, which, and how. IEEE Commun. Surv. Tutorials **21**(4), 3796–3838 (2019). https://doi.org/10.1109/COMST.2019.2928178
14. Nagasubramanian, G., Sakthivel, R.K., Patan, R., Gandomi, A.H., Sankayya, M., Balusamy, B.: Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. Neural Comput. Appl. **32**(3), 639–647 (2020)
15. Tanwar, S., Parekh, K., Evans, R.: Blockchain-based electronic healthcare record system for healthcare 4.0 applications. J. Inf. Secur. Appl. **50**, 102407 (2020). https://doi.org/10.1016/j.jisa.2019.102407
16. Daraghmi, E.-Y., Daraghmi, Y.-A., Yuan, S.-M.: MedChain: a design of blockchainbased system for medical records access and permissions management. IEEE Access **7**, 164595–164613 (2019)
17. Zhang, A., Lin, X.: Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J. Med. Syst. **42**(8), 140 (2018). https://doi.org/10.1007/s10916-018-0995-5
18. Kshetri, N.: Blockchain and electronic healthcare records [cybertrust]. Computer **51**(12), 59–63 (2018). https://doi.org/10.1109/MC.2018.2880021
19. Siyal, A.A., Junejo, A.Z., Zawish, M., Ahmed, K., Khalil, A., Soursou, G.: Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptography **3**(1), 3 (2019). https://doi.org/10.3390/cryptography3010003

Subcellular Structures Classification in Fluorescence Microscopic Images

Saif Ur Rehman Khan[1(✉)], Asif Raza[2], Inzamam Shahzad[1], and Shehzad Khan[3]

[1] School of Computer and Engineering, Central South University, Changsha, China
saifurrehman.khan@csu.edu.cn
[2] Department of Computer Science, Bahauddin Zakariya University, Multan, Pakistan
[3] Department of Computer Science, Air University, Multan, Pakistan

Abstract. Evaluation of cellular protein localization is becoming progressively important. Even after the whole human genome has been sequenced, numerous years will be required to study the structure, function, and each protein localization. Localization information is very important because it provides a context for a protein's structural and functional information. For instance, two proteins that possess comparatively similar function and structure may in fact be found in different compartments within the cell hence, these might be included in unrelated cellular processes. Localization data for several proteins were collected using fluorescence microscopy. The resulting patterns were described using a variety of numeric features including local binary pattern (LBP), Haralick's texture features, edge histogram descriptor (EHD), Segmentation-based Fractal Texture Analysis (SFTA) and after that these features were combined to form a single feature vector. This feature vector is then given as input to the classifier to classify the image into 10 different classes for 2D Hela dataset and into 5 classes for CHO dataset. Support vector machine (SVM) with chi-square kernel is used to solve the classification problem. Proposed framework obtained **98.9%** overall accuracy on Hela dataset and **99.6%** on CHO dataset. The obtained accuracy is **0.9%** higher on 2D Hela dataset and **0.6%** higher on CHO dataset as compared to highest computed accuracy.

Keywords: Fractal Texture Analysis · Support Vector Machine · local binary pattern

1 Introduction

A vital piece of the portrayal of a protein is the assurance of the subcellular organelles or structures to which it limits. This data is profitable because it gives a setting to the protein's structure and capacity. For instance, two proteins that are conjectured to have comparative structure and capacity may in truth restrict to various compartments inside the cell and in this manner, be included in unmistakable cell forms. The most well-known strategy for deciding subcellular area is understanding of fluorescence magnifying instrument pictures, both of cells recolored with monoclonal antibodies against

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 271–286, 2025.
https://doi.org/10.1007/978-3-031-77620-5_20

an endogenous protein or of cells communicating a GFP-labeled protein from a transfected develop. As of now the understanding is performed outwardly by the specialist. Such subjective understandings might be impacted by examiner predisposition can't be effortlessly affirmed by different agents, don't loan themselves to factual investigation, and don't give a methodical depiction that can be entered in database.

A mechanized framework for deciphering pictures of confinement example would in this manner have number of points of interest over current practice. These would incorporate objectivity, dependability, and repeatability. We have attempted to create and test techniques for quantitatively depicting such examples [3]. According to the research that has been done, almost everyone would agree that there is currently no collection of work that has been dedicated to providing a quantitative description of where proteins are found. There is no guarantee that biologists have no interest in characterizing the locations of proteins, but this is not often the case. On the other hand, it is frequently necessary to define how a newly discovered protein will be found inside of a cell. Regrettably, at this time, these descriptions are subjective, and as a result, they are not necessarily comparable between different investigators. When assigning a localization pattern to a protein, there is not a standard set of classifications that can be used. This is true even if the investigator's bias could be reduced to a minimum.

In point of fact, due to the complexity and variety of protein localization patterns, it is impossible to construct a set of categories that are straightforward enough to let investigators to make subjective assignments of patterns using those categories. As a result of this, the localization of a new protein is typically explained in broad terms, and it is typically done so within a specific sub-domain of cell biology. By consulting the Swiss-PROT database, one can learn about these issues as well as a variety of others. Annotated protein sequences can be found in the Swiss-PROT database. This database provides information on protein structure, function, post-translational modification, variations, and more. In addition to that, one of the fields is devoted to the subcellular localization. When the localization field of the Swiss-PROT database is analyzed by determining the frequency of each distinct localization term1, a number of issues become apparent. To begin, there is a lack of a systematic approach to the descriptions of the localization. The person who entered the information into the database has added their own subjective commentary to many of the entries.

The principal goal of this research work is to display practical use of CBIR system for medical experts. The focus of the research is on the use of various feature extraction techniques in classification. Followings are the most important objectives of the proposed research work.

- Experiment with various feature extraction techniques.
- Experiment with hybrid feature vector, which is obtained by combining the output of different feature extraction techniques.
- Propose a model for classification for medical images, which offers high accuracy as compared to the existing ones.

2 Literature Review

Fluorescence microscopy, pattern recognition, and machine learning are three of the fields that have contributed to the development of the technology that has recently been used to build applications such as sub-cellular protein localization. Other fields that have contributed to the development of this technology include electron microscopy, computational learning, and pattern recognition. This research aims to establish methodologies that will enable the numerical description and subsequent classification of the patterns that can be seen in fluorescent light microscope images of cells. The research was funded by the National Institutes of Health (NIH) and is being funded by the National Science Foundation (NSF). After labeling one or more sub-cellular structures with fluorescent dyes, these images are acquired by capturing images of the ensuing pattern of fluorescence using a microscope. The labeling of the sub-cellular structures can be done in either direction. This results in the difficulty of characterizing these patterns in a manner that is amenable to additional processing, which in turn results in the difficulty of actually acquiring the images themselves [10].

The process of automated sub-cellular localization has quite a few positive applications and benefits. The most essential benefit is that a previously impossible level of standardization may now be achieved through the use of quantitative descriptions of images. A rapid comparison of a new pattern with a large number of already produced patterns in the database could be of tremendous potential use. The same can be said for the study of the interactions between proteins. If we had access to a system like this one, we would be in a far better position to get an understanding of the intricate mechanisms that govern protein interaction and localization.

Identification of proteins with subcellular localization by computational means corresponds to a classification challenge. Because the search space for classifiers that model each individual pixel is too large for practical purposes, machine learning approaches typically do not classify the phenotypes directly from the raw image data. This is because all of these approaches are affected by the Curse of Dimensionality [2], which states that these approaches all share a common flaw. Because of the complexity of these algorithms, we must construct a much more limited number of functions that operate on the raw input image. The outputs of these functions are the only ones that are taken into consideration when classifying the image. Extraction of features is the term used for this process. Applying dimensionality reduction methods and selecting the dimensions that contain the most relevant information is another option. This is erred to as feature selection. Typically, feature selection is used in tandem with feature extraction [40]. Feature extraction is referred as the input pixel covariance has structure [39], and certain functions of the input are a priori known to not hold discriminative power. Sometimes customized characteristics are utilized, and these features may be based on a numerical method (like skeletonizing), or they could be based on additional information provided by the experimental setup. Both of these options are possible (intensity overlap with an additional marker) [41]. Murphy et al. outlined and continue to update a collection of subcellular localization features (SLFs) that is comprised of multiple categories of picture features. They have been making almost all of their classification decisions based on this foundational set for describing protein spatial distributions [42].

The discipline of machine learning includes a vast array of algorithms that may predict class labels by making use of a labelled set of instances (training set) that is supplied by an experienced individual (Supervised Learning Approach). Among them, the following are some of the ones that have been taken into consideration for the classification of different cell phenotypes: Neural networks [42], Support vector machine (SVM) [38, 44]. The task of classification is difficult due to a number of different facets of the problem. First, there is a huge number of alternative localizations (more than twenty), yet classifiers are normally created using a binary classification framework. For instance, the SVM method involves finding the hyper-plane that provides the best separation between two different sets of vectors in an enhanced space that was created by utilizing kernel functions [45].

3 Methodology

The application of computer vision techniques to the image retrieval problem, also known as the difficulty of searching for digital images in huge databases, is what is known as content-based image retrieval or CBIR for short. The fundamental applications of CBIR are medical analysis, research, and teaching. A substantial advantage originates from the territory of educating. Here instructors can utilize tremendous storages to locate some fascinating cases to show to students. These selected cases are Chosen cases are shown and construct in light as well as outwardly comparative images are introduced to improve the instructive abilities. And huge archives are also utilized by medical students for educational purpose. Another advantage is originated from research territory; the researcher can incorporate their case in their explorations. At last, the most critical and troublesome application region of CBIR is diagnostic; this leads to the combination of the system to the daily life. Content-based image retrieval (CBIR) system allows perusing the database and finding analysis based on visual resemblances. In this chapter, we are going to discuss proposed methodology and different techniques used in our framework. The proposed framework consists of several stages which include feature extraction, feature vector construction, dimensionality reduction and training of classifier and finely the modality classification for the given query image. Figure 1.

3.1 Feature Extraction

The data can be changed into a more limited set of characteristics if an algorithm's input data is too extensive to be processed and there is a good likelihood that it contains redundant information. In this case, the data will be transformed (features vector). This method is often erred to as the "extraction of features" technique. It is hoped that the chosen characteristics will include relevant information derived from the supplied data. Because of this, it will be possible to carry out the activity that was planned by making use of this condensed representation rather of the complete original data.

Features for a digital image are distinct quantifiable properties. The selection of separating and autonomous features is a vital step for a successful CBIR system, the type of the features is generally numeric; however basic components, for example, strings and diagrams are utilized as a part of recognition and retrieval frameworks. The idea of feature

correlated to the controlled variable in the linear regression. The process of mining and selection of a feature is a blend of skill and science, the development of such framework to do so is known as feature engineering [23]; it requisite several experiments with various possibilities and grouping of many automated techniques and domain knowledge. Mechanizing this process is known as feature learning [24] where machine learns the feature by itself. In our framework, we have used a set of features, our methodology can be portrayed as scaling up to use as many features and data as possible. The experiments exhibit, that expanding either axis tend to increase performance. Features used in our framework are Haralick's Features [4], local binary pattern (LBP) [22], edge histogram descriptor (EHD) [25], Segmentation-based Fractal Texture Analysis (SFTA) [26].

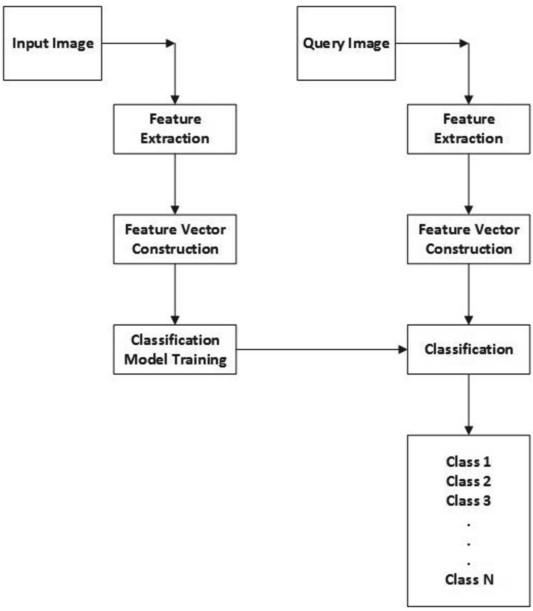


Fig. 1. Block Diagram of the Proposed Technique

3.2 Local Binary Pattern (LBP)

The fundamental thought behind the Local binary pattern (LBP) [22] methodology is to utilize the data about the surface from a nearby neighborhood. To begin with, we specify a radius R. Following this, the algorithm creates a binary pattern or code that represents the nearby texture in the area set of P pixels. The binary pattern is generated by taking into consideration the center value as a threshold value. The obtain value is then converted to decimal by using Eq. 1–2.

$$LBP(x_c, y_c) = \sum_{n=0}^{7} m(g_n - g_c)2^n \tag{1}$$

$$m(k) = \begin{cases} 1, k \geq 0 \\ 0, k < 0 \end{cases} \tag{2}$$

where g_c represents the value of the center pixel and g_n represents the value of eight surrounding pixels and function *m (k)* returns a binary value.

The length of LBP histogram depends on several neighbors. We utilized uniform pattern for experiments because it reduces the size of the histogram by combining the entire non-uniform pattern into a single bin. We experimented with the radius size of 1, 2, and 3 and setting the neighborhood size to 8, 16 and 24 respectively.

3.3 Edge Histogram Descriptor (EHD)

The edge histogram descriptor (EHD) quantifies the degree to which an image's edges are dispersed locally. When the primary texture is not consistent, edge dispersion is a useful mark for comparing images since it shows the variation in the texture. EHD first isolates the image into 4 × 4 grids, and then specifies the edge in each and every one of those sub images. This is how it determines the edge. The edges that were extracted from the sub-image are sorted into the following five categories: vertical, horizontal, 45°, 135°, and non-directional. The existence of an edge in each category results in the development of a histogram bin, which results in a histogram with a total of 80 bins.

An interesting variation of EHD is to compute an extended histogram by making use of a histogram that has already been retrieved and partitioned into 80 bins. By mixing the image blocks, it is possible to extend the capabilities of an 80-bit histogram. A global histogram, which is created by putting all 16 picture blocks together, and a semi-global histogram are the names given to the extended bins (formed by pooling by image blocks four rows and four columns and five groups). This result is presented in five bins for the global histogram as well as for the semi-global histograms that are derived from the eighty local histogram bins. Therefore, the total number of bins comes to 150. An interesting variation of EHD is to compute an extended histogram by making use of a histogram that has already been retrieved and partitioned into 80 bins. By mixing the image blocks, it is possible to extend the capabilities of an 80-bit histogram. A global histogram, which is created by putting all 16 picture blocks together, and a semi-global histogram are the names given to the extended bins (formed by pooling by image blocks four rows and four columns and five groups). This result is presented in five bins for the global histogram as well as for the semi-global histograms that are derived from the eighty local histogram bins. Therefore, the total number of bins comes to 150.

3.4 Feature Vector Construction

In machine learning and computer vision, the feature vector is used to characterize some object, feature vector consists of n-dimensions each dimension of the vector contains some numerical information regarding an object, which is used to encourage statistical investigation. Figure 2 shows the process of feature vector construction.

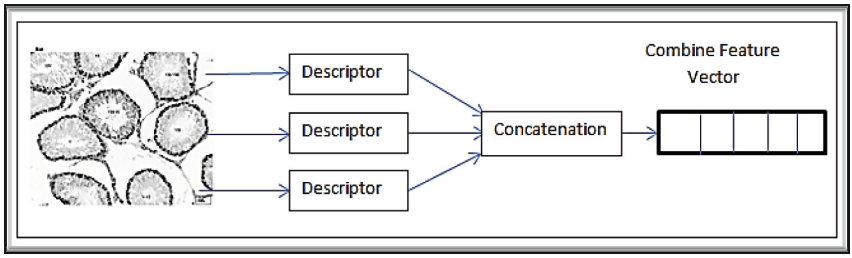


Fig. 2. Process of Combined Feature Vector Construction

3.5 Classification

We have utilized support vector machine (SVM), which is widely adopted supervised learning model [27]. The studies show that SVM with an early fusion of several features produces the best performance. For multiclass SVM, we have considered chi-square kernel in the form of Eq. 3, here X, Y are N dimensional inputs and K is the kernel function that maps the data from N dimensional space to M dimension space, usually M is much larger than N. Studies show that if features are in the form of a histogram, the Chi-square kernel yields better performance as compared to the other kernels 30.

$$K(X, Y) = \sum_i x_i \frac{y_i}{x_i + y_i} \tag{3}$$

For the purposes of categorization in this study project, we made use of the LIB-SVM toolkit. We used the one-vs-all technique, and as part of this approach, we trained a binary classifier that was distinct to each class. This allowed us to handle the difficulty of multi-class classification. Examples that are considered to be in a favorable light are those that correspond to the aforementioned category, whilst situations that have not yet been settled are erred to as examples that are considered to be in a negative light. There were numerous substantial irregularities within the data set. A few classes have an extremely low number of training instances, and while working with them, binary classification learners experience unbalanced distributions even though the class distribution is balanced in the training set. This is because the set of negatives people observe is often a lot larger than the set of positives they see, and this is the reason why this is the case. Because of this, the model almost always considers the one-vs-all method to be lopsided in terms of power distribution. In order to find a solution to this issue, we gave each positive and negative class a certain amount of weight [24].

4 Evaluation and Results Details

The performance of proposed framework is evaluated in the terms of Accuracy, Precision, Recall, F-score and ROC analysis. In following equations TP, FP, TN and FN represents true positive, false positive, true negative, false negative respectively.

$$Accuracy = \frac{TP + TN}{T + N} \tag{4}$$

$$Precision = \frac{TP}{(TP + FP)} \tag{5}$$

$$Recall = \frac{TP}{(TP + FN)} \tag{6}$$

$$F = \frac{2(Precision.Recall)}{(Precision + Recall)} \tag{7}$$

4.1 Dataset

We have tested the performance of our proposed model using the 2D HeLa Dataset [6]. Dataset downloaded from link http://murphylab.web.cmu.edu/data/. This dataset includes 862 different fluorescence microscopy images that have been categorized into a total of ten distinct groups. In order to provide the simulation with even more accurate results, the CHO dataset that was developed in the AIIA lab was also utilized [22]. The dataset in question will be obtained via the aforementioned website. https://ome.grc.nia.nih.gov/iicbu2008/hela/index.html. The details of both the datasets are presented in Tables 1 and 2, respectively (Figs. 3 and 4).

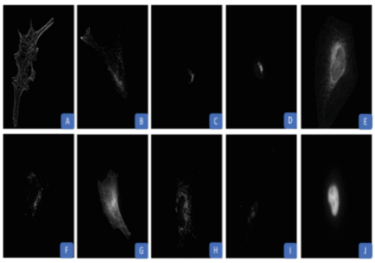


Fig. 3. Representative images from the classes of 2D Hela dataset used as input (A) ActinFilaments, (B) Endosomes, (C) ER, (D) Golgi_gia, (E) Golgi_gpp, (F) Lysosome, (G) Microtubules, (H) Mitochondria, (I) Nucleolus, (J) Nucleus.

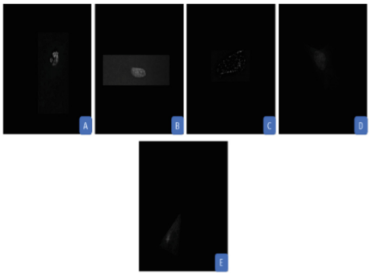


Fig. 4. Representative images from the classes of CHO dataset used as input (A) giantin, (B) Hoechst, (C) lamp2, (D) nop4, (E) tubulin

Table 1. 2D Hela Dataset

	Class Name									
	ActinFilaments	Nucleus	Endosomes	ER	Golgi Giantin	Golgi GPP130	Lysosome	Microtubules	Mitochondria	Nucleolus
Accuracy	98	87	91	86	87	85	84	91	73	80

Table 2. CHO Dataset

	Class Name				
	Giantin	Hoechst	Lamp2	Nop4	Tubulin
Accuracy	77	67	97	33	51

4.2 Results for Individual Feature Extraction Methods

4.2.1 Classification on Local Binary Pattern Descriptor (LBP)

We extracted LBP feature from the image based on different size radius and a different number of neighbors. Table 3 and 4 shows the results of experiments on Hella dataset and CHO dataset. Many image regions are relatively uniform, and it is valid to investigate whether the robustness of the features can be improved in these regions. That is why we did not consider LBP alone for classification.

Table 3. Class Wise Accuracy Using LBP on 2D Hela Dataset

	Class Name									
	ActinFilaments	Nucleus	Endosomes	ER	Golgi Giantin	Golgi GPP130	Lysosome	Microtubules	Mitochondria	Nucleolus
Accuracy	100%	93.10%	73.62%	66.27%	95.40%	63.52%	88.09%	89.01%	65.75%	98.75%

Table 4. Class Wise Accuracy Using LBP on CHO Dataset

	Class Name				
	Giantin	Hoechst	Lamp2	Nop4	Tubulin
Accuracy	86.61%	98.55%	93.81%	100%	94.11%

1) **Classification Based on Edge Histogram Descriptor**

EHD characterizes local edge spreading in the image; the features are computed for the whole image by setting the threshold value to 0.10. Table 5 and 6 shows the obtained results for edge histogram descriptor on Hella dataset and CHO dataset.

Table 5. Average Accuracy Using EHD on 2D Hela Dataset

	Class Name									
	ActinFilaments	Nucleus	Endosomes	ER	Golgi Giantin	Golgi GPP130	Lysosome	Microtubules	Mitochondria	Nucleolus
Accuracy	100%	95.40%	93.40%	98.83%	97.70%	95.29%	95.23%	97.80%	90.41%	98.75%

Table 6. Average Accuracy Using EHD on CHO Dataset

	Class Name				
	Giantin	Hoechst	Lamp2	Nop4	Tubulin
Accuracy	97.40%	100%	100%	100%	100%

4.2.2 Classification Based on SFTA Features

SFTA (Segmentation-based Fractal Texture Analysis) extracts texture *features* from an image. Table 7 and 8 shows the obtained results for SFTA on Hella dataset and CHO dataset.

Table 7. Classification Performance of SETA on 2D Hela Dataset

	Class Name									
	ActinFilaments	Nucleus	Endosomes	ER	Golgi Giantin	Golgi GPP130	Lysosome	Microtubules	Mitochondria	Nucleolus
Accuracy	97.95%	95.40%	71.42%	81.39%	97.70%	85.88%	80.95%	84.61%	57.53%	93.75%

Table 8. Classification Performance of SETA on CHO Dataset

	Class Name				
	Giantin	Hoechst	Lamp2	Nop4	Tubulin
Accuracy	96.10%	0%	100%	100%	100%

4.3 Results for Hybrid Features

Several studies have shown that use of diverse features captures different information of the image and thus, their combination offers a complete representation of the visual contents of an image and clearly provides better performance as compared to single feature approach [11, 24]. Classification results are presented in the form of accuracy, precision, recall and F-score. Table 9 displays the detail performance in the term of accuracy for every individual class for 2D Hela dataset.

Table 9. Detail Performance Per Class in terms of Accuracy

Class Name	Accuracy	Precision	Recall	F1-Score	Area Under Curve
Actin	100	1	1	1	1.0000
Endosome	98.8372	0.9884	1	0.9942	0.9904
ER	95.8044	0.9560	0.9886	0.9721	0.9895
Golgi_gia	100	1	0.9775	0.9886	1.0000
Golgi_gpp	97.6471	0.9765	0.9881	0.9822	0.9895
Lysosome	97.6190	0.9762	0.9862	0.9762	0.9851
Microtubules	100	1	1	1	1.0000
Mitochondria	100	1	0.9605	0.9799	0.9962
Nucleolus	100	1	1	1	1.0000
Nucleus	100	1	1	0.59	1.0000

4.3.1 ROC Analysis

ROC analysis is also carried out on results of hybrid features. The area under the ROC curve is calculated for each class and then average area under the curve is also computed. Figure 5 shows the ROC plot for all 10 classes.

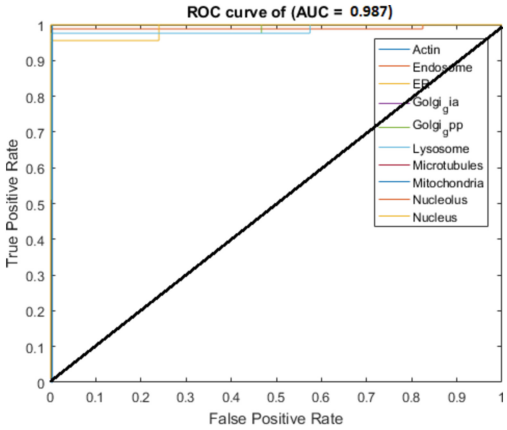


Fig. 5. ROC Curve for 2D Hela Dataset using SVM classification

4.4 Performance Comparison

The best accuracy reported by using 2D Hela cells dataset is 98% and by using CHO dataset is 99%. Obtained accuracy by proposed methodology is 98.9% for Hella Cells dataset and 99.6% for CHO dataset, which is 0.9% and 0.6% higher than [1, 12] respectively.

According to best of our knowledge, the conclusion from experimentations is that the results acquired with our methodology are better from previously reported results. It is due to fact that the dataset is so much diverse that single feature extraction algorithm with particular settings is not sufficient to extract information that provides better classification and retrieval results. We utilized a different type of features extraction algorithms that capture texture and other visual information; furthermore, we tried to employ different setting for every algorithm to extract more and more information that helped us in the classification task (Fig. 6).

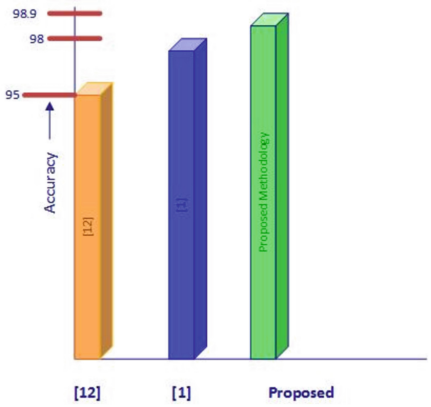


Fig. 6. Performance Comparison

The yellow bar graph shows the accuracy reported by using 2D Hela cells dataset [12] is **95%** and yellow bar graph shows the accuracy in [1] is **98%** and green bar shows accuracy achieved by our proposed framework is 98.9%. Obtained accuracy by proposed methodology is **0.9%** higher than [1, 12] respectively (Fig. 7).

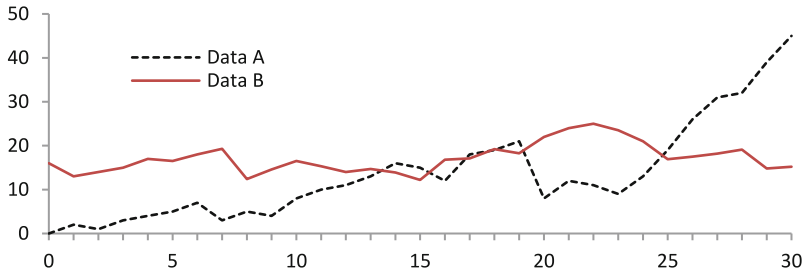


Fig. 7. Result Comparison of Data A and Data B Over a Range of 0 to 30

5 Conclusion

In this research, we present the methodology in detail that we utilized for the fluorescent microscope images. More particularly, we utilized the dataset of the 2D Hela cells and CHO. 2D Hela cells dataset contains 10 classes and CHO dataset contains 5 classes. We experimented with several types of visual features, the features that we employed in our research consist of, Haralick's Features, SFTA Features, local binary pattern (LBP), edge histogram descriptor (EHD). First, we experimented with each individual feature extraction technique. We also experimented with combined visual features obtained by different settings for SFTA, Haralick's, LBP, and EHD. Finally, the experiments are carried out for the hybrid feature. The experimentation (for individual feature extraction method) reveals that the SFTA are best performing individual features in our framework and exhibited the accuracy of 90% and 96% on 2D Hela and CHO dataset respectively. Haralick's features demonstrated second best performance as individual feature extraction techniques and exhibited the accuracy of 73% and 72% respectively on 2D Hela and CHO dataset. Other features like color edge histogram descript (EHD) exhibited the accuracy of 63%, 88% respectively on 2D Hela and CHO dataset.

After selection of best performing set of features, early fusion (Concatenation) is applied on features, to form a combined hybrid feature vector and experiments carried out on hybrid feature vector. The hybrid features exhibited the accuracy of 98.9% on 2D Hela dataset and 99.6% on CHO dataset. The comparison of the performance for hybrid features is compared with other performances mentioned in the literature, on this dataset the best-reported accuracy in 2D Hela dataset was 98%. The results of our proposed methodology are approximately 0.9% and 0.6% higher than the best reported results on the 2D Hela dataset and the CHO dataset, respectively. This is because the use of diverse features captures different information of image, and as a result, their combination offers a complete representation of the visual content of an image. This is due to the fact that, the use diverse features capture different information of image, and as a result, their combination offers a complete representation of the visual content of an image.

Funding. Not Applicable.

Data Availability Statement. Data are available from the authors upon reasonable request and with permission of Author.

Competing Interests. All authors agree on work and have no Competing interests.

References

1. Boland, M.V., Murphy, R.F.: A neural network classifier capable of recognizing the patterns of all major subcellular structures in fluorescence microscope images of HeLa cells. Bioinformatics **17**(12), 1213–1223 (2001)
2. Hamilton, N.A., Pantelic, R.S., Hanson, K., Teasdale, R.D.: Fast automated cell phenotype image classification. BMC Bioinform. **8**(1), 110 (2007)

3. Murphy, R.F., Boland, M.V., Velliste, M.: Towards a systematics for protein subcellular location: quantitative description of protein localization patterns and automated analysis of fluorescence microscope images. ISMB **8**, 251–259 (2000)
4. Chen, S.C., Zhao, T., Gordon, G.J., Murphy, R.F.: Automated image analysis of protein localization in budding yeast. Bioinformatics **23**(13), i66–i71 (2007)
5. Chebira, A., et al.: A multiresolution approach to automated classification of protein subcellular location images. BMC Bioinformatics **8**(1), 210 (2007)
6. Huang, K., Lin, J., Gajnak, J.A., Murphy, R.F.: Image content-based retrieval and automated interpretation of fluorescence microscope images via the protein subcellular location image database. In Biomedical Imaging, 2002. In: Proceedings. 2002 IEEE International Symposium on, pp. 325–328. IEEE (2002)
7. Chen, S.C., Murphy, R.F.: A graphical model approach to automated classification of protein subcellular location patterns in multi-cell images. BMC Bioinform. **7**(1), 90 (2006)
8. Chen, S.C., Gordon, G.J., Murphy, R.F.: A novel approximate inference approach to automated classification of protein subcellular location patterns in multi-cell images. In Biomedical Imaging: Nano to Macro, 2006. 3rd IEEE International Symposium on, pp. 558–561. IEEE (2006)
9. Chen, X., Velliste, M., Murphy, R.F.: Automated interpretation of subcellular patterns in fluorescence microscope images for location proteomics. Cytometry A **69**(7), 631–640 (2006)
10. Boland, M.V., Markey, M.K., Murphy, R.F.: Classification of protein localization patterns obtained via fluorescence light microscopy. In Engineering in Medicine and Biology Society, 1997. In: Proceedings of the 19th Annual International Conference of the IEEE, vol. 2, pp. 594–597. IEEE (1997)
11. Buck, T.E., Rao, A., Coelho, L.P., Fuhrman, M.H., Jarvik, J.W., Berget, P.B., Murphy, R.F.: Cell cycle dependence of protein subcellular location inferred from static, asynchronous images. In: Engineering in Medicine and Biology Society, 2009. EMBC 2009. Annual International Conference of the IEEE, pp. 1016–1019. IEEE (2009)
12. Tahir, M., Khan, A.: Protein subcellular localization of fluorescence microscopy images: employing new statistical and Texton based image features and SVM based ensemble classification. Inf. Sci. **345**, 65–80 (2016)
13. Haralick, R.M., Shanmugam, K., Dinstein, I.: Textural features for image classification. IEEE Trans. Syst. Man, Cybern. **SMC-3**(6), 610–621 (1973)
14. Lin, C.C., et al.: Boosting multiclass learning with repeating codes and weak detectors for protein subcellular localization. Bioinformatics **23**(24), 3374–3381 (2007)
15. Raza, A., Meeran, M.T., Bilhaj, U.: Enhancing breast cancer detection through thermal imaging and customized 2D CNN classifiers. VFAST Trans. Softw. Eng. **11**(4), 80–92 (2023)
16. Cortes, C., Vapnik, V.: Support-vector networks. Mach. Learn. **20**(3), 273–297 (1995)
17. Lin, Y.S., Lin, C.C., Tsai, Y.S., Ku, T.C., Huang, Y.H., Hsu, C.N.: A spectral graph theoretic approach to quantification and calibration of collective morphological differences in cell images. Bioinformatics **26**(12), i29–i37 (2010)
18. Mei, S.: Multi-kernel transfer learning based on Chou's PseAAC formulation for protein submitochondria localization. J. Theor. Biol. **293**, 121–130 (2012)
19. Shi, J.Y., Zhang, S.W., Pan, Q., Cheng, Y.M., Xie, J.: Prediction of protein subcellular localization by support vector machines using multi-scale energy and pseudo amino acid composition. Amino Acids **33**(1), 69–74 (2007)
20. Khan, S.U.R., Zhao, M., Asif, S., Chen, X., Zhu, Y.: GLNET: global–local CNN's-based informed model for detection of breast cancer categories from histopathological slides. J. SuperComput. **80**, 7316–7348 (2023)
21. Mallat, S.G.: A theory for multiresolution signal decomposition: the wavelet representation. IEEE Trans. Pattern Anal. Mach. Intell. **11**(7), 674–693 (1989)

22. Ojala, T., Pietikainen, M., Maenpaa, T.: Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. IEEE Trans. Pattern Anal. Mach. Intell. **24**(7), 971–987 (2002)
23. Khan, S.U.R., Zhao, M., Asif, S., Chen, X.: Hybrid-NET: a fusion of denseNet169 and advanced machine learning classifiers for enhanced brain tumor diagnosis. Int. J. Imaging Syst. Technol. **34**(1), e22975 (2024)
24. Dimitrovski, I., Kocev, D., Kitanovski, I., Loskovska, S., Džeroski, S.: Improved medical image modality classification using a combination of visual and textual features. Comput. Med. Imaging Graph. **39**, 14–26 (2015)
25. Won, C.S.W., Park, D.K.P., Park, S.-J.P.: Efficient use of MPEG-7 edge histogram descriptor. ETRI J. **24**(1), 23–30 (2002)
26. Khan, N.Y., McCane, B., Wyvill, G.: SIFT and SURF performance evaluation against various image Deformations on benchmark Dataset. In: 2011 International Conference on Digital Image Computing: Techniques and Applications, Institute of Electrical and Electronics Engineers (IEEE), pp. 501–506 (2011)
27. Keller, J.M., Gray, M.R., Givens, J.A.: A fuzzy k-nearest neighbor algorithm. IEEE Trans. Syst. Man Cybern. **SMC-15**(4), 580–585 (1985). https://doi.org/10.1109/TSMC.1985.6313426
28. Vedaldi, A., Zisserman, A.: Efficient additive kernels via explicit feature maps. IEEE Trans. Pattern Anal. Mach. Intell. **34**(3), 480–492 (2012)
29. Haralick, R.M.: Statistical and structural approaches to texture. Proc. IEEE **67**(5), 786–804 (1979)
30. von Zernika, F.: Beugungstheorie des schneidenver-fahrens und seiner verbesserten form, der phasenkontrastmethode. Physica **1**(7–12), 689–704 (1934)
31. Boland, M.V., Murphy, R.F.: After sequencing: quantitative analysis of protein localization. IEEE Eng. Med. Biol. Mag: Q. Mag. Eng. Med. Biol. Soc. **18**(5), 115–119 (1998)
32. Jurvelin, J.S., Müller, D.J., Wong, M., Studer, D., Engel, A., Hunziker, E.B.: Surface and subsurface morphology of bovine humeral articular cartilage as assessed by atomic force and transmission electron microscopy. J. Struct. Biol. **117**(1), 45–54 (1996)
33. Jennrich, R.I., Sampson, P.: Stepwise discriminant analysis. Stat. Methods Digit. Comput. **3**, 77–95 (1977)
34. Roques, E.J., Murphy, R.F.: Objective evaluation of differences in protein subcellular distribution. Traffic **3**(1), 61–65 (2002)
35. Murphy, R.F., Velliste, M., Porreca, G.: Robust numerical features for description and classification of subcellular location patterns in fluorescence microscope images. J. VLSI Sign. Process. Syst. Sign. Image video Technol. **35**(3), 311–321 (2003)
36. Huang, K., Murphy, R.F.: Automated classification of subcellular patterns in multicell images without segmentation into single cells. In: Biomedical Imaging: Nano to Macro, 2004. IEEE International Symposium on, pp. 1139–1142. IEEE (2004)
37. Hu, Y., et al.: Automated analysis of protein subcellular location in time series images. Bioinformatics **26**(13), 1630–1636 (2010)
38. Huh, S., Lee, D., Murphy, R.F.: Efficient framework for automated classification of subcellular patterns in budding yeast. Cytometry A **75**(11), 934–940 (2009)
39. Hyvärinen, A., Hurri, J., Hoyer, P.O.: Natural Image Statistics: A Probabilistic Approach to Early Computational Vision, vol. 39. Springer Science & Business Media, London (2009)
40. De Carvalho, M.A., Lotufo, R.D.A., Couprie, M.: Morphological segmentation of yeast by image analysis. Image Vis. Comput. **25**(1), 34–39 (2007)
41. Zhao, T., Velliste, M., Boland, M.V., Murphy, R.F.: Object type recognition for automated analysis of protein subcellular location. IEEE Trans. Image Process. **14**(9), 1351–1359 (2005)

42. Danckaert, A., Gonzalez-Couto, E., Bollondi, L., Thompson, N., Hayes, B.: Automated recognition of intracellular organelles in confocal microscope images. Traffic **3**(1), 66–73 (2002)
43. Huh, W.K., et al.: Global analysis of protein localization in budding yeast. Nature **425**(6959), 686–691 (2003)
44. Xu, P., Chan, A.K.: Support vector machines for multi-class signal classification with unbalanced samples. In: Neural Networks, 2003. Proceedings of the International Joint Conference on, vol. 2, pp. 1116–1119. IEEE (2003)
45. Latif, A., Ambreen, M., Raza, A., Rehman Khan, S.U., Khan, S.: Impact of Big Data Analytics and artificial intelligence on talent management. J. Jilin Univ. Eng. Technol. **42**(01) (2023). https://jilindaxuexuebao.com/details.php?id=https://doi.org/10.17605/OSF.IO/A5UPN

Bioelectric Signal Acquisition and Design of Portable ECG for Medical Internet of Things Applications

Abrar Ashraf[1](✉), Sadia Sahar[1], Muhammad Waseem Iqbal[2], Danish Irfan[3], M. Ameer Hamza[1], Sylvester Joseph[4], and Muhammad Tassawar Iqbal[5]

[1] Department of Computer Science, Superior University, Lahore, Pakistan
abrarashraf20@gmail.com
[2] Department of Software Engineering, Superior University, Lahore, Pakistan
[3] Department of Information Technology, Superior University, Lahore, Pakistan
[4] Trondheim, Norway
[5] COMSATS University Islamabad, Wah Campus, Islamabad, Pakistan

Abstract. In contemporary times, heart diseases have emerged as the leading cause of untimely deaths. To tackle this alarming situation, engineers have developed a range of medical devices for diagnosing and scrutinizing various diseases. Numerous patients suffer from heart problems that pose critical threats to their lives, thereby necessitating continuous monitoring via traditional monitoring systems such as Electrocardiography (ECG). However, this technique is available only in hospitals, making it prohibitively expensive and inaccessible to remote patients. The advent of wireless technologies has paved the way for building a network of connected devices through the internet. To address this issue, a proposed ECG monitoring system comprises an AD8382 ECG sensor for reading patient data, an Arduino Uno, an ESP32 Wi-Fi module, and an IoT Blynk application. Implementing this healthcare system would enable doctors to remotely monitor patients using the IoT Blynk application installed on their smartphones, which processes and visualizes the patient's ECG signal. This monitoring process can be carried out at any time and from any location, without requiring patients to visit the hospital. To conclude, the compact and integrated system design could revolutionize the healthcare industry by making it more accessible and affordable to patients. By providing real-time monitoring, this system could help doctors diagnose and treat heart diseases more effectively. Therefore, it is imperative to promote such innovative technologies to improve healthcare services worldwide.

Keywords: Bioelectric Signal · Portable · Portable ECG for Medical · Internet of Things

1 Introduction

Bioelectric signals refer to the electrical activity produced by living organisms, such as the brain and heart [7, 8]. These signals can be measured and analysed to gain insight into the functioning of the body. Bioelectric signals can be used in various medical

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 287–297, 2025.
https://doi.org/10.1007/978-3-031-77620-5_21

applications, such as diagnostic testing and monitoring of conditions like epilepsy and heart disease. The normal ECG signal segmentation are PR interval, QT interval and QRS complex. At beginning of the signal, the P wave appears and terminate at the beginning of the QRS complex segment. Normal time duration for PR interval is 0.12s to 0.20 s. It is mentioned as PR interval in above Fig. 1. QRS complex start from Q wave, after the R peek it is ends at S wave. QRS represents the ventricular depolarization duration and normal range is less than 0.10 s. Q wave to T wave segment represent electrical systole. The normal time interval of QT is less than 0.42 s. The RR interval is for to measure the heart rate variability (HRV) time and frequency features [6].

The procedure followed in clinical practice to obtain a standard 12-lead ECG involves the placement of ten electrodes. These electrodes comprise four limb electrodes and six thorax electrodes, with some electrodes serving the dual function of being part of two pairs and providing two leads. The grounding electrode or reference point for the chest leads is established by connecting the right foot to the limb electrodes [1]. In ECG testing, the limb electrodes are commonly referred to as aVR (right hand), aVL (left hand), and aVF (left foot). These three limb leads also serve the function of creating leads I, II, and III, which together form the Einthoven's triangle (as illustrated in Fig. 2). The center of this triangle is a Wilson reference terminal.

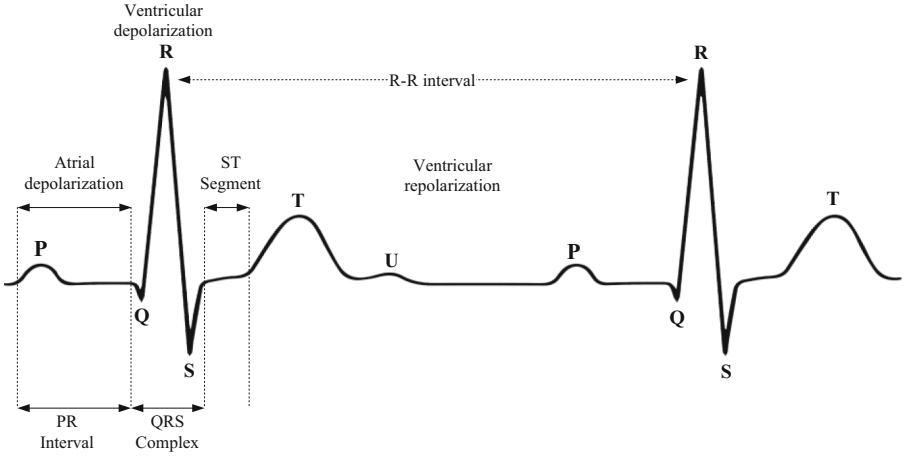


Fig. 1. Normal ECG Signal

The amplitude of the ECG signal falls within a range of 10 microvolts to 4 millivolts, rendering it feeble and prone to various interferences or additional cardiac activity. In addition to the sinoatrial node (SA), several other parts of the heart have their own rhythms and characteristics, including the atrioventricular (AV) node, Purkinje fibres, and ventral clarity. The most significant frequency of this signal lies within a range of 0.05–100 Hz. For diagnostic purposes, a sampling frequency of 500 Hz is recommended. The considered frequency range may be reduced to 0.5–50 Hz for long-term monitoring purposes and to 30–50 Hz during stress tests with a lower sampling frequency of 100 Hz.

Conversely, a broader frequency band of 0.05 to 500 Hz is required for high-resolution ECG [1].

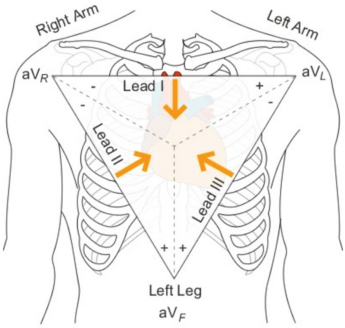


Fig. 2. Einthoven's Triangle - Line of Site of the Bipolar Leads [11]

1.1 Internet of Medical Things (IoMT)

The phrase IoT typically refers to a dynamic and extensive network framework comprised of an immense amount of network connections and computing capacities that extend beyond what is typically considered a computer, such as objects, sensors, and everyday items [2]. The advent of the Internet of Things (IoT) has enabled the development of devices that can generate, consume, and exchange data with minimal human intervention. This has led to a significant transformation in many aspects of our lives, including home automation, energy management, networked vehicles, intelligent traffic systems, and health monitoring devices.

One of the areas where IoT has had a significant impact is in the healthcare sector, particularly in patient monitoring and tracking management. The widespread implementation of IoT has provided healthcare providers with new opportunities to improve access and interconnection of devices used in healthcare. Thanks to the expeditious progress of the cyber realm, cloud computation, and online assimilation of medical supervision and management platforms, hospitals and care centres can now leverage IoT to enhance patient care. IoT-enabled devices can be used to monitor vital signs, track medication adherence, and provide real-time alerts in case of emergencies. This allows healthcare professionals to provide timely interventions, which can lead to improved patient outcomes.

1.2 Electrocardiography

The bioelectrical signal, specifically of our attention is the electrocardiogram (ECG). An electrocardiogram (ECG or EKG) is a test signals that measures the electrical activity of the heart [2, 6, 7]. It records the heart's rhythm and can detect any abnormalities. This test is non-invasive, and typically performed by placing electrodes on the chest, arms, and legs [6]. The resulting tracing of the cardiac electrical activity is then analysed by

a healthcare professional to assess the heart's health and detect any potential problems, such as heart attack, arrhythmias, and other cardiac conditions.

1.3 ECG Waveform

The ECG waveform is divided into several segments, including the P wave, Q, R, S complex, and T wave, each of which corresponds to a different stage of the cardiac cycle [6]. Abnormalities in these segments can indicate issues such as arrhythmias, heart attacks, and other heart conditions.

In conclusion, the implementation of IoT in healthcare has transformed the way we manage and monitor patients. IoT-enabled devices provide healthcare professionals with real-time data, enabling them to provide timely interventions and improve patient outcomes. Therefore, it is essential to continue investing in IoT-enabled healthcare devices and solutions to provide better care to patients [2]. Embedded technologies play a crucial role in disseminating healthcare to individuals in distant and remote areas by furnishing them with a surveillance system that offers an uninterrupted stream of precise data for optimal healthcare verdicts. As the technology is developed to assemble, scrutinize, and transmit data, the Internet of Things (IoT) continues to ameliorate, and the healthcare applications and systems driven by IoT are surfacing at a rapid pace [2].

The collection of electrocardiograms (ECG) data has traditionally been done in medical facilities using large, stationary equipment. These gadgets are equipped with 12 electrodes, which make them highly accurate in measuring heart activity over a short period of time. However, due to their weight and size, they are difficult to carry, making patients' movements and activities highly restricted during data collection. Moreover, the high cost of these devices makes it impossible for patients to use them at home, leading to frequent hospital visits that strain the healthcare system [1, 2, 6, 9].

2 Literature Review

Anand Kubal and Chandra shekarappa K [4]. Proposed a E-Health monitoring system that utilize raspberry pi board with 3 sensors and a camera to collect, process and push the patient's health data to the server through Wifi integrated in raspberry pi board. The literature review shows that the monitoring system utilize two raspberry pi boards, one is in the healthcare facility to get access to the patient health information connected through the IP address and another is the patient's raspberry pi interfaced through sensors to pass the health data to server. In summary, Author suggested system is costly solution to this system specifically whereas Internet of Things (IoT) devices are getting economical day by day, the raspberry Pi along with the camera is not less expensive. Suggested solution is not easy to handle or operative without the dedicated technical individual.

Dathar Abas Hasan and Ayad Ghany Ismaeel, [2]. Highlights that the proposed system aims to minimize time delays in accessing a patient's health data and displaying results on a physician's laptop or mobile device. This is achieved through the utilization of the Blynk application, which is readily available on the Google Play Store. The system is built on the Arduino UNO Microcontroller and the AD8232 module, which contains a non-operational amplifier with a low pass filter. The module is designed with

a 3.5 mm audio jack interface that allows for the easy connection of electrodes probes. The system's main strengths, as identified by the author, include its ease of use and accessibility, portability, remote operation capabilities, cost-effectiveness, and ease of deployment.

R. Lakshmi Devi and V. Kalaivani, [6]. Discussed that IoT-based cardiac arrhythmia monitoring system, equipped with statistical and dynamic features, has great potential in enhancing the accuracy of the classifier. With our system, healthcare professionals can easily monitor and diagnose the condition of their patients in real-time. In conclusion, our IoT-enabled ECG tele monitoring system offers a promising solution for accurately and promptly diagnosing cardiac arrhythmia diseases. By improving the accuracy of the classifier, we can enhance the efficacy of the treatment. The previous related work doesn't present an ECG system that have small integrated solution, real-time, low-cost and to access remotely.

3 Methodology

The complex framework that has been suggested comprises an intricate array of hardware components, including bandpass filter circuitry, FET operational amplifier (TL084), Microcontroller Atmega328p, and ESP32 Wifi Module. These instruments have been thoughtfully integrated into a small printed circuit board (PCB). To fully comprehend the intricate nature of this system, one must first grasp the intricate workings of each component. The bandpass filter circuitry plays a crucial role in filtering out specific frequencies while allowing others to pass through. This is accomplished through the utilization of specific electronic components and circuitry.

The FET operational amplifier (TL084) is a specialized device that amplifies electrical signals without introducing any significant distortion. Its unique properties make it an ideal component for use in this complex system, as it enables the faithful reproduction of signals with minimal distortion. The Microcontroller Atmega328p is a sophisticated computing device that is responsible for the overall functioning of the system. Its powerful processing capabilities enable it to perform a wide range of tasks with ease, making it a vital component in this complex framework. The ESP32 Wifi Module is a high-performance wireless communication device that enables the system to communicate with other devices over a wireless network. Its capabilities are truly remarkable, and it is the driving force behind the system's ability to connect with other devices over a wireless network. The anticipated system executes the following steps according to flowchart shown in Fig. 3.

3.1 IoMT Architecture is Typically Comprised of Four Layers

The first layer, which is the Perception layer, encompasses wearable devices, sensors, and other medical devices that gather patient data such as blood glucose levels, blood pressure, and heart rate. The Network layer, which is the second layer, includes communication protocols and network infrastructure that enable secure data transmission over the internet from medical devices to the cloud or other backend systems. The third layer, the Service layer, contains data processing and analytics tools that analyze the

data collected by medical devices, generating valuable insights for healthcare providers and patients.

Finally, the Application layer, the fourth layer, contains various software applications and user interfaces that allow healthcare providers and patients to access and interact with the IoMT ecosystem. By integrating these four layers, IoMT architecture empowers healthcare providers to remotely manage and monitor patient health, ultimately leading to better patient outcomes, and reduced healthcare costs. Nonetheless, security and privacy concerns, as with any interconnected system, must be thoroughly considered and addressed to ensure the confidentiality and safety of patient data.

Architecture of the system include three layers, Network layer (the IoMT cloud and database), End user layer (The patient and doctor or physician), the gateway (Internet access points) shown in Fig. 2.

The architecture of the Internet of Medical Things (IoMT) pertains to the interconnected web of healthcare technologies, medical devices, and sensors that are capable of exchanging data over the internet.

3.2 Signal Acquisition

In electrocardiography, the augmentation process is paramount in order to enhance the voltage of the heart's electric signals. The heart's signals are feeble and can be easily overpowered by the electrical noise in the surroundings. The augmentation process facilitates the elevation of the signal's voltage, generally by a factor of 10 to 1000, for the purpose of its ease in detection and analysis [8]. Moreover, band pass filtration is a crucial element in electrocardiogram analysis. It encompasses the removal of undesirable frequencies from the electrocardiogram signal while retaining the frequencies of significance. The ECG signal's significant frequencies usually fall within the 0.05 Hz to 100 Hz range. The band pass filter is crafted to reduce the amplitudes of the frequencies lying outside this range, which could be caused by the interference of noise or other external sources [1, 5, 8].

The integration of amplification and band pass filtration allows the electrocardiogram signal to be registered with high precision and exactitude. The amplified and filtered signal can be further scrutinized to identify the notable features such as the P wave, QRS complex, and T wave. These features are responsible for specific events in the cardiac cycle. The two stages of amplification and band pass filters used in the suggested design is shown below in the Fig. 5.

3.2.1 Amplification

The important step of the data acquisition segment is the signal amplification through the TL084 chip and three medical grade adhesive electrodes labelled as IN- for the right side, IN + for the left and ampRef for the left leg or reference ground as shown in the Fig. 4.

3.2.2 Bandpass Filters

After the amplification of the acquired signal the bandpass filters are used to eliminate unnecessary signals or input noise. Signal conditioning is achieved using a bipolar point

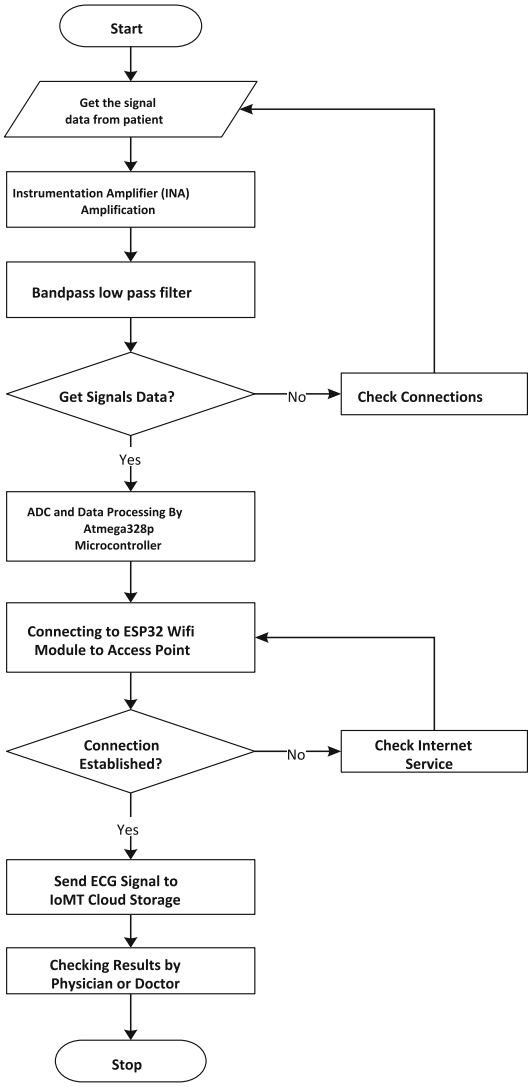


Fig. 3. The Flowchart of the proposed system architecture.

high pass filter which is coupled after the instrumentation amplifier [2]. To reducing the additional noise a low pass filter is used as well [2]. Narrow input frequency band, use for EEG, EOG, and ECG.

3.3 Design

For the design testing and measurement purposes, the prototype is made up with the development kit modules like ESP32 Dev Kit C, Arduino Nano and AD8232. Printed Circuit board (PCB) is designed accomplish through Open-source software KiCad 7. PCB

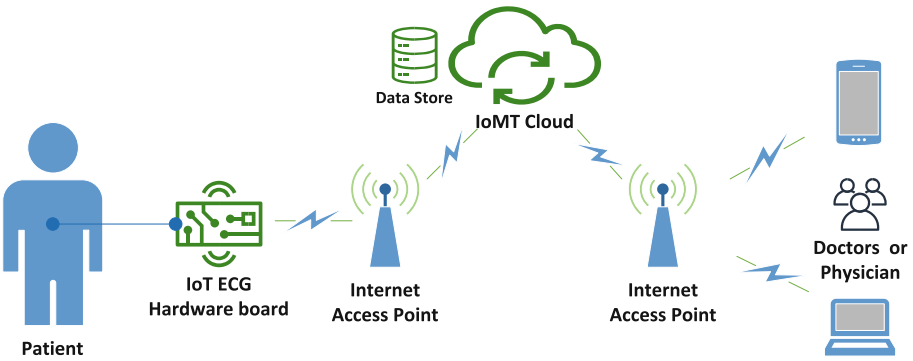


Fig. 4. Architecture of suggested system of (IoMT) based ECG

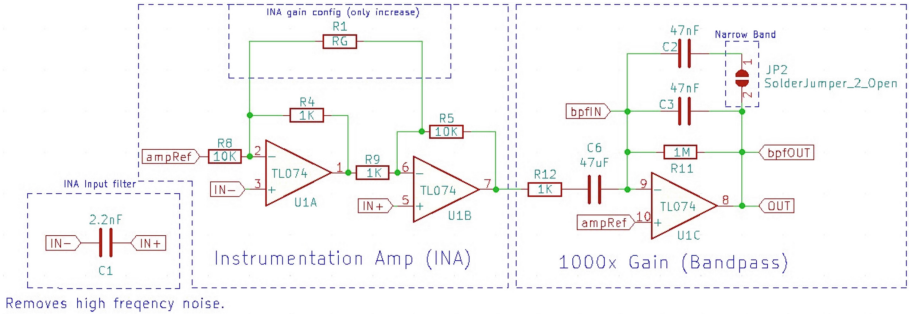


Fig. 5. Instrumentation Amp and 1000x Gain Bandpass Filter

accommodates all the module and provides the better grounding connections therefore better immunity circuit design and ultimately would be good for better signal acquisition. Printed Circuit Board (PCB) with the 3D render is shown below in Fig. 6.

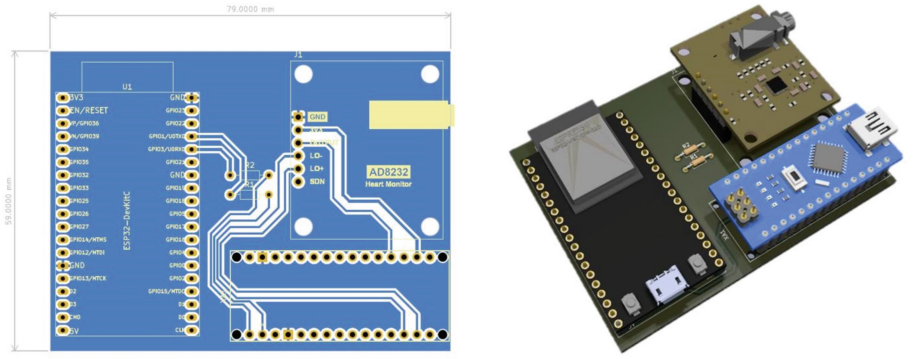


Fig. 6. Printed Circuit Board (PCB) of Mini ECG (Prototype)

4 Experimentation and Results

To acquire the cardiac signal several experiments has been conducted. For the testing purpose, first experiment conducted through the modules with wired connection in between them as shown in the Fig. 7 below. Three electrode probes used on human body according to the Einthoven's triangle (discussed in the introduction section) for ECG signal acquisition.

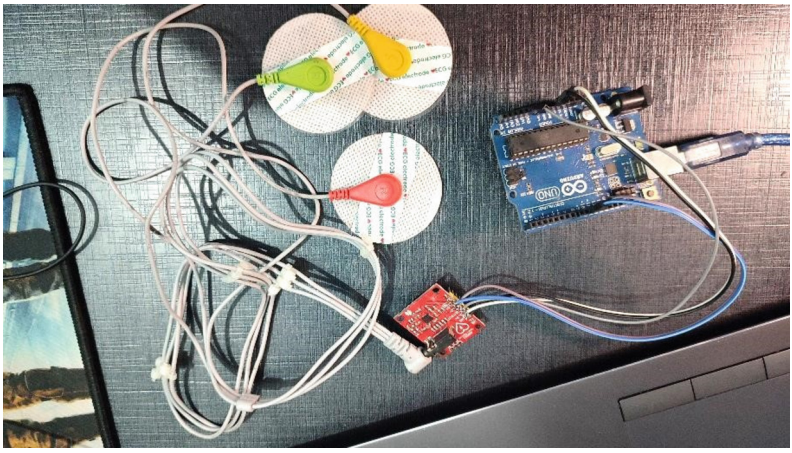


Fig. 7. Arduino UNO and ECG Module Wiring

By uploading the ECG Arduino code to the Arduino controller and setting up the electrodes to human body according to the discussed method, received signal on the Arduino IDE serial monitor shown in the Fig. 8 below. It can be seen that signal is distorted and noisy, it could be due to the misplacement of electrodes or the ground noise that cause problems and performance issues in circuits and can ultimately lead to PCB failures.

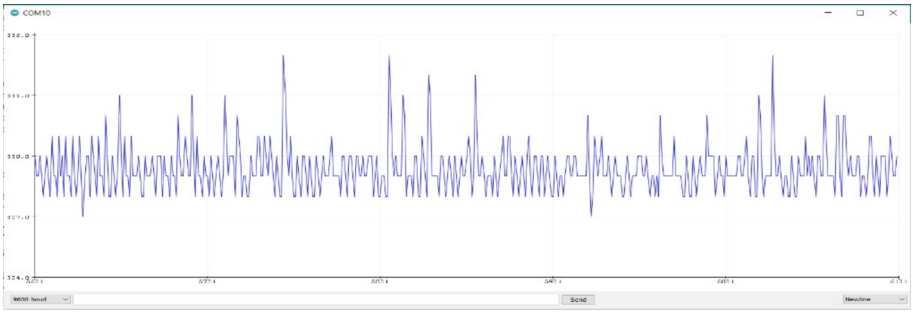


Fig. 8. Magnitude

During the experimentation and testing prototype, there was high instability in signals for instance sometimes microcontroller received signals of our interest and many times it goes very distorted behaviour. After many practices we found that this was causing by the ground loop noise. For the instant solution, placing the wire connections at various location of ground in circuit it was immunized by noise. Signals can also be affected by the human sitting, lying down and arms position. Therefore, relaxed position with some back rest and arms down position provide us some better results can be seen in the Fig. 9.

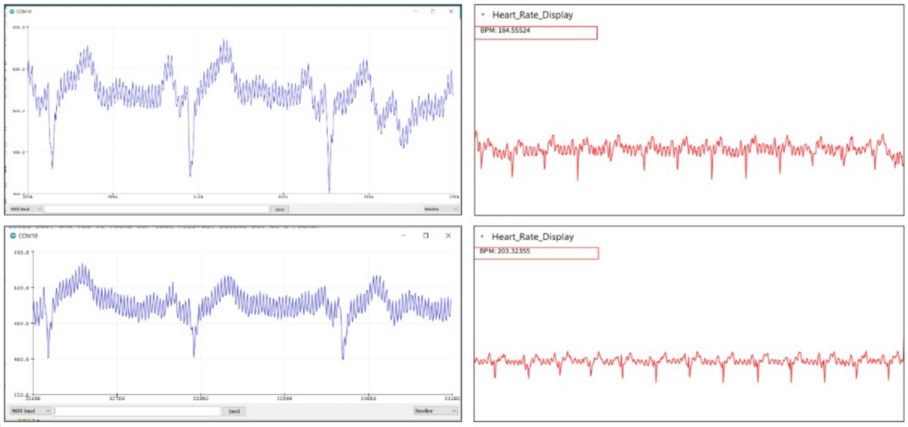


Fig. 9. Signal Acquired Through The Serial Monitor And Plot Interface of Arduino Ide.

After the practicing on the individual wired modules with the different electrode configuration, another implementation has been performed on the proposed ECG design device found in stability and much better signal results can be seen in the Fig. 4.3 above. In the comparison with the original PQRS complex waveform it can be noted there is very less difference about 0.3 mV. To assess how accurately the proposed method acquires and reconstructs, the widespread and extensively adopted Percentage of Root-mean-squared Difference (PRD) was utilized [17].

Fig. 4.3. Signal results from the proposed ECG device, (a) on serial monitor (b) serial plot with soft filter.

5 Conclusion

The detection and treatment of cardiac arrhythmia diseases require a prompt and precise diagnosis. To address this need, we introduce an innovative compact portable ECG device for Internet of Medical Things (IoMT) that enables diagnosis of cardiac arrhythmia diseases as well as through the Wifi enabled ESP32 chip, data can be stored on the cloud database and can be effectively manage the patient's health records and history. Our proposed device remarkably compact size, reducing the need for large, cumbersome ECG systems. For the future it can be more compact that can be achieved by the discreet electronics components on the Printed Circuit Board (PCB).

References

1. Martinek, R., Ladrova, M.: Advanced bioelectrical signal processing methods: past, present and future approach. Sensors **21**(5186), 2021 (2021)
2. Hasan, D., Ismaeel, A.: Designing ECG monitoring healthcare system based on internet of things Blynk application. J. Appl. Sci. Technol. Trends **1**(2), 106–111 (2020). https://doi.org/10.38094/jastt1336
3. Naqvi, M.R., et al.: A concurrence study on interoperability issues in IoT and decision making based model on data and services being used during interoperability. Lahore Garrison Univ. Res. J. Comput. Sci. Inform. Technol. **4**(4), 73–85 (2020)
4. Padmavathi, B., Rana, S.T.: Implementation of IOT Based Health Care Solution Based on Cloud Computing. Int. J. Eng. Comput. Sci. **5**(9), 7 (2016)
5. Kubal, A., Chandrashekarappa, K.: Design of e-health monitoring of patient using internet of things. IJLTEMAS **4**(8) (2017)
6. Singh, Y.N., Singh, S.K., Ray, A.K.: Bioelectrical signals as emerging biometrics: issues and challenges. ISRN Sign. Process. **2012**, 7123032 (2012)
7. Lakshmi Devi, R., Kalaivani, V.: Machine learning and IoT-based cardiac arrhythmia diagnosis using statistical and dynamic features of ECG. J. Supercomput. **76**(9), 6533–6544 (2020)
8. Thilagavathy, R., Venkataramani, B.: A novel ECG signal compression using wavelet and discrete anamorphic stretch transforms
9. Balestrieri, E., De Vito, L.: A novel method for compressed sensing based sampling of ECG signals in medical-IoT era
10. Khan, R., Ghufranullah, S.A., Khan, B.D., Iqbal, M., Pervez, K.F.: Effect of milk replacer on performance parameters of different bovine breeds. Pak. J. Nutr. **11**(12), 1190 (2012)
11. Bhujbal, N., Yadav, P., Choramale, P.: A portable IoT-cloud ECG monitoring system for healthcare **08**(02) (2022)
12. Wai, K.T., Aung, N.P., Htay, L.L.: Internet of Things (IoT) Based healthcare monitoring system using NodeMCU and Arduino UNO. Int. J. Trend Sci. Res. Dev. **3**(5), 755–759 (2019)
13. https://www.nottingham.ac.uk/nursing/practice/resources/cardiology/function/bipolar_leads.php
14. Iqbal, M.W., Ahmad, N., Shahzad, S.K., Naqvi, M.R., Feroz, I.: Usability aspects of adaptive mobile interfaces for colour-blind and vision deficient users. Int. J. Comput. Sci. Netw. Secur. **18**(10), 179–189 (2018)
15. Lee, B.M., Ouyang, J.: Intelligent healthcare service by using collaborations between IoT personal health devices. Int. J. Bio-Sci. Bio-Technol. **6**(1), 10 (2014)
16. Li, C., Hu, X., Zhang, L.: The IoT-based heart disease monitoring system for pervasive healthcare service. Procedia Comput. Sci. **112**, 2328–2334 (2017)
17. Bhattacharya, S., Pandey, M.: Significance of IoT in India's E-medical framework: a study. In: 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), pp. 321–324 (2020)
18. Kamble, P., Birajdar, A.: IoT Based Portable ECG Monitoring Device for Smart Healthcare. In: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), vol. 1, p. 471474 (2019)
19. Nurdin, M.R.F., Hadiyoso, S., Rizal, A.: A low-cost Internet of Things (IoT) system for multi-patient ECG's monitoring. In: 2016 International Conference on Control, Electronics, Renewable Energy and Communications (ICCEREC), pp. 7–11 (2016)
20. Craven, D., McGinley, B., Kilmartin, L., Glavin, M., Jones, E.: Compressed sensing for bioelectric signals: a review. IEEE J. Biomed. Health Inform. **19**(2), 529–540 (2015)

Classification of Cloud Attacks Using Deep Learning

Muhammad Zulkifl Hasan[1(✉)], Muhammad Zunnurain Hussain[2], Muhammad Umer Nadeem[1], Muhammad Zeeshan Nazar[4], Summaira Nosheen[2], Muhammad Atif Yaqub[3], Afshan Bilal[3], Saeed Anwar[1], and Muhammad Ahmad[1]

[1] FoIT and Computer Science, University of Central Punjab, Punjab, Pakistan
Zulkifl.hasan@ucp.edu.pk
[2] Department of Computer Science, Bahria University Lahore Campus, Lahore, Pakistan
[3] National College of Business Administration and Economics, School of Computer Science, Lahore, Pakistan
[4] FAST National University of Computer and Emerging Sciences, Lahore Campus, Lahore, Pakistan

Abstract. Cloud computing has become an integral part of our lives, allowing us to store and access data quickly and easily. Unfortunately, cybercriminals have developed increasingly sophisticated techniques to exploit network vulnerabilities and bring them down. This paper proposes using two pre-trained deep learning models, VGG16 and ResNet50, to classify benign traffic and DrDoS (distributed denial-of-service) attacks in cloud environments. The Cloud Attacks Dataset, sourced from the CICIDS 2019 dataset, includes a comprehensive collection of network traffic instances represented in binary visualization format and is divided into two classes: benign traffic and DrDoS attacks. The dataset has been split into a training set of 5000 images and a testing set of 1168 images with equal representation of benign traffic and DrDoS attack instances. We aim to provide a robust and reliable solution to detect DrDoS attacks and protect networks from malicious activities.

Keywords: DoS · DDoS · DrDoS · CICIDS · VGG16 · ResNet50

1 Introduction

The advancement of technology has changed the world drastically in a brief period [2]. Networking has become an integral part of our lives, connecting us all around the globe. Cloud computing has become a significant part of our lives, storing data and information in an easily accessible form. Data has become the new oil, a source of immense potential that can be used to power the world. Unfortunately, with the prospect of data comes the risks of cybersecurity attackers who have developed increasingly sophisticated techniques to bring down networks [3]. A cyberattack known as a denial of service (DoS) attack on the cloud involves flooding the network with malicious traffic to prevent a cloud service's availability [4]. The resources of the cloud service are

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 298–307, 2025.
https://doi.org/10.1007/978-3-031-77620-5_22

overloaded by this malicious traffic, which blocks legitimate traffic and access to the service. DoS assaults against the cloud can have dire repercussions, such as outages, data breaches, and reputational harm. DDoS (Distributed Denial of Service) attacks aim to make a network or website unavailable to its intended users [5].

It differs from DoS (Denial of Service) in that it comes from multiple sources simultaneously. This makes tracing the source of the attack and identifying the perpetrator difficult. DDoS attacks are especially damaging in the cloud because the cloud environment is not typically designed to handle the massive influx of malicious traffic a DDoS attack can bring. DDoS attacks are classified into volumetric, protocol, and application layer attacks. Large amounts of network traffic are used in volumetric attacks to overwhelm the target network or website. Protocol attacks target the protocols used to communicate between computers, whereas application layer attacks seek to exploit vulnerabilities in the target network's or website's application layer. DDoS attacks of all three types can be highly damaging and costly. DrDoS (distributed reflective denial-of-service) attacks cloud environments [6]. It happens when a malicious actor sends significant traffic to a cloud-based service or data center, causing legitimate users to lose service. DrDoS attacks, as opposed to traditional DoS and DDoS attacks, target cloud-based services and data centers rather than individual systems. DrDoS attacks are far more challenging to detect and defend against because they have frequently distributed across multiple cloud resources or data centers. Furthermore, DrDoS attacks can be highly disruptive, as they can overwhelm an entire cloud infrastructure's resources.

To ensure any organization's security, it is vital to develop practical solutions to detect and mitigate network attacks. DrDoS attacks are extremely dangerous for cloud environments, and it is essential to identify them efficiently to prevent malicious activity on the network. The ability to determine whether a given traffic flow is normal (benign) or if a DrDoS attack is taking place is crucial to taking the appropriate countermeasures. This paper proposes using two pre-trained deep learning models, VGG16 and ResNet50, to classify benign traffic and DrDoS attacks. We aim to provide a robust and reliable solution to detect DrDoS attacks and protect the network from malicious activities.

The proposed research intends to contribute to cybersecurity by delivering a dependable and effective solution for detecting DrDoS threats in cloud systems. Pre-trained deep learning models, such as VGG16 and ResNet50, provide a promising method for accurately classifying benign traffic and DrDoS attacks. This study's scope is to investigate these models' effectiveness in identifying DrDoS attacks. The contribution of this study is its potential to improve the security of cloud-based services and data centers by providing a reliable approach for detecting DrDoS attacks. This research could potentially prevent significant financial losses, reputational harm, and disruptions caused by this critical cybersecurity issue.

2 Cloud Attacks Dataset

2.1 Description of Dataset

The Cloud Attacks Dataset is a valuable tool for researchers in network security and machine learning [7]. This dataset includes a comprehensive collection of network traffic instances, each represented in binary visualization format, allowing for extensive network behavior analysis. The cases in the dataset are divided into two classes:

benign traffic and DDoS attacks. Notably, the DDoS attacks class is comprised solely of instances of the DrDoS attack type. This specificity allows for a focused examination of this particular type of DDoS attack and its characteristics.

2.2 Overview of the Subsets

The Cloud Attacks Dataset has been split into two subsets to validate results. The training dataset contains 5000 images, with 2500 images belonging to the benign traffic class and 2500 images belonging to the DrDoS attack class, as shown in Fig. 1. The testing dataset comprises 1168 images, with equal representation of benign traffic instances and DrDoS attack instances, as shown in Fig. 2. This balanced distribution of the cases in the two datasets facilitates accurate evaluation of machine learning models and other analysis techniques.

2.3 Source of Cloud Attacks Dataset

This Cloud Attacks Dataset was sourced from the CICIDS 2019 dataset, widely recognized as a comprehensive collection of modern network attacks and benign traffic instances [8]. The dataset is available for public use on the Mendeley Data website for research purposes. Including the CICIDS 2019 dataset has significantly enhanced the value of the Cloud Attacks Dataset for network security research.

2.4 Summary of the Cloud Attacks Dataset

In conclusion, the Cloud Attacks Dataset is a valuable resource for those studying network security and machine learning. Its comprehensive collection of network traffic instances is represented in binary visualization format, and its focused examination of the DrDoS attack type makes it a prime resource for developing and evaluating machine learning models and other analysis techniques.

3 Literature Review

Weizhi Meng et al. [9] present a machine learning-based detection scheme for Distributed Denial-of-Service (DDoS) attacks. The method is designed to detect both volumetric and application-layer attacks. The detection scheme is evaluated on simulated and real-world network traffic data sets. The results show that the proposed method effectively detects DDoS attacks with an average accuracy of 99%. Furthermore, the scheme could detect DDoS attacks with a low false positive rate.

Yunqi Li et al. [10] present a machine learning-based approach for detecting Distributed Denial-of-Service (DDoS) attacks in cloud computing. The method utilizes a supervised learning model to identify DDoS attack patterns from network traffic data. The model is evaluated using two real-world network traffic data sets. The results show that the proposed approach effectively detects DDoS attacks with an average accuracy of 92.3%. Furthermore, the process saw DDoS attacks with a low false positive rate.

Yuxin Zhang et al. [11] present a machine learning-based approach for detecting Distributed Denial-of-Service (DDoS) attacks in cloud computing. The method utilizes a supervised learning model to identify DDoS attack patterns from network traffic.

The model is evaluated using two real-world network traffic data sets. The results show that the proposed approach effectively detects DDoS attacks with an average accuracy of 92.3%. Furthermore, the process saw DDoS attacks with a low false positive rate.

J.A.R. Rana, S.P. Chaudhari, and P.M. Borkar. [12] present the design and development of a machine learning-based DrDoS attack detection system. The system utilizes the Random Forest (RF) algorithm to detect DrDoS attacks. The authors conducted experiments using two datasets, namely, the KDD Cup 99 dataset and the KDDCup99-DrDoS dataset, to evaluate the system's performance. The results show that the system effectively detects DrDoS attacks with a precision of 99.77%, recall of 99.90%, and an F1-score of 99.83%. The authors also discuss the importance of feature selection in improving the system's accuracy.

4 Methodology

4.1 Data Collection and Preprocessing

The Cloud Attacks Dataset used in this study is freely available on the Mendeley Data website for research purposes. The collection has 5000 photos, including 2500 images for benign traffic and DrDoS attacks. The images have already been preprocessed, which includes resizing to 60 × 60 pixels, RGB color space conversion, and normalization. This guarantees that the pictures are standardized and ready for machine learning models to be trained on.

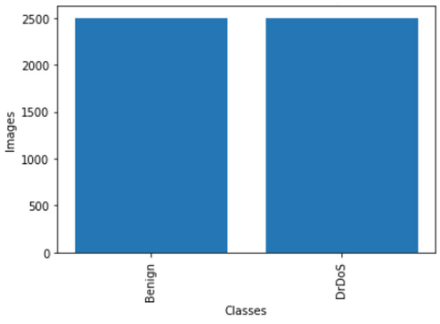


Fig. 3. Left: Class Distribution: Original Dataset

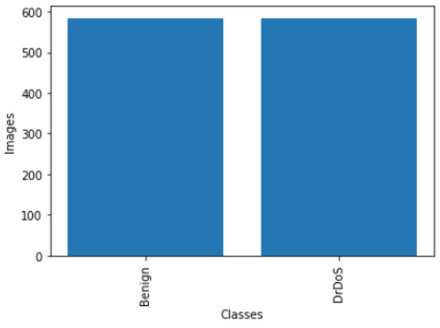


Fig. 4. Right: Class Distribution: Resampled Dataset

4.2 Feature Extraction

For feature extraction in this work, we used the transfer learning technique with pre-trained VGG-16 and ResNet-50 models. Transfer learning is a sophisticated machine learning technique that uses knowledge learned from a previously trained model to improve the training of a new model [14]. This method allows the latest model to benefit from the prior model's learning and expertise, resulting in faster and more precise outcomes. Transfer learning aids in the development of models that are better able to spot and anticipate patterns in data.

4.3 Classification

The pre-trained VGG-16 and ResNet-50 models using ImageNet dataset weights were used to binary classify the images as benign traffic or DrDoS attack instances. To handle binary classification, the base models were loaded without their classification layers, and a new input layer with a size of 60 $\times$ 60 and three channels was added, followed by a global average pooling 2D layer, a dropout layer with a rate of 0.2, and a dense prediction layer with one neuron and a sigmoid activation function.

5 Experimentations

This section aims to present an experimental methodology for classifying images based on whether they are benign traffic or DrDoS attacks using transfer learning with pre-trained VGG-16 and ResNet-50 models. We first describe the data split methodology used for training and validation, then explain the transfer learning approach utilized in our study. Next, we provide detailed descriptions of the VGG-16 and ResNet-50 models used for the classification task. Finally, we discuss the issue of generalizability.

5.1 Data Split Methodology

In this research, we divided the training portion of the Cloud Attacks Dataset into two sets: 75% for training purposes and 25% for validation purposes [13]. This division resulted in 3750 images for training, with 1875 images for each class, as depicted in Fig. 3. The validation portion consisted of 1250 images, with 625 pictures for each category, as shown in Fig. 4. The testing dataset was left as provided.

5.2 Callback Functions in Experiments

Callbacks are a powerful tool in the machine learning process that allows you to monitor and control the training process [15]. They provide several useful functions, such as preventing overfitting, visualizing training progress, debugging code, saving checkpoints, and generating logs. These functions help ensure that the training process is efficient and effective, ultimately leading to better results. In our experiment, we utilized callbacks to aid in optimizing the training process. Specifically, we employed early stopping with a patience of 4 and a reduction of the learning rate with a tolerance of 2 and a factor of 0.1 [16, 17]. This allowed us to monitor the training progress and adjust the learning rate as necessary, with a minimum threshold of 0.0000001, to ensure that the training proceeded effectively and efficiently.

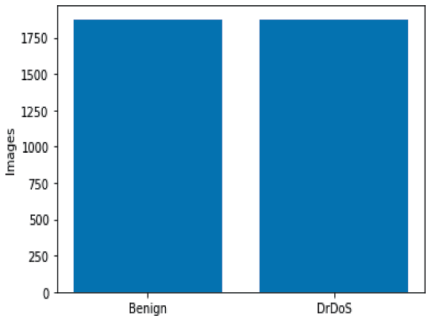


Fig. 1. Images in Training Dataset After Split

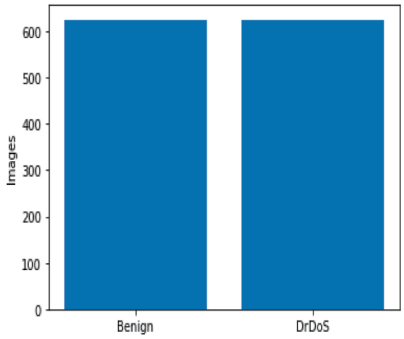


Fig. 2. Images in Validation Dataset After Split

5.3 Pre-trained VGG-16 Model

VGG-16 is a deep learning model developed by the Visual Geometry Group at Oxford University [18]. It contained 16 layers and was designed to achieve top performance in the ImageNet Large Scale Visual Recognition Challenge in 2014. The model has been pre-trained on the ImageNet dataset, which includes various images and can classify images into 1000 different classes. Our study used it to detect security attacks in networks by utilizing its pre-trained knowledge for image classification to identify DrDoS attacks.

5.4 Pre-trained ResNet-50 Model

ResNet-50 is a powerful deep-learning model developed by Microsoft and won the ImageNet Large-Scale Visual Recognition Challenge in 2015 [19, 20]. It is a network comprising 50 convolutional layers and features shortcut connections, allowing the model to learn identity functions with fewer parameters. The pre-trained version of ResNet-50 has been trained on the ImageNet dataset, making it well-suited for detecting complex patterns, handling noise, and learning non-linear features. In our study, the pre-trained ResNet-50 was utilized for detecting DrDoS attacks due to its strong ability in these areas, without extensive training, saving time and resources.

5.5 Issue of Generalizability

The generalizability of a model to effectively classify new, unseen data is a critical component in evaluating its success in machine learning. Transfer learning with pre-trained VGG-16 and ResNet-50 models was used in our study to classify images as benign traffic or DrDoS attacks, with high accuracy rates on test data. However, due to the fixed distribution of instances in our dataset, the generalizability of these models to other scenarios or datasets remains uncertain. To address this constraint, future research should investigate the usage of varied datasets and evaluate models on new, unseen data to examine their real-world applicability thoroughly.

6 Result Analysis and Discussion

VGG-16 was tested on both the validation and testing datasets and achieved an accuracy of 99.92% and 99.6%, respectively. The validation accuracy can be seen in Fig. 5, and the loss is displayed in Fig. 6.

VGG-16 was tested on 1168 images from the testing dataset, accurately classifying 583 images as "Benign Traffic" and 581 images as "DrDoS attack." However, the model made four incorrect predictions, labeling 3 "DrDoS attack" images as "Benign Traffic" and 1 "Benign Traffic" image as "DrDoS attack." These results are depicted in Fig. 7, with 1164 correct predictions out of 1168 images. The precision, recall, and f1-score can be found in Table 1.

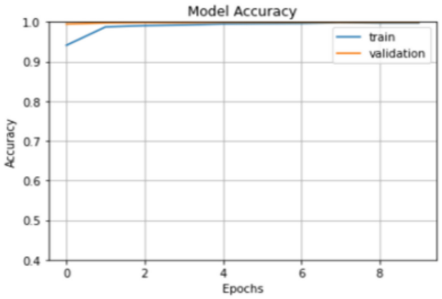


Fig. 5. Training & Validation Accuracy Curves of VGG-16

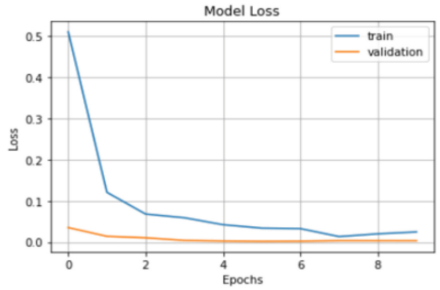


Fig. 6. Training & Validation Loss Curves of VGG-16

The ResNet-50 model was tested on both a validation dataset and a testing dataset. The model achieved 100% accuracy on the validation dataset and 99.6% on the testing dataset. The model's accuracy on the validation dataset can be seen in Fig. 8, while the loss can be seen in Fig. 9.

The ResNet-50 model made predictions on the 1168 images in the testing dataset, correctly classifying 581 images as Benign Traffic and 581 as DrDoS attacks. However, there were three instances where a DrDoS attack image was misclassified as Benign and three cases where a Benign image was misclassified as a DrDoS attack. The model's accuracy was 1162 correct predictions out of 1168 images, as shown in Fig. 10. The model's precision, recall, and f1-score can be found in Table 2.

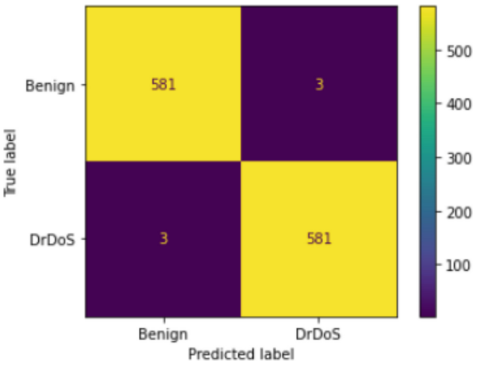


Fig. 7. Confusion Matrix of VGG-16

Table 1. Performance Metrics for Classification Model

	Precision	recall	f1-score	Support
Benign	0.99	0.99	0.99	584
DrDoS	0.99	0.99	0.99	584

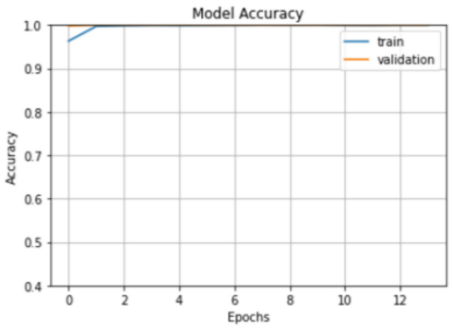


Fig. 8 Training & Validation Accuracy Curves of ResNet-50

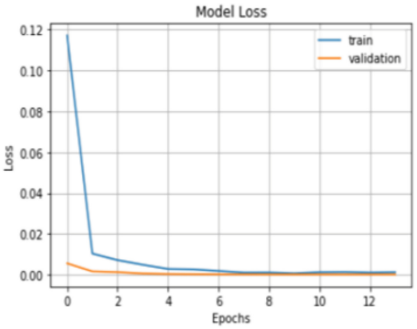


Fig. 9. Training & Validation Loss Curves of ResNet-50

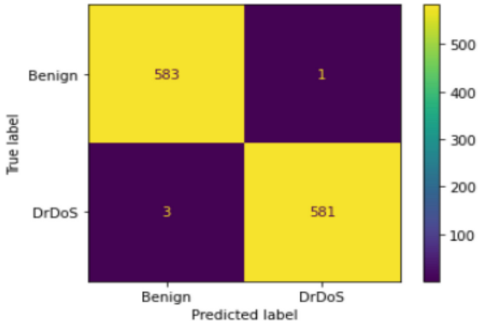


Fig. 10. Confusion Matrix of ResNet-50

Table 2. Evaluation Metrics for Model Performance

precision	recall	f1-score	Support	
Benign	0.99	0.99	0.99	584
DrDoS	0.99	0.99	0.99	584

7 Conclusion

The proposed solution can be used by organizations to detect and prevent malicious activities, improving the security of their cloud environment. This research paper aims to provide a solution to detect DrDoS attacks in cloud environments. The authors used two pre-trained deep learning models, VGG16 and ResNet50, to classify benign traffic and DrDoS attacks in the Cloud Attacks Dataset, sourced from the CICIDS 2019 dataset. The dataset was split into a training set of 5000 images and a testing set of 1168 images with equal representation of benign traffic and DrDoS attack instances. The results showed the effectiveness of the proposed solution in detecting DrDoS attacks in cloud environments.

References

1. teQwise, "Why is Cloud Computing So Important?" TeQwise. [Online]. Available: https://www.teqwise.com/news/why-is-cloud-computing-so-important-2/. [Accessed: 06-Feb-2023]
2. "12 benefits of cloud computing," Salesforce.com. [Online]. Available: https://www.salesforce.com/ap/products/platform/best-practices/benefits-of-cloud-computing/. [Accessed: 06-Feb-2023]
3. N. Morgan, "Cloud cyber attacks: The latest cloud computing security issues," Triskelelabs.com. [Online]. Available: https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues. [Accessed: 06-Feb-2023]
4. Cloudflare.com. [Online]. Available: https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/. [Accessed: 06-Feb-2023]
5. "What is a DDoS Attack: Types, Prevention & Remediation," Onelogin.com. [Online]. Available: https://www.onelogin.com/learn/ddos-attack. [Accessed: 06-Feb-2023]
6. "ShieldSquare block," Radware.com. [Online]. Available: https://www.radware.com/security/ddos-knowledge-center/ddospedia/drdos-attack/. [Accessed: 06-Feb-2023]
7. S. Sambangi, "Cloud attack dataset for building machine learning and deep learning models." Mendeley, 23-May-2022
8. "CICIDS 2019 Dataset." 02-Mar-2021
9. A Machine Learning-Based Detection of Distributed Denial-of-Service Attacks. 2020
10. A Machine Learning-Based Approach for Detecting Distributed Denial-of-Service Attacks. 2018
11. A Machine Learning-Based Approach for Detecting Distributed Denial-of-Service Attacks in Cloud Computing. 2018
12. J. A. R. Rana, S. P. Chaudhari, and P. M. Borkar, Eds., DrDoS Attack Detection Using Machine Learning Techniques. 2019
13. "Keras ImageDataGenerator with flow_from_directory()," Studymachinelearning.com. [Online]. Available: https://studymachinelearning.com/keras-imagedatagenerator-with-flow_from_directory/. [Accessed: 06-Feb-2023]
14. "Transfer learning and fine-tuning," TensorFlow. [Online]. Available: https://www.tensorflow.org/tutorials/images/transfer_learning. [Accessed: 06-Feb-2023]
15. "Tf.Keras.Callbacks.Callback," TensorFlow. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf/keras/callbacks/Callback. [Accessed: 06-Feb-2023]
16. "Tf.Keras.Callbacks.EarlyStopping," TensorFlow. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf/keras/callbacks/EarlyStopping. [Accessed: 06-Feb-2023]
17. "Tf.Keras.Callbacks.ReduceLROnPlateau," TensorFlow. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf/keras/callbacks/ReduceLROnPlateau. [Accessed: 06-Feb-2023]
18. "VGG16 and VGG19," Keras.io. [Online]. Available: https://keras.io/api/applications/vgg/. [Accessed: 06-Feb-2023]
19. "ResNet and ResNetV2," Keras.io. [Online]. Available: https://keras.io/api/applications/resnet/. [Accessed: 06-Feb-2023]
20. "Papers with code - ImageNet dataset," Paperswithcode.com. [Online]. Available: https://paperswithcode.com/dataset/imagenet. [Accessed: 06-Feb-2023]

Facial Expression Recognition Using Convolution Neural Network

Abaid Ullah(✉)

MSCS-S19-006, Superior University Lahore, Lahore, Pakistan
md.arif@superior.edu.pk

Abstract. The present research focuses on the facial expression of different peoples by using Convolution Neural Network, CNN, Communication is basic need of human. Many existing researches show that fifty to ninety percent of communication is nonverbal. In future the advanced generation of computing like as pervasive computing and artificial intelligence required central multicultural human communication system close to the nature of human. In human computer interaction (HCI) nonverbal communication has too much importance. There are many methods and techniques that are used to recognize the facial expressions and some genetic facial expressions are found in every person and all the different facial expression have their own meanings and people from different culture have their own way to express. These expressions are sadness, fear, happiness, surprise, anger and neutral. So, it is very difficult to recognize different facial expression of the peoples belongs to different culture so in this research work we proposed a technique to recognize facial expression-based CNN. For this we use two different datasets one is JAFFE that is stand for (Japanese facial expressions) and second is TFEID that is stand for (Taiwanese facial expression image database) To recognize facial expression we use CNN and extract common facial features and on basis of similarity measure get unique and common feature then remove common feature to minimize use of memory and use only unique feature to measure the similarity, we detect facial expression accurately with unique expression features. Our proposed methodology identifies the expressions with less memory usage, less time complexity and more accuracy than the existing techniques. By using this technique, we can solve real life problems with better way and detect cross cultural facial expression successfully.

Keywords: CNN · artificial intelligence · multicultural · HCI · expression · JAFFE · TFEID · common feature · unique feature

1 Introduction

Human body is consisting of many parts that are used to identify the person and we can also understand many of the information from the specific movements of different parts of body. The part of body that is used as most expressive index is our face. Many of the things that are in our mind are present by our face expressions. Our face is the most expressive part of our body. It is commonly used as a symbol of mind situation.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 308–321, 2025.
https://doi.org/10.1007/978-3-031-77620-5_23

The expressions of our face displayed the emotions and feelings that are perform in our mind. Feeling and expressions are very important in our daily life. The facial is providing a great service that is the requirement of a very significant social function. Thesis's social function make best way to function a social communication and information exchange very effectively. Facial expression is a fundamental and basic function of our society without it we cannot properly play our role in our life. Not only human even then other creations are using facial expression for communication purpose. According to Rechael E. Jack. expressions of face are the important source of fascination and empirical exploration in between different philosophers, psychologist and biologist from many of the centuries for serving the function of fundamental functions of human society [1].

In the late twentieth century, Paul Ekman and his colleagues took up this idea. Paul Ekman revealed evidence that some facial expressions are common and these general facial expressions are related to each other particular emotions such as pleasure, fury, fear, surprise, grief, disgust, and contempt.

He also looked into the roots of cultural differences, observing that environmental influences were to blame for many of the apparent disparities in facial expression between cultures [4].

Anger, disdain, disgust, fear, joy, grief, and surprise are among universal facial expressions that have good support (Fig. 1).

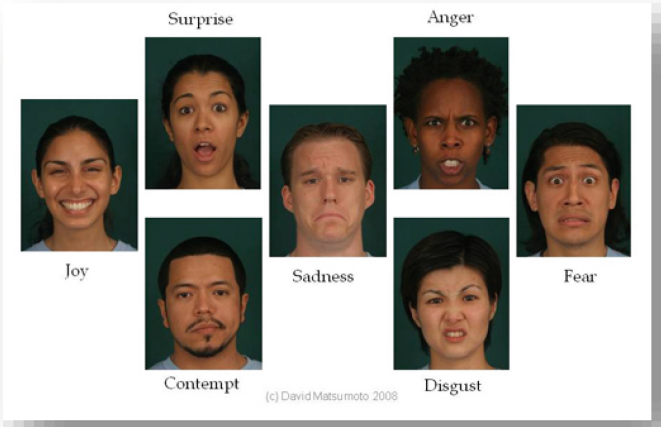


Fig. 1. Basic Emotions. [4]

Basic Emotions: Six or Seven?

Paul Ekman named six at first, but then added 'contempt' to the list. Rage, disgust, fear, joy, sadness, surprise, and disdain are some of the most basic expressions. He also looks at the origins of cultural differences, noting that there are a variety of apparent

differences in facial expression between cultures. Different macular activity patterns correspond to the primary expressions. People's facial emotions tend to mimic their verbal responses, according to research. According to an Ekman exhibit that exhibited a succession of photos showing the six basic emotions to individuals from many different nations, participants from a range of Western, Asian, and indigenous cultures were extremely accurate in recognizing these fundamental yet diverse emotions.

When we make a facial expression, we are communicating basic feelings of muscle activity (Table 1).

Table 1. Model of six universal emotions [14]

EXPRESSION	MOTION CUES	PSEUDO-MUSCLES USED
Happiness	raising and lowering of mouth corners	6 linear muscles
Sadness	lowering of mouth corners raise inner portion of brows	6 linear muscles
Surprise	brows arch eyes open wide to expose more white jaw drops slightly	3 linear muscles
Fear	brows raised eyes open mouth opens slightly	5 linear muscles 1 sphincter for the mouth
Disgust	upper lip is raised nose bridge is wrinkled cheeks raised	6 linear muscles
Anger	brows lowered lips pressed firmly eyes bulging	4 linear muscles 1 sphincter for the mouth

The fields of image processing, machine learning. And other sample identification, face expression has long been a difficult topic to solve. In a human computer assisted interaction scenario, it is critical for recording the internal emotion state.

Because facial expression categorization is so important, a lot of work has gone into establishing accurate systems. Although several machine learning algorithms for identifying culture-specific facial expressions have been created [4–7], no viable technique for recognizing multicultural facial expressions has been established [8, 9]. Smart meetings, social robots, surveillance of visual and conferencing videos are examples of applications in real-world facial expression of cross-cultural recognition. The reason for this is because as a result of differences in traits, the face structure fluctuates excessively.

This diversity is the reason of; current classification of facial expression systems is capable of recognizing culturally distinct facial expressions. As a result, more research into multicultural facial expression recognition algorithms is necessary. The aim of this research is to develop a fusion strategy based on neural networks to detect differences in the representation of facial expressions cross cultures. Identifiers must be eligible to distinguish between Japanese, and Taiwanese cultures, as well as Japanese and Taiwanese subjects (Fig. 2).

Fig. 2. Multicultural facial structures. (R1) Moroccan (R 2) Caucasian (R 3) Taiwanese (R 4) Japanese

They devised a one-of-a-kind ANN-based data gathering strategy artificial neural network. The created combined perfect is made up of predictor Meta level and base level, classifiers. A group probability distribution of binary usage (BNNs). With each ANNE representing a possible facial expression. As a result of the binary system, each ANNE can approve or reject the animation of an expression. They say that a strategy they propose is effective independent of cultural, racial, ethnic, or geographic barriers.

2 Problem Statement

The methods for FER are classified broadly into many of categories. The different methods utilize different techniques to recognize the facial expressions. Each existing method has some limits and draw backs there is a problem to identify the limitation and drawbacks. It is found that if a method improve accuracy it has to compromise about complexity on the other hand if reduce the complexity the accuracy has to be compromise. There is a need to introduce a combined technique that improves the facial expression recognition with Maximum accuracy and Minimum complexity. In this research I introduce a light weight Method with less complexity and maximum accuracy.

3 Research Questions

- How to make a lightweight classifier for facial expression recognition?
- How to improve the accuracy?
- How to reduce the complexity?

4 Literature Review

To combine approach's main goal is to assemble a series of classifiers that all categories the same starting class. Rather of utilizing just one classifier, the greatest global classifier with the most accurate and trustworthy conclusions is built by merging the results of many classifiers. The simplification error is reduced by combining the provisions of several classifiers, according to machine learning testing. Bagging, boosting, and stacking are the most frequent methods for generating connected s. The goal of combining classifiers is to minimize the number of classifiers in the mix as well as the expression recognition error classifier. The optimization problem of selecting the optimum Optimization problem is to select the optimal number of classifiers from a set of classifiers while maintaining classifier accuracy [1].

The topic of facial expression recognition across cultures was commonly ignored until near the beginning 2009. The problem of recognizing global facial expressions identification has gotten little attention since universal facial expression datasets are rarely employed. Matsumoto et al. [1] the facial expressions of American, Japanese, and British students have been used to study cross-cultural emotions.

Across cultures, each word had the same signal clarity.

Using machine learning, Dailey et al. [2] built a method for recognizing cross-cultural face expressions. The researchers came to the conclusion that even little differences in multicultural facial photos can have an impact on classifier performance. A similar experiment was carried out by Da Silva and Pedrina [3]. Six fundamental facial expressions, according to the authors, are natural and universal, with slight differences. By integrating four separate benchmark databases, the scientists were able to create a multicultural dataset.

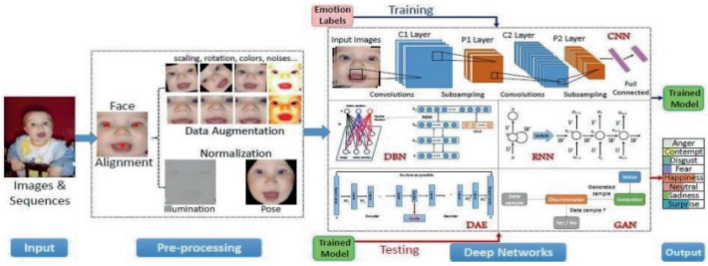
The proposed technique failed to identify an optimal mix of characteristics and classifiers for efficiently identifying multicultural face expressions. Zia and Jaffar [4] also suggested an unique incremental learning strategy for properly understanding multicultural face expressions. The recommended incremental learning approach allows the predictor to gradually understand the cultural variance. Four separate facial expression databases were gradually used to train the classifiers.

To assess the performance of trained models, the Assess facial expression database was employed. It was created by combining the images of a large number of female actors from various sources. The solution performed better the latest technology by a wide margin. The approaches for recognizing multicultural facial expressions mentioned in [5–7] encourage generate a diverse database of cross-cultural facial expressions, as well as more highly developed predictions algorithms capable of accurately recognizing multicultural facial expressions.

The deep fusion CNN is described as a method for combining two-dimensional and three-dimensional face expression detection into a single model. The first extracted type of texture among the six categories of two-dimensional face expression characteristics is maps, geometry, curvature, texture, and normal components.

He developed a high-speed Boltzmann machine for analyzing multimodal coordinates and offered teaching propagation strategies to handle morphology with a hidden-related statement. Simultaneous FER activation, such as facial suspension and AU face identification, has been reported to increase Facial Expression Recognition performance

[7]. Rather from the intrusive Facial Expression Recognition, [8] proposed a face-based GAN structure in which the originator stacks photos while maintaining identification and display properties, then distinguishes the original photographs from previously produced facial images.



To ease this issue, they influence both real and context-oriented provisions, as a component of a more extensive feeling acknowledgment structure. They decided to use the standard CNN-RNN curriculum as the basis for our proposed cluster-to-order learning model (seq2seq). In addition to learning via the RGB input method, they generate an auditory stream that synthesizes the removed post-spectral programs. Our extensive testing on the challenging, recently collected AFF-Wild2 dataset validates our intuitive multi-stream, multi-module approach to "in nature". The emphasis is on the valuable effects of the human body and visual scenery, with parts of the sensory detection scale still being left out to some extent. [11].

In this paper they propose an original profound learning system named spatial-transient intermittent neural organization (STRNN) to bring together the learning of two diverse sign sources into a spatial-transient reliance model. In STRNN, to catch those spatially co-occur rent varieties of human feelings, a multi-directional re-current neural organization (RNN) layer is utilized to catch long range context-oriented signs by crossing the spatial locale of each time cut from various points. Then, at that point, a bi-directional fleeting RNN layer is additionally used to learn discriminative fleeting conditions from the groupings connecting spatial elements of each time cuts created from the spatial RNN layer.[12]

5 Data Collection and Methodology

Data collection
Our objective is to create a system that can identify seven facial expression of cross cultures such as:

Expressions

(1) Sad
(2) Happiness
(3) Anger
(4) Fear
(5) Natural

(6) Contempt
(7) Surprise

Cultures
The two cultures that I used to create this system are:

(1) Japanese
(2) Taiwanese

Facial Expression Databases
Participants in the cross-cultural database taking from the given below cultures, ethics and graphic regions:

1. JAFFE that is stand for (Japanese female facial expressions).
2. TFEID that is stand for (Taiwanese facial expression image database)

Methodology

Step 1

Select the two databases " JAFFE that is stand for (Japanese female facial expressions) " and "TFEID that is stand for (Taiwanese facial expression image database)".

Step 2

1. Extract the common feature (CF) between both of the selected databases ("JAFFE that is stand for (Japanese female facial expressions)." and "TFEID that is stand for (Taiwanese facial expression image database)") by using intersection of both data bases.

$$\mathrm{CF} = (\mathrm{JAFFE}) \cap (\mathrm{TFEID})$$

Step 3.

Extract the unique feature of the selected "Japanese Female Facial Expression (JAFFE)") by using complement of CF features in JAFFE. Unique feature in Japanese database "UJ"

$$\mathrm{UFJ} = \mathrm{CF}^{\mathrm{C}} = (\mathrm{JAFFE}) - \mathrm{CF}$$

Step 4.

Extract the unique feature of the selected "TFEID that is stand for (Taiwanese facial expression image database)" by using complement of CF features in TFEID. Unique feature in Taiwanese database "UT"

$$\mathrm{UFT} = \mathrm{CF}^{\mathrm{C}} = (\mathrm{TFEID}) - \mathrm{CF}$$

Step 5.

Extract the common feature of the seven universal expressions of selected "Japanese Female Facial Expression (JAFFE)") by using interaction of the features of all seven expression in JAFFE for Japanese culture identifier JCI.

$$\text{JCI} = (\text{j.Sad}) \cap (\text{j.Happy}) \cap (\text{j.Anger}) \cap (\text{j.Fear}) \cap (\text{j.Natural}) \cap (\text{j.Contempt}) \cap (\text{j.Surprise})$$

Step 6.

Extract the common feature of all the seven expression by the selecting "TFEID that is stand for (Taiwanese facial expression image database)" by using the intersection of the common features in TFEID for Taiwanese cultural identifier TCI.

$$\text{TCI} = (\text{t.Sad}) \cap (\text{t.Happy}) \cap (\text{t.Anger}) \cap (\text{t.Fear}) \cap (\text{t.Natural}) \cap (\text{t.Contempt}) \cap (\text{t.Surprise})$$

Step 7.

1. Take an input image
2. Detect and crop the face
3. Extract expression feature
4. Find the value of the correspondence scale with JCI (SJCI).
5. Find the value of the correspondence scale with TCI (STCI).

Step 8.

Compare both the value of similarity measure with JCI (SJCI) and the value of similarity measure with TCI (STCI) to find the maximum similarity.

$$\begin{aligned}&\text{if (SJCI} < \textit{STCI})\\&\{\text{RC} = \text{The culture is Taiwanies}\}\\&\text{else}\\&\{\text{RC} = \text{the culture is Japanies}\}\end{aligned}$$

Step 9.

Find the value of similarity measure with UFJ (SUFJ) and value of similarity measure with UFT (SUFT). And find the greater value to finalize the culture (Figs. 3 and 4).

$$\begin{aligned}&\text{if (SUFJ} < \textit{SUFT})\\&\{\text{FRC} = \text{The culture is Taiwanies}\}\\&\text{else}\\&\{\text{FRC} = \text{the culture is Japanies}\}\end{aligned}$$

Step 10.

After identifying the culture use the same database against the identified culture and then apply the complete process to recognize the facial expression.

```
if (FRC = T)
{Identify  facial expression using TFEID}
else
{Identify facial expression using JAFFE}
```

6 Results

It also shows that the proposed structure works well when the classifier is trained and evaluated using images of faces of the people living in different regions/continents of the world. This uniformity in the correctness of detection of expression again supports simplification of artificial neural network evaluation (A.N.N.E.) assemblies. Crowd detection also allows people to effectively identify the emotions of strangers, which is an interesting additional factor (Fig. 5).

It implies that differences in face appearance have no impact on people' capacity to correctly categories facial emotions. The results in Table 5 back up these claims that the suggested method performs better on unknown samples. When the classifier is taught and evaluated on the photos of faces from different civilizations, facial expression recognition accuracy is a remarkable 50%, however, the classification accuracy ranges from 80% as shown in Table 5. It is high, which indicates the accuracy of the ANNE clusters. These results show that the ANNC ensemble works without fail no matter meanwhile images of a face from different civilizations/cultures are used to train or test purpose.

In accordance of the research offered in table number six, when face photos from one civilization/culture are used to train classifier, face images from other cultures are used to test the classifier. All through BNN training, we found that different is a set of parameters needed when using diverse sets of data.

We found that exercise a binarized neural network (B.N.N.) requires different sets of parameters when using different datasets to train similar classifier. Because facial databases are inherently variable, it is difficult for a classifier to know inherited variation across different databases. As a result, strategies for understanding ethnic differences and detecting multicultural facial expressions must be created. This research looked at the impact.

By focusing on the focus area of expression, the influence of cultural differences is minimized. Furthermore, the use of several binarized neural network (B.N.Ns.) in the bottom layer reduces the impact of differences in the representation of face expressions and then face composition. Performance Assessment with Verification.

Here is 10 folds of cross validation are used for the purpose of generalize performance of suggested merge process. With 300 ANNCs trained using principle components

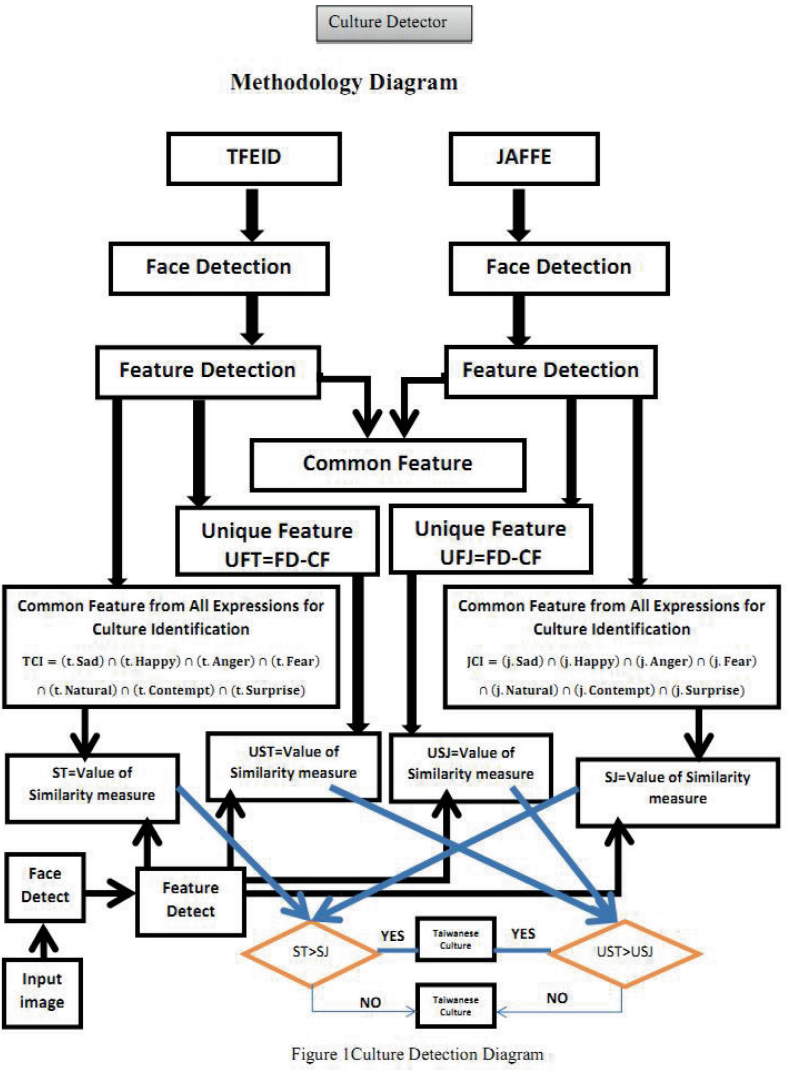


Figure 1Culture Detection Diagram

Fig. 3. Culture Detection Diagram

analysis (PCA) and (NB) prediction feature vectors, we got an average expression recognition correctness/accuracy that was 89.31% using 10-fold cross-validation. Varying the training and testing sets, these results show that the proposed approach is generalizable. Table of precisions of current methods when images of faces were used from diverse civilizations/cultures for training and test binary neural networks.

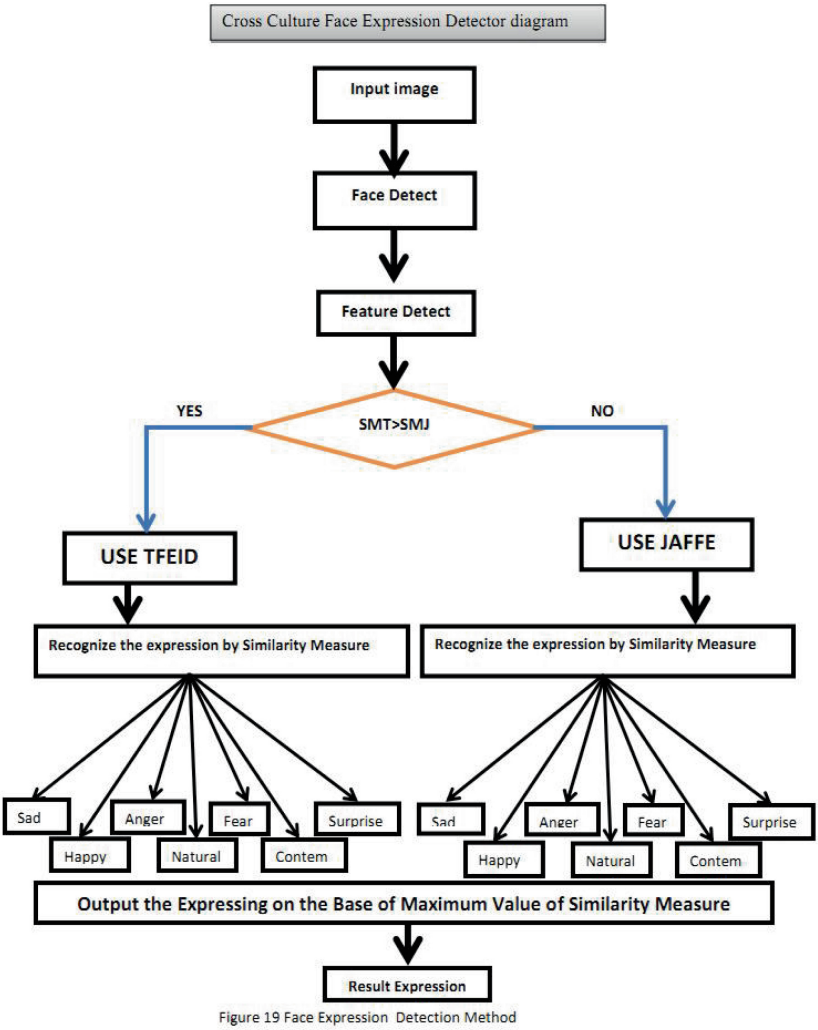


Fig. 4. Face Expression Detecion Method

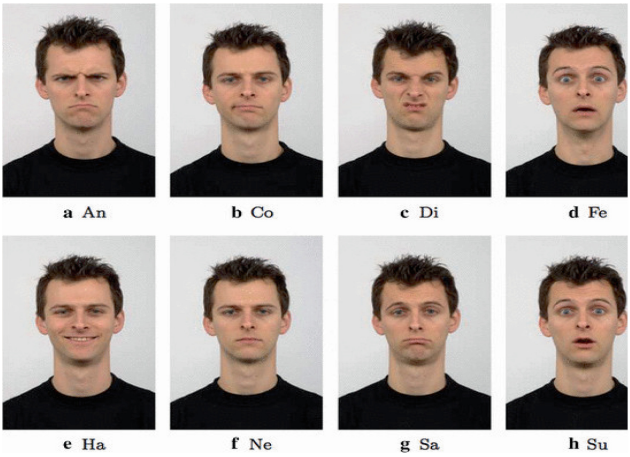
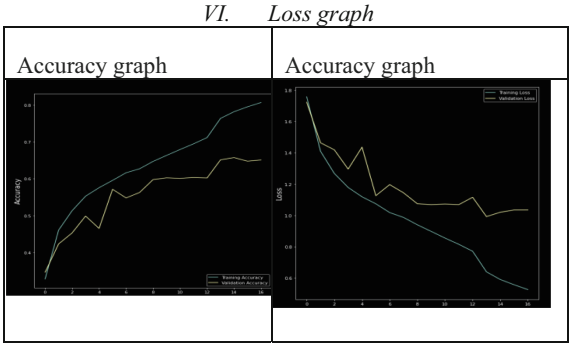


Fig. 5. Samples

7 Loss Graph



The lack of a positive link between two expressions is seen in Fig. 11. The pairs of facial expressions sadness & anger and fear & surprise have modest negative values of correlation, indicating that the facial expressions are equivalent pair. This factor means that some groups of facial expressions are more alike than others. It means that both sets of expressions share the same facial features. However, by examining the many diverse combinations of facial expressions, a new relationship may emerge.

Similarly, the melancholy and surprise combo bear a stronger connection to other emotion combinations. Correlation coefficients are used to compare two sentences to see how similar or dissimilar they are. Which of the following emotions have the least in common with fury and surprise? We may claim that the facial structures of these two expressions are similar, rendering the classifier incapable of distinguishing between them. Similarly, happiness & surprise, anger & surprise, sadness & surprise, and fear & anger emotion pairs had less similarity than other facial expression pairs.

8 Conclusions

Two major concerns are addressed by the facial expression recognition system: 1) inter-expression similarity, 2diversity in face structure. Face recognition differs widely between different peoples as a result of these challenges. A CNN with OpenC Vface expression database is being created to address the issue of intercultural variance and to demonstrate Expression variety. The proposed methodology assures the less use of memory than existing previous methodology and find the results is less amount of time. Classifiers can better detect facial expressions and learn about variants in expression demonstration by focusing on manifestation attentiveness components like eyes, nose and lips. A database is used to train a pool of binary classifiers to detect expression representation variances. For the same text, binary classifier be trained cultural contrast. When there are several expressions, it also learns the difference between expressions. This diverse FER system has been proposed and developed in this thesis by using specific techniques of image processing and machine learning by combining the different data bases I will introduce an efficient face expressions recognizer.

9 Future Work

By using facial expression recognition, a lie detector can introduce, a silent secrete feedback conducting device can invent.

References

1. Ekman, P., Sorenson, E.R., Friesen, W.V.: Pan-cultural elements in facial displays of emotion. Science **164**(3875), 86–88 (1969)
2. Ekman, P., Friesen, W.V.: 'Constants across cultures in the face andemotion. J. Personality Soc. Psychol. **17**(2), 124 (1971)
3. Ekman, P.: Universals and cultural differences in facial expressions of emotion. Nebraska Symp. Motivat. **19**(1), 207–283 (1971)
4. Wang, Z., Xiao, N.: Using MD-Adaboost to enhance classifier of facial expression recognition. J. Comput. Inf. Syst. **9**(3), 923–932 (2013)
5. Levi, G., Hassner, T.: Emotion recognition in the wild via convolutional neural networks and mapped binary patterns. In: Proceedings of the ACM International Conference Multimodal Interaction ICMI, pp. 503–510 (2015)
6. da Silva, F.A.M., Pedrini, H.: Effects of cultural characteristics on building an emotion classifier through facial expression analysis. J. Electron. Imaging **24**(2), 023015 (2015)
7. Zia, M.S., Jaffar, M.A.: 'Cross-cultural emotion classification based on incremental learning and LBP-features.' Appl. Math. Inf. Sci. **9**(5), 2651–2656 (2015)
8. Moeslund, T., Hilton, A., Krüger, V., Sigal, L. (eds.): Visual Analysis of Humans: Looking at People. Springer London, London (2011). https://doi.org/10.1007/978-0-85729-997-0
9. Minaei-Bidgoli, B., Kortemeyer, G., Punch, W.: Optimizing classification combineds via a genetic algorithm for a web-based educational system. In: Proceedings of the International Workshop Syntactical Structural Pattern Recognition Statistic Pattern Recognition, Berlin, Germany, pp. 397–406 (2004)
10. Altinçay, H.: Optimal resampling and classifier prototype selection in classifier ensembles using genetic algorithms. Pattern Anal. Applic. **7**(3), 285–295 (2004)

11. Minaee, S., Minaei, M., Abdolrashidi, A.: Deep-emotion: facial expression recognition using attentional convolutional network. Sensors **21**(9), 3046 (2021)
12. Kumar, S., Bhuyan, M.K., Iwahori, Y.: Multi-level uncorrelated discriminative shared Gaussian process for multi-view facial expression recognition. Vis. Comput. **37**(1), 143–159 (2021)

Distinguishing Parkinsons Disease and Essential Tremors by Using Machine Learning

Muhammad Hassan(✉), Uzair Saeed, and Majid Hussain

Department of Computer Science, The University of Faisalabad, Faisalabad 38000, Pakistan
hxnzahid@gmail.com, uzair.saeed@tuf.edu.pk

Abstract. PD and ET are neurodegenerative diseases with motor signs, including tremors, making diagnosis difficult. This work uses machine learning to establish an automated method to identify PD and ET by analysing the various traits and patterns that characterise the two conditions. Demographic, medical, and sensor-based motor characteristics are collected to achieve this. These datasets train machine learning models such as SVM, RF, and ANN to learn the complex correlations and patterns of PD and ET. Identifying the most distinguishable traits of PD and ET requires feature engineering. The statistical, time-based, and spectral properties of the motor symptoms of PD and ET are extracted from the data. The features are selected using rigorous methods. Cross-validation measures accuracy, sensitivity, specificity, and AUC-ROC to evaluate machine learning models. Comparative investigations show machine learning algorithms' strengths and weaknesses in identifying PD from ET. This research is of great therapeutic importance, as an automated and reliable diagnostic tool can help clinicians make accurate and rapid diagnoses. Identifying PD and ET early improves patient care and management. Machine learning models also enable additional data sources and refinement of diagnostic algorithms. Machine learning can identify Parkinson's disease from Essential Tremor. This research develops an automatic and reliable diagnostic tool using large data sets and powerful machine learning methods. The findings help to distinguish PD from ET, improving clinical outcomes.

Keywords: Parkinson's Disease · Essential Tremors · image processing · Machine learning

1 Introduction

The brain is the centre of control of the body and as such is vital to the health of all other organs of the body. Therefore, any damage to this extremely fragile organ might have severe consequences. One such neurological ailment that profoundly affects the brain and causes a variety of symptoms of deterioration is Parkinson's disease (PD). According to the work of Pereira et al. (2017), PD can be defined as a neurodegenerative disorder that causes long-term brain cell death in affected areas.

PD symptoms are similar to those of other disorders, such as ageing and essential tremor, especially in the early stages of each disease (Samii et al.) Therefore, it is crucial

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 322–329, 2025.
https://doi.org/10.1007/978-3-031-77620-5_24

to correctly diagnose PD so that people can get the care they need. Differentiating PD from other neurological disorders can be difficult and often requires the use of sophisticated diagnostic tools.

Disease symptom detection is an area where mathematics, and more specifically deep learning (DL) mathematical models, have shown great promise as tools (Pereira et al., 2018). Imaging and time series datasets are only two examples of the kinds of data that might benefit from DL approaches, which can include specialised neural network design. For example, magnetic resonance imaging and PET scans provide visual representations of the brain structure that can be used in imaging databases. Time series datasets, on the other hand, are made up of lists of data points that are organised by date, and thus capture the dynamic nature of illness development.

Given deep learning's recent triumphs across several areas, it is crucial to investigate its potential use in PD diagnosis. Researchers are putting the capacity of DL models to understand the intricate patterns and correlations of the data set to good use by researchers to improve diagnosis and classification. Using deep learning techniques on suitable data sets has the potential to greatly advance our knowledge of PD and the precision of its diagnosis.

Given the rapid progress made in the area, it is imperative that we examine the use of deep learning methods for the diagnosis of PD. To further understand how DL models might differentiate PD from other disorders, this study analyses and interprets imaging and time series information. The results have important implications for the development of better diagnostic tools, the promotion of earlier interventions, and the customisation of treatment plans for people with PD.

Any impairment in the brain, such as that caused by Parkinson's disease (PD), can have a negative impact on an individual's general health because of the complex interplay that exists between the brain and the other organs in the body. Differentiating PD from other disorders is essential to receive the correct therapy. An accurate diagnosis of symptoms may be possible with the use of mathematical models and deep learning in particular. This study intends to add to the expanding body of information and maybe change the area of PD diagnosis by exploring the application of deep learning techniques, especially in the setting of PD.

2 Literature Review

2.1 Parkinson's Disease

Parkinson's disease (PD) is a progressive neurodegenerative disease that is defined by the destruction of dopamine-producing cells in the area of the substantia nigra pars compacta of the brain. Symptoms of PD include tremors, stiffness, and slow movement. According to Vallejo et al., lack of dopamine can cause motor symptoms such as resting tremor, stiffness, bradykinesia, and postural instability. About 10 million people worldwide have been diagnosed with PD and one million people in the United States have PD (Parkinson's Disease Foundation). PD is more common in nations with an ageing population.

2.1.1 Characteristics of Parkinson's Disease

Nonmotor symptoms, such as cognitive impairment, can also be a part of PD. Motor symptoms, such as resting tremor, cogwheel stiffness, bradykinesia, and postural instability, are among the most defining characteristics of Parkinson's disease. The usual frequency of resting tremor in patients with PD is between 3 and 5 hertz (Hz) (Samii et al., 2004). When joints suffer resistance, known as cogwheel stiffness, the result is jerky motion rather than fluid motion (Khan Academy, 2015). Bradykinesia is a condition characterised by a slowdown in voluntary movement (Samii et al., 2004; Khan Academy, 2015), most noticeably in fine motor activities such as handwriting. Later stages of the disease are characterised by postural instability, which in turn causes imbalance (Samii et al., 2004).

Some of the nonmotor symptoms of PD might appear years before motor symptoms. Hyposmia (decreased ability to smell), REM sleep behaviour disorder, constipation, and depression are all linked to sleep deprivation (Meireles et al., 2020). Patients with PD also show cognitive deterioration, which can range from mild cognitive impairment (PD-MCI) to dementia (PDD). Unlike PDD, which is characterised by more severe cognitive impairments such as memory loss, executive dysfunction, attention loss, and behavioural and neuropsychiatric symptoms, PD-MCI describes atypical thinking and memory problems that do not significantly disrupt daily activities (Fig. 1).

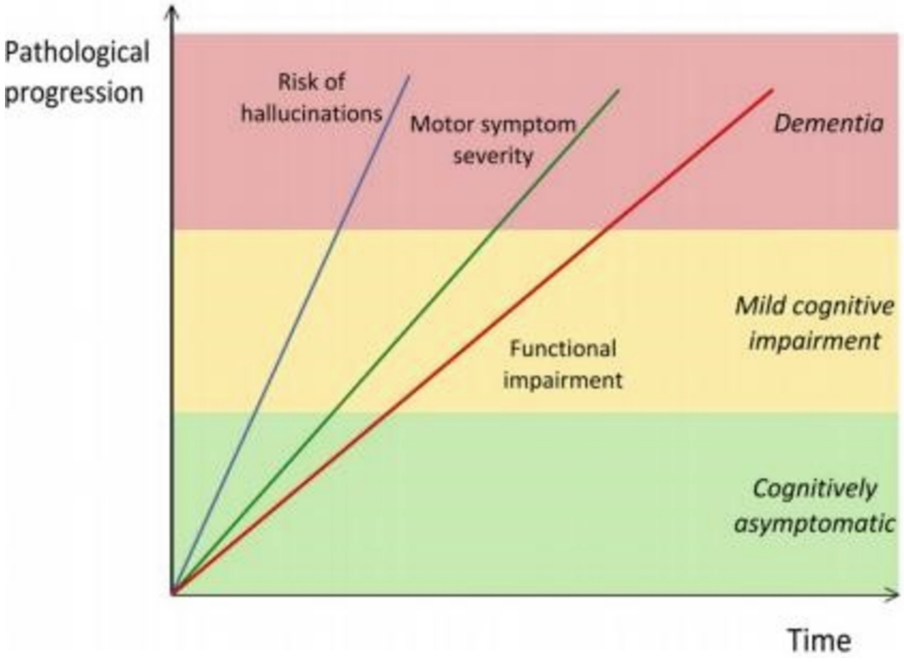


Fig. 1. Progression of Parkinson's disease symptoms

2.1.2 Methods for Parkinson's Disease

It may be difficult to distinguish PD from other types of parkinsonism that have similar symptoms. Parkinsonism is a group of symptoms that includes tremors, stiffness, and bradykinesia (Parkinson's Disease Foundation, 2015). These symptoms can have other origins, such as vascular abnormalities or other neurodegenerative diseases. Non-motor symptoms related to PD, which can arise before motor symptoms and do not respond to levodopa therapy, suggest that a diagnosis based solely on motor criteria may not be adequate.

Diagnostic precision has been improved by including factors such as asymmetry and a strong response to levodopa therapy. The diagnostic criteria developed by the UK Parkinson's Disease Society Brain Bank aim to improve PD diagnosis by overcoming these obstacles. The diagnostic specificity of the revised criteria has been proven in studies to be between 76% and 90% (Berg et al., 2021).

It is essential for diagnosis and treatment to know how symptoms of PD symptoms develop over time. Postural instability often occurs in the later stages of the disease, while motor characteristics are typically visible during the early stages (Kalia et al., 2015). Parkinson's disease is a multifaceted neurodegenerative condition characterised by a wide range of motor and non-motor symptoms.

3 Datasets

As part of the data collection procedure, participants use a smart pen and a tablet measuring 20.3 by 32.5 centimetres to replicate a cube and a spiral pentagon. Time, position (in x and y coordinates), angle of the pen (in x and y planes), and force applied to the pen were recorded as the drawing progressed.

The characteristics of the data sets are shown in Table 1 below, with a representative subset of rows displayed.

Table 1. Time-series dataset example

Timestamp	x coordinate	y coordinate	pen angle in x plane	pen angle in y plane	pressure
0	0.600615155	0.579739793	0.675101995	−495138138	0.052785925567
8	0.600688906	0.579739793	0.675101995	−495138138	0.075268819928
9	0.60078741	0.579739793	0.669257224	−505829692	0.092864125967
24	0.600910441	0.579739793	0.669257224	−0.505829692	0.120234601199

The coordinates and pressure values are all within the range [0, 1], as seen in the table above. The time stamp is an integer that begins at 0, while the angles of the pen are represented in the range [−1, 1]. In particular, if the pressure reading is 0, the pen was not touching the paper.

4 Methodology

In this chapter, we will walk you through every step of our method, from gathering raw data to analysing the final output.

4.1 Pre-processing of Data

The relevance of data pre-processing in machine learning cannot be overstated. Data cleaning, for example, involves identifying and dealing with NULL values (empty values) and noise as part of this critical stage. Furthermore, unfavourable characteristics of the dataset might be removed by pre-processing. There is a correlation between the use of data preprocessing and improved machine learning performance (Kotsiantis et al., 2016).

4.1.1 Data Wrangling (or Preparation)

Preparing data for use as input in machine learning algorithms such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) involves transforming the data into a suitable format for these networks. It is not uncommon for various algorithms to have varying input format requirements (Endel et al., 2021).

4.1.2 Input/Output: Image Processing

To increase the number of samples in a dataset, image processing may be used to produce new pictures from an existing set of photos. The modified photographs are duplicates of the originals that have been randomly rotated, shifted horizontally and vertically, zoomed in or out by a given amount, or flipped horizontally. By reducing the likelihood that the model would be overfit, augmentation can help prevent overfitting; by expanding the training set, it can help increase classification accuracy (Ahmad et al., 2017).

We improve our model's resilience and generalisation capabilities through the use of various image processing techniques so that it may learn more efficiently from the data at hand.

5 Experimental Results

The experimental findings from our model evaluation are presented below. To gain insight into the learning process, we examine the consistency of the validation error and accuracy over time.

5.1 Error and Precision of Plot Validation Across Time

In this graph, we contrast the training process depicted in the previous plot with the validation process, depicted here. This figure is used to track how well the model performs on data that it has never seen before. A single fold of an experiment using Recurrent Neural Networks (RNNs) in the pentagon data set is shown in Fig. 2-right.

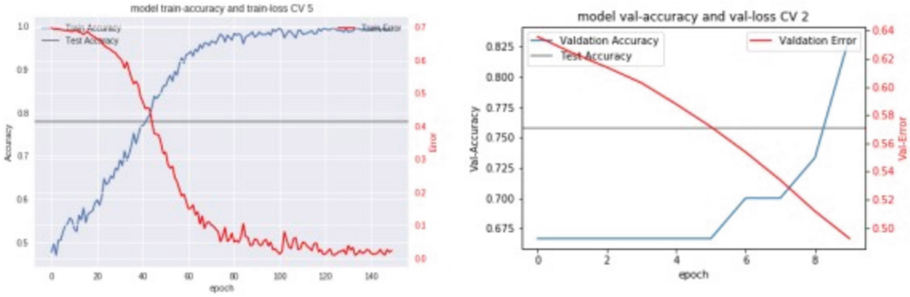


Fig. 2. Depicts the relationship between epochs and accuracy and error in model training (left) and model validation (right).

Each fold in every trial is plotted individually so that we can evaluate the model's performance and settle on the best training set size. Overfitting occurs when the number of epochs used in training is increased beyond a certain threshold, while underfitting occurs when the number of epochs is decreased below that threshold. These plots help us find the sweet spot that guarantees efficient model training.

5.2 Accuracy Progressions Showing Precision and Recall

Figure 2 also illustrates some sample precision recall curves together with mean precision (AP) values. Insights into the model's versatility can be gleaned from these curves, which represent the trade-off between precision and recall for various classification levels.

These visual representations are critical for our study because they help us understand the findings and make choices about how long to train the model and how best to optimise its performance.

5.3 A Process for Categorising Time Series

The purpose of the workflow depicted in Fig. 3 is to utilise RNN on our time series datasets to distinguish between the PD class and the healthy class. Beginning with the raw data and ending with analysis and evaluation, this workflow will be broken down into its component parts.

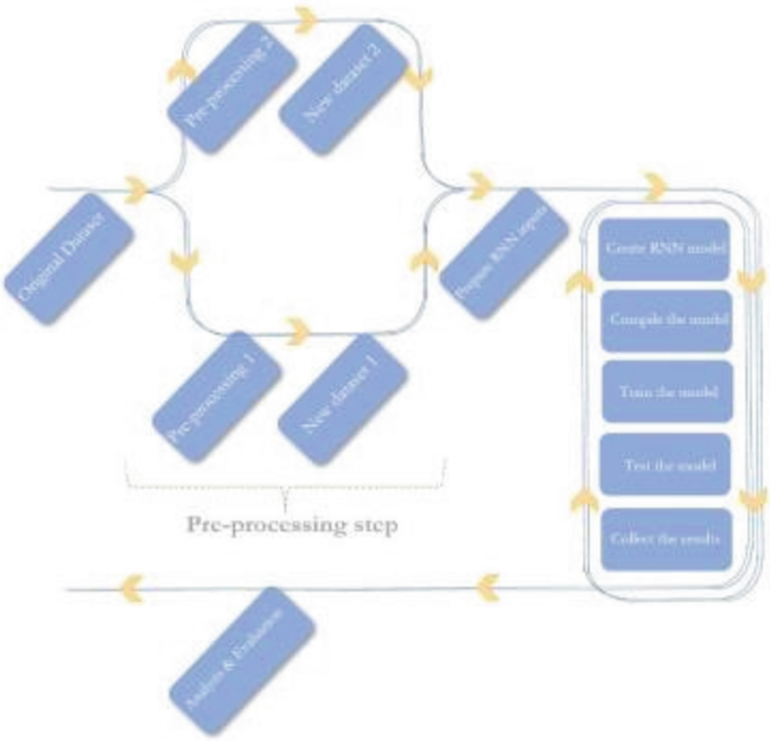


Fig. 3. Flow chart for RNN-based experiments

6 Conclusion

We investigate the identification of Parkinson's disease using deep learning. Our study applied Recurrent Neural Networks (RNN) and Convolutional Neural Networks (CNN) to Cube and Pentagon PD datasets. These data sets included time series and pictures. Our experimental procedures were carefully built to evaluate these deep learning models on multiple modified data sets to find the best deep learning approach, dataset, and type of data set. The workflows included data processing, classification, crossvalidation for the collection of results, statistical analysis of the performance of the experiment, and model evaluation based on promising results. Deep learning systems classify motor signals and pictures. The results also show that harder exams are better at identifying sick people from healthy people.

References

Samii, A., Nutt, J.G., Ransom, B.R.: Parkinson's disease. Lancet **363**, 1783–1793 (2004)

Pereira, C.R., Weber, SA, Hook, C., Rosa, G.H., Papa, J.P.: Deep learning aided parkinson's disease diagnosis from handwritten dynamics. In: Graphics, Patterns and Images (SIBGRAPI), 2018 29th SIBGRAPI Conference on, pp. 340–346. IEEE (2018)

Pereira, C.R., Pereira, D.R., Papa, J.P., Rosa, G.H., Yang, X.-S.: Convolutional neural networks applied for parkinson's disease identification. In: Holzinger, A. (ed.) Machine Learning for Health Informatics, pp. 377–390. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-50478-0_19

Vallejo, M., Jamieson, S., Cosgrove, J., Smith, S.L., Lones, M.A., Alty, J.E., Corne, D.W. Exploring diagnostic models of Parkinson's disease with multiobjective regression. In: Computational Intelligence (SSCI), 2016 IEEE Symposium Series on, pp. 1–8. IEEE (2016)

Pereira, C.R., Pereira, D.R., da Silva, F.A., Hook, C., Weber, S.A., Pereira, L.A., Papa, J.P.: A step towards the automated diagnosis of parkinson's disease: analyzing handwriting movements. In: Computer-Based Medical Systems (CBMS), 2015 IEEE 28th International Symposium on, pp. 171–176. IEEE (2015)

Khan Academy Movement signs and symptoms of Parkinson's disease | NCLEX-RN | Khan Academy (2015). https://www.youtube.com/watch?v=4qdD4Ny34cc. Accessed 07 May 2023

Meireles, J., Massano, J.: Cognitive impairment and dementia in Parkinson's disease: clinical features, diagnosis, and management. Front. Neurol. **3**, 88 (2020)

Berg, D., et al.: Changing the research criteria for the diagnosis of Parkinson's disease: obstacles and opportunities. Lancet Neurol. **12**(5), 514–524 (2021)

Kotsiantis, S.B., Kanellopoulos, D., Pintelas, P.E.: Data preprocessing for supervised leaning. Int. J. Comput. Sci. **1**(2), 111–117 (2016)

Endel, F., Piringer, H.: Data Wrangling: making data useful again. IFAC Papers OnLine **48**(1), 111–112 (2021)

Ahmad, J., Muhammad, K., Baik, S.W.: Data augmentation-assisted deep learning of handdrawn partially colored sketches for visual search. PLoS ONE **12**(8), e0183838 (2017). https://doi.org/10.1371/journal.pone.0183838

A Jurisprudence for Pakistan's Digital Forensic Investigation Framework Regarding Cybersecurity

Ehtisham Ul Haque[1] and Waseem Abbasi[2(✉)]

[1] Department of Computer Science, COMSATS University Islamabad, Abbottabad Campus, Islamabad 22200, Pakistan

[2] Department of Computer Science, The University of Lahore, Sargodha Campus, Lahore 40100, Pakistan

Abstract. The increasing prevalence of technology-related crimes has brought attention to cyber forensics worldwide. Its purpose is to identify and preserve digital evidence, extract information, and analyze it to aid in making time-sensitive decisions. However, Digital Forensic Investigations (DFIs) lack a solid framework that provides dependable insight into significant cyber-attack patterns. According to the Global Cyber Security Index (GCI), Pakistan's technological and organizational efforts are lacking, posing a threat to national security. This article focuses on the establishment of a state coordinated DFI framework to address challenges posed by cybercrime. To construct a conceptual model for DFI infrastructure, a policy-based approach and various elements such as legal, technical, organizational, capacity building, and cooperative efforts are employed. This model is organized into pillars to simplify the DFI infrastructure. The main goal of this study is to offer empirical evidence to policymakers in order to develop a comprehensive DFI framework in Pakistan and provide recommendations for enhancing the infrastructure to effectively combat cybercrime.

Keywords: cyber landscape · cybersecurity · digital forensics · digital investigation · incident response

1 Introduction

Technology driven services, especially cloud-based storage solutions have gained immense popularity over time, majorly because they offer a secure and user-friendly approach. This fact has allowed more people nowadays to get their critical data stored online on open-source platforms like Dropbox, One Drive, Google Drive etc. Some concerns arise with this growth in use since there is always an associated potential risk for a cyber-attack. The result of such a scenario is that sensitive important private data i.e. bank details or credit/debit card information may end up being stolen or interfered with publicly.

One way through which Law enforcement agencies (LEAs) are attempting to control the damage of such breaches is by taking steps to minimize these vulnerabilities and

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 330–338, 2025.
https://doi.org/10.1007/978-3-031-77620-5_25

educating the public about probable risks associated with cybercrime. What's more. The increasing prevalence of anti-forensic methods is proving challenging for investigators engaging in digital forensic investigations. While considering all the different elements which are integral to a comprehensive investigative approach that encompasses preparation, collection, examination, analysis, identification and digital evidence interpretation [1]. Its' important that the current anti forensic techniques do not eventually decay it and critical evidence should be collected ensuring strict adherence to legal guidelines to make it capable of holding up under scrutiny before a judge.

Globally, the increased use of digital platforms for the storage of data in many organizations has led to a rapid rise in cybercrime [2, 3]. To combat cybercrimes, law enforcement and security organizations worldwide have devised various mechanisms. In recent times, there has been a notable increase in the number of studies aimed at organizing and defining the various stages of the digital forensic investigation process. The field of Digital Forensic Investigations (DFIs) encompasses a wide range of intricate tasks, activities, processes, and subdomains [4]. In 2022, there was a significant rise in cybercrime and cyber-attacks due to the advancement of anti-forensic techniques [5]. Perpetrators now only require an internet connection and computer; thus, the widespread availability of free computer software and tools facilitates their exploitation of vulnerabilities. Researchers in this field are actively exploring diverse strategies and tools to enhance the resilience of digital content against unauthorized access and deceptive practices, thereby mitigating the risks posed by cyber-attacks.

Organizations have at their disposal various measures such as procedures, guidelines, policies, baselines, and global practices to impose restrictions on cyberspace misuse. The National Institute of Standards and Technology (NIST) has developed a framework and set of standards that assist organizations in proactively countering potential cyberattacks and evaluating their security structure [6]. These standards and frameworks are frequently revised every three years, with mandatory upgrades for corporations. An effective cyberattack often necessitates the cooperation of several threat actors, and the escalating threat landscape makes data theft a persistent risk that is challenging to prevent. Attackers employ basic attacks as the most convenient means of gaining access to system assets, subsequently leveraging their impact to execute more sophisticated hybrid attacks. In Pakistan, an example of such policies is the Prevention of Electronic Crimes Act (PECA) 2016 [7]. The Government of Pakistan mandates compliance with this act by all residents of Pakistan, including foreign nationals within the country's borders.

The purpose of this article is to perform an in-depth analysis of Pakistan's current cybercrime investigative infrastructure. The research aims to investigate the country's cyber threat landscape and assess the capacity of the existing infrastructure to deal with such attacks. The research will look at many areas of cybercrime investigative infrastructure, such as the legislative framework, available resources, and the obstacles that relevant agencies confront. Nevertheless, it is important to note that the research conducted focuses solely on analyzing the cybercrime investigation infrastructure in Pakistan and does not encompass broader dimensions landscape of the cybersecurity. Factors such as national and domestic level cyber security strategies, policies, and socioeconomic influences that shape the cyber threat landscape are not explored in this study. Furthermore, it should be recognized that the findings and conclusions are specific to the examined country and may not be directly applicable to other regions. It is essential to consider

these limitations as the research heavily relies on publicly available data and literature, thus being constrained by the sources utilized. It is crucial to emphasize that the present body of research on Digital Forensic Investigation (DFI) infrastructure is limited.

By emphasizing the following important factors, this research aims to significantly advance our knowledge:

- In-depth analysis of the infrastructure's challenges, scope, processes, and policies, with a focus on policy, jurisdictional, technical, legal, academic organizational and cooperative ventures.
- The primary objective of this study is to establish an empirical foundation to assist policymakers in formulating a comprehensive framework for cybercrime investigation in Pakistan. Additionally, it provides valuable insights and recommendations to enhance the existing infrastructure and effectively combat cybercrime within the country.
- The study endeavors to develop robust legal actions that can bolster the Digital Forensic Investigation (DFI) framework and align it with internationally recognized global best practices and standards. The study strives to optimize the global effectiveness of digital investigation and publicize responsible utilization of digital technologies.
- This study is designed to address the prevailing deficiencies in the legal structure governing DFI and propose recommendations for its enhancement. By doing so, it aims to contribute to the ongoing initiatives aimed at combating cybercrime in Pakistan.

The study examines different aspects of digital forensic investigations (DFIs) in Pakistan, including regulations, institutional scope, scrutiny and development, procedures and mechanisms, and applied aptitude to deal with e-crime investigations. In order to gather data for this research, primary sources such as administrative papers, previous studies from local and international organizations, reports focusing on cybercrime and digital forensics in Pakistan, as well as demonstrations by governing authorities and publications from the International Telecommunication Union (ITU) have been taken into account.

The paper is organized as follows: Sect. 2 discusses related work; Sect. 3 highlights the current cyber landscape of Pakistan and identifies some key issues in Pakistan for which DFI would be helpful; Sect. 4 introduces the contextual framework and detailed dimensions for an operational DFI in Pakistan; and Sect. 5 concludes the paper.

2 Related Work

In recent years, significant advancements have been made in the development, formalization and standardization of digital forensic procedures and processes [8]. The National Institute of Standards and Technology (NIST) plays a decisive role by providing valuable standards for conducting computer and network forensic investigations within the IT domain [9]. Similarly, the National Criminal Justice Reference Service (NCJRS) [10] provides rules and data on the digital forensic procedures used by law enforcement, such as identifying, gathering, obtaining, and storing digital evidence [11, 12]. Nevertheless, further research in this field is necessary [13]. Digital forensics finds its primary applications in law enforcement and incident response (IR). Incident response entails managing

and addressing incidents within cyber (IT) environments, while digital forensic analysis in law enforcement involves examining digital evidence to determine the occurrence of criminal activity and, if established, attributing responsibility and prosecuting offenders. While both disciplines employ digital forensics in similar ways, this study specifically concentrates on the utilization of digital forensics within law administration.

In developed nations such as the United States and the United Kingdom, the increasing development of technology has led to the establishment of digital forensics investigation (DFI) as a highly respected professional and academic discipline [14]. These countries have established a well-defined infrastructure for conducting digital investigations, encompassing the remote sector, police, and covert services. They have comprehensive legislation addressing computer misuse and widely accepted recommendations for the contribution and handling of digital testimony. In this study, we refer to the collective legislative bodies, educational programs, research documents, procedures, standards, guidelines and baselines as the framework for Digital Forensic Investigations (DFIs). Developed nations have implemented strategies such as fostering cooperation between criminal law enforcement agencies (LEAs) and research laboratories and institutes at universities. This collaboration aims to strengthen the Criminal Justice System (CJS) by leveraging expertise in forensic sciences and research. The researcher society in Pakistan holds the potential to serve as a valuable resource for updating outdated practices and advancing forensic science. Such advancements would contribute to an overall improvement in crime detection and the prosecution of criminal cases throughout the country [15].

In developing Asian countries, digital forensics has gotten insufficient attention. According to the study of literature, DFI research has mostly been undertaken in developed countries. There is a scarcity of accurate information about the state of digital forensics in Pakistan. Although the internet is widely used in the country, it is also commonly exploited for illicit purposes. The government has not dedicated enough resources to tackle cybercrime, resulting in a backlog of cases and an increase in complaints. There was no formal framework for investigating cybercrime in Pakistan until a few years ago, and there was a dearth of experience in the sector. The National Response Center for Cybercrime (NR3C) was established by the government to address these issues and is overseen by the Federal Investigative Agency (FIA) [16, 17]. The administration is tasked with addressing various aspects of digital forensics, cyber fraud, and technical investigations. However, despite efforts, digital crime remains a persistent issue in Asia, with notable instances of credit card fraud, false identification, SIM-box fraud, money laundering, and financing terrorism showing significant increases. Considering the substantial rise in cybercrime cases within the country from 2020 to 2022, along with the overall state of digital governance, it is anticipated that the figure of cybercrime suitcases will remain to escalate as Pakistan's digital landscape progresses [18].

The field of digital forensics is relatively new compared to traditional forensics [11]. However, in the past 35 years, law enforcement investigators have made significant efforts to develop innovative strategies for analyzing computers and other electronic devices in criminal cases [19]. As a result of the increasing demand for digital evidence to be presented in court, law enforcement agencies were forced to disseminate their findings to a larger audience. Nonetheless, the effectiveness and efficiency of traditional forensic

investigation techniques remain a concern. Some investigators have been criticized for their cynicism and resistance to modern methods and tactics and have failed to keep up with contemporary practices. Moreover, adequate training to acquire the necessary skills is often lacking [21].

3 Current Cyber Landscape of Pakistan

In 2020, the International Telecommunication Union (ITU) [22] released the Global Cybersecurity Index (GCI), which rated Pakistan 79th in terms of cybersecurity. The ITU unit nations' devotion to cybersecurity is assessed using five criteria: legal mechanism, organizational measures, capacity measures, technical measures and cooperation. Figure 1 depicts the GCI's rating. It is worth noting that Pakistan has declined from 66th to 79th in 2020. This decline can be attributed to the lack of progress in the five pillars of commitment, whereas other countries have shown commitment to these areas. Unfortunately, Pakistan is not adequately prepared for cyberattacks as it lacks both a National Computer Emergency Response Team (CERT) and a sectorial CERT [20, 21]. The absence of adequate preparedness is not unexpected, considering the general vulnerability of the public to digital threats resulting from a absence of extensive cybersecurity information and an free-for-all online circumstances.

Institutions that heavily rely on computer technology face inherent vulnerabilities to malicious cyberattacks. Even armed forces have embraced network-enabled technology, exposing them to potential disruptions by adversaries. The growth of the communications industry has fostered an unprecedented level of global interconnectedness through modern communication devices, amplifying the potential impact of any system compromise. While a few organizations are separately striving to establish lay-off measures in this domain, there is a deficiency of coordination between national efforts. Additionally, security corporations' function within their respective sectors and necessitate enhanced collaboration to ensure a comprehensive response. Despite the prevalence of cybercrimes in contemporary society, a substantial number of incidents go unreported. It is also progressively frequent for perpetrators to employ innovative techniques to hack into systems and unlawfully extract funds from collection accounts.

Until recently, Pakistan had an underdeveloped framework for managing cyberspace, resulting in the absence of technological corporations like the national CERT and sectoral CERTs. As a result, organizations such as telecommunication, defense, banking and gas relied on cooperative efforts to mitigate cyberattacks. However, this lack of coordination poses a threat to the country's infrastructure, as successful cyberattacks targeting one industry could have a cascading effect on others that depend on their services. To effectively counter complex cyberattacks and hybrid warfare, the Pakistani military lacks an integrated tri-services command, commonly referred to as an "Inter-Services Cyber Command" (ISC2). Additionally, the limited availability of efficient cybersecurity assets is a significant challenge in Pakistan. This can be attributed to various aspects, comprising the absence of a firm career foot path in the cybersecurity field, limited opportunities for professional development, accreditation, and the retention of highly skilled cybersecurity professionals.

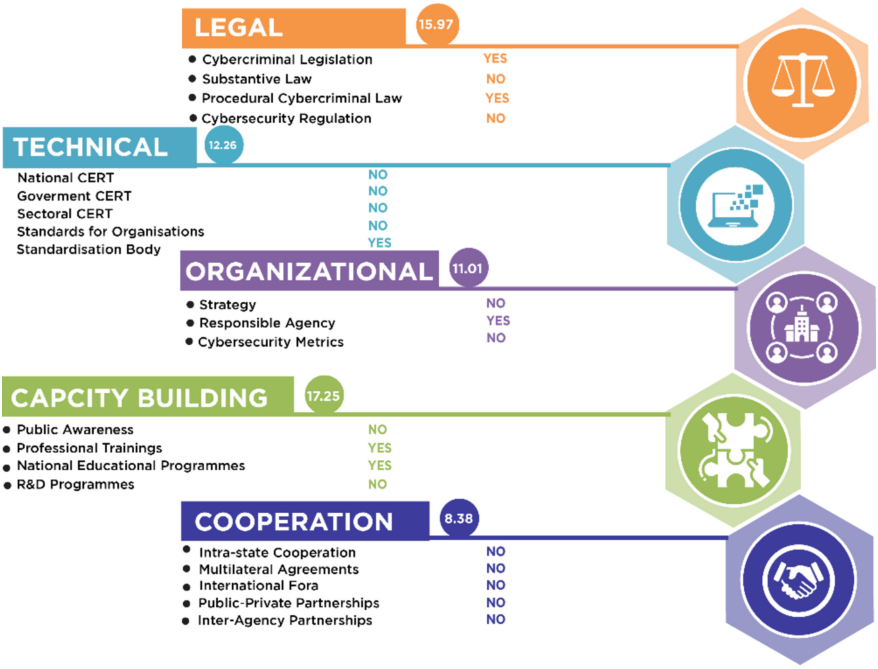


Fig. 1. Pakistan Current Cyber Landscape.

4 Contextual Model

The examination of DFI will center around six primary components, which are derived from the 2020 Global Cybersecurity Index [22]. These elements encompass the framework for multi-stakeholder collaboration in cybersecurity as outlined by the International Telecommunication Union (ITU), aiming to foster synergy between existing and future initiatives. The six foundational pillars consist of policy, legal framework, technical framework, organizational aspects, capacity building, and cooperation. These dimensions form the basis of the investigation, as they delineate the critical elements of digital investigation on a global scale. Digital forensics can be applied in almost every sector and field. The details of the six dimensions of the digital forensic investigation framework can be found in Fig. 2.

In Pakistan, the current state of DFI position remains weak, lacking a comprehensive and proactive security program. The existing counter-cybercrime measures seem reactive in nature and focus on damage control rather than prevention [20]. These measures are inadequately detailed, under-resourced, and mostly superficial in nature. The traditional "security box centric" approach of addressing DFI concerns is too narrow-minded and fails to consider innovative solutions. Furthermore, there is a lack of consensus within the same organization, resulting in a wastage of time and resources. Governance and documentation are also problematic, with excessive academic policies and procedures but poor execution strategies. In most cases, only a small percentage of the approved policies are implemented.

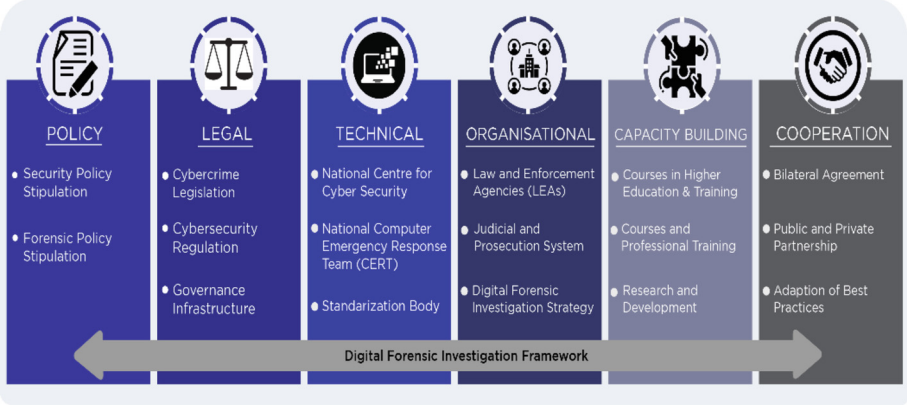


Fig. 2. Digital forensic investigation framework.

It is important for various stakeholders within Pakistan's administrative landscape, including the CJS, LEAs, educational institutes, departments, and ministries to collaborate effectively in order to foster the advancement of digital forensic skills at the national level. This collaboration can be accomplished through initiatives such as forming public-private partnerships, encouraging private-sector cooperation, facilitating inter-state and intra-state partnership speeding up efforts to embrace and integrate digital forensics on a broader scale. The study will focus on key aspects related to the establishment of a robust digital framework.

5 Conclusion

Pakistan's current cyber landscape is confronted with a range of challenges, including deficit of cybersecurity comprehension, trained personnel, and an underdeveloped investigative structure. The country lags in high-tech and administrative initiatives, rendering it susceptible to cybercrime threats. The adoption of DFI framework holds immense capability in tackling these issues and strengthening the overall cybersecurity of Pakistan. DFI offers a constituted and broad approach to recognizing and probing cybercrimes, thereby fostering a more robust and secure cyber environment in the country. Nonetheless, concerns regarding the effectiveness and feasibility of DFI persist. Adequate resource allocation and funding for DFI initiatives may pose a challenge, particularly considering the constrained resources available for cybersecurity endeavors. Moreover, the scarcity of skilled professionals may impede the capability to efficiently tackle complicated cyber risks. The implementation of DFI must navigate the legal and ethical implications surrounding data protection and privacy rights, ensuring that it supports the ethics and morality of the nation. Proper policy approach, legal measures, technical and organizational measures must guide the implementation of DFI to safeguard the rights of individuals, privacy and organizations. In conclusion, DFI signifies a fundamental stride towards fortifying Pakistan's cybersecurity posture and focusing the encounters confronting its current state of the cyber landscape.

References

1. Horsman, G., Sunde, N.: Unboxing the digital forensic investigation process. Sci. Justice **62**(2), 171–180 (2022)
2. Vasyukov, V.F., Khisamova, Z.I.: Investigation and seizure of electronic media in the production of investigative actions. Revista de Direito, Estado e Telecomunicacoes **13**(2) (2021)
3. Kundi, G.M., Nawaz, A., Akhtar, R., MPhil Student, I.E.R.: Digital revolution, cyber-crimes and cyber legislation: a challenge to governments in developing countries. J. Inf. Eng. Appl. **4**(4), 61–71 (2014)
4. Karie, N.M., Kebande, V.R., Venter, H.S., Choo, K.K.R.: On the importance of standardising the process of generating digital forensic reports. Forensic Sci. Int.: Rep. **1**, 100008 (2019)
5. Nduka, R.E., Basdeo, V.: The need for harmonised and specialised global legislation to address the growing spectre of cybercrime. Southern Afr. Public Law **36**(2), 22 (2021)
6. Barrett, M.: Framework for improving critical infrastructure cybersecurity version 1.1, NIST cybersecurity framework (2018). https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework. Accessed 14 Oct 2022
7. Arshad Khan, E.: The prevention of electronic crimes Act 2016: an analysis. LUMS LJ **5**, 117 (2018)
8. Arshad, H., Jantan, A.B., Abiodun, O.I: Digital forensics: review of issues in scientific validation of digital evidence. J. Inf. Proc. Syst. **14**(2), 346– 376 (2018)
9. Owen, P., Thomas, P.: An analysis of digital forensic examinations: mobile devices versus hard disk drives utilising ACPO & NIST guidelines. Digit. Investig. **8**(2), 135–140 (2011)
10. National Institute of Standards, Technology (NIST), and United States of America. Forensic examination of digital evidence: A guide for law enforcement (2004)
11. Kent, K., Chevalier, S., Grance, T.: Guide to integrating forensic techniques into incident. Tech. Rep. 800–86 (2006)
12. ISO-IEC 14882: 2011 information technology—programming languages—C++. International Organization for Standardization, Geneva, Switzerland **27**, 59 (2012)
13. International Telecommunication Union. next-generation digital forensics: Challenges and future paradigms. In 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 205–212. IEEE (2019)
14. Boachie, F.K.: ICT infrastructure required for sustainable library services in the 21st century issues and challenges from a developing country's perspective. In 2018 5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services (ETTLIS), pp. 12–15. IEEE (2018)
15. Farooq, A., Waheed, U.: Forensics: science of justice in Pakistan. Asian J. Biol. Life Sci. **2**(2) (2013)
16. Jamshed, J., Rafique, W., Baig, K., Ahmad, W.: Critical analysis of cybercrimes in Pakistan: legislative measures and reforms. Int. J. Bus. Econ. Aff. **7**(1), 10–22 (2022)
17. Lusthaus, J.: Front matter. In Cybercrime in Southeast Asia: Combating a Global Threat Locally (p. [i]-01). Australian Strategic Policy Institute (2020). http://www.jstor.org/stable/resrep25127.1
18. Irfan, E., Ali, Y., Sabir, M.: Analysing role of businesses' investment in digital literacy: a case of Pakistan. Technol. Forecast. Soc. Chang. **176**, 121484 (2022)
19. Vincze, E.A.: Challenges in digital forensics. Police Pract. Res. **17**(2), 183–194 (2016)
20. Haque, E.U., Abbasi, W., Murugesan, S., Anwar, M.S., Khan, F., Lee, Y.: Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. IEEE Access **11**, 40049–40063 (2023). https://doi.org/10.1109/ACCESS.2023.3268529

21. Khan, M.A.: Nadra database hack in context of cyber kill chain and overview of Pakistan's cyber security. Technical report, EasyChair (2021)
22. Global Cybersecurity Index (2020). International Telecommunication Union (ITU) Publication. url: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/513560_2E.pdf. Accessed 15 Dec 2022

Framework for Efficient Identification of Features Associated with Software Defects Using Spearman Correlation and Apriori Algorithm

Muhammad Umar Sajjad[1], Muhammad Qasim Riaz[2], Usman Qamar[1], Muhammad Danish Riaz[3], Muhammad Talha Imtiaz[1], and Muhammad Arif[4](✉)

[1] Department of Computer and Software Engineering, College of EME, National University of Science and Technology (NUST), Islamabad, Pakistan
usmanq@ceme.nust.edu.pk

[2] Faculty of Computer Science and Engineering (FCSE), Ghulam Ishaq Khan Institute of Engineering Sciences and Technology, Topi, Pakistan
qasim.riaz@giki.edu.pk

[3] Department of Computer Science, National University of Computer and Emerging Sciences (NUCES) – FAST, Islamabad, Pakistan

[4] Department of Software Engineering, Gold Campus, Superior University, Lahore, Pakistan
arif@superior.edu.pk

Abstract. In this modern era of science and technology the use of software and computer aided programs has increased very rapidly. With the increase in use the data and size of the computer software is also increased. Due to which the collection of large amounts of software testing data to support the software development and maintenance process has become difficult. In this paper we used data engineering techniques to discover the information from the software testing data. It will help to increase the reliability and quality of the product. First, we find the correlation between the different parameters of the software testing data set using the correlation analysis. Then we defined the analysis objects and applied the Apriori algorithm-based association rule algorithm model in multiple iterations to get more accurate results. Finally, the associations and relations obtained by analysis are shown.

Keywords: Data Analysis · Software Testing · Correlation Analysis · Association Rule Mining · Software Defect

1 Introduction

Software engineering is one of the most focused fields in this era. Due to the advancement in technology the amount of data generated during the different phases of the software development process has increased very rapidly. Especially in phase of the software testing and software quality check. To perform analysis at such an extensive data we

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 339–349, 2025.
https://doi.org/10.1007/978-3-031-77620-5_26

need a different approach. We can use different kinds of statistical techniques to find relationships between the different variables of both quantitative and qualitative data. Techniques like the correlation and association rule mining can be used to find the most related features and variables [1]. Similar kind of correlation and Apriori based association finding techniques will be used in this paper to find out the relationship between the line of codes and defects figured out during the software testing process.

Central focus should be to figure out the rules from old software test data set to run the activities related to SDLC in future. Test data is data which has been specifically designed to be used in tests, typically of a software system. To attain the above stated goals Data Engineering based techniques should be used to purify, analyze and express data using existing technology or developing new algorithms for the software testing process. This process is used to discover use of full knowledge and information for software development team and other persons involved in development activities like managers or technical leads [2].

Mostly test cases are designed on base of human expertise and test automation tools are used only to execute pre-planned test cases. Test cases evaluation depends upon the human who may have limited knowledge of software. This manual testing technique has a large amount of loss in word economy. In this paper we created association rules using different data mining techniques to find a relationship between different testing variables [3].

2 Literature Review

To conduct effective research a strong knowledge base is required. To make a strong knowledge base we have reviewed state of the art more than 100 research papers all of them are selected based on relatedness to our research. Other factors also include the year of publication, publication agency etc. Selected papers are included in the references section. We choose a well-defined selection and rejection criterion mentioned by Kitchen Ham in [4]. Most of the papers we selected for the literature review are published after 2015. To perform a quality literature review we only included papers from best ranked online databases like Springer, Science Direct or Elsevier and only included those conference papers which are ranked and indexed by Scopus. Some comments on the related studies are mentioned in next sections.

A study was conducted in 2015 about the fault prediction of different kinds of software systems using expert systems and the data mining applications [4]. Similarly [5] conducted another research and presented the "HySOM" a software fault detection and prediction model using the supervised learning techniques and applied the same techniques on the data set of NASA software systems. Correlation based model is derived for both functional size of the software and the effort required for the software testing process [6]. Analysis of test coverage is performed using Bisayan and correlation-based data engineering techniques and applied them on the case study for finding the relationship between the amount of the testing data and the effort required to find out the defects from such a large amount of code [7]. The applications of data engineering and process mining for finding out the defects in different software processes using the different data mining-based software testing techniques is shown in the [8].

In this paper we have applied the correlation and Apriori based association rule mining technique to find out the association between the line of codes and the defects at a data set which contains the software testing data after applying different software testing techniques. Similar kind of the work is performed by the [9] in which he also applied the correlation and association rule mining to find out the associations in different aspects using the software testing data set.

Data mining is domain for mining the knowledge form huge amount of data using different association rules here in this paper author used Apriori based association mining technique to mine relationships and associations in testing data variables. Different degrees of level of confidence and level of support can be used to figure out the relationships and association rules between different variables of testing data [9].

Yang et al. in [10] talks about the effort estimation in all stages of the software development life cycle (SDLC) according to the author the testing phase requires 21.57% of effort which also requires large amount of time, but use of the data mining approaches this effort can be reduced significantly.

As the process of maintenance is started the rate of modification in the software also increased significantly so it is very necessary to conduct the regression testing. Retesting a system using Regression testing also increases the cost and time to maintain or develop the system. To make debugging easier prioritize test cases in regression testing. The author discusses prioritizing and ranking the test cases using Association Rules Mining. In this process we save the whole history of faults which occurred during any phase of the development. It helps to keep records of which component of system contain a greater number of faults. When we change something in a system, we test these parts of the system in detail. Using this approach, we prioritize the test cases with respect to Average Percentage of Fault Detection (APFD) [11].

3 Methodology

The data set which is obtained after applying the software testing process has many dimensions related to the tested software. e.g., size of the software, time taken for the testing of the software, the language in which it is being developed, and the total number of test cases applied on the software to generate this kind of data set, total number of the defects found after applying the different kinds of the test cases etc. But only those features will be selected which effects most the quality of the software testing process. The following Fig. 1 shows how quality testing can be performed using the data engineering process. The extraction of the data from the software testing data set is consisting of the following mentioned subsequent phases:

- First, select a small amount of data from the software testing data set. But it should contain all types of features. Now appropriate statistical analysis should be used to find out the relation between all features of the data set. And last, the unrelated features should be eliminated. In this way we can obtain our basic data set to perform all other computations which are stated in the next steps.
- Now here in this step we analyzed the data which was extracted during the first step.

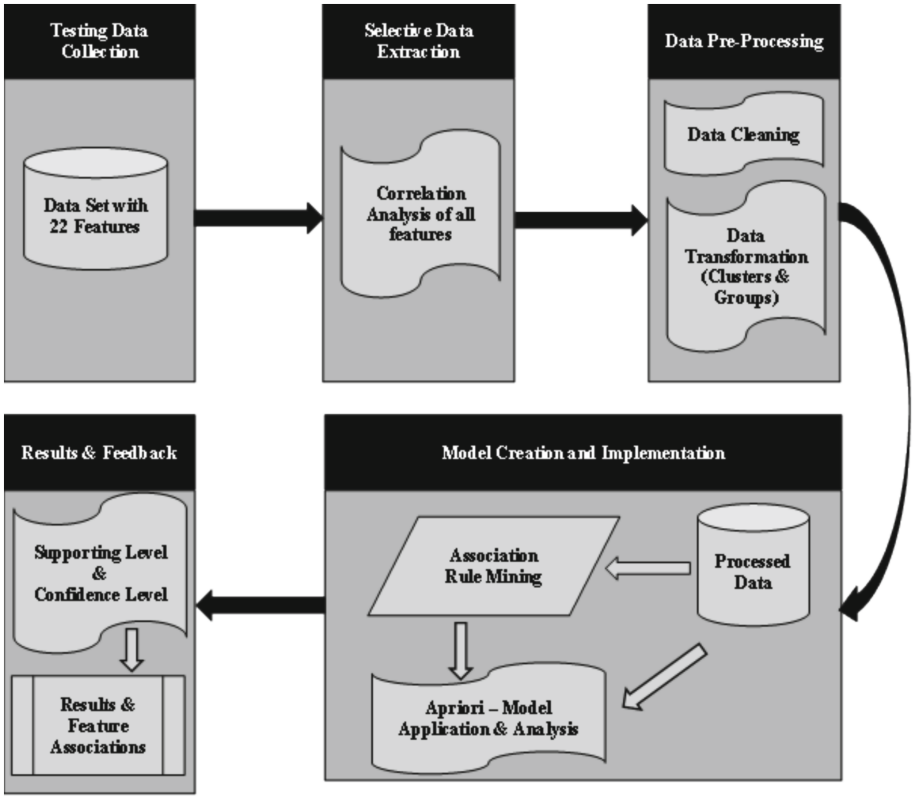


Fig. 1. Overall flow of work and research methodology

- We named it "Pre-Processing Data". Then we deleted the records which contain the missing values. Then transformed the new data into the model to make it more consistent and reliable.
- Then association rule-based algorithm is used at the model-based software testing data set which was obtained in the last phase. The association algorithm will help in finding the associations between the different features of the data set.
- After performing all the above operations now, we have a model data set. Now we can apply these similar techniques and outcomes to real and newer operational data sets. After performing all computations, we will get the associations and relations between selected features.
- A glimpse of original software testing data and features is displayed in Table 1. **Note:** The original names of testers are hidden to avoid privacy issues.

3.1 Spearman Rank Correlation

Correlation based techniques are used to find out the relationships between the different features of the data. It shows the positive results if the selected features have directly proportional relationship and shows the negative results vice versa. There are two types

Table 1. Head of dataset showing some important features.

Sr #	Tester Name (Dummy)	Software Size (Line of Code)	Software Size (KB)	No. of Test Cases	No. of Defective Test Cases	Comment Rate	Programming Language
1	xyz	86233	7.1	1717	187	211	Java
2	abc	57413	5.6	2976	304	134	Java
3	abc	94745	7.9	2844	358	421	PHP
4	mno	102821	11.1	3855	350	671	C++
5	mno	101797	10.8	3029	331	134	C++
6	xyz	18153	9.1	1373	232	35	Java
7	xyz	5707	7.2	1555	138	87	Java
8	pqr	86153	7.0	1717	187	103	PHP

of correlations (a) Spearman Correlation (b) Pearson Correlation. The Pearson method can be applied only when the data satisfies the normal distribution. But sometimes data may not be in normal distributions. Similarly, in this case data doesn't follow the normal distribution curve. That's why we applied the Spearman Rank Correlation (shown in Eq. 1) to find out the relationship between the required features. The mathematical relationship is shown following.

$$r_s = 1 - \frac{6\sum_{i=1}^{n}(R_i - Q_i)^2}{n(n^2-1)} \tag{1}$$

We ranked value of two variables x_i, y_i *according to the arrangement of variables.* X_i *Rank is shown by* R_i *and rank of* y_i *shown by* Q_i. R_i - Q_i represents rank difference of x_i, y_i.

To find out the accurate solution for acceptance and rejection of null hypothesis the level of significance should also be tested along with the Spearman Rank Correlation. The following Table 2 shows the level of significance at 5% and at 1% respectively along with the number of values in the left most column.

The Spearmen method is used to analysis software testing data. The data which we analyzed consist of variables which are shown in the Table 1 i.e., size of the software ("*Software Size-KBs*"), time for the starting of testing of the software ("*Start Time*"), the language ("*Language*") in which it is being developed, and the total number of the test cases ("No of Test Cases") etc. All the above-mentioned columns and features of Table 1 are visibly relevant to each other. Our central focus in the paper is to find the relationship between the defects ("*Number of Defects*") of the software and the other features of the given data. The results after applying the correlation are shown in the following Table 3.

Now according to the correlation results shown in the Table 3 and Figs. 2, 3 and 4. The number of test cases and the size of the software are the most highly correlated variables with the number of defects. So, we can say that the number of defects in any

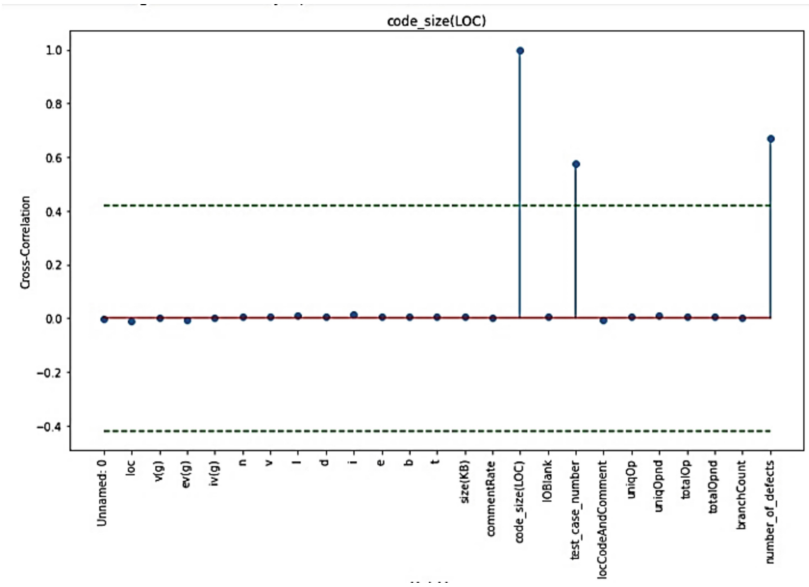


Fig. 2. Correlation of Software Size (LOC) or Code Size with other features (we can that only No. of test cases and No. of defects have significant correlation above the threshold of 0.5)

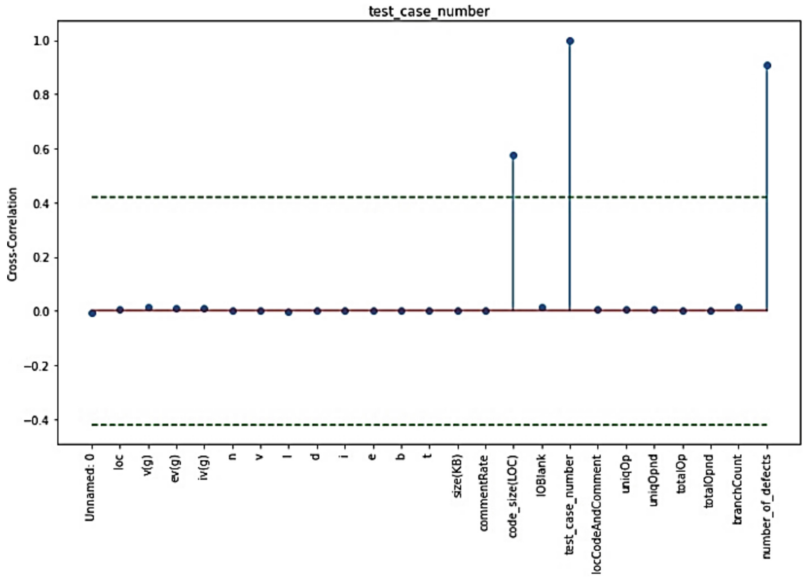


Fig. 3. Correlation of No. of defects with other features (we can that only Software Size/Code Size and No. of defects have significant correlation above the threshold of 0.5).

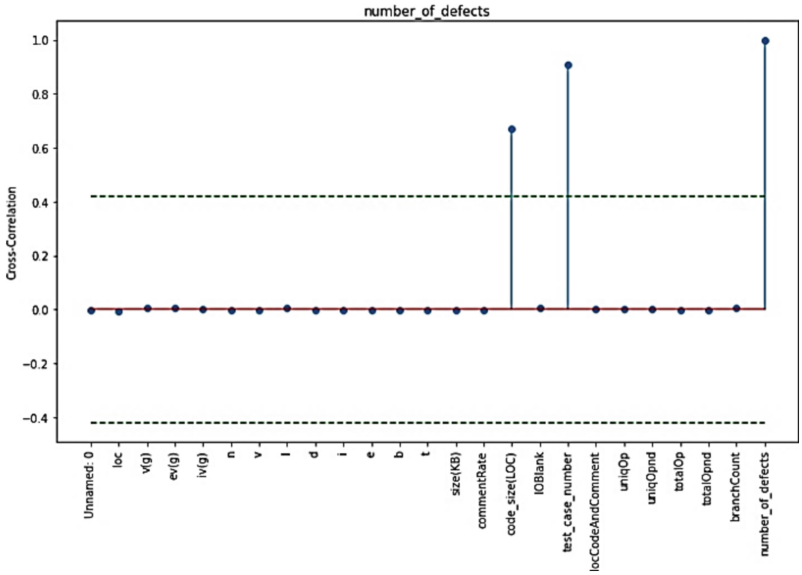


Fig. 4. Correlation of No. of test cases with other features (we can that only Software Size/Code Size and No. of test cases have significant correlation above the threshold of 0.5).

Table 2. Level of significance

N	LEVEL OF SIGNIFICANCE AT 5% - 0.05	LEVEL OFSIGNIFICANCE AT 2.5% - 0.025
21	0.370	0.436
22	0.361	0.425
23	0.353	0.416
24	0.344	0.407
25	0.233	0.398
26	0.337	0.390

Table 3. Significant correlation

Sr #	Correlation Description	Correlation Coefficient
1	No. of Defective Cases VS No. of Test Cases	+0.9101
2	No. of Defective Cases VS Software Size (LOC)	+0.6688
3	No. of Test Cases VS Software Size (LOC)	+0.5761

software depends a lot on the number of test cases we conducted for the testing and the size of that software.

3.2 Apriori Based Association Rule Mining

Apriori based Association calculation algorithm is also a well-known branch of the data engineering process sometimes it is also termed as "Market Basket Analysis". It is used to find the relationship between various entities and items related to supermarkets and economic systems. In terms of datamining, we mostly use it to find out the relationships and the associations between different items which are hard to find manually.

To show the proper dispersion and distribution of data here we used the two new parameters i.e., test case density per 100(TCD) line and defect density per 1000 line (DD). Both are calculated and mentioned following.

$$\text{TCD} = \text{No. of test cases/software size} \times 100$$

$$\text{DD} = \text{No. of defects/software size} \times 1000$$

Now after calculation these two ratios we grouped our data set into the clusters because association rule mining technique cannot be implemented at the continuous data, so we converted our data set into clusters by giving scope signs as shown in following Tables 4 and 5.

Table 4. Clusters of test case density per 100 lines

Order	Scope (1 Per 100 Line)	Scope Sign
1	(0–3)	V1
2	(3–9)	V2
3	(9–14)	V3
4	(14–20)	V4
5	(20-Infinity)	V5

Association Rules General Formula

Level of Support: Level of support is defined as real time occurrence of X and Y at a same time.

$$Support(X \rightarrow Y) = P(X \cup Y)$$

Level of Confidence: The Likelihood of occurrence of item set X with likelihood of occurrence of item set Y.

$$Confidence(X \rightarrow Y) = P(X|Y)$$

Table 5. Clusters of defect density per 1000 line

Order	Scope (1 Per 1000 Line)	Scope Sign
1	[0–5]	U1
2	(5–10]	U2
3	(10–15]	U3
4	(15–20]	U4
5	(20-Infinity]	U5

Table 6. Individual cluster-based occurrence and supporting level of test case density and defect density.

Sr #	Item Set	Occurrence	Supporting Level
1	V1	3446	0.3166
2	V2	5600	0.5145
3	V3	698	0.0641
4	V4	351	0.0322
5	V5	790	0.0726
6	U1	2479	0.2277
7	U2	4655	0.4277
8	U3	2084	0.1915
9	U4	678	0.0623
10	U5	989	0.0909

Table 7. Final association between test case density and defect density

Sr #	Item Set	Occurrence	Supporting Level
1	V1, U1	2073	0.601
2	V2, U3	3332	0.595

Minimal Level of Support and Minimal Level of Confidence

A value defined by the data engineer based on his experience is known as the "Threshold Value". This value is used to change the level of support. Some time it is also known as the "Minimum level of support."

While on the other hand, another type of threshold value which is used to change the level of confidence is known as the "Minimum level of confidence". It also helps us in figuring out the variables with lowest possible relationship or association. But any

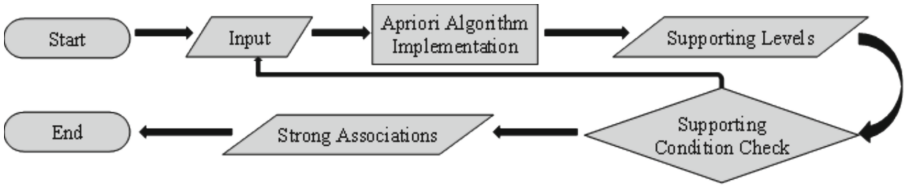


Fig. 5. Modeling and Implementation cycle of Apriori Algorithm

association rule will be strong if both threshold of the level of support and the threshold of the confidence are fulfilled.

A set of items is combination of total items is known as X set of items if it owns X no. of items. e.g. {xyz, abc, efg} is a set of 3 items Transaction amount of any set of items is knows as occurrence incidence it's also known as level of supporting.

Model for Testing the Association Rules

The above Fig. 5 elaborates that the above model consists of the six different steps which includes input of data, Apriori Algorithm Disposal and Outputs of the final associations.

Association Rules Analysis of Testing Data

First, test case density is calculated and then we check the level of support for the different orders sets. As displayed in the following Table 6.

The level of support of V1 and V2 is greater than the threshold value, so we can say the most recurrent items in the given sets are V1 and V2.

After finding the density ratios we figured out the most common set of items in the following Table 7 using the items of test case set and defect sets.

The most common set of items are trimmed and checked with threshold level of ten percent. And the threshold for the level of confidence is set as sixty percent. Then the level of confidence is figured out for both V1 and V2 with U1 and U3 respectively. All of them are greater than 59 percent. After performing all the above general calculations, the final association and relationships are shown in the following Table 7.

4 Conclusion

In common words, as we all know that software testing is one of the most important phases of the software development life cycle which helps in reducing the number of defects and increasing the quality of the software. In this paper our aim was to find the factors that cause an increase or decrease the in identification of defect rate of a software. For this purpose, we first applied the Spearman Rank Correlation to figure out the relevant features then we applied the Apriori based association rule mining technique to generate the associations among these variables. Only those parameters are used which effects most the quality of the software. i.e. size of the software ("Software Size-LOC"), time for the starting of testing of the software ("Start Time"), the language ("Language") in which it is being developed, and the total number of the test cases ("No of Test Cases") etc. the association algorithm cannot be applied at the continuous data, so we make

clustering calculated the density functions with respect to size of the software. Then we used iterative Apriori technique to find the associations between these density functions. Finally, after finding the associations we analyzed the number of test cases applied and the size of the software the two most associated variables with the number of defects in the software product.

References

1. Toure, F., Badri, M., Lamontagne, L.: Innov. Syst. Softw. Eng. **14**, 15 (2018). https://doi.org/10.1007/s11334-017-0306-1
2. Nalepa, G.J.: Using rules to support software testing. In: Modeling with Rules Using Semantic Knowledge Engineering. Intelligent Systems Reference Library, vol. 130. Springer, Cham (2018)
3. Kitchenham, A., Kitchenham, B.: Guideline for performing systematic literature reviews in software engineering. EBSE Technical Report EBSE-2007–01 (2007)
4. Erturk,E., Sezer, E.A.: A comparison of some soft computing methods for software fault prediction. Expert Syst. Appl. **42**, 7 (2015)
5. Abaei, G., Selamat, A., Fujita, H.: An empirical study based on semi-supervised hybrid self-organizing map for software fault prediction. Knowl. Based Syst. **74**, 28–39 (2015)
6. Čeke, D., Milašinović, B.: Early effort estimation in web application development. J. Syst. Softw. **103**, 219–237 (2015)
7. Cotroneo, D., Leo, D.D., Natella, R., Pietrantuono, R.: Prediction of the testing effort for the safety certification of open-source software: a case study on a real-time operating system. In: 12th European Dependable Computing Conference (EDCC), Gothenburg, pp. 141–52 (2016)
8. Keith, B., Vega, V.: Process mining applications in software engineering. In: Mejia, J., Muñoz, M., Rocha, Á., San, Feliu T., Peña, A. (eds.) Trends and Applications in Software Engineering. CIMPS. Advances in Intelligent Systems and Computing, vol. 537. Springer (2016)
9. Rehman, S., Sharma, A.: Privacy preserving data mining using association rule based on Apriori algorithm. In: Singh D., Raman B., Luhach A., Lingras P. (eds.) Advanced Informatics for Computing Research. Communications in Computer and Information Science, vol. 712. Springer, Singapore (2017)
10. Yang, Y., He, M., Li, M., Wang, Q., Boehm, B.W.: Phase distribution of software development effort. In: Proceedings of the Second ACM-IEEE International Symposium on Empirical Software Engineering and Measurement, ESEM 2008, pp 61–69. ACM, New York (2008)
11. Acharya, A.A., Mahali, P., Mohapatra D.P.: Model based test case prioritization using association rule mining. In: Jain L., Behera H., Mandal J., Mohapatra D. (eds.) Computational Intelligence in Data Mining - Volume 3. Smart Innovation, Systems and Technologies, vol. 33. Springer, New Delhi (2015)

Segmentation of Brain Tumor Using U-Net Approach

Samra Riaz(✉) and Syed Muhammad Anwar

Department of Software Engineering, University of Engineering and Technology, Taxila, Pakistan
samrariaz1@gmail.com, s.anwar@uettaxila.edu.pk

Abstract. In this study, a methodology is presented for segmenting brain tumor using the U-Net deep learning approach. The accurate segmentation of brain tumors is critical for their diagnosis and treatment, and the U-Net architecture has demonstrated promising results in biomedical image segmentation tasks. The proposed methodology consists of three primary stages: Data Preparation, Data Pre-processing, and Brain Tumor Segmentation. The model is trained on a BraTS 2020 dataset of MRI brain scans that includes both Tumor and Non- Tumor samples. The U-Net architecture is utilized, and the achieved results shows a maximum accuracy of 99.6% for various epochs. The proposed approach has substantial potential for improving the accuracy of brain tumor diagnosis and treatment, leading to better patient outcomes. This research highlights the effectiveness of deep learning in medical image segmentation tasks and underscores the importance of accurate segmentation in brain tumor diagnosis and treatment.

Keywords: Dice Similarity Coefficient (DSC) · U-Net · Segmentation

1 Introduction

The primary type of brain tumor is called gliomas, which originate from glial cells of the brain and found approximately 80.0% of all malignant brain tumors. It's worth noting that all gliomas are not cancerous, and they can typically be considered into two grades: high-grade glioma (HGG) and low-grade glioma (LGG) [1].

According to the WHO tumors categorized into four grades. LGG comprises Grade I and Grade II tumors, which are typically slow-growing and benign [2].

In contrast, HGG encompasses Grades III and IV tumors, which are malignant and likely to recur. Patients diagnosed with Grade I tumors typically having long-term survival rate since these tumors are mostly benign. On the other hand, patients with HGG have a much shorter survival time due to the aggressive nature of these tumors, with some not surviving more than a year. Detecting glioma at an early stage can help the radiologist to evaluate the condition of patients and create an appropriate treatment plan [3].

Magnetic resonance imaging (MRI) techniques are utilized to diagnose and assess the prognosis of brain tumors. The technique of MRI, which is non-invasive, is commonly

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 350–361, 2025.
https://doi.org/10.1007/978-3-031-77620-5_27

used to locate brain tumors in three dimensions. MRI produces high-quality images with superior soft-tissue contrast without employing ionizing radiation, in contrast to X-ray and CT imaging. To diagnose brain gliomas four MRI sequences obtained which include T1-weighted, T1-weighted contrast-enhanced (T1ce), T2 weighted, and Fluid attenuated inversion recovery (FLAIR) [5, 6]. The process of isolating suspicious segments from MRI images is known as image segmentation [7].

In current years, several DL based techniques have been developed, particularly for analyzing medical images. In computer vision and medical image analysis DL models have outperformed machine learning techniques. However, automated segmentation is not sufficient for devising treatment plans and making diagnoses; the use of survival analysis is necessary [3].

Our objective is to distinguish abnormal tissues from normal tissues, extract features, or simplify image description. There are three distinct types of image segmentation: manual segmentation, semi-automatic segmentation, and automatic segmentation [5]. Manual segmentation involves a significant amount of time and workload, as well as human interaction. Semi-automatic segmentation, on the other hand, requires less human involvement, resulting in higher accuracy and faster processing speed. Automatic segmentation aims to identify tumors and their sub-regions without any human interaction [6].

This paper designed a deep learning method that gives more accurate segmentation results. The key aim and objective of the research work is to:

- Design an effective deep learning model for Brain Tumor Segmentation.
- Extract features from tumor regions.
- Improve results for clinical adaptability and relevance.

Our goal is to concentrate on the semantic segmentation technique to segment brain tumors from multimodal MRIs. The strategy we employed was the winning solution for the BraTS 2020 competition.

2 Related Work

Automatically segmenting brain tumors for cancer diagnosis is a difficult task. However, the presence of public datasets and the established BRATS benchmark created a standard platform for researchers to develop and evaluate their methods objectively in comparison to existing techniques. A review of both traditional techniques and deep learning-based state-of-the-art methods is presented in [9]. Glioma segmentation is currently considered the domain of deep learning methods due to their reported high performance. In segmentation methods, transferring previous knowledge to probabilistic maps or selecting highly representative features for classifiers is a difficult task. One of the advantages of convolutional neural networks (CNNs) is their ability to learn complex, representative features for both tumor tissues and healthy brain tissues directly from multi-modal MRI images, without the need for manual feature extraction.

The study presents and compares two methods for segmenting high-grade glioma (HGG, grade IV) using clinical patient data and MRI. The first method uses balloon inflation to split long edges and detect high-intensity tumor boundaries for segmentation.

The second approach involves setting up a weighted and directed graph to achieve an optimal segmented result, while the first method is based on voxel classification. The evaluation and comparison of these two methods are based on the Dice Similarity Coefficient (DSC), a validation metric used to measure the similarity between different segmentation results [7].

The DFMNet, a 3D dilated multi-fiber network, is employed to segment brain tumors of patients, providing clear tumor information. To extract meaningful features and avoid overfitting issues for OS prediction, the PECL-DenseNet is utilized. The process of forecasting the duration of the OS involves extracting features from various sources, such as the deep CNN, PECL-DenseNet, handcrafted features, and spot encoded segmented features. These extracted features are utilized to train a GBDT regression model [8].

The utilization of k-mean clustering and EMAP algorithm constitutes an automated and reliable technique for the segmentation of brain tumors. This technique is capable of identifying both the whole tumor and sub-tumor regions from MRI images of both low-grade glioma and high-grade glioma. Computational time and accuracy are evaluated for this technique, which is tested on LGG and HGG MRI images from the BraTS 2015 dataset. The technique achieved 92% accuracy, which compares favorably with other techniques that rely on expensive algorithms. By using pre- and post- processing techniques, the accuracy of this technique can be further improved for low-contrast images [9].

For brain tumor segmentation, a Parcellation Atlas is used to map each subject's data, and the strategy is to merging the lesions present in the MRI image to generate an input that can be fed into a patch-based neural network. For survival prediction, the following steps are performed: 1) Generate a tumor mask prediction for each individual subject., 2) extract tractography features from the training subjects, 3) perform feature normalization, and 4) Utilize the tractography features to train SVM classifier. The survival prediction of patients is evaluated using the BraTS 2018 dataset [10].

An automatic glioma segmentation method is performed in three steps: the first step is to convert images into super pixel images using k-mean clustering that is perfectly fitted to tumor boundaries. The second step is to calculate features (tumor texture, tumor intensity, curvature feature, fractal texture) and the label of super pixels, which is used to produce the training set. In the third step, an SVM model is trained to classify the super pixel images into either tumor or non-tumor regions. This method achieves good segmentation performance in the BraTS 2017 dataset [11].

Accurate and reliable explanation of Glioblastoma tumor and survival prediction are critical for the timely treatment of tumor patients. Research has indicated that an automated algorithm can be utilized in GBM tumor for the extraction of the whole tumor, enhancing core and edema. This algorithm leverages fuzzy links between voxels to calculate affinity and relies on a single seed point to facilitate the precise segmentation of brain tumors. Multi-network MRI information can also be utilized to enhance the performance of segmentation. The algorithm has demonstrated a high level of accuracy, achieving over 90% accuracy for the whole tumor and 60% accuracy for edema and enhancing core. Spatial mapping or habitats can be used for survival prediction of patients [12].

Deep neural network (DNN) is a highly effective tool for automatically segmenting brain tumors into three distinct regions such as whole tumor, tumor core, and enhancing tumor. This method facilitates the accurate detection and localization of tumors. In addition, a radiomic tool can be utilized to find the survival of patients by analyzing various tumor features such as age, location, and shape. The BraTS 2018 dataset is employed for segmentation and survival challenge purposes [13].

The two primary objectives involve utilizing 3D MRI brain images to accomplish two main tasks: 1) segmenting the tumor and 2) predicting patient survival. To achieve these goals, the first step in tumor segmentation involves identifying the tumor's location in the MRI image. Following this, the tumor is segmented into subregions: edema, tumor core, and enhanced tumor. In segmentation, brain images are first cropped into a brain mask that built on voxels that have a non-zero value. Next, standard deviation and mean are computed, and then data is normalized [9].

In order to segment brain tumors, a U-net architecture is utilized, with the aim of reducing layer depth to decrease the number of parameters and speed up processing while maintaining high accuracy. This model is applied to segment both the whole tumor and tumor sub-regions, such as non-enhancing, edema, necrosis, and enhancing tumor [14].

To perform glioma segmentation and survival prediction, an automatic framework based on deep CNN is utilized. To improve the system's robust performance for segmentation purposes, a CNN architecture is used. To predict patient survival, a cross-validation and decision tree approach is used to select features that are extracted from the segmentation results [15].

3 Proposed Methodology

This portion describes in detail our proposed methodology. Our proposal involves utilizing a U-Net model for brain tumor segmentation. The proposed methodology is presented in Fig. 1. The model contains three main steps: preparation, preprocessing and last step is segmentation. The proposed model uses u-net architecture and perform segmentation.

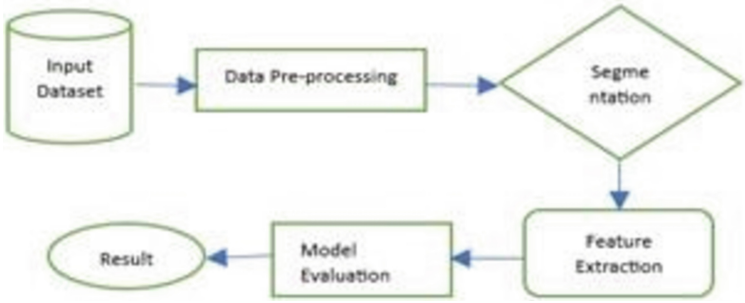


Fig. 1. Outline of proposed methodology.

3.1 Data Preparation (Dataset)

The initial stage of any machine learning task involves obtaining the dataset that will be used in subsequent stages. In this project, the Brats20 image dataset was utilized, which comprises images stored in the NIfTI file format, commonly used for MRI files. The dataset is organized into primary folders containing both training and validation data. Training set is **80%** and lastly validation set is **20%**. To diagnose brain gliomas four MRI sequences obtained which include T1-weighted, T1-weighted contrast-enhanced (T1ce), T2 weighted, and Fluid attenuated inversion recovery (FLAIR).

The main aim of BraTS is to evaluate sophisticated methods for delineating brain tumors in MRI images. The dataset includes MRI scans from various institutions, with a primary emphasis on segmenting intrinsically heterogeneous brain tumors, particularly gliomas (Fig. 2).

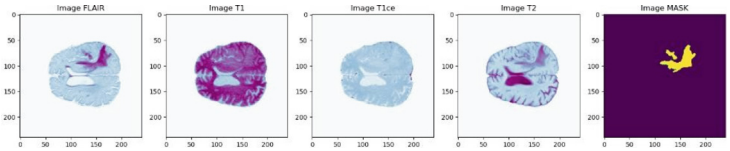


Fig. 2. Images generated by BraTS 2020

3.2 Segmentation

In the segmentation phase U-Net Architecture is used. The detail of this architecture is given below.

U-Net. UNet is a convolutional neural network (CNN) that has found diverse applications in computer vision tasks, which is originally designed for biomedical image segmentation. This architecture contains an encoder-decoder path connected by a bottleneck named "UNet" comes from the networks U-shaped.

In our proposed work, we train U-Net model for doing segmentation of a required Dataset designed for image segmentation. Figure 3 is the architecture of the CNN model in which we firstly take image from dataset BraTS 2020. Next step is to perform data augmentation. Data augmentation is a method utilized in machine learning and computer vision to enlarge a dataset by generating new instances from the available ones. This involves employing a range of transformations or alterations on the initial data, such as rotation, scaling, flipping, cropping, or introducing noise, to generate new versions of the data that maintain their relevance and representation of the original dataset.

Second step is to normalize and preprocess data. Data preprocessing refers to the process of cleaning, transforming, and preparing raw data before it is used for analysis or modeling. After getting preprocessed data, U-Net model is applied that is fully convolutional neural network. In U-Net there is a series of convolutional layers and pooling layers for down sampling, followed by the series of convolutional and up sampling layers of up sampling. Subsequently, the network employs skip connections to merge

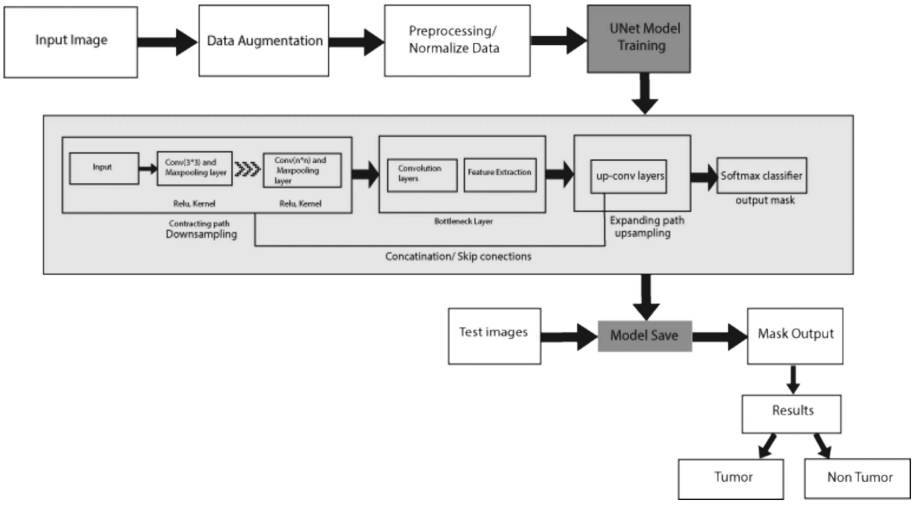


Fig. 3. Proposed multi-layer U-Net model

the feature maps obtained from both the down-sampling and up-sampling pathways to enhance the accuracy of segmentation.

During down sampling path, the feature maps are typically reduced in spatial dimensionality by applying pooling operations and channel/filter increase. Using skip connections, the reduced segmented feature maps are concatenated with their corresponding feature maps from up-sampling pathway.

Therefore, there is no need to flatten the feature maps, as they are concatenated and passes directly to the next layer.

We used Adam Optimizer in order to decrease the loss obtained from categorical cross entropy [16] as this optimizer is the best-known optimizer used in order to train the model more efficiently and in less time. Due to multi-class nature of BraTS images Dataset, we use categorical-cross entropy. ReLu activation function is applied on U-Net which helps to activate few neurons and computations can easily be performed. Mathematically, the ReLu function is denoted by Eq. (1).

$$f(a) = \max(0, a) \tag{1}$$

ReLu function states that if this function gets negative input value, it returns zero. But, on the other hand, if the function obtains any positive value as input value x, then it returns that particular value. So, in result the output value generated contains the values ranging from 0 to infinite range.

Lastly, at the output stage dense layer is added with Soft-max activation function. It is often used as the last layer in a neural network to map the learned features to the class probabilities. In numerous neural network designs, including feedforward neural networks and convolutional neural networks, the SoftMax function serves as the output layer. During the training phase, the SoftMax layer is fine-tuned that reduce the minimum cross-entropy loss between the predicted probabilities and actual labels. At the time of inference, the SoftMax layer provide predicted class based on the highest probability.

Test image is passes through trained U-Net model and then image is segmented into 2 classes a tumor or a non-tumor class.

4 Evaluation and Results

We carried out our model experiments on Windows 10 platform, utilizing an Intel Core i5. Python (version 3.11) was the programming language used to implement the experiments, with the scikit-learn library serving as the machine learning tool of choice. The scikit-learn library is an open-source tool that can be accessed for free.

4.1 Train/Test Split

We have divided the dataset as 8:2 train-test splitting. Training set is 80% and Validation set is 20%.

We calculated the accuracy on the test data that is 99.6%.

4.2 Model Parameters

Following performance parameters are used in the proposed methodology that is given below:

The BraTS 2020 Dataset, which we utilized, is a categorical dataset comprising two classes tumor or non-tumor. For our multi-class classification model, we use Categorical Cross Entropy loss function, which is well-suited for models with multiple output labels. Our simulation environment involved 35 epochs, with ReLu and Softmax functions used in the proposed models. ReLu is preferred because it prevents all neurons from activating at once. Instead, when an input value is negative, the function is not activated and the value is converted to zero. This allows for only a few neurons to be activated and the network to be free for computation (Fig. 4).

SoftMax function is the activation function that apply on the final output layer to normalize the output value and perform classification tasks. Finally, we used Adam as the optimizer for our neural network, as it is known to efficiently train networks in a shorter period of time.

The representation of Brats 2020 Dataset in various form is given below:

4.3 Evaluation Metrics

In image segmentation, evaluating the performance of a segmentation model often involves using metrics that measure the similarity between the predicted segmentation masks and the corresponding ground truth masks. Some commonly used metrics for segmentation include:

Accuracy:
Accuracy is a metric that calculates the proportion of accurately classified pixels in the predicted mask, expressed as a percentage.

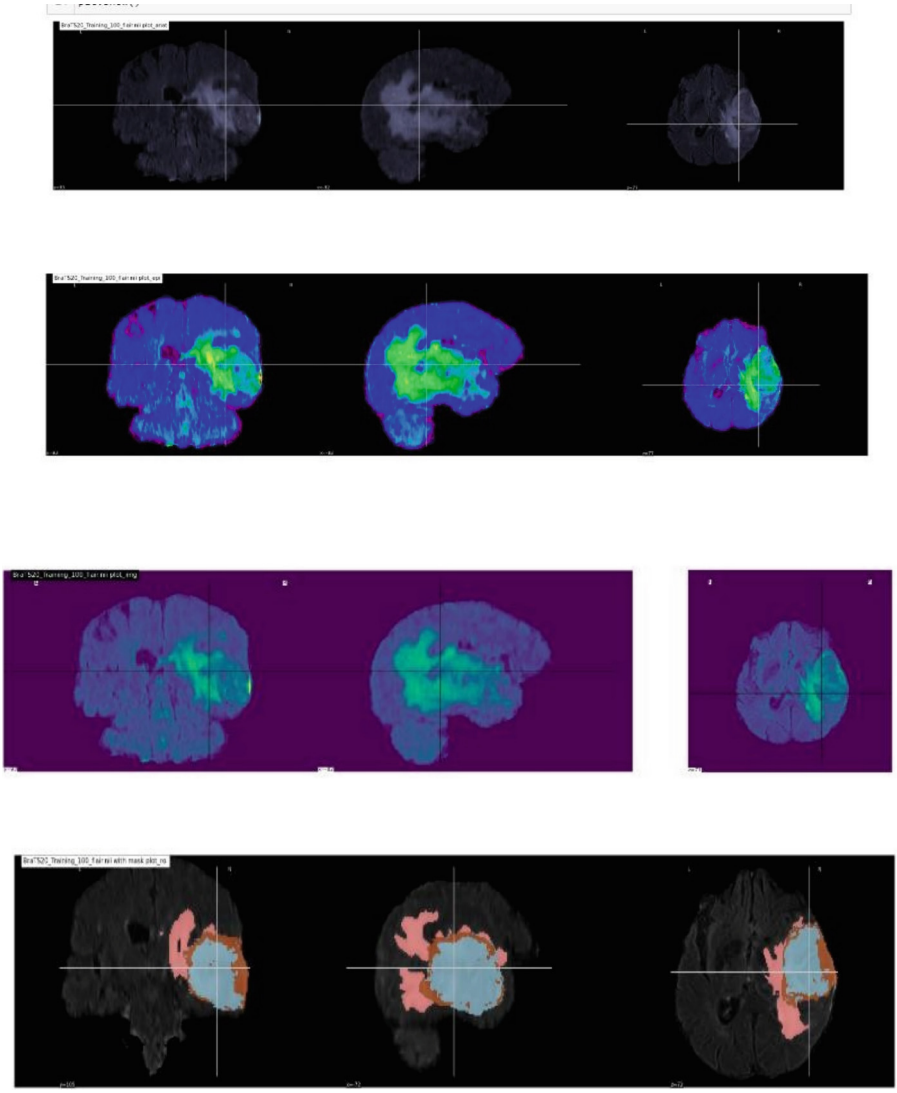


Fig. 4. Training Dataset Representation in various form

Dice Coefficient:

Dice coefficient is used to measure comparison between the predicted mask and corresponding ground truth mask.

These metrics can help evaluate the dice-coefficient and accuracy of the segmentation output and also identify areas where the model may perform poorly. Tables 2, 3 and Fig. 5 shows the result of Accuracy by using U-Net Architecture. Table 4 and Fig. 6 shows the result of Dice Co-efficient by using U-Net Architecture.

4.4 Results

In this section, detailed results obtained from the U-Net architecture is explained that is useful in the brain tumor segmentation problem. Different types of experiments are done in order to get improved results using deep learning.

Results obtained for different Epochs using U-Net is discussed below:

Table 1. Model parameters.

Parameters	Values
No. of channels	2
Epochs	35
Learning Rate	0.001
Class mode	Categorical
Activation function	ReLU and Softmax
Loss function	Categorical cross entropy
Optimizer	Adam

Table 2. Training of Accuracy using U-Net Architecture

	Accuracy	Loss
Epoch 5/35	98.6	0.04
Epoch 10/35	99.2	0.03
Epoch 15/35	99.4	0.02
Epoch 20/35	99.5	0.01
Epoch 25/35	99.6	0.01
Epoch 30/35	99.6	0.01
Epoch 35/35	99.6	0.01

Table 2 shows the performance of the U-Net model on different Epochs. We can observe that the results obtained using U-Net shows maximum accuracy of 99.6%.

Table 3. Validation of Accuracy using U-Net Architecture

	Accuracy	Loss
Epoch 5/35	98.1	0.05

(*continued*)

Table 3. (*continued*)

	Accuracy	Loss
Epoch 10/35	98.5	0.04
Epoch 15/35	98.8	0.03
Epoch 20/35	99.2	0.02
Epoch 25/35	99.3	0.02
Epoch 30/35	99.3	0.02
Epoch 35/35	99.3	0.02

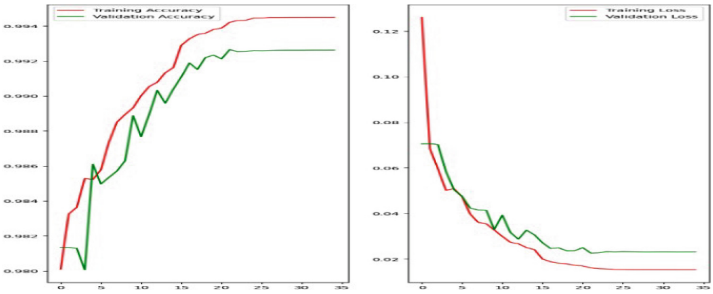


Fig. 5. Performance metrics using accuracy

Table 3 shows the accuracy and loss results obtained using U-Net. From the figures, it is clear that the accuracy rate is increasing for each iteration and loss is decreasing.

Figure 5 shows results obtained for different Epochs using U-Net architecture. It is clear from the results calculated that the highest accuracy of 99.6% is obtained.

Table 4. Dice Coefficient using U-Net Architecture.

	Training	Validation
Epoch 5/35	0.35	0.35
Epoch 10/35	0.41	0.42
Epoch 15/35	0.62	0.59
Epoch 20/35	0.63	0.62
Epoch 25/35	0.64	0.63
Epoch 30/35	0.64	0.63
Epoch 35/35	0.64	0.63

Table 4 displays the performance of the model on each iteration. The results obtained using U-Net shows maximum accuracy of 64% at training stage and of 63% at validation step.

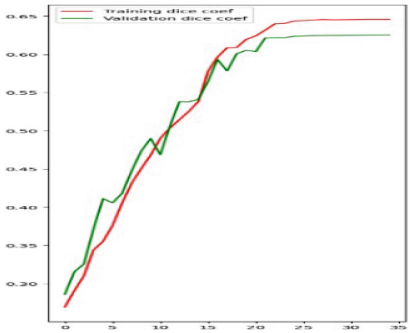


Fig. 6. Performance metrics using Dice Co-efficient

Figure 6 shows the Dice Co-efficient measured using U-Net architecture. From the figures, it is clear that for different Epochs, dice coefficient is increasing for each iteration both for training and validation.

5 Conclusion

This study describes a new method for detecting brain tumors using deep learning. The method involves three stages: Data Preparation, Pre-processing of data, and Segmentation. A multi-layer U-Net is proposed for segmentation, which utilizes different layers and the BraTS images dataset for experimentation. The U-Net model achieved better accuracy results in segmenting the images. The proposed approach was evaluated using two performance metrics, with the maximum accuracy of 99.6% achieved using the U-Net model. Future work may focus on evaluating survival prediction of brain tumor patient.

Data Availability. This work was performed using BraTS Dataset (https://www.kaggle.com/awsaf49/brats20-dataset-training-validation/code).

References

1. C. N. N. Architecture, brain tumor segmentation and survival prediction using automatic hard mining in 3D, pp. 1–11
2. Ye, J., et al.: Tumor grade and overall survival prediction of gliomas using radiomics **2021** (2021)
3. Myronenko, A.: 3D MRI brain tumor segmentation using autoencoder regularization
4. R. Features, S. Engineering, and U. E. T. Taxila, brain tumor survival prediction using radiomics features, pp. 1–9

5. Shaheen, A., Bukhari, S.T., Nadeem, M., Burigat, S., Bagci, U.: Overall survival prediction of glioma patients with multiregional radiomics **16**(July), 1–16 (2022). https://doi.org/10.3389/fnins.2022.911065
6. Isensee, F., Kickingereder, Wick, W., Bendszus, M., Maier-hein, K.H.: Brain tumor segmentation and radiomics survival prediction: contribution to the BRATS 2017 challenge (2017)
7. Wu, Y., Zhao, Z., Wu, W., Lin, Y., Wang, M.: Automatic glioma segmentation based on adaptive superpixel, 1–14 (2019)
8. Li, Z., Wang, Y., Yu, J., Shi, Z., Guo, Y., Chen, L.: Low-grade glioma segmentation based on CNN with fully connected CRF **2017** (2017)
9. Ali, I., Direko, C.: Review of MRI-based brain tumor image segmentation using deep learning methods **102**, 317–324 (2016). https://doi.org/10.1016/j.procs.2016.09.407
10. Egger, J., Kuhnt, D., Carl, B., Freisleben, B., Kolb, A.: A comparison of two human brain tumor segmentation methods for MRI data
11. Guo, X., Yang, C., Lam, P.L., Woo, P.Y.M.: Domain knowledge based brain tumor segmentation and overall survival prediction **1**, 1–11
12. Weninger, L., Rippel, O., Koppers, S., Merhof, D.: Segmentation of brain tumors and patient survival prediction: methods for the BraTS 2018 challenge. Springer International Publishing (2019).https://doi.org/10.1007/978-3-030-11726-9
13. Kao, P., Ngo, T., Zhang, A., Chen, J.W., Manjunath, B.S.: Overall survival prediction, pp. 1–14
14. Bhadani, S., Mitra, S., Banerjee, S.: Fuzzy volumetric delineation of brain tumor and survival prediction. Soft Comput. (2020). https://doi.org/10.1007/s00500-020-04728-8
15. Carver, E., et al.: Automatic brain tumor segmentation and overall survival prediction using machine learning algorithms, vol. 1. Springer International Publishing. https://doi.org/10.1007/978-3-030-11726-9
16. Kingma, D.P., Ba, J.L.: Adam: a method for stochastic optimization. In: 3rd International Conference on Learning Representations, ICLR 2015 - Conference Track Proceedings, pp. 1–15 (2015)
17. VGG-16 | CNN model

Design and Implementation of an On-Board System for a Spider Robot

Nasir Nauman[1,3(✉)], Hirra Mustafa[1,2], Abrar Ashraf[1,3], and Hisham Khalil[3]

[1] Department of Computer Science, Superior University, Lahore, Pakistan
be107902@gmail.com
[2] Department of Computer Science, Sharif College of Engineering and Technology, Lahore, Lahore, Pakistan
[3] Embedded System and Robotics Lab, Department of Technology, The University of Lahore, Lahore, Pakistan

Abstract. This paper presents the design of a system onboard spider robot for rescue services. The spider has the six-leg walking pattern that contains the total number of 18 servo motors. In order to reduce the payload, the abdomen of the spider is made with RF4 printed circuit board (PCB). Whereas, the abdomen is also used as the main structure of the robot to attach the rest of the system. Wherein, two pulse-width modulations (PWM) module are controlled by Arduino Nano, the Bluetooth module is used for communication link and bulk converter for the power supply. The spider robot is operated with an in-house developed Android application. It has been observed that the spider robot has a stable walking response along with the multiple excise performance.

Keywords: System on board · Spider robot · Android control

1 Introduction

In the modern era of technological development, spider robots have become a new approach that needs to be explored. Normally, robots have wheels to move around and they are limited to plain surfaces. In the search and rescue operation in deep forest, the spider type robots are more likely to move freely as compared to wheel-based robots. To overcome this issue, researchers are considering the different approaches such as four or six leg based robots.

In [1], a four-leg spider was developed with the self-adaptive approach while the controlling scheme has been based on LabVIEW. One can observe from Fig. 1 that the spider was made with metallic legs and abdomen which usually made the robot heaver. A Work was found on six-leg spider with walking algorithm [2] and feedback using ultrasonic sensing. In this work, the detail of movements of an individual walking pattern has been listed in tabular format. Moreover, the presented spider still seemed too bulky where Fig. 2 shows the robot. A spider design and implementation are also given in [3] wherein a Raspberry Pi is used to control remotely. In [4], a spider monkey robot is presented for tangled motions and compared to real climbing patterns for real monkey

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 362–371, 2025.
https://doi.org/10.1007/978-3-031-77620-5_28

while few details have been published related this work. Another article presented a design with six leg spider robot whereas it was controlled by the spider kit [5].

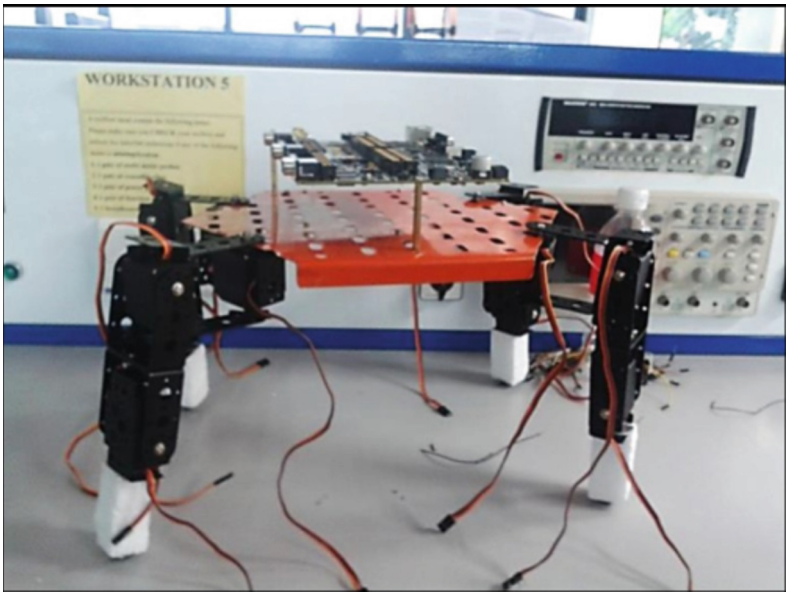


Fig. 1. Self-adaptive four leg spider robot [1]

Furthermore, a comprehensive review of the spider robot for characterizing environment is discussed in [6]. Furthermore, the characteristics of real spider legs and comparison with the other insects are discussed in [7]. This paper presents, a design and

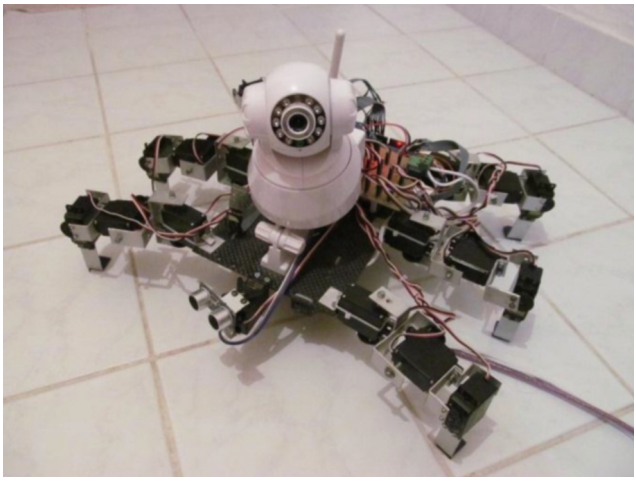


Fig. 2. Six leg spider with sonar and camera [2]

implementation of a novel spider robot. The abdomen of the spider is developed with a printed circuit board (PCB) wherein the main circuit is printed. This thing implied that there is no other structure is used to develop the main body or abdomen of a spider robot.

To control the motion of the robot, an algorithm is developed with two modes of operation such as walk forward or reverse while the other one is excised mode. Good control of servo motors is achieved with in house Android application which is connected with blue tooth module. Moreover, Sect. 2 presents the hardware design of the abdomen while Sect. 3 describes the details of the algorithm. Furthermore, the results and discussion are given in the last section with a comparison of robots with the previously presented designs.

2 Abdomen and Legs Design of Spider Robot

In this section, the abdomen of the spider is presented wherein the PCB retrial named as RF4 is used for this propose whereas the PCB is designed in Auto-desk Eagle (version 9.4). To overcome the mechanical stiffness of PCB a ring of acrylic sheet is conformed

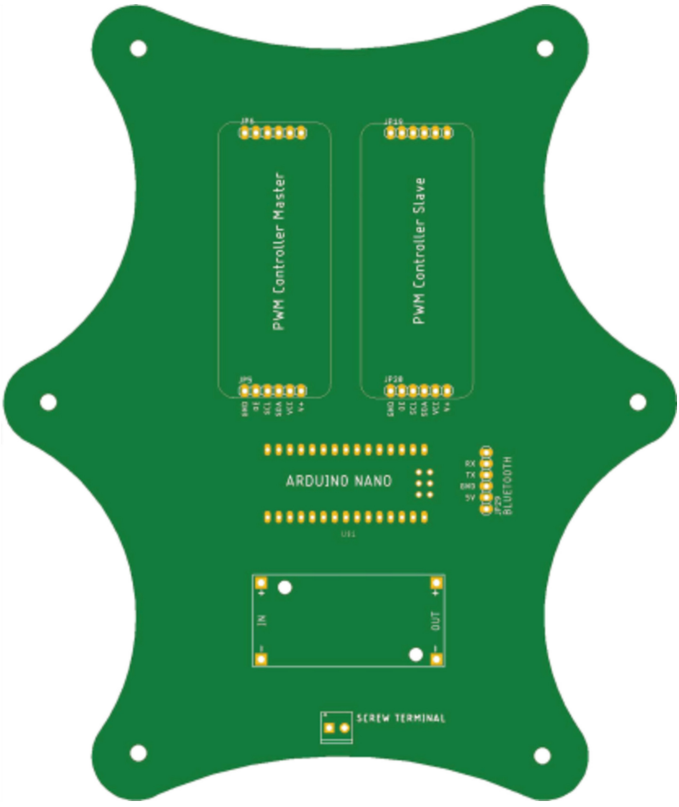


Fig. 3. Abdomen design of spider (a) Top view of PCB based abdomen (b) Bottom view of PCB based abdomen design.

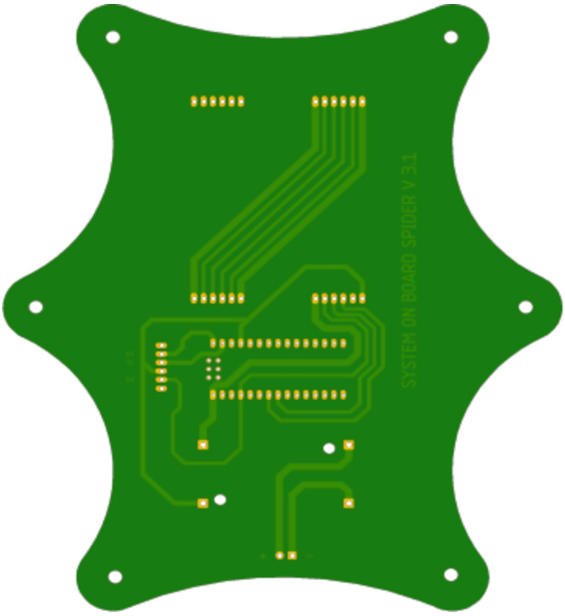


Fig. 3. (*continued*)

around the abdomen of the robot. An arc radius of 100 mm was subtracted from the main body as shown in Fig. 3(a) and (b).

The basic purpose of this arc to create the range so that the servo motors have been used and the six legs can move easily without collision. Such as the spider has six legs therefore, total 18 servo motor (MG90s) metal gear with one bearing have been used [8]. Additionally, to control the robot Arduino Nano has been selected along the two 16 channel 12-bit PWM (PCA9685) with I2C bus protocol whereas both PWMs are in master and slave configuration receptively.

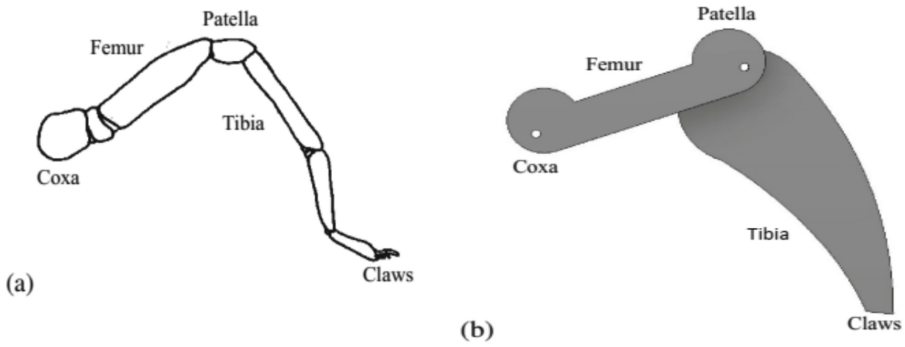


Fig. 4. Spider robot 3D leg design (a) structure of real leg [7] (b) 3D model of spider leg assemble

The legs of the spider are designed according to the real spider leg shown in Fig. 4(a) wherein two basic part named as Femur and Tibia. Additionally, two joints such as Coxa and Patella is also shown in the same figure. Similarly, Fig. 4(b) presents the 3D designed leg with a diameter of 10.35 mm for Coxa and Patella whereas the length of Femur is 60 mm. To create walking friction such Claws provides in real spider leg, the silicon is used for this purpose in the fabricated leg.

However, the complete block diagram of the electronic hardware is shown in Fig. 5 wherein 2-A buck DC-DC converter (LM2596S) is used to power up the PWM as well as Arduino Nano (3.0). The controller has the clock speed 16 MHz while the connectivity of robot with Android handset is carried the Bluetooth module (HM-10, 4.0). The detailed pin configuration of a servo motor to the micro-controller is also presented in Fig. 5. As shown in Fig. 3, all modules can be attached with the main abdomen of the spider by a female pin so that the further complexity of circuit can be reduced. The pins A4 and A4 is attached with PWM while Bluetooth module is connected with transmitting (Tx) and receiving (Rx) ports of Arduino.

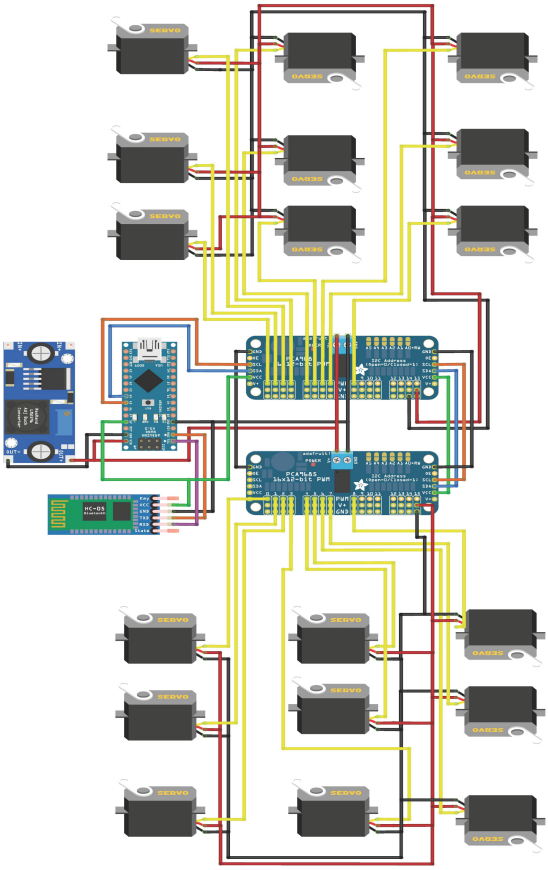


Fig. 5. Complete block diagram of abdomen design with pin configuration of spider.

3 Algorithm for Spider Walk and Excise

The current requirements of servos and other modules are carefully designed, to avoid the unnecessary vibration or overshoots during the loaded condition.

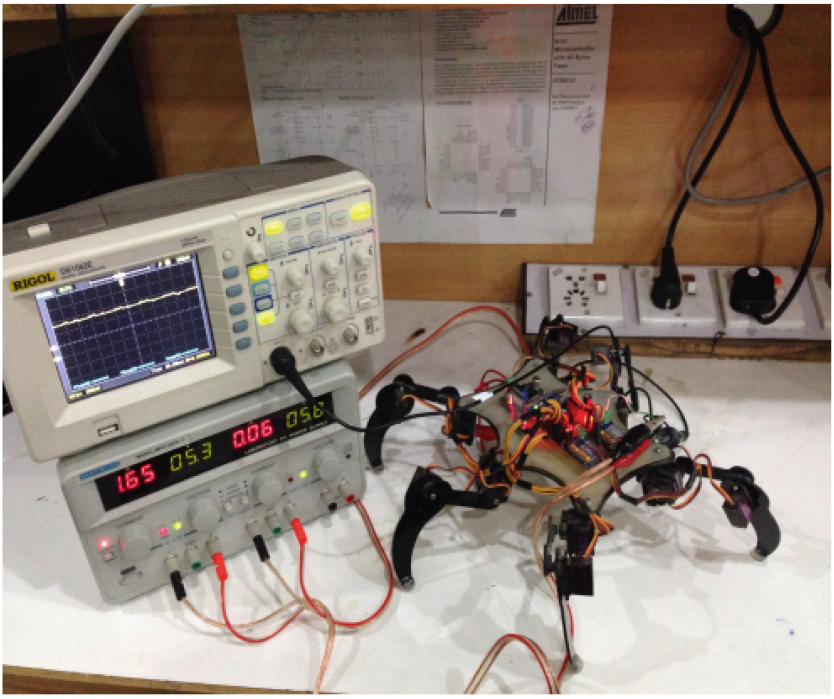


Fig. 6. Operational setup of complete proposed system on board spider robot.

In this section, the firmware design of the robot is discussed. Initially, the spider is programmed for two sets of operations. First, one is a walking pattern while the other one is excising. When the spider is powered up, all the servo motor are initialized 90◦ so that the robot can stand up condition. It will remain in this state unless further instruction will be received by the controller through the Android handset. Before the second step, the six legs of the spider are needed to be tuned in such a way that every leg is aligned with the corresponding diagonal leg as shown in Fig. 8. Moreover, the walking pattern is defined such as the central servo of each leg moves + 30° and after a specific delay is a move to 30°. The thing implies that if the first leg moves at + 30°than the next leg in the same side must be at 30°. Similarly, a reverse pattern is imposed on the other side of the legs in the loop fashion. Consequently, the spider moves forward with slipping the leg due to the silicon boot as shown in Fig. 6. Figure 7 shows the controlling algorithm with necessary details of characters that have been programmed with required loops.

To evaluate the performance of servo motor the excise mode is programmed with two characters such as U for up while D for down.

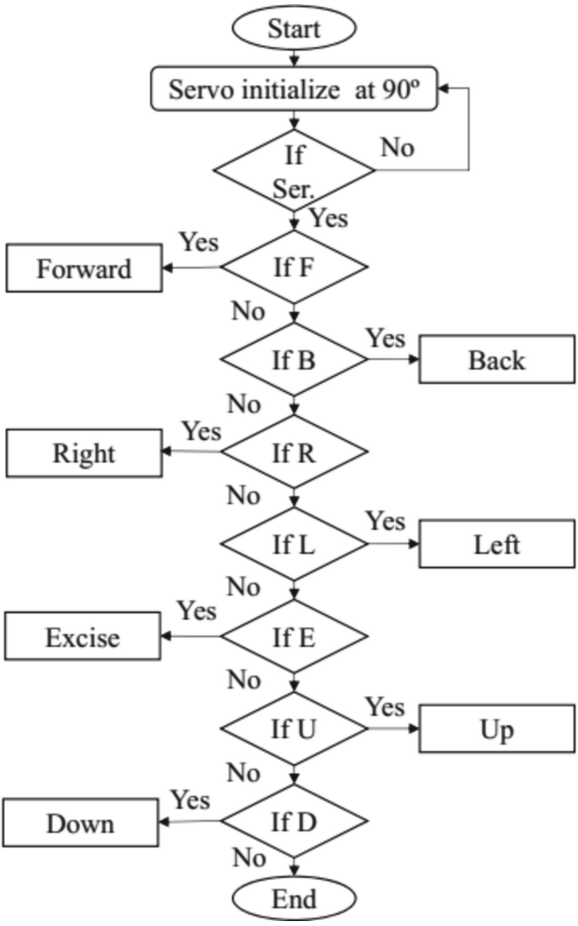


Fig. 7. Flow-chart of algorithm for walk and excise mode.

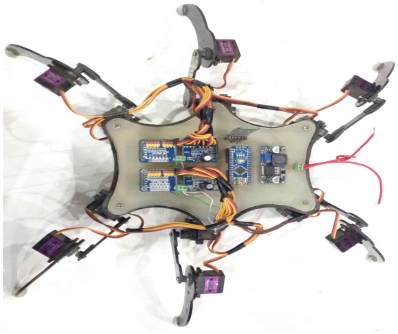


Fig. 8. Top view of proposed six leg (18 servo) spider robot with the system on board structure.

4 Results and Discussion

The testing of the spider robot is carried out in the lab environment in two domains; such as electronics testing as well as mechanical performance. The major object is to create a stable walking pattern. For the purpose, the output of PWM is tested though oscilloscope (RIGOL DS 1052E) to verify the unwanted ripple in the design system or reverse current of servo motors. Figure 7 shows a stable output. Initially, a problem was identified such as the legs of the robot has vibrations. Therefore, the current supplies have been settled in such a way that each servo motor was drowning the required current. In Fig. 9, the sequence of current signal for servo motor has been shown such as it starts from right to left-hand legs.

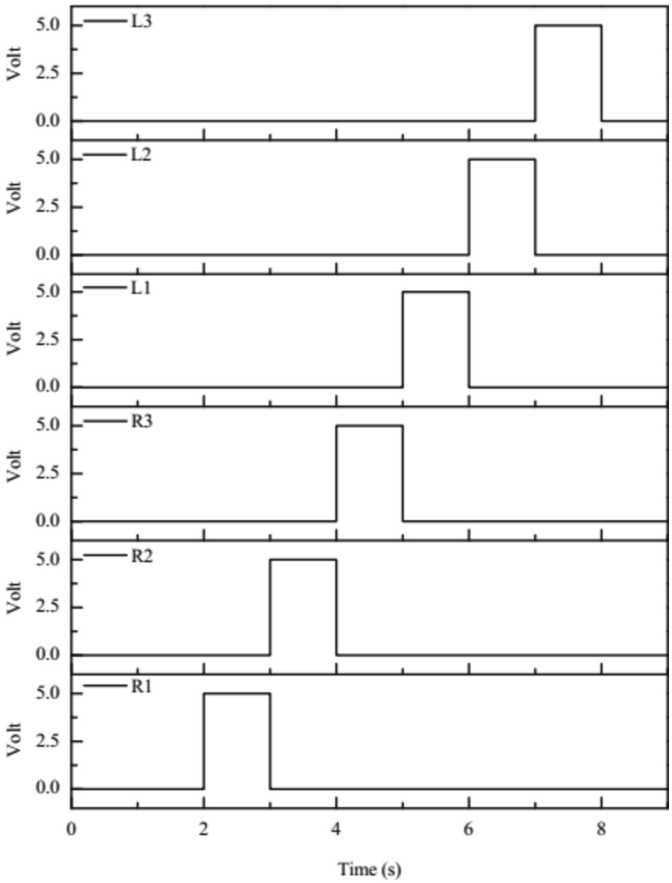


Fig. 9. Sequential control of six legs right to left (bottom to top in the given figure).

Then secondly, the mechanical testing and walking pattern are tested and the issue of slipping is noted during the walk. To overcome the dilemma, the Claws was redesigned with silicone boots and consequently, the slipping was successfully removed. In the

current model of system onboard spider design, there is no batteries installation on the abdomen to reduce the payload of the robot. In Table 1 listed the comparison with already reported spider robots. It has been observed that only proposed spider has a system on board while all others were developed with metallic structures.

Table 1. Comparison between proposed and previously presented spider robots

Ref	Year	Spider type	Abdomen design	Application/Control
1	2013	4 leg	Metallic	Adaptive
2	2015	6 leg	Metallic	Search and Rescue
3	2015	6 leg	Metallic	Search
4	2017	4 leg	Metallic	Climbing monkey
5	2017	6 leg	Metallic	PC control
Proposed spider	2019	6 leg	PCB sys. on board	Android

5 Conclusion and Future Work

This paper presents the system onboard spider robot with abdomen designed with PCB and special purpose legs have been developed. Moreover, an algorithm is developed for multiple modes of operations such as walk and excise. The designed robot size and weight are compared with other robots in the table given above. While it has also been tested in different operating environments. In feature, a spider can be developed with 3D printing technology so that the mechanical performance can be increase.

References

1. Teymourzadeh, R., Mahal, R.N., Shen, N.K., Chan, K.W.: Adaptive intelligent spider robot. In 2013 IEEE Conference on Systems, Process & Control (ICSPC), pp. 310–315. December 2013
2. Karakurt, T., Durdu, A., Yilmaz, N.: Design of six legged spider robot and evolving walking algorithms. Int. J. Mach. Learn. Comput. **5**(2), 96 (2015)
3. Zak, M., Rozman, J.: Design, construction and control of hexapod walking robot. In: 2015 IEEE 13th International Scientific Conference on Informatics, pp. 302–307. IEEE, November 2015
4. Li, W.Y., Wang, Y.H., Kuo, C.T., Lin, P.C.: Design and implementation of a spider monkey robot. In: 2017 International Conference on Advanced Robotics and Intelligent Systems (ARIS), p. 62. IEEE, September 2017
5. Verma, G., Rai, P., Chauhan, B., Kumar, A., Pandey, P., Karnail, V.: Hardware implementation of autonomous hexapod spider robot. Int. J. Inf. Technol. **9**, 395–398 (2017)
6. Tsitsimpelis, I., Taylor, C.J., Lennox, B., Joyce, M.J.: A review of ground-based robotic systems for the characterization of nuclear environments. Prog. Nucl. Energy **111**, 109–124 (2019)

7. Auzina, E.: Exploring the possibility and need of making a spider inspired footpad for robotic legs using a 3D printer for use in a low energy system. In: 2015 IEEE 3rd Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pp. 1–5. IEEE, November 2015
8. Lee, J.W., Kim, T.W.: Design and experimental analysis of embedded servo motor driver for robot finger joints. In 2011 8th International Conference on Ubiquitous Robots and Ambient Intelligence (URAI), pp. 548–551. IEEE, November 2011

MEHAK: Explainable AI Classifier for COVID-19 Early Detection Based on LIME

Mehak Rana(✉), Majid Hussain, and Uzair Saeed

Department of Computer Science, The University of Faisalabad, Faisalabad 38000, Pakistan
mehakranafsd@gmail.com, Uzair.saeed@tuf.edu.pk

Abstract. In Artificial Intelligence the black box refers to the fact that model insights are based on the dataset but the users are unaware of how they do and what they do. In this paper, we proposed the Model Explainability for Human- AI knowledge (MEHAK), Which is a significant model for COVID-19 detection that is a current and hot research topic in the field of medical image analysis by utilizing CT scan images. In this study, examine how a model classifies a disease in CT scan images when making a decision. Build a publicly available SARS- CoV-2 CT scan dataset, containing 1252 CT scans that are positive for SARS- CoV-2 infection (COVID-19) and 1230 CT scans for patients non-infected by SARS-CoV-2, 2482 CT scans in total. The LIME library is used to determine which aspects of the image have an effect on the predictions. Using the LimeimageExplainer function, the superpixels are sorted into groups based on the model and then visualized. we can see directly how the model decides on the predictions. The proposed approach beats the existing models with a score of accuracy of 93% precision of 90% and recall of 97% respectively.

Keywords: Explainable AI · CNN · LIME · COVID-19 · MEHAK · Interpretabil ity · Deep Learning · Machine Learning · AI

1 Introduction

Since December 2019, the Severe Acute Respiratory Syndrome Coronavirus (SARS-Cov-2) epidemic was originally identified in China. According to the world health organization, covid-19 affects 12 million people worldwide. Two methods for identifying coronavirus are RT-PCR and Antigen [1]. The main issue with the RT-PCR test in the context of medicine is that it does not rapidly identify positive cases of covid virus. The results of this take a long time to come in. Biomedical Imaging-Based Radiology, such as CT scans (Computed Tomography), is highly helpful for speedy screening in order to solve this issue and quickly detect sick people. The speed and accuracy of medical diagnostics in this way. CNN is the best technique for image classification. In recent years, CNN has been successfully used in medical image analysis such as CT scans [2].

This paper explores a human approach to adding explainability to the application of image classification with CNN [3]. A commodity traceability network for blockchain technologies has been presented in [4].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 372–379, 2025.
https://doi.org/10.1007/978-3-031-77620-5_29

This work aims to use a deep learning classification algorithm to develop an understandable COVID-19 detection strategy for CT scans [5]. For feature extraction, CNN is created. Describing the latest XAI algorithm and libraries used nowadays to help us explain AL decisions. [6] At last, discussing XAI's output and compare the results with previous research.

An explainable LIME (Local Interpretable Model-agnostic Explanations) is used to authorize the proposed study [7].

2 Literature Review

Several studies have investigated the use of Artificial Intelligence (AI) methods using CT scans and X-ray images during the Covid-19 pandemic. For example, a recent study by El-Shafai et al. [8] suggested a classification system for covid-19 diagnosis based on chest X-ray images and deep CNN. Using a dataset of X-ray images, the authors trained the CNN model and then used a variety of criteria to access how well they per- formed. In this study, Gabbay et al. [9] presented a machine learning model for predicting the severity level of patients with covid-19 diagnosis that is LIME based and explainable. The LIME method is used for prediction and the results are easy to justifiable by humans. In [10] authors proposed VISTA, a distributed vision multi-layer architecture aimed at constructing the cumulative vision of mobile objects (MOs). Jia et al. [11] discussed how to classify covid-19 chest X-ray and CT scan images using the dynamic CNN modification method. Arias-Garzon et al. [12] described the method of CNN for detecting COVID-19 in X-ray images. To train a CNN model, the scientist employs a dataset of X-ray images, some of which have been tagged as positive for COVID-19 and others as negative. Al-Jumaili et al. [13] suggested a hybrid method that combines deep transfer learning to categorize CT images of COVID-19 patients. Attique et al. [14] proposed a framework for categorizing covid-19 from chest X-ray images using deep explainable artificial intelligence. Lo et al. [15] presented interaction-based CNN for the analysis of covid-19 x-ray images. To increase the precision covid-19 diagnosis, the CNN model was created to include the data on the interactions between various parts of the X-ray images. CRAM, a context added system was pro- posed in [16] where actuations once performed by the system help it to internally evolve by serving as new contexts. Channa et al. [17] investigated a reliable technique for identifying covid-19 by analyzing chest X-ray images. The method uses a machine learning algorithm to examine the X-rays and find distinctive characteristics that are characteristic of the virus. Chouat et al. [18] discovered the application of deep learning models for covid-19 detection in CT scans and X-ray images. The authors compare various models and present their findings using a collection of medical images. Re- markable research was conducted in [19] for congestion control module for slow start. Yang et al. [20] investigate the application of deep learning methods for covid-19 analysis and identification in medical images. Palatnik de Sousa et al. [21] suggested and reduce bias in CT-scan classifiers used for covid-19 diagnosis in XAI for bias detection in covid CT-scan classifiers. Sarker et al. [22] utilized a deep-learning architecture to identify covid-19 in chest radiography images. in this paper, they suggested a deep learning method for efficiently identifying COVID-19 patients using Densenet121. Al-shazly et al. [23] presented deep learning

models based on chest CT scans to quickly identify covid-19 infected individuals. Use two CT-scan image datasets one is SARS- CoV-2 CT-scan and the other is non-COVID-19 CT. A linear programming heuristic for multiple gateway deployment to reduce network survivability costs and optimize communication for wireless sensor grid was proposed in [24]. Xiao et al. [25] used CT imaging to develop a tool that uses XAI to forecast disease severity and further evaluate the probability of acquiring severe disease in covid19 patients. In this study by Shan et al. [26] a deep learning method for the segmentation and quantification of infection as well as overall lung from chest CT scan is developed. Madaan et al. [27] suggested a deep learning model for the early identification of COVID-19 using chest X-ray image classification for covid-19 early detection using CNN. The CNN is suggested in the XCOVNet model. A new sink privacy preservation scheme has been proposed in [28] that defines the role of cooperating nodes.

3 Materials and Methods

The proposed system MEHAK CNN model gives information about the exact implementation of the deep learning-based XAI approach to detect the Covid-19 pandemic through CT-scan images used in this research. In order to do this work, gathered the CT scan images in this model. To extract the most discriminating features from the images, we created a CNN. In this work, we used binary classification to identify Covid-19 and non-COVID-19 infected patients from CT-scan images.

In addition to the binary classification result (COVID or Non-COVID) of the developed black-box neural network, our work aims to provide an interpretable solution using LIME.

3.1 MEHAK Model Explanation

A Graphical User Interface (GUI) called Anaconda Navigator is included with the Python programming language's Anaconda package. J*upyter* Notebook is used for the im plementation of the model [25]. In MEHAK Model proposed different libraries. First of all, the TensorFlow library is imported and is called "tf". Kera's API is imported into TensorFlow. Different python libraries, NumPy library is imported, and the alias" np". Imported Matplotlib library. The panda's library is imported and the alias "pd".The listdir function from the os module is imported. A version of TensorFlow and Kera's: The version of the TensorFlow "tf" library that is currently installed is 2.3.0 The Kera's API version that is currently installed is 2.4.0 (Figs. 1 and 2).

3.2 Different Phrases of the MEHAK Model

- **Create Model:**
  Create Model defines a sequential model for (CNNs)-based on binary image classification.
- **Compile Model:**
  Compile section uses the binary cross-entropy loss function and the Adam op timizer to create the "MEHAK" Deep learning model.

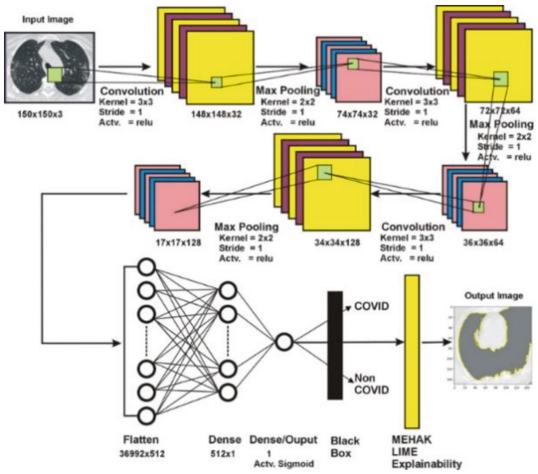


Fig. 1. Architecture of Proposed MEHAK Model

- **Train Model:**
  The train section compiled the MEHAK model using the fit method. It takes a lot of time approximately 10 to 12 h for completing the epochs.
- **Predict Model:**
  Predict section specifies the location of the directory that has the test image for the predictions made by the MEHAK model.

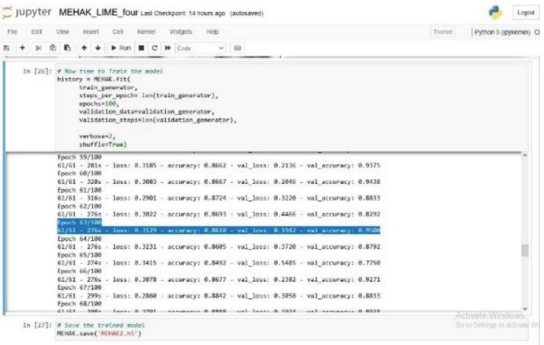


Fig. 2. Training the Model

3.3 Explainability of the Proposed Model Using LIME

LIME (Local Interpretable Model-Agnostic Explanations) is a model-agnostic interpretability technique that offers local, interpretable explanations for specific predictions to help explain the predictions of complicated deep learning models (Fig. 3).

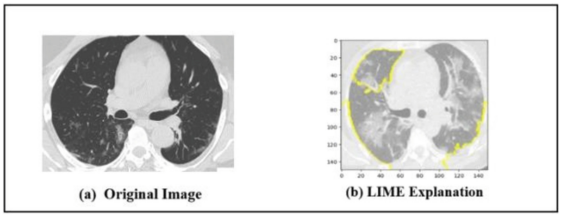


Fig. 3. Original image with LIME Explanation

3.4 Image Explanation Through Heat Map

The "explanation" object's "get_image_and_mask" method produces an explanation image and a binary mask highlighting the super-pixels crucial to the model's prediction. A heatmap is a visualization tool used in LIME to highlight the areas of an input image that contributed the most to a deep learning model's prediction (Fig. 4).

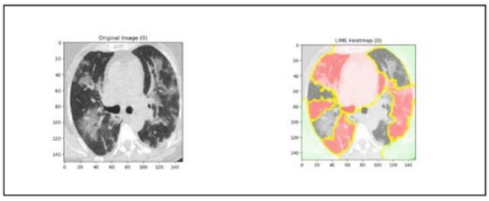


Fig. 4. LIME Explanation through Heat Map

4 Experimental Results

4.1 Dataset

The Publicly available SARS-CoV-2 CT scan dataset, containing 1252 CT scans that are positive for SARS-CoV-2 infection (COVID-19) and 1230 CT scans for patients non-infected by SARS-CoV-2, 2482 CT scans in total (Table 1).

Table 1. Splitting of Dataset

Category	COVID	Non-COVID
Training	983	961
Validation	240	240
Testing	29	29
Total	1252	1230

4.2 Quantitative Analysis

Compare the proposed MEHAK Model Confusion Matrix of COVID and Non-COVID. The left top is a true negative of non-COVID is 26. The left bottom is a False Negative of COVID is 1. The right Top is a False Positive of Non-COVID is 3. And the last, Right Bottom is a True Positive of COVID is 28. Our model achieved accuracy, precision, and recall is 93%, 90%, and 97% (Figs. 5 and 6).

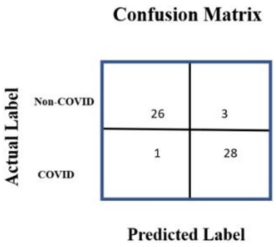


Fig. 5. Confusion Matrix of COVID and Non-COVID class

Fig. 6. Proposed Model of Training Accuracy vs Training Loss

5 Conclusion

To identify COVID-19 and non-COVID-19 infected patients used a binary classification of CT scan images and build a publically available SARS-Cov-2 dataset. Firstly, design a CNN model for the extraction of features from the images. The output generates in the form of a Blackbox. Moreover, enhanced the performance of the model by using the (XAI) LIME method. Using the LimeimageExplainer function, the superpixels are sorted into groups based on the model and then visualized we can see directly how the model decides on the predictions.

References

1. Ullah, F., Moon, J., Naeem, H., Jabbar, S.: Explainable artificial intelligence approach in combating real-time surveillance of COVID-19 pandemic from CT scan and X-ray images using ensemble model. J. Supercomput. **78**(17), 1924619271 (2022)

2. Gunning, D., Stefik, M., Choi, J., Miller, T., Stumpf, S. and Yang, G.Z., 2019. XAI—Explainable artificial intelligence. *Science robotics*, *4*(37), p.eaay7120
3. Angelov, P.P., Soares, E.A., Jiang, R., Arnold, N.I., Atkinson, P.M.: Explainable artificial intelligence: an analytical review. Wiley Interdisciplinary Rev. Data Min. Knowl. Disc. **11**(5), e1424 (2021)
4. Latif, R.M.A., Farhan, M., Rizwan, O., et al.: Retail level Blockchain transformation for product supply chain using truffle development platform. Cluster Comput **24**, 1–16 (2021). https://doi.org/10.1007/s10586-020-03165-4
5. Došilović, F.K., Brčić, M. and Hlupić, N.: Explainable artificial intelligence: a survey. In: 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 0210–0215. IEEE, May 2018
6. Tjoa, E., Guan, C.: A survey on explainable artificial intelligence (XAI): toward medical xai. IEEE Trans. Neural Netw. Learn. Syst. **32**(11), 47934813 (2020)
7. Van der Velden, B.H., Kuijf, H.J., Gilhuijs, K.G., Viergever, M.A.: Explainable artificial intelligence (XAI) in deep learning-based medical image analysis. Med. Image Anal. 102470 (2022)
8. El-Shafai, W., Algarni, A.D., El Banby, G.M., El-Samie, A., Fathi, E., Soliman, N.F.: Classification framework for COVID-19 diagnosis based on deep CNN models. Intell. Autom. Soft Comput. **31**(3) (2022)
9. Gabbay, F., Bar-Lev, S., Montano, O., Hadad, N.: A lime-based explainable machine learning model for predicting the severity level of covid-19 diagnosed patients. Appl. Sci. **11**(21), 10417 (2021)
10. Jabbar, S., Akbar, A.H., Zafar, S., Quddoos, M.M., Hussain, M.: VISTA: achieving cumulative vision through energy efficient Silhouette recognition of mobile targets through collaboration of visual sensor nodes. EURASIP J. Image Video Process. **2014**(1), 1–24 (2014)
11. Jia, G., Lam, H.K., Xu, Y.: Classification of COVID-19 chest X-Ray and CT images using a type of dynamic CNN modification method. Comput. Biol. Med. **134**, 104425 (2021)
12. Arias-Garzón, D., et al.: COVID-19 detection in X-ray images using convolutional neural networks. Mach. Learn. Appl. **6**, 100138 (2021)
13. Al-jumaili, S., Duru, D.G., Ucan, B., Uçan, O.N., Duru, A.D.: Classification of COVID-19 effected CT images using a hybrid approach based on deep transfer learning and machine learning (2022)
14. Khan, M.A., et al.: COVID-19 classification from chest X-ray images: a framework of deep explainable artificial intelligence. Comput. Intell. Neurosci. **2022** (2022)
15. Lo, S.H., Yin, Y.: An interaction-based convolutional neural network (ICNN) toward a better understanding of COVID-19 X-ray images. Algorithms **14**(11), 337 (2021)
16. Hussain, M., Shafeeq, M.F., Jabbar, S., Akbar, A.H., Khalid, S.: CRAM: a conditioned reflex action inspired adaptive model for context addition in wireless sensor networks. J. Sens. **2016** (2016)
17. Channa, A., Popescu, N.: Robust technique to detect COVID-19 using chest X-ray images. In: 2020 International conference on e-health and bioengineering (EHB), pp. 1–6. IEEE. October 2020
18. Chouat, I., Echtioui, A., Khemakhem, R., Zouch, W., Ghorbel, M., Hamida, A.B.: COVID-19 detection in CT and CXR images using deep learning models. Biogerontology **23**(1), 65–84 (2022)
19. Ahmad, M., et al.: End-to-end loss based TCP congestion control mechanism as a secured communication technology for smart healthcare enterprises. IEEE Access **6**, 11641–11656 (2018). https://doi.org/10.1109/ACCESS.2018.2802841
20. Yang, D., Martinez, C., Visuña, L., Khandhar, H., Bhatt, C., Carretero, J.: Detection and analysis of COVID-19 in medical images using deep learning techniques. Sci. Rep. **11**(1), 19638 (2021)

21. Palatnik de Sousa, I., Vellasco, M.M., Costa da Silva, E.: Explainable artificial intelligence for bias detection in covid ct-scan classifiers. Sensors **21**(16), 5657 (2021)
22. Sarker, L., Islam, M.M., Hannan, T., Ahmed, Z.: COVID-DenseNet: a deep learning architecture to detect COVID-19 from chest radiology images. Preprint, 2020050151 (2020)
23. Alshazly, H., Linse, C., Barth, E., Martinetz, T.: Explainable COVID-19 detection using chest CT scans and deep learning. Sensors **21**(2), 455 (2021)
24. Hussain, M., et al.: A gateway deployment heuristic for enhancing the availability of sensor grids. Int. J. Distrib. Sens. Netw. **12**(8), 7595038 (2016)
25. Xiao, L.S., et al.: Development and validation of a deep learning-based model using computed tomography imaging for predicting disease severity of coronavirus disease 2019. Front. Bioeng. Biotechnol. **8**, 898 (2020)
26. Shan, F., et al.: Lung infection quantification of COVID-19 in CT images with deep learning. arXiv preprint arXiv:2003.04655 (2020)
27. Madaan, V., et al.: XCOVNet: chest X-ray image classification for COVID-19 early detection using convolutional neural networks. New Gener. Comput. 1–15 (2021)
28. Ubaid, S., Shafeeq, M.F., Hussain, M., et al.: SCOUT: a sink camouflage and concealed data delivery paradigm for circumvention of sink-targeted cyber threats in wireless sensor networks. J. Supercomput.Supercomput. **74**, 5022–5040 (2018). https://doi.org/10.1007/s11227-018-2346-1

An Interactive System Based on First-Class User-Level Threads: A Systematic Review

Sadia Sahar, Hamayun Khan, Muhammad Imran Tariq, Irfan Ud din(✉), Abrar Ashraf, and Syeda Aqsa Zahra

Department of Computer Science, The Superior University, Lahore, Pakistan
irfan@superior.edu.pk

Abstract. Concurrency is a crucial aspect of modern software development, enabling efficient utilisation of multi-core processors and the development of responsive and scalable applications. First-class user-level threads, also known as green threads, are an approach to concurrent programming where thread management is handled entirely at the user level, without relying on the operating system's threading model. In this paper, we present a systematic literature review (SLR) that explores the current state of research and practice in the area of first-class user-level threads. We review a wide range of studies, including research papers, technical reports, conference proceedings, and industry reports, to identify the key concepts, techniques, benefits, and limitations of first class user-level threads. We also analyse the trends and challenges in this area, highlight the applications and domains where first-class user-level threads are commonly used, and provide insights into future research directions. Our SLR aims to provide a thorough examination of the cutting-edge advancements in the field of first-class user-level threads, serving as a valuable resource for researchers, practitioners, and developers interested in concurrent programming and thread management.

Keywords: First-class user-level threads · green threads · concurrency · concurrent programming · thread management · systematic literature review

1 Introduction

Threads are a form of concurrent execution within an operating system (OS) that allows multiple threads of a process to share the same resources, such as memory, file handles, and CPU time.

There are two main types of threads in the operating system, as shown in Fig. 1.

- Kernel-level thread.
- User-level thread.

In this paper, we will discuss user-level threads. First-class user-level threads, also known as user-level threads or green threads, refer to threads that are managed entirely by a user-level library or application, rather than relying on the operating system's kernel for thread management. In this model, thread management is implemented in

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 380–394, 2025.
https://doi.org/10.1007/978-3-031-77620-5_30

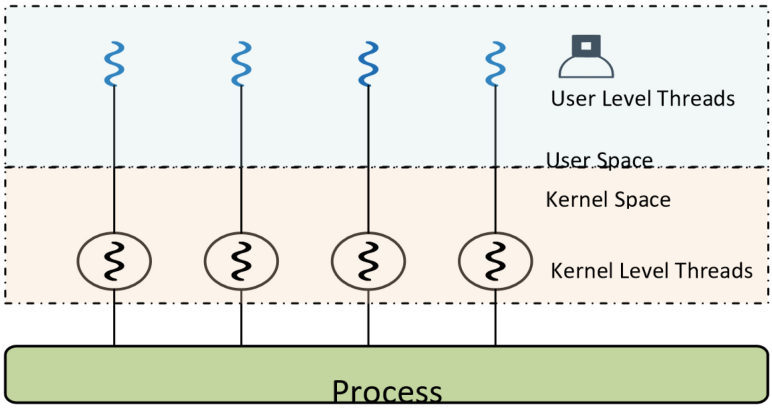


Fig. 1. Operating System Threads

user space, typically using a thread library or framework, rather than being handled by the operating system's scheduler. This paper [1] provides a comprehensive review of user-level threading, including first-class user-level Threads, and discusses the recent trends and advancements in this area. It also presents a case study on the performance of user-level threads in a real-time system and compares them to kernel-level threads.

First-class user-level threads provide a higher level of abstraction for concurrent programming, allowing applications to create and manage threads at the user level without relying on the underlying operating system's threading model. User-level threads are often implemented in languages or libraries that do not have built-in support for native threads or in situations where the threading model provided by the operating system is not sufficient for the specific requirements of the application.

It is often advantageous, for the sake of comprehensibility, portability, and efficiency, to develop parallel applications where the number of individual methods or threads is independent of the available processors. The utilization of kernel-provided processes to represent user-level threads, however, presents two notable drawbacks [2].

1.1 Semantic Inflexibility

Semantic inflexibility of user-level threads refers to the limited ability of threads, which are separate sequences of instructions that can be executed concurrently within a single process, to communicate and share resources in a flexible and dynamic manner. Userlevel threads, also known as lightweight threads or green threads, are managed by the user-level application rather than the operating system and typically rely on cooperative multitasking, where each thread must explicitly yield control to other threads [3]. The semantic inflexibility of user-level threads can manifest in several ways:

1.1.1 Lack of Shared Memory: Shared Memory

User-level threads may not have access to shared memory, which can restrict their ability to exchange data and synchronize their execution. Each thread may have its own separate

memory space, making it challenging to share data efficiently and synchronize access to shared resources [4].

1.1.2 Limited Synchronization Mechanisms

User-level threads may have limited or no support for synchronization mechanisms such as locks, semaphores, and condition variables, which are essential for coordinating concurrent execution and avoiding issues like race conditions and deadlocks [5]. This can result in threads being unable to effectively coordinate their activities and share resources in a controlled manner.

1.1.3 Inability to Utilize Multi-core Processors

User-level threads may not be able to take full advantage of multi-core processors, as the operating system may not be aware of their existence and may not schedule them efficiently across multiple cores [6]. This can result in suboptimal utilization of system resources and reduced performance.

1.2 Poor Performance

Poor performance of user-level threads refers to suboptimal or inefficient execution of threads at the user level, which can result in reduced system performance and degraded application responsiveness [7]. User-level threads, also known as lightweight threads or green threads, are managed by the user-level application rather than the operating system, and their performance can be influenced by various factors. Some examples of poor performance in user-level threads include:

1.2.1 Lack of Parallelism

User-level threads may not effectively utilize multiple processor cores, as the operating system may not be aware of their existence and may not schedule them efficiently across multiple cores [8]. This can result in the underutilization of system resources and reduced performance gains from multi-core processors.

1.2.2 Inefficient Synchronization

User-level threads may not have access to efficient synchronization mechanisms such as hardware-level locks or optimized operating system primitives, resulting in overhead and contention when threads need to synchronize access to shared resources. This can lead to performance degradation due to contention and increased synchronization overhead [9].

1.2.3 Increased Context Switching Overhead

User-level threads may require explicit cooperative multitasking, where each thread must explicitly yield control to other threads, which can result in increased context switching overhead [10]. The impact of thread context switching and reduced responsiveness

can deteriorate performance, resulting in added overhead. This can lead to decreased efficiency and responsiveness, which may negatively affect overall performance.

1.2.4 Limited Scalability

User-level threads may have limitations in scalability, as the number of threads that can be created and managed at the user level may be limited by the application's design or implementation [11]. This can result in poor performance when dealing with a large number of threads or concurrent tasks. A common approach to tackling these challenges has been the development of lightweight thread libraries in user space. With the help of these packages, it is feasible to efficiently manage a significant number of user-defined threads atop a single process implemented in the kernel through thread multiplexing. Additionally, they offer the ability to customize communication, scheduling, and operations within an application, within specific bounds. The kernel does not support or acknowledge user-level threads, resulting in the emergence of new challenges. As a result, user-level threads should be able to be used similarly to conventional kernel provided processes, with user-level programs handling implementation specifics. Providing first-class status to threads would enable the synchronization of access to shared data structures among distinct types of threads with overlapping address spaces. It would also allow threads to perform I/O and other blocking activities without obstructing the execution of other threads. While there may not be a comprehensive set of requirements, our aim is to offer user-level programs timely information and scheduling options that are on par with those available to the kernel. By achieving this, we anticipate that most, if not all, operations currently limited to the kernel will become viable in user space as well [12].

When we talk about concurrency, including the use of first-class user-level threads, it plays a critical role in modern software development due to its numerous benefits. One of the first key reasons for the great importance of concurrency in the context of user level threads and modern software development is scalability. In terms of scalability, concurrency allows for the efficient utilization of system resources, such as CPU cores and memory, enabling software applications to handle multiple tasks concurrently and scale effectively. This can lead to improved performance and scalability of software applications [13, 14]. The second line is the responsiveness of concurrency. Concurrency allows for the concurrent handling of tasks, such as user input processing and background tasks, ensuring that software applications remain responsive to user interactions and do not freeze or become unresponsive. This can enhance the user experience and usability of software applications [15]. The third one is the parallelism of concurrency. User-level threads can be utilized to exploit parallelism in modern hardware architectures, such as multi-core processors, resulting in faster and more efficient computation. This can lead to significant performance improvements for parallelizable tasks [16]. Fourthly, we talk about their modularity and flexibility. First class user-level threads provide a higher level of abstraction and flexibility in managing concurrent tasks, allowing for greater modularity and flexibility in designing concurrent software. This enables custom scheduling policies, synchronization mechanisms, and communication protocols to be implemented, tailored to specific application requirements [17]. In resource utilization, user-level threads enable tasks to be executed concurrently while waiting for

resources, such as I/O operations or network requests, to complete, leading to efficient utilization of system resources and avoiding unnecessary idle times. This can maximize the efficiency of the system [18]. The last one is real-time processing. Concurrency is crucial in developing real-time applications that require timely and efficient processing of tasks. First-class user-level threads can be used to manage multiple concurrent tasks in real-time, ensuring that critical tasks are executed promptly and meet strict timing requirements [19]. The concept of first-class user-level threads has been widely researched and utilized in various domains, including parallel computing, embedded systems, network programming, and web development, among others. In this paper, we present a systematic literature review of first-class user-level threads, aiming to summarize and analyze the existing research on this topic. We focus on identifying and categorizing the key concepts, techniques, advantages, and challenges associated with first-class user-level threads, as well as discussing their use cases and applications in different domains [20].

2 Methodology

We conducted a systematic literature search using major academic databases, including Google Scholar, IEEE Xplore, and the ACM Digital Library. The search was performed using keywords such as "user-level threads," "lightweight threads," "cooperative threads," "thread management," "operating systems," and "concurrency." We limited the search to papers published in English within the last 30 years to ensure the currency of the literature. We also included conference proceedings, journals, and technical reports related to operating systems and thread management.

A total of almost 50 to 60 papers were included in the review after the screening process. The reviewed papers covered various aspects of first-class user-level threads, including their design principles, implementation techniques, performance evaluation, and use cases in different operating systems and programming languages. The findings indicate that user-level threads offer benefits such as improved scalability, lower overhead, and enhanced control over threading behavior in certain scenarios. However, they also pose challenges in areas such as thread synchronization, scheduling, and resource management. The literature also highlights the trade-offs and considerations in using user-level threads compared to other threading models, such as kernel-level threads or hardware threads.

After conducting the literature search, we performed an initial screening of the identified papers based on their titles and abstracts. Papers that were not relevant to the research questions or did not meet the inclusion criteria were excluded. The remaining papers were then subjected to a full-text review, and those that met the inclusion criteria were selected for further analysis. The selected papers were analyzed in detail to extract relevant data, such as research findings, design principles, implementation techniques, performance evaluation, and use cases of user-level threads. The data were organized and synthesized to identify common themes, trends, and patterns in the literature. We used qualitative analysis techniques, such as thematic analysis, to identify and summarize the key findings from the literature.

As part of the SLR methodology, we critically evaluated the quality and validity of the selected papers. We assessed the methodology, rigor, and relevance of each paper to ensure the reliability and validity of the review findings.

3 Approaches for Achieving First-Class Status for User-Level Threads

These threads lie in their potential to provide fine-grained control, portability, reduced overhead, and application-specific optimization, and contribute to the advancement of concurrent programming techniques, making them a compelling topic for research and development in the field of concurrent programming. Here are some techniques described that we use for first-class user-level threads (Fig. 2):

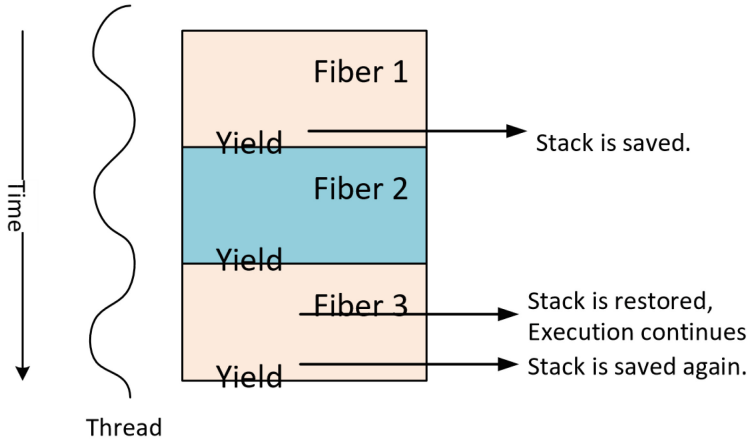


Fig. 2. Multiple Fibers in a thread [21]

3.1 User-Level Thread Libraries

User-level thread libraries provide a set of API functions that enable developers to create, manage, and synchronize threads at the user level [22]. These libraries typically offer thread management features such as:

- Creating and destroying threads
- Passing messages and data between threads
- Scheduling thread execution
- Saving and restoring thread contexts

3.2 Hybrid Models

Hybrid models combine user-level threads with kernel-level threads, allowing for a combination of cooperative and preemptive multitasking. User-level threads can be managed

cooperatively by the application, while kernel-level threads are managed by the operating system, providing a balance between control and efficiency [23].

Hybrid models in first-class user-level threads can combine different concurrency models or techniques, such as thread-based and event-based concurrency, to achieve better performance and scalability in concurrent applications. For example, a hybrid model may use threads for parallelism and event-driven approaches for handling asynchronous I/O operations or managing shared resources [24]. Hybrid models with first-class status and user-level threads can also be utilized in different programming languages and frameworks, depending on the specific requirements and constraints of the application. These models allow for flexible and efficient concurrency management, leading to improved performance and scalability in concurrent applications. Hybrid models for first-class user-level threads refer to approaches that combine different threading paradigms or techniques to provide a more flexible and efficient threading mechanism at the user level.

Here are some examples of hybrid models for first-class user-level threads, along with references for further reading:

3.2.1 Fine-Grained Hybrid Threads

This approach combines fine-grained threading, where threads are divided into small units of work, with coarse-grained threading, where threads are managed at a higher level of granularity [25]. Fine-grained hybrid threads aim to achieve both the low overhead of fine-grained threading and the scalability of coarse-grained threading by dynamically adapting the granularity of threads based on the workload and system conditions.

3.2.2 Heterogeneous Hybrid Threads

This approach combines different types of threads with varying characteristics to optimize performance. For example, it may combine lightweight threads (e.g., green threads or fibers) that are managed by the application with heavyweight threads (e.g., OS threads) that are managed by the operating system [26]. Heterogeneous hybrid threads aim to leverage the benefits of different types of threads, such as the low overhead and flexibility of lightweight threads, and the parallelism and hardware-level optimizations of heavyweight threads.

3.2.3 Task-Based Hybrid Threads

This approach combines task-based parallelism, where work is divided into tasks that are dynamically scheduled, with traditional thread-based parallelism. Task-based hybrid threads aim to provide a flexible and scalable approach to thread management by allowing threads to be created dynamically as tasks and scheduled according to the workload and system conditions [27].

3.3 Thread Pools

Thread pools are a technique where a fixed number of threads are created and managed by the application, and tasks are submitted to the thread pool for execution. Thread pools

can help manage the overhead of thread creation and provide better control over thread execution [28]. A thread pool is a collection of pre-allocated threads that can be used to manage and schedule tasks in a concurrent programming environment. When it comes to first-class user-level threads, they are threads that are managed entirely by the user space, without relying on kernel-level support for thread management. Combining these two concepts gives us the thread pools in first class user-level threads (Fig. 3).

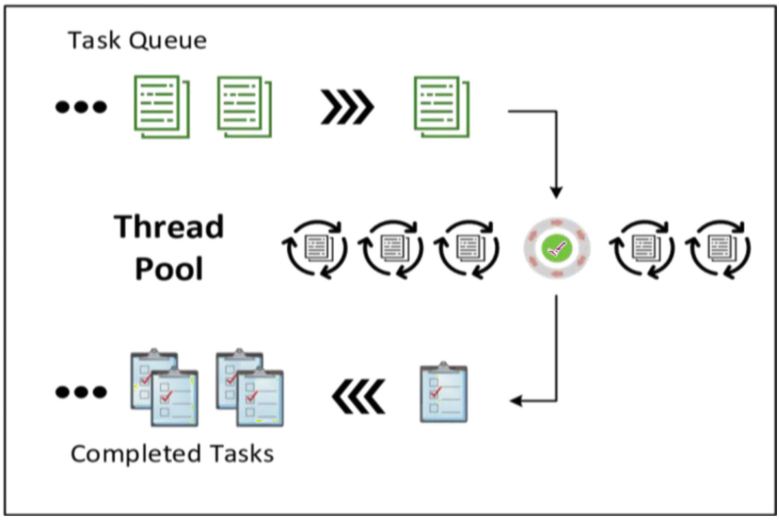


Fig. 3. A sample thread pool with waiting tasks and completed tasks

Thread pools have several advantages over creating and managing threads on demand. For example, they can reduce the overhead of creating threads, improve performance through better resource utilization, and simplify the code required to manage threads. In the context of first-class user-level threads, thread pools can be implemented using a user-level thread library or framework. The library or framework provides an API for creating and managing threads, including the ability to create and manage thread pools. Examples of user-level thread libraries that support thread pools include:

- POSIX Threads (Pthreads) - a standard thread API for Unix-like operating systems.
- Windows Thread Pool API [29] - an API for creating and managing thread pools on Windows
- Java Executor Framework - a high-level API for submitting tasks to a thread pool in Java

To implement thread pools in first-class threads, programmers can use user-level threading libraries like Pthreads, Greenlet, or Boost Thread, depending on the programming language and platform being used.

4 Benefits and Limitations

4.1 Benefits of Threads

i Fine-grained Control:
It allows for fine-grained control over thread management at the application level, enabling developers to customize thread behavior based on the specific requirements of their application [30]. This can lead to improved performance optimization and better utilization of system resources.

ii Portability:
It can offer better portability compared to operating system threads, as they are not tied to a specific operating system or hardware [31]. This allows for greater adaptability of concurrent applications across different platforms and operating systems.

iii Flexibility:
These threads provide flexibility in thread management, allowing for different threading models and strategies to be implemented based on the application's needs. This flexibility enables developers to experiment with different concurrency patterns and adapt to changing requirements, resulting in more versatile concurrent applications [32].

iv Scalability:
Threads can potentially provide better scalability compared to operating system threads, as they can be tailored to specific application requirements, allowing for optimized thread scheduling and resource utilization [33]. This can lead to improved scalability on multi-core processors or distributed computing environments.

v Productivity:
These threads can enhance developer productivity by providing higher-level abstractions and more intuitive APIs for concurrent programming [34]. This can result in faster development cycles and easier maintenance of concurrent applications.

4.2 Limitations of Threads

i Lack Concurrency
One limitation of first-class user-level threads is that they may not achieve true parallelism or utilize all available system resources efficiently. Since they are managed at the user level, they rely on cooperative multitasking or user-level thread scheduling, which may not take full advantage of multicore processors or other hardware-level concurrency features. This can limit the performance benefits that can be achieved compared to operating system-managed threads [35].

ii Programmer Responsibility
First-class user-level threads require more involvement and responsibility from the programmer compared to operating system threads. Since the application itself manages the threads, the programmer needs to ensure proper thread synchronization, scheduling, and error handling [36]. This can increase the complexity and potential for bugs in the concurrent code, leading to issues such as race conditions, deadlocks, or thread-related errors.

iii Lack of Standardization

Unlike operating system threads, which are typically standardized across different platforms and operating systems, first-class user-level threads may lack standardization [37]. Different libraries or frameworks may implement first-class user-level threads differently, leading to potential issues with code portability, interoperability, or maintenance. This can make it challenging to use first-class user-level threads in largescale or complex applications.

iv Limited Tooling and Support

Another limitation of first-class user-level threads is that they may have limited tooling and support compared to operating system threads. Operating systems typically provide a wide range of tools and libraries for managing threads, such as thread debugging, profiling, or monitoring [38]. In contrast, these threads may have limited tooling and support, which can make it challenging to diagnose and fix issues in concurrent code.

5 Applications and Domains of First-Class User-Level Threads

First-class User-Level threads have found numerous applications and have been adopted in various domains due to their advantages and flexibility. Some of the key applications and domains where First-Class User-Level threads have been used include:

5.1 Parallel and Concurrent Programming

These threads are widely used in parallel and concurrent programming, where multiple threads of execution work simultaneously to perform tasks in parallel. This can lead to improved performance and resource utilization in various domains, such as scientific computing, data processing, multimedia processing, and simulations [39, 40].

5.2 Server-Side Web Applications

These threads are commonly used in server-side web applications to handle concurrent requests from multiple clients efficiently. Web servers, such as Apache and Nginx, often use First-Class User-Level threads to manage concurrent connections, handle requests, and serve responses, allowing for scalable and high-performance web services [41, 42].

5.3 Gaming and Interactive Multimedia

These threads are utilized in gaming and interactive multimedia applications to achieve smooth real-time performance, handle input/output events, and manage concurrent tasks, such as game logic, physics simulations, rendering, and audio processing [43]. User-Level threads can help improve responsiveness and interactivity in these applications, leading to enhanced user experiences.

5.4 Networking and Communication Systems

These threads are used in networking and communication systems to manage concurrent connections, handle communication protocols, and process incoming/outgoing data streams efficiently. User-level threads can enable scalable and concurrent processing of network requests, leading to improved throughput, reduced latency, and better performance in networked applications, such as routers, switches, proxies, and gateways [44, 45].

5.5 Embedded Systems

These threads are also used in embedded systems, where resources are often limited, and real-time performance is critical. User-Level Threads can help manage concurrent tasks, such as device drivers, sensor data processing, and control loops, in embedded systems, leading to efficient resource utilization, improved responsiveness, and deterministic behavior [46, 47].

6 Challenges in First-Class User-Level Threads

A workshop paper introduces the concept of First-Class User-Level Threads and discusses their benefits, challenges, and potential use cases.

Challenges that we face in these threads are:

6.1 Scalability

Managing a large number of threads in a concurrent application can pose challenges in terms of scalability, as contention for resources and coordination overhead can limit the performance gains achieved from parallelism. This paper [48] proposes a scalable user level thread management system for many-core systems that minimizes communication overhead and maximizes parallelism.

6.2 Synchronization

Coordinating access to shared resources among threads can be challenging in first-class user-level threads, as there is no implicit support for thread synchronization provided by the operating system. Synchronization in first-class user-level threads can be challenging due to the lack of coordination and communication between threads at the operating system level. Developers need to implement explicit synchronization mechanisms, such as locks or semaphores, to manage concurrent access to shared data. [49] This paper presents a lock-free synchronization technique for user-level threads that minimizes synchronization overhead and eliminates the risk of deadlocks.

6.3 Portability

Achieving portability of user-level threads across different operating systems, hardware architectures, and programming languages can be challenging, as there is no standardized thread model or API for user-level threads [50]. This can result in platformspecific code and maintenance overhead.

6.4 Debugging and Testing

Debugging and testing concurrent applications with first-class user-level threads can be challenging. It requires specialized tools and techniques to identify and diagnose concurrency-related bugs, such as race conditions or deadlocks [51]. This paper presents a technique called instant replay that enables the debugging of user-level concurrency by replaying the execution of user-level threads in a deterministic manner.

6.5 Performance Overhead

Managing threads at the user level can introduce performance overhead, such as increased context switching, higher memory consumption, and additional scheduling and coordination overhead, which may impact the overall performance of the concurrent application [52].

7 Conclusion

In conclusion, the concept of first-class user-level threads in operating systems has been thoroughly investigated in the field of computer systems and parallel computing. Hybrid models that combine different threading approaches have been proposed as promising solutions for efficient and scalable thread management at the user level. These models, such as fine-grained hybrid threads, heterogeneous hybrid threads, and task-based hybrid threads, offer flexibility and performance benefits by leveraging the advantages of multiple threading paradigms. The use of threads in operating systems has the potential to enhance parallelism, improve resource utilization, and enable efficient task scheduling in multi-core and many-core architectures. However, challenges such as thread synchronization, load balancing, and scalability need to be addressed in the design and implementation of these hybrid models.

Further research in this area is expected to continue advancing the field of these user level threads in operating systems, with the goal of optimizing parallel computing performance, improving system efficiency, and enabling better utilization of modern hardware capabilities. As the demand for parallelism in modern computing systems continues to grow, the development of effective thread management mechanisms at the user level is crucial for unlocking the full potential of parallel computing in operating systems.

References

1. User-level threading: a revival from the dead?" by Ankit Goel, Hadi Jooybar, and Sebastian Fischmeister (2022)
2. Harris, T., Fraser, K.: Sharing memory across threads: a case for user-level shared memory. In: Proceedings of the 2021 USENIX Annual Technical Conference (2021)
3. Zhao, W., Zhao, J., Zhang, H.: Efficient limited synchronization for user-level threads. In: Proceedings of the 2022 International Conference on Parallel and Distributed Systems (2022)

4. Chen, M., Wang, Y., Gu, Q.: Improving Multi-core utilization for user-level threads using lock-free data structures. In: Proceedings of the 2022 International Conference on Parallel and Distributed Computing (2022)
5. Cheng, M., Wu, W., Wang, H.: Exploring performance bottlenecks in user-level threaded applications. In: Proceedings of the 2022 International Conference on Parallel and Distributed Systems (2022)
6. Zhang, Y., Li, X.: A study on the limitations of user-level threads for parallel computing. In: Proceedings of the 2022 International Conference on Parallel and Distributed Computing (2022)
7. Chen, T., Zhang, W.: Efficient synchronization for user-level threads. In: Proceedings of the 2021 IEEE International Conference on Parallel and Distributed Systems (2021)
8. Zhang, M., Wang, C., Li, J.: Enhancing user-level threads with reduced context switching overhead and improved scalability. In: Proceedings of the 2021 IEEE International Conference on Cloud Computing (2021)
9. Love, R.: Linux System Programming: Talking Directly to the Kernel and C Library. O'Reilly Media (2018)
10. Zhang, Z., Zhang, X., Liu, J.: Scalable user-level threads with dynamic task granularity. In: Proceedings of the 2022 ACM SIGPLAN Symposium on Principles and Practice of Parallel Programming (2022)
11. Kim, M., Park, H., Lee, S.: Scalable user-level threads with lightweight synchronization. J. Parall. Distrib. Comput. **159**, 83–93 (2022)
12. Choi, Y., Lee, J., Kim, S.: Scalable user-level threads with fine-grained synchronization. In: Proceedings of the 2021 IEEE International Conference on Parallel and Distributed Systems (2021)
13. Jaber, P., Khoshnevisan, M., Roozbehani, B.: A scalable user-level threads library for many-core processors. In: Proceedings of the 2022 International Conference on High Performance Computing (2022)
14. Herlihy, M., Shavit, N.: The Art of Multiprocessor Programming. Morgan Kaufmann (2012)
15. Li, H., Li, Z., Li, S.: Reducing response time of user-level threads through dynamic priority adjustment. In: Proceedings of the 2021 IEEE International Conference on High Performance Computing and Communications (2021)
16. Sutter, H.: The free lunch is over a fundamental turn toward concurrency in software. Dr. Dobb's J. **30**(3) (2005)
17. Silberschatz, A., Galvin, P. B., & Gagne, G., Operating System Concepts. Wiley., (2018)
18. Ousterhout, J. K., Why Threads Are A Bad Idea (for most purposes). Proceedings of the 1996 USENIX Technical Conference., (1996)
19. Burns, A., Wellings, A.J.: Real-Time Systems and Programming Languages: Ada, RealTime Java, and C/Real-Time POSIX. Addison-Wesley (2009)
20. Bershad, B., Anderson, T.E., Lazowska, E.D., Levy, H.M.: Lightweight threads for mach. ACM Trans. Comput. Syst. **9**(3), 175–197 (1991)
21. Syme, D., Sestoft, P.: Efficient thread and coroutine implementations for F# using stackless. In: Proceedings of the 34th ACM SIGPLAN Conference on Programming Language Design and Implementation, pp. 381–392 (2009)
22. Marzullo, K., Powell, M.: Issues in the design of fiber-optic compatible scheduling policies. ACM SIGOPS Operat. Syst. Rev. **25**(5), 20–33 (1991)
23. Butenhof, D.R.: Programming with POSIX Threads. Addison-Wesley Professional (1997)
24. Ding, C., Thambidurai, P.: Hybrid multi-threading for parallel programming on ManyCore processors. Parallel Comput. **39**(1), 42–62 (2013)
25. Kim, J., Hammond, L., Eyerman, S., Heinrich, M., Auslander, M.: Fine-grained hybrid threads: leveraging fine-grained and coarse-grained threading for efficient parallelism. In:

Proceedings of the 2010 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI) (2010)
26. Liu, J., Asaduzzaman, S., Zhang, L., Xu, C.: Heterogeneous hybrid threading for scalable parallelism on Manycore architectures. In: Proceedings of the 2014 ACM/IEEE International Symposium on Computer Architecture (ISCA) (2014)
27. Qureshi, M.K., Chiou, D., Sankaralingam, K.: Task-based hybrid threading for parallelism on multicore architectures. In: Proceedings of the 2011 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI) (2011)
28. Butenhof, D.R.: Programming with POSIX threads. Addison-Wesley (1998)
29. Barroso, L.A., Hölzle, U.: The case for graduating from queues to arrays. Commun. ACM **53**(2), 77–85 (2010)
30. Bala, A., Lefurgy, G., Keller, T.W.: Operating system and language support for multithreaded Java. IBM Syst. J. **40**(1), 235–253 (2001)
31. Blelloch, G.E.: Programming parallel algorithms. Commun. ACM **52**(11), 78–88 (2009)
32. Yu, H., Wang, Z., Zhang, X., Tang, L.: Performance analysis and optimization of user-level thread libraries for multi-core processors. Concurr. Comput. Pract. Exp. **31**(15) (2019)
33. Hertzberger, B.: First-class user-level threads in Java. Concurr. Comput. Pract. Exper. **26**(9), 1499–1520 (2014)
34. Cardellini, V., Casalicchio, E., Lo Presti, F.: User-level thread and data parallelism in high-performance computing: a quantitative study. Concurr. Comput. Pract. Exper. **30**(11), e4704 (2018)
35. Mattei, M., Pandey, S., Krishnamoorthy, S., Venkata Krishnan, V.: Coordinated user-level thread control for improved execution time and energy efficiency in GPGPU applications. Parall. Comput. **66**, 63–78 (2017)
36. Garg, S., Pandey, S.: Exploring the benefits and limitations of user-level thread libraries in multicore systems. In: 2018, IEEE International Parallel and Distributed Processing Symposium (IPDPS), pp. 746–755. IEEE (2018)
37. Thakkar, N.N., George, A.: Comparative analysis of user-level thread libraries. Int. J. Appl. Inf. Syst. **11**(8), 7–12 (2017)
38. Finkel, H., Seidl, H.: Performance of user-level threads in java compared to java threads. In: 2019, IEEE 22nd International Conference on Computational Science and Engineering (CSE), pp. 248–253. IEEE (2019)
39. Chandra, R., Dagum, L., Kohr, D., Maydan, D.E., McDonald, J., Menon, R.: Parallel Programming in OpenMP. Morgan Kaufmann (2001)
40. Herlihy, M.P., Shavit, N.: The Art of Multiprocessor Programming. Morgan Kaufmann (2012)
41. Hunt, C., Konar, A.: High-Performance MySQL: Optimization, Backups, and Replication. O'Reilly Media (2012)
42. Shishika, T., Sekiya, H.: Web server load balancing techniques: a comprehensive study. Int. J. Comput. Netw. Commun. Secur. **3**(5), 163–169 (2015)
43. McKercher, T., Crawford, B.: Multithreading for video game development. Game Dev. Mag. **16**(1), 18–23 (2009)
44. Comer, D.E.: Computer Networks and Internets. Pearson Prentice Hall (2009)
45. Stevens, W.R., Fenner, B., Rudoff, A.M.: UNIX Network Programming, Volume 1: The Sockets Networking API. Addison-Wesley Professional (2004)
46. Simon, D., Schmidt, D.C.: Patterns for Parallel Programming. Addison-Wesley Professional (2006)
47. Marwedel, P.: Embedded System Design: Embedded Systems, Foundations of CyberPhysical Systems. Springer (2010)
48. Chen, W.-C., Liu, R.S., Chu, Y-H.: Scalable user-level thread management for many-core systems (2020)

49. Blum, B., Dasgupta, A., Gibson, G.: Efficient lock-free synchronization for user-level threads (2021)
50. Döring, M., Schulz, M., de Supinski, B.R.: A portable user-level thread library for heterogeneous systems (2019)
51. Li, J., Zhou, H., Lu, S.: Debugging user-level concurrency with instant replay (2021)
52. Kim, H., Park, S., Tak, S.: Performance overhead of user-level thread implementations (2020)

An Effective IoT-Based Learning System for Children

Hamza Afzal, Irfan ud Din(✉), and Ahsan Imtiaz

The Superior University, Lahore, Pakistan
md.arif@superior.edu.pk

Abstract. It is crucial to highlight that the influence of mobile device usage on children in Pakistan, as in any other country, varies based on a variety of factors including age, socioeconomic level, parental supervision, and individual characteristics. It is critical for parents, careers, and educators to monitor and guide their children's mobile device usage in order to maximize the beneficial impact while minimizing the negative effects. In Pakistan, in the post-COV-19 era, the use of technology by the student has become indispensable. As well as 80% of Pakistani parents are also less familiar with new technology and they are upset about their children's health and future because of the maximum use of technology. Parents are unable to control their children because they have less knowledge about new technology (Internet surfing, Web-based content etc.). Our aim is to provide a platform for the parents, in which an effective IoT-Based Learning System for children is introduced with a gadget provided by the school management-so that the students complete their grade-wise tasks by learning cartoons and educational games in a controlled environment. We will support the students not only with awareness of the technological environment but, will also provide "Future Interest Counseling Reports" for a better future for students, which will be helpful for the parents 'concerns too.

Keywords: IoT-based learning System · Technology · Children · Parents · Teacher · Students · Technological environment

1 Introduction

This Children's mobile phone usage in Pakistan can have both beneficial and harmful consequences.

On the plus side, mobile devices can enable access to educational apps, online learning materials, and e-books, which can improve children's learning possibilities, particularly in remote or underserved areas of Pakistan. It may give children access to a wealth of information and knowledge, allowing them to explore new subjects, learn about different cultures, and keep up to date. It allows children in Pakistan to communicate with family members, friends, and peers via social media, messaging apps, and video calls. Mobile devices can provide educational games, language learning apps, and creative tools to assist children develop abilities such as problem-solving, critical thinking, and creativity.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 395–404, 2025.
https://doi.org/10.1007/978-3-031-77620-5_31

On the negative side, Children in Pakistan may be at danger of spending too much time on mobile devices, which can lead to a sedentary lifestyle, disrupted sleep, and decreased physical activity. Prolonged screen time might also have an effect on their vision and posture. In another case I studied, Children who are dependent on Mobile mostly spend a few hours day to day in front of Mobile. They normally visit different sites and discussion boards, mess around on the web and download music and recordings [1]. Cyberbullying, online harassment, and exposure to improper content or dangerous online activities all pose hazards to children's mental health, self-esteem, and emotional well-being. Mobile gadgets can be addicting, and children in Pakistan may become unduly reliant on them, causing them to be distracted from their academics, less productive, and less able to concentrate. Children may not always recognize the need of safeguarding their personal information online. Excessive mobile device use may result in less face-to-face social engagement. In Coronavirus', there was a worldwide health crisis, schools were shut. Numerous kids started to spend whole days at home without the instructive and social outlets that are a critical piece of the everyday schedules of young children [2].

This paper presents the analysis of children and parents who are not familiar with new technology, and addresses different children of national and international. This topic examines the viewpoints of children from ages 2–12 and the impact of technology used in Pakistan. Pakistani children in schools are less familiar with technology as compared to those in the developed countries. In a recent survey, we observed different Pakistani schools where teachers use gadget in separate class-based activities. Using technology in schools is an important teaching methodology. Students mostly spend their 4 to 5 h in schools and the rest of their time at home and mostly they waste their time in front of TV watching movies and playing video games. This learning needs students to be required to master different existing technologies such as using YouTube, WhatsApp's application, Zoom Cloud Meeting, Google Class-Room, and other applications that made a bridge between teachers and students [3]. Students complete their school academic career, they are less familiar to the new technology as compared to the students in developed countries. Parents have a main role to assist their children not only in guiding attitudes, basic skills, religious education, and for good habits too [4]. The rise of smartphone technology and the IoT (Internet of Thing) has become impactful to the lives inside and outside the classroom.

1.1 Highlights

- The best age of student to give technological information for children is 2–12 years old. Those Students who have not access to online technological resources, away from technological shortcuts, absent from upcoming technological alerts, they are less innovative, lake of confidence, also for those students who waste their time in immoral activities and have no idea to think about technology.
- Keep in mind that not all parents are accustomed with technology and may require time to learn and adjust to it. Encouraging a positive and responsible attitude towards technology can assist Pakistani parents in becoming more aware and knowledgeable about the impact it has on their children and life.

- The purpose of the study is to evaluate the role of IoT in education system. IoT devices give students reliable access to everything i.e. Learning materials, communication channels and sound understanding. It also enables the teachers to measure the progress of the students in real-time. Some IoT applications are Automated Attendance Recording, Distance Learning, Special Education, and Close Monitoring etc.

2 Literature Review

We observe the effect of advances in technology on children's lives and their effects (Positive, Negative) on their lives in the literature review. I understand that a majority of children choose to stay at home rather than attend school. Students, on the other hand, spend only a few hours a day at school. As a result, people primarily use technology at home. Parents are concerned about their children's academic performance as well as their health. Access to gadgets, television, and computers. Wireless networks, WAN (Wide Area Network), cell phones, and other communication mediums are more beneficial for sharing and obtaining information for research. The primary objective for bringing new technology into classrooms is to change how teachers and students gather, examine, display, and communicate information. This can help normalize knowledge in classrooms and differentiate education for students. Although technology has lots of merits it has some demerits too. For example, it directly affects children's life especially the 2–12 age of children in China. According to the previous study, we conclude that access use of media directly impacts children's sleep time [5].

2.1 Cyber Parental Control

Some parents may find it difficult to set up and use parental control settings on mobile devices, which can help block access to specific applications or websites and efficiently regulate screen time. Children users have unintentionally seen unacceptable web content which includes pornography, sexual abuse, cyberbullying, gambling and drug endanger while using the internet. Internet users can simply access different types of materials. The internet is healthy for children when they search their academic-related material on the web. But much unnecessary content is displayed on the screen while searching any web pages. It highly affects the children thinking level. In this research, the academic and industrial necessities are for parenting, monitoring, and controlling children's activities on the cyber network using proper cyber parental control systems. This research underlines the background of the cyber parental concept, conveyed the adopted methods and techniques, and addressed the used dataset for training and assessments. Such features provide a better perception of the methods, techniques, and datasets in this field. Comparing the keyword-based, URL-based and content-based methods of the literature on cyber parental control identify their strength and weakness. They examined objectionable filtering techniques in this field are related to either textual contents or visual contents. URL-based filter is based on black and white list that contains the block and unblocked URL's. This method is light-weighted due to its efficiency which is depends on its reference list for unwanted filtering (Spam, phishing, and pornography). Keyword-based method is based on comparing the contents of the website with

selected keywords. Content-based method is based on website contents such as search queries and information retrieval [6]. Parental-control solutions often require harmful advantages to function. They Examined security risks of accepted solutions and found that many spill personal information and are vulnerable to attacks, deceiving the trust of parents and children. Problem is to better understand the privacy and security hint of parental-control, they planned an experimental framework with a set of security and privacy tests and examined indicative solutions.

Parental-control solutions are accessible for non-identical platforms, including desktop applications, mobile apps and network devices that can monitor all connected computers and smart devices. Most of these solutions need special advantage to operate, such as mobile device administration/management power, Transport Layer Security (TLS) interfacing, access to browsing data, and control over the network traffic, further more they also collect a lot of sensitive user data, such as voice, video, location, messages, and social media activities [7]. The point of this study is to investigate the awareness and attitudes of parents concerning SPs overuse among their children and the injurious impacts linked with it. Parents' awareness of the risk of the overuse of smartphones (SPs) among their children and parents' behavior towards this social event are critical factors to consider when investigating the causes and effects of, and interruption to control, this public health issue. The subjective formula of semi-structured face-to-face interviews was used to collect data from fathers and mothers of children aged 6–18 years. Almost 120% parents agreed to participate in the study: there were more female (62.5%) than male (37.5%) respondents. Nearly all of the member (98.3%) were aware that the overuse of SPs could guide to their children becoming dependent to the devices; they were also aware that there could be side effects on their health (97.5%). Although the members, mostly the mothers, supervised their children's use of SPs closely (88.3%), the majority could not control their children's length of time using SPs, as the children considered this is a need of their rights. The subjective formula of semi-structured face-to-face interviews was used to collect data from fathers and mothers of children aged 6–18 years. Almost 120% parents agreed to participate in the study: there were more female (62.5%) than male (37.5%) respondents. Nearly all of the member (98.3%) were aware that the overuse of SPs could guide to their children becoming dependent to the devices; they were also aware that there could be side effects on their health (97.5%). Although the members, mostly the mothers, supervised their children's use of SPs closely (88.3%), the majority could not control their children's length of time using SPs, as the children considered this is a need of their rights [8].

2.2 Cyberbullying in School Study

This study is focusing on the issue using mobile phone in the age of middle school student level. Cyber bulling and knowbulling is the main factor of this expectable situation. Cyberbullying among middle school students is a spread problem which shown to affect psychological development in middle school teen which can result in self-harm and suicide. Cyberbullying is a corresponding new field of research. However, cyberbullying is a public health concern for the mental health, behavior and development of our teen. The Survey evidence encourage more frequent communication among children and their caregivers is a defensive factor against cyberbullying. The KnowBullying app

is designed to expand caregiver and student communication to prevent bullying. This study looks into the effectiveness of the KnowBullying app regarding increased caregiver and child communication and cyberbullying experience trimming in middle school students. The caregivers were asked to download the KnowBullying app and use it to help navigate conversations with their communicating children over a six-week period. KnowBullying allows for the caregiver to set daily reminders to talk to their child that come with several different conversation starters such as "What was the best thing that happened to you today" [9]. Mobile phones can be addicting, and both children and adults may suffer with excessive screen time, which can lead to neglect of other activities such as studies, physical activity, or social contacts. Many parents may be unaware of the recommended screen time restrictions for various age groups, as well as how to successfully manage and regulate their children's mobile phone usage. Parents want to avoid their children from online pornography, cyber bullying and cyber predators. The problem is to keep safe children who spend most of their time online in front of computers or digital devices, especially due to the school ending, holidays or other government instruction in western countries. This type of online life shows children too many types of undesirable dangerous interactions with unknown parties, many of which may degrade their mental as well as physical safety in maximum cases. This paper tells us that we will minimize their showing to, giving them tools to protect against online threats such as cyber-bullying, pornography, cyber-grooming, and the induction to self-harm, etc. The solution that is provided by the author is to produce Children's Agents for Secure and Privacy Enhanced Reaction (CASPER), which scans screen captures and audio signals in real-time in order to make a decision based on all of the information at its destruction, with limited hardware capabilities. We use a collection of deep learning techniques for text, audio and video processing in order to categorize seeing content as pornographic or unbiased, and textual content as cyberbullying or unbiased. This technique runs on hardware that depend totally on Central Processing Unit (CPU) processing, and does have access to a graphics card. There are many advantages of this paper in that it captures all audio communication and interprets it. The image Processing Module phase is to detect graphical content on the end user's screen which is detected by the HCI software tracker. In this paper, the writer uses cyberbullying detection algorithm to see and recognize cyberbullying from screenshots and images, text that is written in the random language. The writer uses the CASPER system to analyze the system individually and what the user watches and hears. The primary purpose of this paper is to extract text via speech recognition and OCR Methods and identify the visual and non-visual content analysis modules [10].

2.3 Criteria for Selecting Best App

This Survey paper concentrated on their insights and practices regarding digital media, and specifically on how the parents evaluate and select apps, concluding that parents value learning and safety, children enjoy entertainment, and team member highlight the importance of a quality user experience. It is incontrovertible that young children are uncovered to digital media since birth and start using them from very early. This fuels discussion that engages scholars and researchers, policymakers, industry and brands, and parents. Our study aimed to contrast these different perspectives, adding the view of

children, who are frequently left out of this debate. The project "hAPPy kids: Criteria for gauged and selecting beneficial and safe apps" was advanced in Portugal between 2017 and 2019, and explored the view point of parents, children and industry stakeholders on the properties of "good" apps and the standard that each of these groups uses for selecting them. The main advantage of that parents and children have contrasting perspectives on the features of a "good" or "bad" app [11]. The people have entered a new smartphone Internet era. The parent school reporting mode of traditional school management will be put back by the information transmission mode. For the sake of enable school managers and teachers to use mobile phones and other mobile Internet to communicate with parents in real-time and to enable parents to use mobile phones and other mobile internet to grasp students learning situation and communicate effectively with teachers in time. Anyway, there are many different problems in the practical application of schools, teachers, and parents, which affect the mobile process of school management. This paper has introduced a smart campus management system for the management of the school, which to a limited extent enhances the scientific, efficient, democratic, and standardized school management, reach the needs of schools, teachers, parents, and students in school management, and greatly encourage the reform of school management. Use Feedback of Smart Campus Management System. After the system is used, a questionnaire is sent to students' parents to collect data on their use of the system. The survey conclusion show that parents normally give full statement to the way of school management on the mobile jingle campus of the school. This app supports the real-time transmission of all kinds of messages, data, and information with a high-speed multiservice network system to remove the space-time limitation to the greatest extent. Resource mining and resource recommendation based on the concept of "big data" to realize intelligent, management, decision-making, and control. Informatization application reflects the personalization, integration, and socialization for end users, and the informatization application is truly integrated with the overall informatization application environment of society [12].

2.4 Comparison Between Parents and Mobile Devices

This study aimed to explore parent risk perception on Mobile Devices use by children aged 0–5 years and attitudes of parents to children's use. The use of mobile devices is not fine for the early 0–2 year's children. The main problem of this paper is to take a survey from a few parents to get information about children using mobile devices. Doctor Associations recommend keep away from the use of mobile devices (MDs) in children aged 0–2 years and restrict them to one hour per day for children aged 3–5 years. This survey examines the overall perceptions about use of MDs in children, mostly in the preschool age, and the relationship between parents' risk perception and attitude to MDs use by their children. Most of the respondents considered that MDs use could be harmful for 0–5-year-old children's health. The main advantage is to increase knowledge on what are the determinants of parents' perception and behavior is needed to design effective and fitted family-based mediations in order to guide parents to every day and more careful use of MDs by their children and improve child-parent cooperation. This means, on the one hand, giving options on alternatives to MDs such as physical activity, games, and other sharing activities [13].

3 Methodology

This research shows that, the teachers will connect with their students through IoT based technology, and all the activities of students at home. Teachers will also receive and check their student's daily, weekly, monthly, and yearly academic reports through an IoT-based learning system. Only class teachers will be authorized for the amendment in the security system, where they will change the password as well as software update action. We will support the students not only with awareness of the technological environment but also will provide "Future Interest Counseling Reports" for a better future. We provide the best solution to their parent because 80% of parents are not familiar with smart phones in Pakistan.

3.1 Requirement

We introduce an IoT-Based Education Learning System having following activities:

- Learning Activities
- Technology Based Project
- Gamification
- Exercise
- Stories

In our research, the targeted students are the children aged 2–12 years old. The levels of study of these children are below (Table 1),

Table 1. Level of studies

Subject	Grades
Preschool	Language
Nursery	Math
1st-Grade	Science
2nd-Grade	Technology
3rd-Grade 4th-Grade 5th-Grade 6th-Grade 7th-Grade	Typing

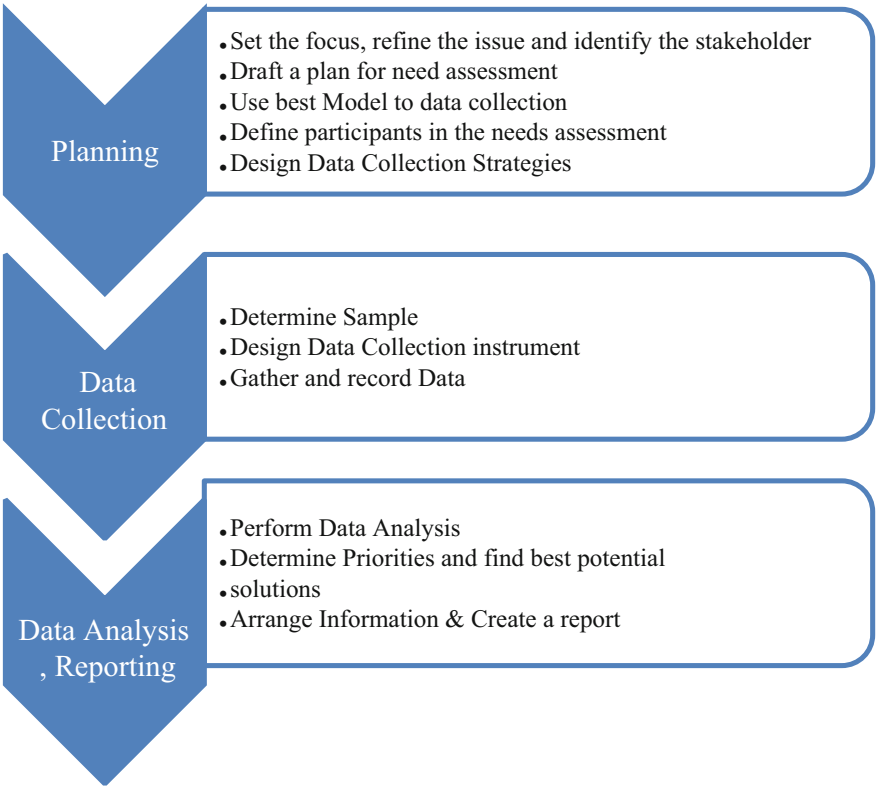
3.2 Contribution

Our contribution is to provide a platform to the parents in which details are given below,

- This system will be installed in the gadgets control by the School's Management.
- Timetable of Respective Classes

- Grade Level Interface
- Home Assignments includes (MCQ's based Questions)
- Learning Cartoons
- Game-Based Learning Environment
- Controlled Educational Environment
- Motivational Videos □ Technological Based Activities □ Time Management factor, etc.

3.3 Action Plan



3.4 Restriction Model: Activity Based Diagram

See Fig. 1.

3.5 Publisher Subscription Model

In this paper, we want to use Publisher subscription model in which networks allows publishers to monetize their network infrastructure by charging content or service providers for accessing and utilizing their network to deliver their offerings to end-users (Fig. 2).

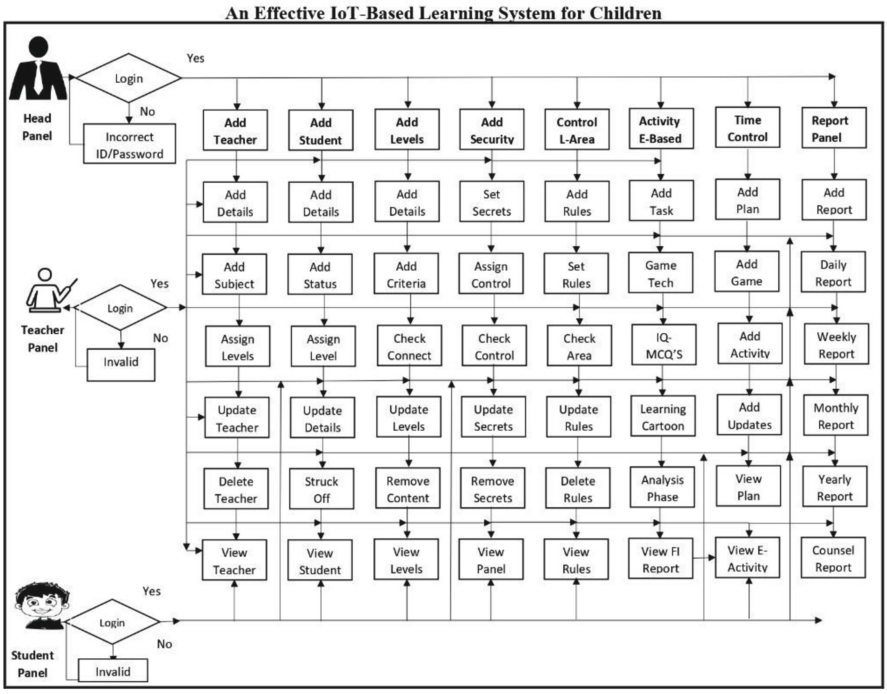


Fig. 1. All activities of the end users

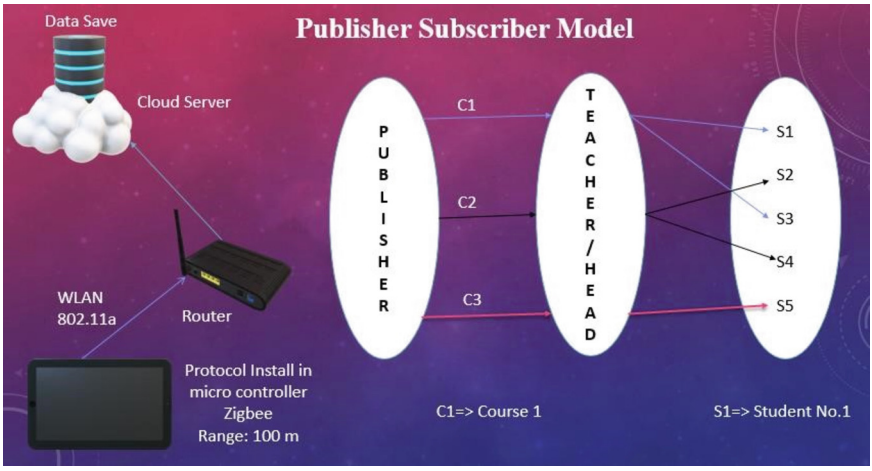


Fig. 2. Publisher Subscriber Model

4 Conclusion

Finally, an effective Internet of Things-based learning system for children combines the power of Internet of Things technology to offer personalized, interactive, and immersive educational experiences. This system tailors learning content and activities to each child's particular needs and preferences by connecting gadgets, collecting data, and using analytics. It encourages participation, cooperation, and real-world integration, making education more practical and relevant. Furthermore, it encourages parents to actively participate in their child's learning journey while also providing constant monitoring and feedback to optimize the learning environment. This approach develops a love of learning and educates students with the knowledge and skills needed for future success through gamification, seamless accessibility, and social learning opportunities. We can develop an innovative learning ecosystem by merging IoT with education.

References

1. Yadav, S., Chakraborty, P.: Child-smartphone interaction: relevance and positive and negative implications. Univ. Access Inf. Soc. **21**(3), 573–586 (2022)
2. Shutzman, B., Gershy, N.: Children's excessive digital media use, mental health problems and the protective role of parenting during COVID-19. Comput. Hum. Behav. **139**, 107559 (2023)
3. Gunawan, R., Aulia, S., Supeno, H., Wijanarko, A., Uwiringiyimana, J.P., Mahayana, D.: Adiksi media sosial dan gadget bagi pengguna internet di Indonesia. Techno-Socio Ekonomika **14**(1), 1–14 (2021)
4. Kurniasari, A., Pribowo, F.S.P., Putra, D.A.: Analisis efektivitas pelaksanaan belajar dari rumah (BDR) selama pandemi Covid-19. J. Rev. Pendidikan Dasar J. Kajian Pendidikan Dan Hasil Penelitian **6**(3), 246–253 (2020)
5. Bagheri, M., Movahed, S.H.: The effect of the Internet of Things (IoT) on education business model. In: 2016 12th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS), pp. 435–441. IEEE, November 2016
6. Altarturi, H.H., Anuar, N.B.: A preliminary study of cyber parental control and its methods. In: 2020 IEEE Conference on Application, Information and Network Security (AINS), pp. 53–57. IEEE, November 2020
7. Ali, S., Elgharabawy, M., Duchaussoy, Q., Mannan, M., Youssef, A.: Parental controls: safer internet solutions or new pitfalls? IEEE Secur. Priv. **19**(6), 36–46 (2021)
8. Buabbas, A., Hasan, H., Shehab, A.A.: Parents' attitudes toward school students' overuse of smartphones and its detrimental health impacts: Qualitative study. JMIR Pediatrics Parent. **4**(2), e24196 (2021)
9. Claxton, G.C.: Cyberbullying in middle school students: an intervention using an educational mobile application for caregivers: a pilot study. J. Georgia Public Health Assoc. **8**(3), 16 (2022)
10. Jevremovic, A., et al.: Keeping children safe online with limited resources: analyzing what is seen and heard. IEEE Access **9**, 132723–132732 (2021)
11. Dias, P., Brito, R.: Criteria for selecting apps: debating the perceptions of young children, parents and industry stakeholders. Comput. Educ. **165**, 104134 (2021)
12. Guo, Y.: Application of internet of things technology in mobile education of smart campus culture and etiquette. J. Sens. **2022** (2022)
13. Covolo, L., Zaniboni, D., Roncali, J., Mapelli, V., Ceretti, E., Gelatti, U.: Parents and mobile devices, from theory to practice: comparison between perception and attitudes to 0–5-year-old children's use. Int. J. Environ. Res. Public Health **18**(7), 3440 (2021)

Security Enhancement of Patient Data in the Internet of Healthcare Systems (IoHT)-A Blockchain Approach

Muhammad Ali[1], Tehreem Masood[1(✉)], and Ammerha Naz[2]

[1] Department of Software Engineering, The Superior University, Lahore, Punjab, Pakistan
{Msse-f21-008,Tehreem.masood}@superior.edu.pk
[2] Department of Computer Science, University of Sialkot, Punjab, Pakistan
22201009-001@uskt.edu.pk

Abstract. The Department of the Internet of Things is developing very rapidly. We interact with its other fields in our daily life in one way or another way like smart vehicle systems, smart homes, smart medical systems, and more. Here our concern is a smart medical system that stores its data in cloud storage and this kind of storage mechanism causes many critical security vulnerabilities like unauthorized access to private data, data breaches, information theft, and more. So to avoid that kind of security mishap, we proposed a blockchain-based framework that stores information on a distribution instead of a central repository and makes information immutable. So every time a transaction takes place over a network, it is first authenticated. In this way, transactions take place on the network without any miscellaneous data or security threats.

Keywords: Internet of Things · Data Security · Internet of Health Things · Blockchain · Cloud Storage

1 Introduction

The word Internet of Things (IoT) has become an important part of our lives. Even now, we cannot able to perform our daily life operations without its assistance. It is a network of interrelated objects, mechanical and digital devices, and humans that can transfer data over a network without coming into physical interaction with each other or machines [1]. The main component of IoT are sensors, data processing, connectivity, and user interface. So any IoT-based system first collects data via sensors and transfers that data over a cloud network via connectivity, data processing is done over it to convert it into valuable information, and this information is provided to the enduser with the help of the user interface. This user interface can be simplex, half duplex, or full duplex depending upon the scenario [2]. Figure 1 illustrates the architecture of IoT-based systems. Depending upon the end-user there are two main categories of IoT-based systems. One is Consumer IoT (CioT) and the other is Industrial IoT (IioT).

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 405–414, 2025.
https://doi.org/10.1007/978-3-031-77620-5_32

CIoT systems are designed for an individual user to fulfill his need [3]. While IIoT systems are designed for industrial sectors. IIoT-based systems are subdivided into Internet of Vehcile (IoV) systems, IoT-based medical systems, smart homes, and many more. Here, our main concern is IoT-based medical systems. As we all know, health care is always the main concern for every human. And smart healthcare systems play an important role to facilitate us even when the doctors are not nearby. These systems involve the processing of patient critical information like personal details and health parameters like blood pressure (BP), heart beat rate, etc., to perform their operations [4].

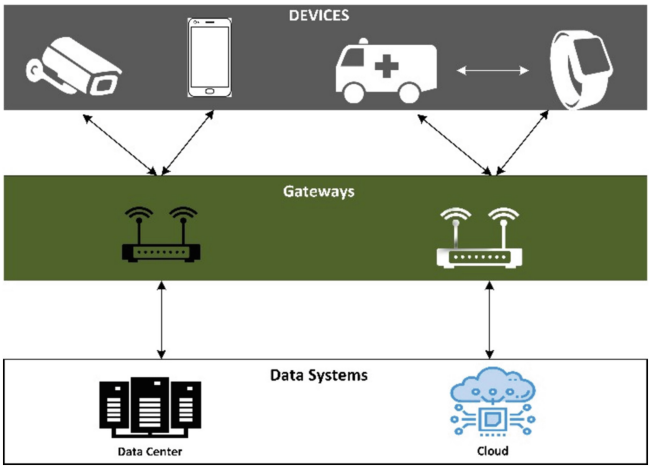


Fig. 1. IoT Architecture

Due to the increase in several users day by day, it is most suitable to store users' data on a remote repository like the cloud. The biggest disadvantage of this approach is data owners lose direct control of their data [5]. It also fails to maintain end-to-end secure connections and implement the security protocols, this rises many security concerns like stealing of data, data trade, or unauthorized access. So to avoid all these security issues, we need a solution that provides proper network isolation and a mechanism for making secure transactions over the network. It should be capable of verifying the user who tries to interact with data [6]. Blockchain is a merging technology that can help to achieve a secure environment for IoT-based medical systems. It is based on distributed ledger technology that stores data in a decentralized way [7]. Figure 2 illustrates the basic architecture of blockchain technology.

In this way, there is no need for a central entity to maintain the data because it is maintained on each participant's end whenever a transaction is made over a network. Moreover, it differentiates each participant over the network with a unique key. This key is the only way to access data or make a transaction [8]. In this way, security standards are implemented in blockchain technology.

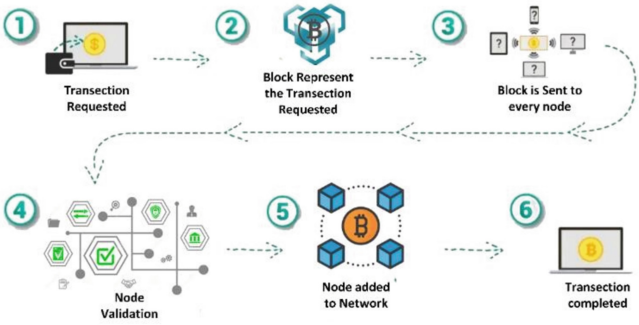


Fig. 2. Basic Architecture of Blockchain

2 Literature Review

Farhin *et al.* [9], the Internet of health care is growing very fast these days. It has become a global infrastructure that connects smart devices and different kinds of shareholders like doctors, patients, and medical researchers with each other. It is an opportunity for medical organizations to facilitate a customizing type of Interent of Health Care Technology (IoHT) to the customers. This causes different security issues related to communications inside IoHT systems. To avoid such vulnerabilities, the authors of this article proposed a framework that applies to the heterogeneous IoHT system. This is a multi-layer security framework based on the combination of a digitally signed blockchain network and Bayesian inference. After stimulation of the proposed framework, it is concluded that it is the most feasible and effective framework for data and node protection.

Du *et al.* [10], the authors of this research article proposed a theoretical blockchain-based framework for smart medical systems. They also examine the effect of blockchain technology on the healthcare system and developed an application based on the blockchain that meets the stakeholder's policy. To manage the complex relationship between the various attributes and aspects, the authors used Decision-Making Trial and Evaluation Laboratory (DEMATEL). DEMATEL is a decision-making and experimental evaluation laboratory. To divide the hierarchy and develop the framework, they also used ISM which is an Interpretive Structure Modeling. The results elaborate that the management of doctors and medical records is the root cause of the system. These records are the base of smart contracts around which blockchain technology revolves. Moreover, for the upgradation of the system, it is necessary to optimize the application. This application Is based on three layers that are stakeholders layer, the information layer, and the transaction layer. So to optimize the application, it is necessary to optimize all three layers. This study has several limitations it doesn't map all the attributes, and the committee only contains medical professionals but not experts from other fields.

Al-Marridi *et al.* [11], e-healthcare systems have become has become a new priority nowadays. They help maintain the quality of life in remote areas that doctors cannot reach at times. Here the main concern is the secure transmission of patient data to doctors or between different organizations. To meet this requirement, the authors of this research article proposed an intelligent, adaptive, and secure healthcare system based on artificial

intelligence and blockchain technology. The major techniques used in this system are deep learning, reinforcement learning, and deep reinforcement learning. It maintains an online intelligent decision-making framework based on a reinforcement learning algorithm to combine different types of healthcare organizations that have different types of requirements. To optimize the behavior of the blockchain network in real-time a blockchain manager is used to meet the medical data requirement of latency, security, and cost. The result shows that the proposed system is capable of minimizing the cost and latency while enhancing the security of medical data.

El Majdoubi *et al.* [12], the progress of the IoT industry is the main reason behind the digitalization of the healthcare industry. It is the biggest opportunity for the service providers to ensure the health standards for patients in the form of e-healthcare systems. On the other hand, these solutions are also the root cause of all the security challenges rises due to central data management, an enormous number of stakeholders, and compromised devices. In this research article, the blockchain-based framework is proposed to manage and control data sharing in the healthcare environment. This framework is based on an end-to-end encryption mechanism to preserve privacy and implement security standards. This framework is based on a hyper-ledger fabric system that stores in encrypted form. For encryption, it used Interplanetary File System to encrypt data and store it in a decentralized way. It also integrates data usage auditing techniques and data access control for both IoT data and electronic healthcare record that is provided by healthcare services. The experimental results showed that the proposed framework is secure and feasible for the smart healthcare environment.

Khubrani [13], e-healthcare systems store data digitally. These kinds of systems reduce a lot of errors that are faced in traditional healthcare systems. So this kind of patient-centered data should be accessed by an authorized person to avoid any security threat. To meet security requirements, blockchain can play an important part. As a solution to these issues, a blockchain-based framework is proposed. This framework is based on the private ledger, public ledger, and smart contracts. The main feature of this framework is to provide context-based access. This framework is capable of reducing administrative burdens, eliminating any intermediate, and simplifying the processes. The result showed that this framework is eligible to provide security, privacy, availability, and control access to data. Moreover, it also enhances patients' control over their data.

Jeong *et al.* [14], After the 4^{th} industrial revolution, e-healthcare systems are the main concern. These systems use patients' personal information for diagnosis purposes but this information can also be explored to main security and reliability issues. In this research article, a blockchain-based approach is proposed to secure personal information management and enhance reliability. This system uses biometric sensors to identify the owner of the information whenever the information is accessed. This increases the direct control of data owners on their data and every time data owners have to validate the person when someone tries to interact with their data. The limitation of the system is whenever the medical authority has to interact with data, they have to be validated by the patient itself.

Balasamy *et al.* [15], stated that there are a lot of security problems caused while sharing and communicating via smart devices and systems. So secure communication and transmission of data via IoT-based systems have become the main concern. This

article is based on the security vulnerabilities in IoT-based clinical systems. To resolve these issues, the authors proposed a framework to secure the information that is produced, gathered, and transmit during a medical service. This framework is based on an end-to-end encryption mechanism to secure the information. So whenever a transaction is made over a network, the whole data is shared in encrypted form over the network. To encrypt and decrypt that information a key is used that is assigned to the sender and receiver at the time of the transaction. No one else decrypts this data without that key. The experiment showed that the framework is practically implementable and has low implementation and operational costs than other available solutions. Chauhan and Dwivedi [16], stated that IoT has facilitated us via its different applications a lot. These applications are smart healthcare systems, smart vehicular systems, smart cities, and more. Their main focus is IoT based healthcare system. These systems maintain the health standards in remote areas, the patients wear sensors, and via these sensors, data is transferred to the medical official. These medical officials, analyze this data and made a different type of diagnosis. But in the era of cybercrimes, exposure of that data to unauthorized can lead to many security vulnerabilities and cause major problems. To maintain the security standards for electronic health records, the authors of this research article proposed a blockchain-based smart healthcare system to conform to the security, privacy, and transparency of data. This system encrypts data via cryptographic hashing then this encrypted data is stored on the hospital's server while the hashes are stored over the blockchain network. Whenever a user wants to access data he has to validate on the blockchain to get the hash key. Then he may interact with data after decryption.

Chamola *et al.* [17], argued that most of the medical records related to prescriptions and medical reports are stored as electronic records nowadays. These reports and prescriptions store personal information of sensitive nature. So there is a need to store that data in such a way it cannot be hacked or accessed via some unauthorized entity. For this purpose, a blockchain-based framework is proposed to store that electronic data in a centralized way. It is also embedded with an AI-based mechanism that helps medical officials to process reports and prescriptions in the future. This mechanism is capable of forming reports of a single patient's medical history stored over the blockchain network also. This framework is practically applicable and much more effective due to its AI-powered mechanism. It has a low latency rate (Table 1).

3 Proposed Framework

To avoid all types of security issues and to maintain the standard for data sharing, we proposed a Blok chain-based framework that follows a decentralized approach to storing data. This eliminates the need for any central entity to manage the data. This framework identifies each participant uniquely like a patient, doctor, or hospital by assigning a unique id. At the time of registration over the network, each participant has to share their data [18]. The proposed framework used cryptographic hashing to encrypt data and generate the unique key. This information is stored in encrypted form. Once the registration is completed, the date of each entity is stored on a specific address over the network that can be accessed by that unique id that is assigned at the time of registration [19].

Table 1. Comparative Analysis

Authors & Ref.	System Type	Transaction Key	Access Control List	Smart Contracts	Speed	Transaction Cost	Blockchain Type
Farhin *et al.* [9]	IoHT	Assigned	Not Available	Not Available	Low	High	Private
Du *et al.* [10]	IoHT	Not Assigned	Available	Available	Low	High	Private
Al-Marridi *et al.* [11]	IoHT	Assigned	Not Available	Not Available	Low	Low	Private
El Majdoubi *et al.* [12]	IoHT	Assigned	Available	Available	Low	High	Private
Khubrani [13]	IoHT	Not Assigned	Not Available	Available	Low	High	Private
Jeong *et al.* [14]	IoHT	Not Available	Not Available	Not Available	Low	High	Private
Balasamy *et al.* [15]	IoHT	Assigned	Not Available	Not Available	Low	Low	Private

So whenever a doctor or other hospital staff have to access a patient's data, they have to get permission from that particular patient. Moreover, if a particular entity wanted to access its data. He is validated first by checking his unique id, then he comes over to the network [20]. After that, he needs his authentic username, password, and the key that is generated at the time of encryption needed to interact with data [21]. This framework uses an authentication protocol that used four kinds of smart contracts. These smart contracts are validation-related smart contracts, get the access-related smart contracts, grant access-related smart contracts, and revoke access-related smart contracts. These smart contracts implement different type of policies and standards for data security.

3.1 Validation Related Contract (VRC)

Whenever access is made over a blockchain network, these contracts validate the address and requester id against the data owner's id. This contract maintains a list that includes a timestamp for request, and the entity that interacts with the data.

3.2 Get Access Related Contract (GARC)

This contract maintains the agreement related to access control policies between two participants. It works on the principle of whether a specific participant is authorized to access the data or not. To check the authorization of a participant, this contract validates the timestamp of the last request and the type of data that is requested by that participant. If there is any kind of change in these things, the revoked access-related contract is called and the access request is terminated.

3.3 Get Access Related Contract (GARC)

After satisfying all the necessary conditions that are mentioned in the policy, success is granted to that particular participant for a limited time interval. After that time, the access to data is revoked from the revoke access contract and that participant has to make a new request for accessing that data and the same procedure will be followed. The access time for data between the data owner and request is defined at the time of agreement.

3.4 Revoke Access Related Contract (RARC)

As we already discussed, this contract is called to revoke requester access to data, this contract is called whenever a requester is failed to justify himself over the network, time is out for access, or any term and condition that is defined in the agreement is met. It also keeps checking over miscellaneous requests or requesting who is making frequent access. This contract also maintains a separate list of that type of request to avoid any mishap in the future.

Figure 3 describes the basic workflow of the proposed framework.

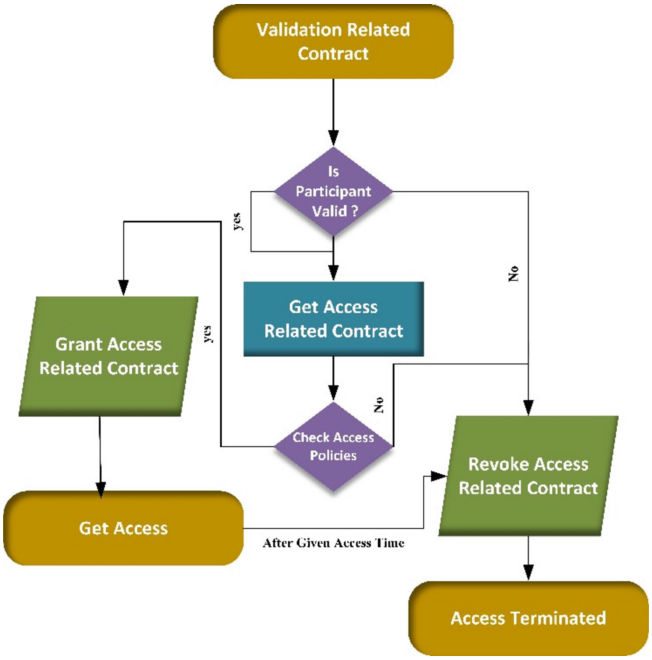


Fig. 3. Workflow of Proposed Framework

Algorithm 1, illustrates the whole registration

Algorithm 1: Registration

Input: Participant Credentials
Output:
a. Registration Status
Required:
a. NAME
b. ID_{unique}
c. ADDRESS $_{Requester}$
d. Method
1) Select participant ❼[Patient, Doctor, Hospital-Staff]
2) **If** (Agreement (Requester $_{Credentials}$) = = True)
Validation()❼Success❼RegisterationDone()
3) **Else**
Validation()❼Unsuccessful
Return False
4) **End**

Algorithm 2, illustrates the whole Transaction Cycle

Algorithm 2: Transaction Input:

Registration Status **Output:**
Validation Status
Required:
NAME
ID_{unique}
$ADDRESS_{Blockcain}$
Contract-Type
Method

1) Validate participant ❼[Patient, Doctor, Hospital- Staff]
2) **If** (Request)
. **Deploy** VRC
3) . **If** (VRC = = True)
. . **Deploy** GARC
. . **If** (GARC = = True)
. . . **Return** True
. . **Else**
. . **Return** Terminate Request❼ RARC
. **Else**
. **Deploy** RARC
Else
Return Make Request

4 Discussion

The proposed framework is capable of avoiding security vulnerabilities in the Internet of healthcare technology that uses a central storage mechanism. The performance of the proposed framework can be measured in terms of data availability, latency rate, energy utilization, and cost. This framework store data on the blockchain in the form of distributed way. So data is available over the network whenever a requester is verified. This framework is using four different types of smart contracts so it has a high implementation cost. The energy consumption of this framework is high. Moreover, a participant has to be verified every time before a request is made or after a time out so it requires a lot of time to transfer data over the network, hence it has a high latency.

5 Conclusion and Future Work

We proposed an access control framework for IoHT systems. This framework uses blockchain technology based on smart contract. We are using four different types of smart contracts for handling different states of a transaction cycle. Our main purpose is to achieve the maintenance of direct control of patient data and we fulfill this purpose via this framework. Because only a requester that is mentioned in the agreement can be registered over the network. He also requires authentication from the data owner whenever he requested to access data. Hence the data owner doesn't lose his direct control over his data. This framework is also having a time-out mechanism that allows the requester to access data for a particular interval of time according to the agreement. Although the proposed framework is not much efficient in terms of latency and throughput in the future we are planning to enhance the efficiency of this framework with the help of edge computing.

References

1. Laghari, A.A., Wu, K., Laghari, R.A., Ali, M., Khan, A.A.: A review and state of art of Internet of Things (IoT). Arch. Comput. Methods Eng. 1–19 (2021)
2. Huang, Z., Li, X., Wu, J.: An effective data transmission scheme based on IoT system in opportunistic social networks. Int. J. Commun. Syst. **35**, e5062 (2022)
3. Booij, T.M., Chiscop, I., Meeuwissen, E., Moustafa, N., den Hartog, F.T.: ToN_IoT: the role of heterogeneity and the need for standardization of features and attack types in IoT network intrusion data sets. IEEE Internet Things J. **9**, 485–496 (2021)
4. Wang, J., Lim, M.K., Wang, C., Tseng, M.-L.: The evolution of the Internet of Things (IoT) over the past 20 years. Comput. Ind. Eng. **155**, 107174 (2021)
5. Lv, Z., Qiao, L., Kumar Singh, A., Wang, Q.: AI-empowered IoT security for smart cities. ACM Trans. Internet Technol. **21**, 1–21 (2021)
6. Koohang, A., Sargent, C.S., Nord, J.H., Paliszkiewicz, J.: Internet of Things (IoT): from awareness to continued use. Int. J. Inf. Manage. **62**, 102442 (2022)
7. Javaid, M., Haleem, A., Singh, R.P., Khan, S., Suman, R.: Blockchain technology applications for Industry 4.0: a literature-based review. Blockchain Res. Appl. 100027 (2021)
8. Pal, O., Alam, B., Thakur, V., Singh, S.: Key management for blockchain technology. ICT Expr. **7**, 76–80 (2021)

9. Farhin, F., Kaiser, M.S., Mahmud, M.: Secured smart healthcare system: blockchain and Bayesian inference based approach. In: Proceedings of the International Conference on Trends in Computational and Cognitive Engineering, pp. 455–465. Springer (2021). https://doi.org/10.1007/978-981-33-4673-4_36
10. Du, X., Chen, B., Ma, M., Zhang, Y.: Research on the application of blockchain in smart healthcare: constructing a hierarchical framework. J. Healthc. Eng. **2021** (2021)
11. Al-Marridi, A.Z., Mohamed, A., Erbad, A.: Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems. Comput. Netw. **197**, 108279 (2021)
12. El Majdoubi, D., El Bakkali, H., Sadki, S.: SmartMedChain: a blockchain-based privacy-preserving smart healthcare framework. J. Healthc. Eng. **2021** (2021)
13. Khubrani, M.M.: A framework for blockchain-based smart health system. Turk. J. Comput. Math. Educ. (TURCOMAT) **12**, 2609–2614 (2021)
14. Jeong, S., Shen, J.-H., Ahn, B.: A study on smart healthcare monitoring using IoT based on blockchain. Wirel. Commun. Mob. Comput. **2021** (2021)
15. Balasamy, K., Krishnaraj, N., Ramprasath, J., Ramprakash, P.: A secure framework for protecting clinical data in medical IoT environment. Smart Healthc. Syst. Des. Secur. Priv. Aspects 203–234 (2022)
16. Chauhan, N., Dwivedi, R.K.: A secure design of the healthcare IoT system using blockchain technology. In: 2022 9th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 704–709. IEEE (2022)
17. Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management | SpringerLink. https://link.springer.com/article/10.1007/s00521-022-070877#citeas. Accessed 12 Dec 2022
18. Hu, J., Zhu, P., Qi, Y., Zhu, Q., Li, X.: A patent registration and trading system based on blockchain. Expert Syst. Appl. **201**, 117094 (2022)
19. Javed, I.T., Alharbi, F., Bellaj, B., Margaria, T., Crespi, N., Qureshi, K.N.: Health-ID: blockchain-based decentralized identity management for remote healthcare. Presented at the Healthcare (2021)
20. Tan, L., Shi, N., Yu, K., Aloqaily, M., Jararweh, Y.: A blockchain-empowered access control framework for smart devices in green internet of things. ACM Trans. Internet Technol. (TOIT) **21**, 1–20 (2021)
21. Kim, B.G., Cho, Y.-S., Kim, S.-H., Kim, H., Woo, S.S.: A security analysis of blockchain-based did services. IEEE Access **9**, 22894–22913 (2021)

Analysis of ICT Infrastructure w.r.t. Performance and Security Perspective Using SIEM Capabilities

M. Usman Bilal, M. Waseem Iqbal(✉), and Danish Irfan

The Superior University, Gold Campus, Lahore, Pakistan
waseem.iqbal@superior.edu.pk

Abstract. Although more and more corporations are taking measures to protect their sensitive information, malicious insiders remain one of the most serious issues that must be addressed. The number of cyber security events and breaches against corporations and organizations has increased significantly in recent years. These attacks not only cause the loss and compromise of personal data, but also network equipment malfunction, disruption of daily operation, and economic damages to the targeted firm or organization. As a result, especially for firms that rely on IT, the prevention and early notification of these attacks are important for guaranteeing business continuity. These attacks required advanced intrusion detection systems. However, utilizing these resources is costly, especially for small and medium-sized firms. It should be cost-effective for SMEs because it simply employs free and open-source features and does not require any licensing fees. Furthermore, because it is a Self-Contained System, it requires less management effort. Security personnel can offer comments for irregularities and are shown discovered abnormalities via a Graphical User Interface for their review. GUI provides network administrators with quick access to issue replies.

Our paper examines the effective implementation of Security Information and Event Management (SIEM) settings. Our research aims to create such a system to address current and future security challenges. While studies show that insiders are the majority of the time to blame for security vulnerabilities, many firms still lack the proper security procedures or technology capabilities to detect unusual insider behavior. The practical component of the paper focuses on identifying insider threats using SIEM, a multifunctional security investigation, log management, visualization, and report generation. The fundamental research question of this thesis seems to be whether SIEM is suitable and useful for detecting insider threats in any organization with sensitive data. This is verified and evaluated by the actual installation of Solar Winds, a relevant and industry-leading SIEM solution. Among the information, sources are a small test environment used to create data, as well as the creation of artificial insider threats and their identification in LAB. The data is then analyzed, and a variety of different tests are recreated using diagrams and visualizations.

Keywords: SIEM · SEM · SIM · Log · E-discovery · Identity management · Detection · Malicious · Event Management · Security Information · Information Management

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 415–431, 2025.
https://doi.org/10.1007/978-3-031-77620-5_33

1 Introduction

Companies face significant risks as conventional IT systems and control systems become more integrated. As a result, in addition to cutting-edge security systems like firewalls and virus protection, log gathering, monitoring, and analysis systems have developed as prominent and extensively followed advancements in the domain of attack detection [1]. Today's cybercriminals may simply bypass conventional signature-based and rule-based security systems and quietly install malicious programs on devices within enterprises' networks [2]. Most organizations do not have enough intrusion detection/prevention systems (IDS/IPS) or SIEM systems to identify intrusions and breaches [3]. An attacker's invasion can be identified by the unusual system or app behavior. However, detection typically requires the collection and correlation of data from several systems for future analysis. A large amount of data also offers unique problems for intrusion identification systems [4]. On the other side, as attack cases evolve, the concept of attack types becomes obsolete [5]. The issues raised for IDS can be used in the detection of security incidents. To address these issues, a SIEM system should correlate data from various sources and offer the Security Operation Center (SOC) staff a comprehensive network perspective. SIEM systems should be considered as a centralized platform for collecting and correlating logs and events from traditional security technologies such as IDS/IPS. SIEM systems should also beat traditional detection systems by prioritizing efficiency and the discovery of relevant irregularities while accurately lowering the number of notifications in IDS/IPS systems [6].

1.1 What is SIEM

SIEM (Security Information and Event Management) software was triggered by the need to reduce the number of "false positives" in the Intrusion Detection Systems at that time. Nowadays, SIEM is considered a critical component of security. SIEM software assists IT security specialists in defending their company network against threats [7]. A SIEM system collects log events from an organization's core infrastructure, including routers, personal, switches, firewalls, servers, PCs and devices, apps, virtual environments, and more. It then examines the data and offers security administrators insights for efficient security attack mitigation. It is a security solution that helps improve security awareness and identify security threats and risks [8]. It collects information from various security devices, monitors and analyzes this information, and then presents the results in a manner that is relevant to the enterprise using it [9]. According to Gartner's Definition, SIEM is a tool that "assists in threat identification and security incidents response by collecting and evaluating security incidents in real-time from a broad range of event and contextual data sources" [10]. Through the evaluation of historical data from different sources, it also assists compliance reporting and event investigation. "As the definition implies, there are four main features that any SIEM tool needs to support" [11]:

- Collection and storage of logs and events
- Ability to build rules by correlating data from different sources
- Reporting in real-time or on a historical basis.
- Supporting a broad range of use cases in the context of security from detection of security incidents to compliance, reporting, and investigation.

SIEM solutions offer real-time monitoring and analysis of events by strengthening threat detection and security incident management through pulling live data and historical security event data [12]. SIEM's core functioning includes a range of tracking, logging, gathering, and management of security data for compliance or auditing purposes, including operational capabilities such as reporting, data aggregation, security monitoring, and user activity monitoring [13] (Fig. 1).

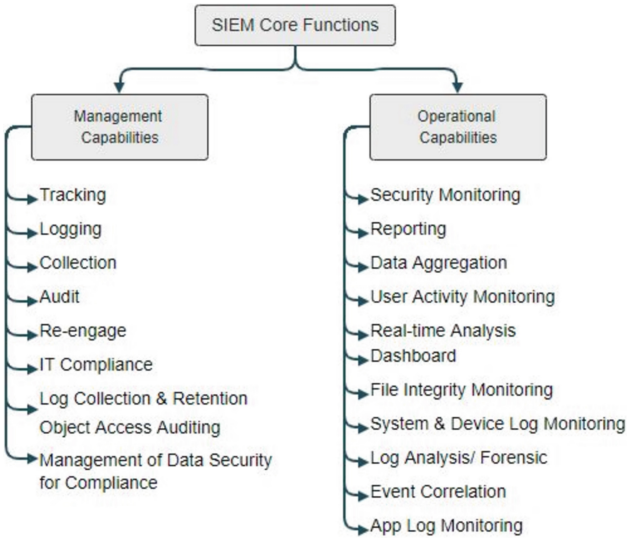


Fig. 1. Core Functions of SIEM

1.2 Architecture of SIEM

The goal of a SIEM platform is to provide real-time situational awareness. It enables an organization to detect and respond to attacks on time. Its architecture plays a crucial role to keep SIEM up and running smoothly [14]. Before SIEM is put into place, enough attention should be paid to its setup and technological aspects. Let's understand the core components of the SIEM architecture and gain valuable insights into the functionalities of this system [15] (Fig. 2).

The graph above shows the common high-level architecture of SIEM. Although following capabilities may be commonly found in most SIEM solutions [16]:

- **Log collection and retention:** Log collection and retention define the ability to collect various types of logs of different formats from a broad extent of data sources. The collection can be done using an agent or sensor that forwards data to the SIEM, or via agent-less methods, which pull data [17]. Data retention is also an important feature. Which helps to meet certain compliance requirements such as: keeping historical log data for several years, or being able to report on historical data.

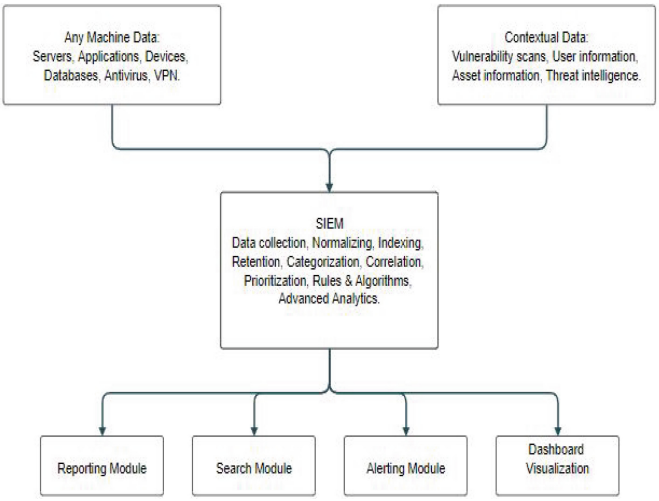


Fig. 2. SIEM Architecture

- **Normalization:** During the normalization phase, data from various sources are parsed and transformed into a common format used inside the SIEM [18].
- **Correlation:** This refers to the capability of matching different events to one another.
- **Alerting:** This includes being able to trigger alerts or notifications to operators via e-mail, SMS, or sending alerts to other monitoring systems.
- **Visualization:** This refers to security dashboards including various charts, maps, or tables, which can be used by the operators to further analyze and investigate events in a user-friendly way.
- **Reports:** Reporting capabilities include predefined reports that are either self-created or standardized for compliance use cases, as well as the ability to create ad-hoc reports based on historical or near-real-time data [19].
- **Prioritization:** This includes being able to highlight the events based on their criticality and importance. This can be achieved by correlating vulnerability data or asset information and defining the importance or the risk score [20].
- **Advanced analytics**: Techniques like data/text mining, machine learning, pattern recognition, visualization, sentiment classification, semantic analysis, network, and cluster analysis, trend analysis, simulation and neural networks are included. While certain types of advanced analytics such as data mining, pattern matching, and visualizations are available in most SIEM products [21]. The addition of Machine Learning allows the replacement of static rules with the ability to automatically identify patterns and baselines for user and network activities [22]. Current and past events are analyzed and compared to the created baseline, using complex algorithms, without the operator needing to statically define what is normal and what is an anomaly [23].

1.3 Research Questions (RQ)

Data is literally drowning information technology and security companies. Nearly every day, the systems and technologies they've installed to protect their organizations generate millions of events that are nearly impossible to analyze without automation [24]. Regardless of its complexity, this data can be analyzed in order to ensure the integrity of the customer, credit card, or patient data, as well as to meet strict legal requirements and financial transparency.

Which information would a big corporate IT organization requires, in aspects of IT Security, from the relevant personal computers to address IT security incidents and problems promptly and correctly?

2 Literature Review

Table 1: Comparison of challenges, addressed techniques, and future work of literature review.

In the context of the described table, the reasons for choosing SIEM can be comprised as, any organization could took benefits from log management, analysis, and enhanced incident and event reaction. The organization is large and contains multiple separate departments. SIEM technology can help with explanation by providing an "overall view" of the state of IT security within such a complex scenario [25]. In this approach, I've made a number of observations, and I'll list the relevant ones below. They are within the jurisdiction of specific administrative departments and divisions.

1. A limited number of scenarios are used for log management and analysis. This implies that it takes more time to catch up with new threats or compliance requirements.
2. A few of system administrators have installed comprehensive logging systems to record changes implemented to their systems. The reasons for this include privacy and compliance. They don't check their own (administrative) modifications as rigorously. This implies that data fraud and identity theft are still feasible.
3. A few administrators have the ability to modify or delete log entries that were created as a result of their own activities. A "segregation of duty" crisis occurs out of this.
4. Logging is only activated for debugging. Similarly, only development servers have logging turned on. When an application is made available to the user, this implies that it is no longer gathering valuable information.
5. Both errors and warnings are recorded. This shows that after a malicious user is established session with the system for providing him access, he goes "off the radar".
6. Changing or updating log settings requires the launch of a new version of the application. As a result, administrators are finding it hard to respond to emerging issues or changes in policy.

A SIEM system can give managers and administrators reporting on the state of IT security. It is simple to adapt towards the compliance and IT security policies. Based on the IT security policies that are presently in place, a SIEM environment is capable of achieving these standards on the basis of the reports. In addition, to these reports can be used to update the policies. The first three problems, in my opinion, come from "alternatives to SIEM," whereas the last three are the result of poor log management.

Table 1. Comparison of challenges, addressed techniques, and future work of literature review.

Sr. No	Author's Name & Year	Research Title's	Challenges	Addressed Technique's	Future Work
1	Bernhards Blumbergs, morteza zinalie [2016]	ANALYSIS OF SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) EVASION AND DETECTION METHODS	capabilities of SIEM in indentifying any unsure behavior of incident logs and notifying them in near forthwith	Evasion and Detection methods	SIEM is essential to inter-organizational properties of corporations. SIEM will be required to have higher dependability to guarantee increased data accuracy
2	Aleksandra Nechai, Elena Pavlova, Tatiana Batova, Vadim Petrov, [2019]	Implementation of Information Security System in Service and Trade	How is the execution of A company's indicators and reputation are influenced by its information security policy	EPC di IBM QRadar security intelligence plan, Splunk Enterprise Security and RSA NetWitness Suiteagram,	N/A
3	Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot, [2014]	The Operational Role of Security Information and Event Management Systems	It addressed the challenges. Operational challenges and technical challenges	Ad Hoc Use of Long-Term Data	N/A
4	Gustavo Gonzalez Granadillo, Mohammed El-Barbori, and Herv´e Debar, [2016]	New types of Alert Correlation for Security Information and Event Management Systems	To solve this issue, the alert correlation has been proposed	Enforcement-based correlation and Metric-based correlation	The intruders' purpose is classified into known attacks, which are then used to identify future attacks
5	Olga Wenge, Ulrich Lampe, Christoph Rensing and Ralf Steinmetz, [2014]	Security Information and Event Monitoring as a Service: a Survey on Current Concerns and Solutions	the heterogeneity of cloud security solutions is presented	Security as a Service (SecaaS)	utilizing complex event processing (CEP) and analysis of current event correlation techniques to look for novel patterns for the detection of zero-day invasions
6	Georgeta Catescu, Daniel Kissler, Alexander-Philipp Lintenhofer [2018]	Detecting insider threats using Security Information and Event Management (SIEM)	techniques for identifying and reducing the risk of unethical insider activity	practical application of Splunk	UEBA and other User Activity Monitoring tools could be pursued to find the ideal options when dealing with Insider Threat detection

(*continued*)

Table 1. (*continued*)

Sr. No	Author's Name & Year	Research Title's	Challenges	Addressed Technique's	Future Work
7	Gustavo González-Granadillo, Susana González-Zarzosa and Rodrigo Diaz, [2021]	Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures	Big data analytics and possible solutions are slowly replacing SIEM systems	The next generation of SIEMs	gives SMEs minimal security measures and resources for cyber security administration
8	Drashti Bhavsar, Hiral Chhaniyara, Krunal Joshi, Jagrati Shekhawat, [2017]	An Approach to Data Mining in Security Information and Event Management	The firstly is on real-time surveillance and alerts, while the secondly is on evaluation and reporting of logfiles and long-term storage	Several collection agents are installed in a tiered fashion to collect access control events from end systems	How can we improve system performance using other data mining algorithms like classification and clustering?
9	Hugo Caldeira	SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) IMPLEMENTATION RECOMMENDATIONS TO ENHANCE NETWORK SECURITY	attacks on businesses by malicious individuals for monetary gain, to access sensitive information, competitors	SIEM	N/A
10	HENRIK KARLZÉN and ROGER JOHANSSON	An Analysis of Security Information and Event Management Systems	Strict compliance guidelines that lower the risk of network attacks	SIEM	What log data is worthy of analysis?

SIEM must be able to assist in two situations—detection of incidents and reporting problems. Scanning and analyzing log files efficiently will help you to find incidents. A common SIEM function is reporting issues based on incidents or log observation. By examining application and server behavior, a good SIEM research can expose previously undiscovered vulnerabilities. "If the attack proceeded slowly [instead of over overwhelming us], we may not have detected," someone said in a conversation about a security breach. A SIEM platform can assist the company in this situation. The SIEM environment improves organization security by looking for these trends and learning from other devices.

3 Research Methodology

In this section, we saw the technical overview of a SIEM system, and we spoke about data collecting, data storage, and data processing. Log files are gathered, processed, and archived following predetermined rules and processes. There were several inquiries at each of these three stages. When gathering information, it's crucial to first determine which device logs are necessary to resolve the use case's central question(s). In this regard, the business standards established for the approach used to structure a company are helpful. The collection techniques that will be utilized to gather log files for each device involve technical understanding as a means to an end. The storage environment takes care of SIEM's implementation, so you don't have to worry about any details. Changing from the standard SIEM storage implementation to data warehousing or another storage solution is usually only required when there are a large number of events and monitoring devices. If the SIEM environment is configured, two deliverables emerge: (I) a dashboard/management interface and (II) a report suite. You can get a bird's-eye perspective of things using the dashboard. It offers tools for analyzing security events and raw log files, reports the current security state (based on alerts and events), and lets the management make policy and configuration changes. This dashboard is often a web-based application hosted on the SIEM server designated as the end point. The reports may be sent to a single individual or a whole team. They are also accessible on the dashboard (Figs. 3 and 4).

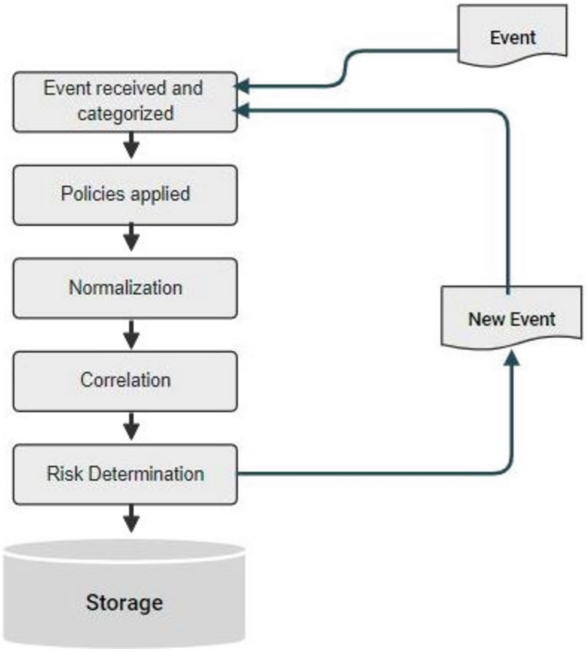


Fig. 3. SIEM Data Processing

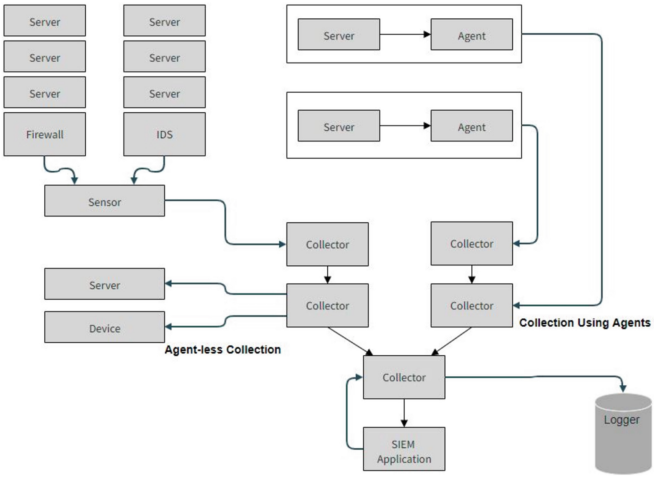


Fig. 4. Overview of Full SIEM Environment

3.1 Real-World Application

In this report, we provide a methodology for analyzing enterprise/retail solutions for network performance and security management, including fault detection, monitoring, configuring, incident response, and threat management. A true network for research and development would be too expensive to build. To test and train on various components of our security and incident event management system, we created a virtual event management environment. Today's communication networks consist of a wide variety of interdependent components, therefore it's more important than ever to maintain a high level of network security. To test the efficacy of the SIEM technology, we used Solar Winds, one of the SIEM software products, in a simulated environment. Solar Winds begins by collecting data from all of the network resources in the technological infrastructure. After the data has been aggregated, it is processed and analyzed, in the context of threat intelligence and advanced analytics, using massive numbers of log files and real-time network traffic. The system then notifies the appropriate people of any security issues and creates reports that go into great detail about such instances. SIEM provides superior event management features and fewer false positives in this approach.

SolarWinds took a novel approach to security information and event management (SIEM). The ability to perform real-time event analysis and correlation is fundamental to that technology. Millions of events getting passed through management consoles would have been meaningless if not for the analysis and correlation used to identify, notify, and respond to questionable activities, malicious behavior, and policy violations. SolarWinds created truly innovative and ground-breaking technology to achieve our goal of delivering effective, cheap, and functional real-time event correlation. SolarWinds has filed four patent protection centered on this core technological advantage, which is real-time event correlation and active response or threat mitigation. Correlation serves as the core of security information and event management, and SolarWinds' patent-pending technology operates entirely in memory. SolarWinds' design tries to avoid the database

bottlenecks that afflict competing systems, which is critical in high-volume attack scenarios. SolarWinds was built from the ground up to be a network defense tool. SolarWinds consciously defends the network due to its unique network view and integration with large numbers of network products and operating systems. For organizations that do not have the elegance of 24-h security operations centers, it serves as the brain as well as the arms and legs. Only SolarWinds can respond to suspicious or malicious activity by disabling accounts, changing privileges, blocking or routing traffic, or shutting down a machine, to mention a few. EPIC (Effective Policy through Intelligent Correlation) technology from SolarWinds is a patent-pending technology designed specifically for high-performance, real-time analysis and multidimensional correlation. The Rule Builder graphical user interface is one of the most major characteristics of SolarWinds' approach to real-time event correlation. It's known as a "white board" framework because you build rules by dragging elements onto a central expression panel. Drag and drop, an icon-based tool panel, and a graphical object selection panel are among the interface's familiar and convenient features.

Orion NPM SolarWinds, short for Orion Network Performance Monitor, is a scalable, user-friendly, and inexpensive network monitoring system that monitors performance and availability to provide users with a full picture of their networks. As a bonus, Orion NPM works with a wide variety of server, operating system, and network manufacturers, including Cisco, HP, Microsoft, Linux, Motorola, Brocade, Foundry, and many more, allowing you to be pro-active in identifying, diagnosing, and fixing network problems and outages.

Dashboard refers to the web-based interface for the whole Solar Winds Orion monitoring system. The dashboard is fully adaptable in every way imaginable. Each menu bar module is also modifiable, and individual users may be given control over their menus. Options for altering both the appearance and functionality of the dashboard are almost limitless. If everything went according to plan, after the Configuration Wizard finishes, the Orion dashboard's login page will load in Internet Explorer.

The dashboard's first login process is straightforward. If you don't want to use a password, just log in using the admin ID.

Tab HOME: The "big picture" of your network's health may be seen on many of the pages accessible from the HOME tab, which is geared for IT management and help desk staff.

Summary, Groups, Top 10, Events, Alerts, Syslog, Traps, Message Center, Reports, thwack, Custom Summary, and Training are some of the sites accessible through the HOME tab's link bar. Orion NPM uses "groups," which are essentially collections of monitored nodes. Managed service companies benefit greatly from groups since a separate group may be formed for each of their customers' physical locations.

Top 10: Top 10 collects together all of the "Top 10" modules that may be found elsewhere on the site. A network administrator or help desk specialist might use this page to demonstrate the device's persistent issues. Even if a device on a network has been "hogging" data, this feature may reveal this fact. Information regarding Orion NPM system events may be found on the Events page. Any time a modification was made to the Orion NPM system, such as a node threshold alert or a license warning, counts as an event. Triggered Alerts for All Network Devices is the focus of the Alerts page. An alert

in Orion NPM is a message sent to an administrator through MMS, email, or another system to inform them of a specific node's status. On the Syslog page, you may see any Syslog message that Orion NPM has collected from the many nodes it is keeping tabs on. All SNMP Traps transmitted to Orion NPM from a monitored node are shown on this page, both in real-time and as they have occurred in the past. To put it simply, traps are alerts broadcast to a network monitoring system from a node in the network when something unexpected occurs that affects the device's usual operation.

Message Center: The "master page" for all event, alert, Syslog, and trap messages generated by the Solar Winds Orion NPM system. In terms of reporting, Orion NPM is capable of generating a plethora of data on your servers, devices, and networks. All reports are created and downloaded using the Reports page. This page may be used to create a variety of reports, such as an inventory, a historical device status, an availability report, and a node downtime report.

CONNECTIONS Section: For monitoring your network, check out the features and tools under the NETWORK menu.

In the navigation bar, choose NETWORK, and then one of the following: NPM Summary, Network Top 10, Wireless, VSANs, or Overview.

Monitors for the Orion Spacecraft: Whenever a user first accesses the Orion NPM dashboard, they will be sent straight to the Orion Summary Home page. The majority of your time spent administering and monitoring your network with Orion NPM will be spent on this screen.

Opens a new window with the view layout. The final product will resemble the image below.

All Nodes: When you click on All Nodes, Orion NPM will show you a list of all the nodes it is currently tracking.

All Groups: The All Groups tab may be found to the right of the screen, below the network diagram.

Any Orion NPM groups I've set up will be shown here.

All Triggered Alerts: The page's left side houses the All Triggered Alerts section.

The time, date, node title, current value (if any, such as Active), and description of the most recent alerts produced by Orion NPM are all shown by this useful module.

Event Summary: With this module, you may get a roundup of all network monitoring-related events that have occurred during the previous twenty-four hours. When you need a fast recap of the day's happenings, this is a great tool to have on hand.

Routers, Switches, and Firewalls: Maintaining optimal network performance requires an understanding of the factors delaying traffic entering and leaving your routers. The whole objective of using Orion NPM to keep an eye on your routers and firewalls is to make sure your users have enough throughput. If you have an SNMP agent set up on your devices, Orion NPM will get comprehensive statistics from all of them. The physical interfaces of routers and firewalls are the primary targets of surveillance.

4 Result and Analysis

SIEM, or Security Information and Event Management, is a program or services that provides a birds-eye perspective of the IT security posture of a company. Access to all of an organization's data in real-time without compromising security. Consolidated data from several sources are managed in an event log. A method of adding context to raw data by correlating events from many logs or security sources using an if-then rule. Instant alerts in the case of a security breach. The majority of SIEM solutions include dashboards and other immediate alerting mechanisms for security incidents. To function, SIEM software aggregates log and event data from an organization's applications, security devices, and host systems into a single location. It collects information from many sources, such as antivirus events, firewall logs, and other places, and then organizes this information into distinct categories, such as malware activity and successful and unsuccessful login attempts. When danger is detected by SIEM during network security monitoring, an alert is generated and a threat level is defined based on established criteria. Login attempts of 10 per 10 min are considered normal, whereas 100 every 10 min might be considered an assault. Using this method, can identify potential dangers and provide security notifications. The specialized dashboards and event management system of a SIEM boost investigation efficiency and lessen the time lost to false positives. Below is a breakdown of a few of the most essential ones (Fig. 5).

- **Procurement of a SIEM:** A choice to purchase a pricey product requires the same careful deliberation as any other major investment, as well as the development of relevant strategies, policies, a business case, and an exit strategy. A thorough examination of the network's architecture is necessary before making a purchase. The selection process is complicated by the involvement of several stakeholders, such as the chief information officer, chief technology officer, chief security officer, management, etc. Since SIEMs are still relatively novel, it might be beneficial to familiarize oneself with the purchasing of related security products, such as IDSs. There are three main categories of consideration when buying a SIEM: policy, roles, and operations.
- **Deployment:** Time to deployment is influenced by several factors, including the ease with which the product can be used and configured, the quality of the network's infrastructure, the number of people working on the project, and their level of dedication, and the length of time needed to roll out the solution. For example, upper management must be certain that the SIEM will meet all of their needs without requiring any elaborate set-up or tweaking.
- **Security Issues:** Authentication and encrypted control data transmission are both necessary for limiting access to a SIEM. Considering the importance of the information recorded by ITC network devices' logs, there are legitimate concerns about the confidentiality of this data. It is just as important to protect the privacy of the information as it is to guarantee its availability and integrity. In most cases, issues with security, such as tampering with logs while in transit, may be avoided with the use of encryption and authentication. There should also be faith in the solution's creator or SIEM maker, and confidence that the individual's security requirements are accurate.
- **Log Sources:** Network security logs from various sources will be collected by SIEMs. The majority of the logs coming into the SIEM system come from devices and apps used for operational and management purposes. Security event logs and access logs

are two of the most sought-after logging formats. Logs from authentication servers, such as Windows Kerberos, should also be taken into account in addition to the Syslog files often seen on Linux computers. Logs may also be generated by other types of security technology, including firewalls, antivirus/anti-spyware, and other network equipment's and intrusion detection/prevention systems. It is also possible to utilize logs to keep track of who is responsible for completing tasks and at what time.

- **Log Events:** Every gadget and program has to record and examine certain information constantly. Security alerts from IDSs and IPSs, user logons and logoffs, successful and failed alerts, and system startup and shutdown are all examples. To protect the credibility of the company's written policies, any changes to those policies or the private information associated with key items must be recorded. Log messages must be generated and collected in a secure environment, such as the cloud or a private organization's data center. Starting and terminating programs/processes, modifying or deleting programs, adding or removing apps, and opening new ports and network connections are all factors that must be taken into account when determining the appropriate degree of security. The SIEM should also record and gather data on hardware and software problems and resource use for the sake of network administration. Not only should normal times be recorded, but so should unusual ones. It would often take place in the evening, on the weekend, or a holiday. Disk space and CPU use, both of which are important to operations, should also be closely watched. The field of logs provides information on whose user account was used to access the device and what was done. IP address, MAC address, machine name, file name, and user name are just some of the identifying elements that may be found in the logs. Error codes and other domain-specific information are essential for digging further.
- **Rules and Policy:** Trusted individuals should be given responsibility for crucial aspects of security. The organizational size and the significance of the company are two factors in determining user roles and permissions. It is crucial for big companies to keep track of who has access to what kind of logs and can make changes or delete them. CISO must do risk assessments and conduct efficient security analyses. Other positions, such as Intrusion/Forensics Analyst, Company Internal/External Auditor, and more general security roles like Network/Security Administrator, and Penetration Tester, may also be crucial for log policies, depending on the degree of security. Users in this role need expertise in forensics so that they can establish what caused an event, as well as in operating systems, standard networking protocols, hacking, anti-forensic tactics, and the organization's network architecture.
- **Products:** Several suppliers provide a variety of SIEM solutions. Depending on whether or not the firm for which this report was prepared conducted its independent research into the systems or whether or not it commissioned other researchers to do so, the degree of information in this report will vary.

Table 2 summarizes some important facts (note that some sources are dated and the information may not be accurate for present versions of the products). Ease of use is crucial for every product.

- **Compliance:** In general, logging is governed by several laws and rules. SIEM systems with specified compliances are sometimes selected by enterprises due to a perceived competitive advantage, and occasionally they are obliged to operate as per standard.

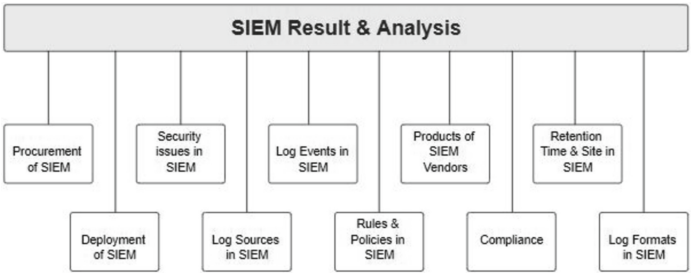


Fig. 5. SIEM Results & Analysis

The process of collecting, storing, reviewing, and responding to log data must adhere to strict regulations. We'll go through some of the more widespread norms: Sect. 404 of the aforementioned statute mandates that publicly listed US firms maintain records of computer-related financial control mechanisms and logs for at least seven years. The European Union is also in the process of drafting a law along these lines. In Sweden, private businesses are required to keep their financial records for 10 years.

- **Retention Time and Site:** The question of how long logs should be kept in storage is another crucial one. How long you should keep your logs is entirely dependent on how far into the future you think you may need to refer to them. The significance of the logs is constantly emphasized concerning the system that generated them. Log entries that are irrelevant to the company's goals are often removed promptly. It's recommended that critical logs containing private information about individuals and systems be kept for at least a year. Logs contain sensitive information; to prevent unauthorized access, companies must have strict rules governing who may access, view, delete, and edit them.
- **Log Formats:** Because there is a wide variety of security-equipment manufacturers, the formats used in their logs will vary widely. The Internet Engineering Task Force (IETF), a global standards body, has been working to provide a uniform format for logs and their associated information. With the help of the Intrusion Detection Message Exchange Formats (IDMEF), data on network intrusions, including the time of the attack, the IP address of the targeted system, and the intensity of the assault, may be gathered. Newly found threat data, on the other hand, is more generic and is released in a variety of forms across websites like Bugtraq, CVE, and OSVDB. Less processing power is needed to normalize the SIEM if log fields are more uniform. Internet Protocol (IP) equipment used by big ISPs, such as routers and switches, must include logging and reliable log transfer to distant servers in a standardized format.

5 Problems and Possible Solutions

Firstly four challenges has been discussed in this section.

1. The requirement to incorporate all devices in the SIEM operation, which signifies that irrespective the scope or focus, many devices will still be compromised.
2. Challenges with log gathering and privacy.

Table 2. Comparison of different vendors' SIEMs.

Functionality	Arc Sight	Q Radar	McAfee	Log Rhythm	USM OSSIM	RSA
Correlation Rules	N	N	Y	Y	Y	N
Data Sources	Y	Y	Y	N	N	Y
Reaction and Reporting	N/A	N/A	Y	Y	N/A	N
UEBA	Y	Y	N/A	Y	N/A	Y
Security	Y	Y	N/A	N/A	N	N

3. The difficulty that SIEM may tend to replace regional IT activities.
4. SIEM's ability to keep very strong controls on administrators, which could result in obsessive management, is an issue.

1. Fortunately, SIEM can be implemented in modern hardware and software to eliminate these issues. New routers must have an agent, and the software must be able to maintain log files. In this manner, as more and more devices already have an agent, the influence of SIEM for a new scope and focused will gradually reduce.
2. The technical ability that all SIEM systems possess to hash or encrypt private information and use regular expressions to match the private data is frequently cited. The solution is to create a procedure that enables IT Security officers to obtain the information that has been decrypted from the log files under the observation of Data Privacy officers.
3. The unique solutions that managers created themselves should endure. They will have more expertise and topic understanding than SIEM can provide. Make their product compatible also with SIEM environment if it is necessary to have these customized solutions integrated into the SIEM environment.
4. Giving administrators access to the reports and the rules that create them is the best way to proceed. They can determine whether the reports are accurate because they have full into the raw log files in any scenario.

6 Conclusion and Future Outlooks

Throughout this report, the adaptive approach for implementing SIEM is discussed, with references to relevant literature and recommendations for deployment. Our research strategy consists of the design and implementation of the study. Technical methodology, implementation, problems & Solution, results and analysis have been addressed in the remaining chapters. Network security will not be improved by using SIEM, as is the case with the vast majority of IT security tools when alarms are ignored despite being logged, no amount of logging will prevent malicious users. The point is to check that there's nothing suspicious happening on a network. However, it is impossible to prove that malicious events may have occurred if IT security measures had not been implemented. Installing SIEM servers and agents will only burden existing infrastructure. Log files are expensive to store because they contain sensitive information that must be protected. Those log

files will require a lot of work and effort to process. While the cost of implementing SIEM can be high, this is rarely the case. The in-depth technical explanations expressed concern about SIEM's effectiveness. Since these four challenges were identified during the methodology's development and application, they are achievable in the future. The efficient production of dynamic reports is a key deliverable of a SIEM environment. The SIEM application is used to generate custom reports, typically through a "point and click" interface. Using frameworks, you can specify what data should be included in the reports that correspond to the use cases and requirements you've gathered so far. For instance, transforming of the multiple vendors' products will probably concentrate more on incorporating more contextual information (such as geographical information and network directory). We can expect development to be driven forward by rising expectations for ease of use, widespread adoption, and regularity of implementation. Moreover, it is likely that policy-oriented automated response capabilities will receive more attention, as they are the ultimate aim of the every security administrator. Increasing management involvement and a focus on compliance are both expected to lead to the introduction of new types of predefined template rules and visualization reports. Although it is not entirely clear with more and more products installed into network environments leading to higher demands, data reduction will gradually decrease as storage costs decrease and processing performance improves.

References

1. Sekharan, S.S., Kandasamy, K.: Profiling SIEM tools and correlation engines for security analytics. In: 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, March 2017, pp. 717–721 (2017). https://doi.org/10.1109/WiSPNET.2017.8299855
2. Rikhtechi, L., Rafe, V., Rezakhani, A.: Secured access control in security information and event management systems, vol. 9, no. 1, p. 12 (2021)
3. Corcoran, J.M.: Security Information & Event Management (SIEM), p. 12
4. Caldeira, H.: Security Information and Event Management (SIEM) Implementation Recommendations to Enhance Network Security, p. 9
5. González-Granadillo, G., González-Zarzosa, S., Diaz, R.: Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. Sensors **21**(14), 4759 (2021). https://doi.org/10.3390/s21144759
6. SIEM (Security Information and Event Management Solutions) implementations in private or public clouds. Sci. Bull. Nav. Acad. **19**(2), (2016). https://doi.org/10.21279/1454-864X-16-I2-058
7. Detken, K.-O., Rix, T., Kleiner, C., Hellmann, B., Renners, L.: SIEM approach for a higher level of IT security in enterprise networks. In: 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Warsaw, Poland, September 2015, pp. 322–327 (2015). https://doi.org/10.1109/IDAACS.2015.7340752
8. Gartner-Critical-capabilities-for-SIEM-2020.pdf. https://www.exclusive-networks.com/se/wp-content/uploads/sites/25/2020/12/Gartner-Critical-capabilities-for-SIEM-2020.pdf. Accessed 06 Oct 2022
9. Anastasov, I., Davcev, D.: SIEM implementation for global and distributed environments. In: 2014 World Congress on Computer Applications and Information Systems (WCCAIS), Hammamet, Tunisia, January 2014, pp. 1–6. https://doi.org/10.1109/WCCAIS.2014.6916651

10. Vazao, A., Santos, L., Piedade, M.B., Rabadao, C.: SIEM open source solutions: a comparative study. In: 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), Coimbra, Portugal, June 2019, pp. 1–5 (2019). https://doi.org/10.23919/CISTI.2019.8760980
11. Nabil, M., Soukainat, S., Lakbabi, A., Ghizlane, O.: SIEM selection criteria for an efficient contextual security. In: 2017 International Symposium on Networks, Computers and Communications (ISNCC), Marrakech, Morocco, May 2017, pp. 1–6 (2017). https://doi.org/10.1109/ISNCC.2017.8072035
12. AlSabbagh, B., Kowalski, S.: A framework and prototype for a socio-technical security information and event management system (ST-SIEM). In: 2016 European Intelligence and Security Informatics Conference (EISIC), Uppsala, Sweden, August 2016, pp. 192–195 (2016). https://doi.org/10.1109/EISIC.2016.049
13. Montesino, R., Fenz, S., Baluja, W.: SIEM-based framework for security controls automation. Inf. Manag. Comput. Secur. **20**(4), 248–263 (2012). https://doi.org/10.1108/09685221211267639
14. Mokalled, H., Catelli, R., Casola, V., Debertol, D., Meda, E., Zunino, R.: The applicability of a SIEM solution: requirements and evaluation. In: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), Napoli, Italy, June 2019, pp. 132–137 (2019). https://doi.org/10.1109/WETICE.2019.00036
15. Irfan, M., Abbas, H., Sun, Y., Sajid, A., Pasha, M.: A framework for cloud forensics evidence collection and analysis using security information and event management: SCN-SI-085. Secur. Commun. Netw. **9**(16), 3790–3807 (2016). https://doi.org/10.1002/sec.1538
16. Bejtlich, R.: The Tao of Network Security Monitoring: Beyond Intrusion Detection. Addison-Wesley, Boston (2005)
17. Kenaza, T., Aiash, M.: Toward an efficient ontology-based event correlation in SIEM. Procedia Comput. Sci. **83**, 139–146 (2016). https://doi.org/10.1016/j.procs.2016.04.109
18. Menges, F., et al.: Towards GDPR-compliant data processing in modern SIEM systems. Comput. Secur. **103**, 102165 (2021). https://doi.org/10.1016/j.cose.2020.102165
19. Novikova, E.S., Bekeneva, Y.A., Shorov, A.V.: Towards visual analytics tasks for the security information and event management. In: 2017 International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT&QM&IS), Saint Petersburg, Russia, September 2017, pp. 90–93 (2017). https://doi.org/10.1109/ITMQIS.2017.8085770
20. Laue, T., Klecker, T., Kleiner, C., Detken, K.-O.: A SIEM architecture for advanced anomaly detection, vol. 6, no. 1, p. 17 (2022)
21. Anumol, E.T.: Use of machine learning algorithms with SIEM for attack prediction. In: Jain, L.C., Patnaik, S., Ichalkaranje, N. (eds.) Intelligent Computing, Communication and Devices, vol. 308, pp. 231–235. Springer, New Delhi (2015). https://doi.org/10.1007/978-81-322-2012-1_24
22. Di Sarno, C., Garofalo, A., Matteucci, I., Vallini, M.: A novel security information and event management system for enhancing cyber security in a hydroelectric dam. Int. J. Crit. Infrastruct. Prot. **13**, 39–51 (2016). https://doi.org/10.1016/j.ijcip.2016.03.002
23. Podzins, O., Romanovs, A.: Why SIEM is irreplaceable in a secure IT environment? In: 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream), Vilnius, Lithuania, April 2019, pp. 1–5 (2019). https://doi.org/10.1109/eStream.2019.8732173
24. Ring, M., Wunderlich, S., Grüdl, D., Landes, D., Hotho, A.: A toolset for intrusion and insider threat detection. In: Palomares Carrascosa, I., Kalutarage, H.K., Huang, Y. (eds.) Data Analytics and Decision Support for Cybersecurity, pp. 3–31. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-59439-2_1
25. Blumbergs, B.: Analysis of Security Information and Event Management (SIEM) Evasion and Detection Methods, p. 65

Author Index

A
Abbasi, Waseem I-73, I-252, II-330
Abdullah, Sanya I-263
Abid, Mian II-171
Afzal, Hamza II-395
Ahmad, Muhammad II-298
Ahmed, Masroor II-1
Ahmed, Muhammad I-358
Ahmed, Yawar I-173
Ahsan, II-128
Ahsan, Muhammad Junaid II-191
Ain, Noor Ul I-116
Akbar, Muhammad Hussain I-337, II-21
Akhtar, Adnan II-223
Akram, Sheeraz I-337, II-21
Ali, Abid II-108
Ali, Muddassar I-130
Ali, Muhammad II-405
Ali, Natasha I-358
Ali, Rasikh I-263
Almufareh, Maram Fahaad I-194
AlWakid, Ghadah Naif I-345
Amir, Muhammad I-252
Anwar, Saeed II-298
Anwar, Syed Muhammad II-350
Aqeel, Muhammad I-37
Arif, M. II-128
Arif, Muhammad II-93, II-149, II-339
Arshad, Hasna II-61
Asaf, Muhammad I-173
Ashiq, Masood II-108
Ashraf, Abrar II-287, II-362, II-380
Ashraf, Mohsin I-241
Ashraf, Muhammad I-206, I-219, I-345
Aslam, Muhammad II-260
Assam, Muhammad II-61

B
Bhatti, Anam Maqsood II-75
Bhatti, Sohail Masood II-191
Bibi, Amina I-11
Bilal, Afshan II-298
Bqa, Rabranea I-1
Bukhari, Faisal I-24, I-116
Butt, Muhammad Adil II-205
Butt, Umair Muneer I-57

D
Din, Irfan Ud II-249
din, Irfan Ud II-380
Din, Irfan ud II-395

E
Ejazulghaffar, Muhammad II-93
Elahi, Ihsan I-105

F
Faraz, Hassan I-263
Fareed, Asim I-51
Farhat, Tayyaba I-263
Farooq, Asif I-241
Farooq, Umar I-194
Faryal, Mehak I-151
Fatima, Anam II-191
Fatima, Noroze II-128

G
Ghadi, Yazeed Yasin I-73
Ghafoor, Hafiz Yasir II-171

H
Hamid, Khalid I-37, I-418
Hamza, M. Ameer II-287
Haque, Ehtisham Ul II-330
Hasan, Muhammad Zulkifl II-1, II-298
Hassan, Ahmed II-93
Hassan, Bilal I-277
Hassan, Muhammad II-322
Humayun, Mamoona I-194, I-345
Hussain, Abida II-149

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2025

M. Arif et al. (Eds.): ICCET 2023, CCIS 2056, pp. 433–435, 2025.
https://doi.org/10.1007/978-3-031-77620-5

Hussain, Majid I-51, I-88, I-97, I-105, I-187, II-239, II-322, II-372
Hussain, Moodser I-313
Hussain, Muhammad Anwar I-232
Hussain, Muhammad Zunnurain II-1, II-298

I
Ibrar, Muhammad I-51
Ilyas, M. Saad Bin II-205
Imran, Ali II-128
Imran, Syed Muhammad Ali II-149
Imtiaz, Ahsan I-11, I-160, II-395
Imtiaz, Muhammad Talha II-339
Iqbal, Adeel I-151
Iqbal, Amna I-187, II-239
Iqbal, Junaid II-108
Iqbal, Muhammad Junaid I-173
Iqbal, Muhammad Saqlain I-173
Iqbal, Muhammad Tassawar II-287
Iqbal, Muhammad Waseem I-37, I-130, I-313, I-321, I-418, II-75, II-191, II-223, II-287
Iqbal, Muhammad I-73, I-252
Iqbal, Waheed I-24, I-116
Iqbal, Waseem II-47
Irfan, Danish I-130, II-287, II-415
Irfan, Hafiz Muhammad II-223
Irfan, Roha I-313
Irshad, Muhammad Ahmad I-321
Islam, Atika I-24
Izhar, Muhammad II-171

J
Jabbar, Taimoor Hassan I-313
Jaffar, Arfan I-337, II-21, II-47, II-93, II-149
Jaffer, Arfan I-358
Jahangir, Rashid II-171
Jameel, Muhammad I-313
Jamshaid, Amir II-223
Javed, Mannan I-219
Joseph, Sylvester II-287

K
Kahloon, Ch Zubair I-337, II-21
Kauser, Maryam I-382
Khalid, Aleena II-249
Khalid, Humaira I-57
Khalil, Hisham II-362
Khaliq, Rida I-57
Khan, Farrukh Aslam I-194, I-206, I-219
Khan, Hamayun II-249, II-380
Khan, Javed Ali II-61
khan, Muhammad Bilal I-241
Khan, Muhammad Farhan I-151
Khan, Muhammad Imran I-151
Khan, Muhammad Irtaza I-241
Khan, Saif Ur Rehman II-271
Khan, Shehzad II-271
Khushi, Hafiz Muhammad Tayyab II-149
Kyinat, Samra II-141

L
Lateef, Anam I-105

M
Mabood, Nouman I-206
Maqbool, Sidra I-160
Masood, Sohail I-337, II-21, II-141
Masood, Tehreem II-405
Mazhar, Anas II-223
Mazhar, Sana I-321
Mazhar, Tehseen I-73, I-252
Meer, Ayaz Ahmad I-277
Mehmood, Danish I-194
Mir, Mariam Munsif I-382
Mubarak, Zaima II-1
Munawar, Munazzah I-51
Mushtaq, Muhammad Yousaf II-223
Mustafa, Hamza II-29
Mustafa, Hirra II-362

N
Nadeem Jabbar, C. H. I-277
Nadeem, Muhammad Umer II-298
Nasim, Fawad I-337, II-21
Nauman, Nasir II-362
Naveed, Touheed II-1
Nawaz, Rida I-404
Nawaz, Usman I-173, I-382, II-108
Naz, Ammerha II-405
Naz, Amna II-249
Nazar, Muhammad Zeeshan II-298
Niaz, Muhammad Ahmad II-223
Noor, Misbah I-37
Nosheen, Summaira II-298

Q
Qamar, Hafiza Iqra I-97
Qamar, Usman II-339
Qureshi, Ali Moiz II-1
Qureshi, Samia Asloob I-1

R
Rafique, Aftab I-382
Rafique, Furqan II-108
Raheel, Muhammad I-130
Rana, Mehak II-372
Rasheed, Maryam II-191
Raza, Asaf II-61
Raza, Asif II-271
Raza, Saim I-187
Raza, Usman Ahmed I-173, I-241, I-382, II-108
Rehman, Ateeq Ur I-73, I-252
Rehman, Attique Ur II-260
Rehman, Faisal I-173, II-108
Rehmat, Nadia I-263
Rezaei, Saeid I-151
Riaz, Muhammad Danish II-339
Riaz, Muhammad Qasim II-339
Riaz, Samra II-350

S
Saeed, Muhammad Mohsin I-418
Saeed, Uzair I-88, I-97, I-105, II-322, II-372
Saghir, Aqib I-277
Sahar, Sadia II-287, II-380
Sahi, Salman Ahmad I-277
Sajid, Omer I-1
Sajjad, Muhammad Umar II-339
Saleem, Maryam II-191
Salim, Kinza I-151
Sami, Mohsin I-241
Sanamaqbool, I-88
Sarwar, Nadeem II-1
Shafeeq, Muhammad Farrukh I-88
Shah, Syed Faisal Abbas I-252
Shah, Syed Yaqub II-61
Shahzad, Danish II-47
Shahzad, Inzamam II-271
Shahzad, Muhammad Khurram I-232
Shahzad, Rohail I-382
Sharif, Hanan II-108
Shehzad, Danish I-11, II-128
Siddique, Imran II-75
Siddiqui, Adeel Ahmad II-1
Sohail, Muhammad I-151
Soomro, Imtiaz Ali II-205
Sulaiman, Sarina I-232

T
Tariq, Ammara I-173
Tariq, Iqra II-205
Tariq, Khizar II-1
Tariq, Muhammad Imran II-249, II-380
Tariq, Noshina I-194, I-206, I-219
Tehreem, Umme I-418

U
Uallah, Naeem II-61
Ullah, Abaid II-308
Ullah, Kainat Azmat II-108
Ullah, Muhammad Farhat I-313
Umar, Muhammad II-239
Usman Bilal, M. II-415

W
Waheed, Namra I-382
Waqas, Sahibzada M. I-345
Waseem Iqbal, M. II-415

Y
Yaqub, Muhammad Atif II-298
Yasir, Siddiqui Muhammad I-277
Younas, Sana I-57

Z
Zafar, Hina I-187, II-239
Zafar, Kashif II-29
Zafar, Muhammad Haseeb II-260
Zahra, Syeda Aqsa II-380
Zainab, II-249
Zakwan, Muhammad I-345
Zia, Saira I-37
Zubair, Muhammad II-141, II-171