

Faisal Rehman
Inam Ullah Khan
Oroos Arshi
Shashi Kant Gupta *Editors*

Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics

Information Systems Engineering and Management

Volume 32

Series Editor

Álvaro Rocha, ISEG, University of Lisbon, Lisbon, Portugal

Editorial Board

Abdelkader Hameurlain, Université Toulouse III Paul Sabatier, Toulouse, France

Ali Idri, ENSIAS, Mohammed V University, Rabat, Morocco

Ashok Vaseashta, International Clean Water Institute, Manassas, VA, USA


Ashwani Kumar Dubey, Amity University, Noida, India

Carlos Montenegro, Francisco José de Caldas District University, Bogota, Colombia

Claude Laporte, University of Quebec, Québec, QC, Canada


Fernando Moreira , Portucalense University, Berlin, Germany

Francisco Peñalvo, University of Salamanca, Salamanca, Spain

Gintautas Dzemyda , Vilnius University, Vilnius, Lithuania


Jezreel Mejia-Miranda, CIMAT - Center for Mathematical Research, Zacatecas, Mexico

Jon Hall, The Open University, Milton Keynes, UK

Mário Piattini , University of Castilla-La Mancha, Albacete, Spain

Maristela Holanda, University of Brasilia, Brasilia, Brazil

Mincong Tang, Beijing Jiaotong University, Beijing, China

Mirjana Ivanović , Department of Mathematics and Informatics, University of Novi Sad, Novi Sad, Serbia

Mirna Muñoz, CIMAT Center for Mathematical Research, Progreso, Mexico

Rajeev Kanth, University of Turku, Turku, Finland

Sajid Anwar, Institute of Management Sciences, Peshawar, Pakistan

Tutut Herawan, Faculty of Computer Science and Information Technology, University of Malaya, Kuala Lumpur, Malaysia

Valentina Colla, TeCIP Institute, Scuola Superiore Sant'Anna, Pisa, Italy

Vladan Devedzic, University of Belgrade, Belgrade, Serbia

The book series “Information Systems Engineering and Management” (ISEM) publishes innovative and original works in the various areas of planning, development, implementation, and management of information systems and technologies by enterprises, citizens, and society for the improvement of the socio-economic environment.

The series is multidisciplinary, focusing on technological, organizational, and social domains of information systems engineering and management. Manuscripts published in this book series focus on relevant problems and research in the planning, analysis, design, implementation, exploration, and management of all types of information systems and technologies. The series contains monographs, lecture notes, edited volumes, pedagogical and technical books as well as proceedings volumes.

Some topics/keywords to be considered in the ISEM book series are, but not limited to: Information Systems Planning; Information Systems Development; Exploration of Information Systems; Management of Information Systems; Blockchain Technology; Cloud Computing; Artificial Intelligence (AI) and Machine Learning; Big Data Analytics; Multimedia Systems; Computer Networks, Mobility and Pervasive Systems; IT Security, Ethics and Privacy; Cybersecurity; Digital Platforms and Services; Requirements Engineering; Software Engineering; Process and Knowledge Engineering; Security and Privacy Engineering, Autonomous Robotics; Human-Computer Interaction; Marketing and Information; Tourism and Information; Finance and Value; Decisions and Risk; Innovation and Projects; Strategy and People.

Indexed by Google Scholar. All books published in the series are submitted for consideration in the Web of Science.

For book or proceedings proposals please contact Alvaro Rocha (amrrocha@gmail.com).

Faisal Rehman · Inam Ullah Khan · Oroos Arshi ·
Shashi Kant Gupta
Editors

Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics

Editors

Faisal Rehman
Department of Robotics and Artificial
Intelligence
National University of Sciences
and Technology
Islamabad, Pakistan

Inam Ullah Khan
Multimedia University
Cyberjaya, Malaysia

Shashi Kant Gupta
Eudoxia Research University
New Castle, DE, USA

Oroos Arshi
University of Petroleum and Energy Study
Dehradun, Uttarakhand, India

ISSN 3004-958X ISSN 3004-9598 (electronic)
Information Systems Engineering and Management
ISBN 978-3-031-81480-8 ISBN 978-3-031-81481-5 (eBook)
<https://doi.org/10.1007/978-3-031-81481-5>

© 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

Emerging Trends in Information System Security Using AI & Data Science for Next-Generation Cyber Analytics is a comprehensive book that explores the integration of AI and data science in cybersecurity. It delves into the evolving landscape of cyber threats and the need for innovative solutions. The book covers topics such as AI's role in securing IoT devices, threat classification techniques, and time series analysis. It also highlights the importance of next-generation defense mechanisms like generative adversarial networks (GANs) and federated learning techniques in combating sophisticated cyber threats while preserving privacy. The book provides real-world insights into data analytics deployment in cybersecurity and ethical considerations in leveraging AI and data science. It advocates for proactive risk mitigation and continuous adaptation in the face of evolving threats. The book is an indispensable resource for cybersecurity professionals, researchers, and students, bridging theory with practice to navigate the complexities of modern cybersecurity challenges.

Islamabad, Pakistan
Cyberjaya, Malaysia
Dehradun, India
New Castle, USA
November 2024

Faisal Rehman
Inam Ullah Khan
Oroos Arshi
Shashi Kant Gupta

Contents

AI-Driven Modern Cybersecurity Approach: A Systematic Literature Review	1
Yasir khan and Muhammad Tufail	
Cyber Security in the Post Quantum Computer Era: Threats and Perspectives	15
Muhammad Sajid Iqbal, Ahthasham Sajid, and Rida Malik	
Deep Neural Network for DoS Detection in Wireless Sensors Networks	31
Hajar Fares, Hajraoui Nirmin, and Hajraoui Abderrahmane	
Survey on IoT Security Threats Application and Architectures	41
Maria Hanif, Ahthasham Sajid, Rida Malik, Fariha Shoukat, and Muhammad Sajid Iqbal	
Lightweight Cryptography Algorithms for IoT Devices	51
Muhammad Farukh Sohail, Malik Muhammad Nadeem, Ahthasham Sajid, Hamza Razza, and Arslan Ali Khan	
Guarding the Digital Gateway: An In-Depth Analysis of Cybersecurity Challenges in India	67
Snehal A. Bagul	
Predictive Modeling for Food Security Assessment Using Synthetic Minority Over-Sampling Technique	93
Imran Khan, Atta Ur Rahman, and Ahthasham Sajid	
Exploring the Secure Unleashing of Digital Potential: A Study on How Cloud Security Works Together with Digital Transformation in Financial Institutions of Pakistan	107
Khurram Shoaib	

Reviewing Theoretical Perspectives on IT Governance and Compliance in Banking: Insights from US Regulatory Frameworks	119
Muhammad Nauman Zakki, Nimra Iftikhar, Saim Saif Ullah Khan, Farhood Nishat, and Oroos Arshi	
Overcoming Challenges and Implementing Effective Information Security Policies for Remote Work Environments	135
Muhammad Nauman Zakki, Nimra Iftikhar, Saim Saif Ullah Khan, Farhood Nishat, and Oroos Arshi	
Generative Adversarial Networks (GAN) Insights for Cyber Security Applications	153
Mohammad Shahnawaz Shaikh	
Future Emerging Challenges and Innovations in Next Gen-Cybersecurity and Information Systems Security	173
Umna Iftikhar, Huma Rashid, and Hafiz Muhammad Attaullah	

Editors and Contributors

About the Editors

Dr. Faisal Rehman is an expert in Robotics, Data Science and Artificial Intelligence, holding a Ph.D. in the field. With more than 10 years of experience, they have worked in teaching, research, and administrative roles. Dr. Faisal has published over a hundred papers, sharing their knowledge and discoveries with the world. He is known as both a researcher and an academician, dedicating their time to advancing understanding in their field. One of Dr. Faisal's key strengths is their ability to collaborate. He worked on a range of research projects, teaming up with experts from different countries. This collaboration helps to bring diverse perspectives and ideas to their work, leading to more innovative solutions. Dr. Faisal is also passionate about sharing their knowledge with others. He often participates in seminars, workshops, and other events where they can connect with fellow researchers and students. By sharing their insights and experiences, Dr. Faisal helps to inspire and educate the next generation of scientists and engineers. Through their work, he aims to make a positive impact on society. He believes that advancements in Robotics and AI have the potential to improve many aspects of our lives, from healthcare to transportation. By contributing to research and education in these fields, Dr. Faisal hopes to help unlock this potential and create a better future for all.

Dr. Inam Ullah Khan is a distinguished academic and industry professional, widely recognized for his contributions to Artificial Intelligence, Artificial General Intelligence, Unmanned Aerial Vehicles, Routing Protocols, Intrusion Detection Systems, Machine Learning, Deep Learning, and Evolutionary Computing. He is the Founder of AI-Explain Your Science (AI-EYS) and a Senior Member of IEEE, with active memberships in prestigious organizations such as the International Association of Engineers (IAENG), IEEE Young Professionals, IEEE Systems Council, and various IAENG societies focused on Artificial Intelligence, Computer Science, Internet Computing & Web Services, Information System Engineering, Scientific Computing, Software Engineering, and Wireless Networks. Dr. Khan currently serves as a

Mentor of Artificial Intelligence at Corvit Systems, Rawalpindi, Pakistan, and as a Global Mentor and Guest Lecturer at Impact Xcelerator, School of Science & Technology, IE University, Madrid, Spain. He is also a Trainer at the National Vocational and Technical Training Commission (NAVTTTC), Pakistan. Additionally, he is a Co-Supervisor in the Lincoln Global Postdoc and Research Associate Programme (LGPR) at Lincoln University College, Malaysia, and an Advisor for Cisco Community Pakistan. Previously, Dr. Khan was a Visiting Researcher at King's College London, UK, and has held faculty positions at several esteemed institutions in Pakistan, including the National University of Technology (NUTECH), Islamabad; Center for Emerging Sciences, Engineering & Technology (CESET), Islamabad; Abdul Wali Khan University (Garden Campus and Timergara Campus); University of Swat; and Shaheed Zulfiqar Ali Bhutto Institute of Science and Technology (SZABIST), Islamabad Campus. Academically, Dr. Khan earned his Ph.D. in Electronics Engineering from Isra University, Islamabad Campus, where he also completed his M.S. in Electronic Engineering. He holds a Bachelor's degree in Computer Science from Abdul Wali Khan University, Mardan, Pakistan. His Master's thesis, titled "Route Optimization with Ant Colony Optimization (ACO)," was published as a book in Germany and is available on Amazon. Additionally, he has completed the Huawei Technologies Pakistan Train the Trainer (TTT) Program. With a prolific research portfolio, Dr. Khan has authored and co-authored over 100 research articles published in leading journals, conferences, and book chapters. He is also an editor for approximately 20 books covering various advanced topics. His expertise has been recognized at the national level, as he has been featured multiple times as a technology expert on Pakistan National Television, showcasing his thought leadership in Artificial Intelligence and emerging technologies. Currently, Dr. Khan is a Postdoctoral Research Fellow at Multimedia University, Cyberjaya, Malaysia, and also serves as Visiting Faculty at Mechatronics Engineering Lab at the NAVTTTC Center of Excellence, Islamabad, Pakistan. Additionally, he is an Adjunct Faculty Member at PSGR Krishnammal College for Women, Coimbatore, India.

Oroos Arshi (Member IEEE) is a Research Scientist at AI-EYS, where she is shaping the future through innovation and academic excellence. She was awarded the Young Researcher Award at the International Conference on Emerging Trends and Innovations (ICETI) 2024. She is an active member of IEEE Women in Engineering, IEEE Robotics & Automation Society, and IEEE Young Professionals. Additionally, she is a member of the International Association of Engineers (IAENG). She completed her postgraduate degree, M.Tech in Cyber Security and Forensics, from the School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India. She earned her undergraduate degree, B.Tech in Computer Science and Engineering, from Integral University, Lucknow, India. She has around 15 international publications in reputed journals, conferences, books, and book chapters. Recently, Oroos published her book titled *Unmanned Aerial Vehicle Swarms for Protecting Smart Cities: Future Trends & Challenges*. In addition to this, six of her books have been accepted as an editor by prestigious publishers, including Wiley, IGI Global, Springer, Apple Academic Press, and Taylor & Francis. She served as a session chair for AIIoT's

Emerging Technologies and Future Applications at the 4th International Conference on Advances in Computation Technology, Computing, and Engineering in Morocco. Additionally, she was the chief organizer and publication chair at the 2nd International Conference on Emerging Trends & Innovation (ICETI) in July 2024. More notably, she has served as a speaker at numerous conferences. Moreover, she has earned both a gold and silver badge for problem-solving in Design Analysis and Algorithm (DAA) from Hacker Rank. Her expertise has been demonstrated on multiple platforms, reflecting her commitment to sharing insights and contributing to advancements in her field globally. Her research interests include Artificial Intelligence, Unmanned Aerial Vehicles, the Internet of Things, Computer Vision, and Natural Language Processing.

Dr. Shashi Kant Gupta Post-Doctoral Fellow and Researcher, Computer Science and Engineering, Eudoxia Research University, USA, in collaboration with Eudoxia Research Centre, India. ORCID: [0000-0001-6587-5607](https://orcid.org/0000-0001-6587-5607). He is a Post-Doctoral Fellow, the Research Institute of IoT and Cybersecurity, Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Taiwan. He is working as Research Fellow, INTI International University, Malaysia. He is currently working as an Adjunct Research Faculty, Centre for Research Impact & Outcome, Chitkara University Institute of Engineering and Technology. Chitkara University, Rajpura, 140401, Punjab, India. He is working as an Adjunct Faculty in the Department of Pure and Applied Mathematics, Saveetha School of Engineering University, India. He is working as Honorary Adjunct Faculty, School of Computing, Maryam Abacha American University of Nigeria (MAAUN), Nigeria. He is working as an Honorary Senior Research Fellow, Department of Scientific Research, Innovation and Training of Scientific and Pedagogical Staff, University of Economics and Pedagogy, Karshi City, Uzbekistan. He is working as a Research Collaborator and Invited Visiting Senior Scientist at the Research Institute of IoT and Cybersecurity, Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Taiwan. He has completed his Ph.D. (CSE) from Integral University, Lucknow, UP, India, & Worked as Assistant Professor in the Department of Computer Science and Engineering, ITM, Lucknow, U.P., India, & Worked as Assistant Professor in the Department of Computer Science and Engineering, PSIT, Kanpur, U.P., India, Worked as Associate Professor, School of Computer Applications, BBD University, Lucknow, UP, India, Worked as Assistant Professor, Department of Computer Science and Engineering, Ambalika Institute of Management and Technology, Lucknow, UP, India, and also worked as Senior Lecturer, Department of IT, MCSCET, Lucknow, UP, India. He is currently working as Founder and CEO of CREP Pvt. Ltd., Lucknow, UP, India. He is a member of Spectrum IEEE & Potentials Magazine IEEE since 2019 and many more international organizations for research activities. He is an Editor-in-chief of International Journal of Data Informatics and Intelligent Computing (IJDIIC) also Editor-in-chief of International Journal of Emerging Technologies in Computer and Communication (IJETCC). Senior Editor in Global Research Journal from London Organization of Skill Development, London,

UK. He has published many research papers in reputed international journals, conferences & seminars with SCOPUS and SCI indexing. He has got many awards from many international and national organizations. He has organized various Faculty Development Programs, Seminars, Workshops, and Short-Term Courses at University level. His main research work focuses on Cloud computing, Big Data Analytics, IoT and Computational Intelligence-based Education. He is currently working as a reviewer and editorial in various international journals. He is currently editor in many edited books of different publishers like CRC Press, Taylor and Francis group Publication, Routledge Publisher, Bentham Science Publishers, Springer Nature Publisher, Wiley Publisher, etc. He has published many patents like Indian, Germany, UK, etc., in the field of CSE and IT. He has more than 12 years of teaching experience, 2 years of Industrial Experience and more than 2.5 years as CEO and Founder of a firm.

Contributors

Hajraoui Abderrahmane Equipe of Telecommunication and Detection, Faculty of Science, Abdelmalek Essaadi University, Tetouan, Morocco

Oroos Arshi Department of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India

Hafiz Muhammad Attaullah Faculty of Computing, Mohammad Ali Jinnah University, Karachi, Pakistan

Snehal A. Bagul Department of Management Studies, Sandip Institute of Technology and Research Centre, Savitribai Phule Pune University, Nashik Campus, India

Hajar Fares Equipe of Telecommunication and Detection, Faculty of Science, Abdelmalek Essaadi University, Tetouan, Morocco

Maria Hanif Department of Computer Science, IQRA University, Islamabad, Pakistan

Nimra Iftikhar Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

Umna Iftikhar Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan

Muhammad Sajid Iqbal Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Arslan Ali Khan Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Imran Khan Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Saim Saif Ullah Khan Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

Yasir khan Department of Science and Technology and Information Technology (ST&IT), Peshawar, Pakistan

Rida Malik Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Malik Muhammad Nadeem Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Hajraoui Nirmin Laboratory of Remote Sensing and Geographic Information System, ENSA, University of Abdelmalek Essaadi, Tetouan, Morocco

Farhood Nishat Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

Atta Ur Rahman Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Huma Rashid Faculty of Computing, Mohammad Ali Jinnah University, Karachi, Pakistan

Hamza Razza Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Ahthasham Sajid Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan;
Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Mohammad Shahnawaz Shaikh Department of Artificial Intelligence and Data Science, Parul Institute of Engineering and Technology, Parul University, Vadodara, Gujarat, India

Khurram Shoaib Avionics Engineering Department, Air University, Islamabad, Pakistan

Fariha Shoukat Department of Information Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Muhammad Farukh Sohail Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

Muhammad Tufail Department of Computer Science, Government Postgraduate College, Nowshera, Pakistan

Muhammad Nauman Zakki Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan

AI-Driven Modern Cybersecurity Approach: A Systematic Literature Review



Yasir khan  and Muhammad Tufail

Abstract With the proliferation of internet-connected devices and the ongoing digitization initiatives undertaken by organizations, there has been a significant surge in cyber-attacks in recent years. The increase in cyber threats demands a fundamental change in cyber security measures, prompting an extensive review of artificial intelligence (AI) use. This survey explores the domains of Machine Learning (ML), Deep Learning (DL), and Natural Language Processing (NLP) in the field of cyber security, illustrating their complex roles and contributions. The paper investigates the latest developments in ML, highlighting its ability to adapt, the complex layers of DL, and the linguistic intelligence of NLP. The paper explores machine learning to detect known risks and deep learning to tackle complicated challenges. It then smoothly transitions into discussing the linguistic analysis of NLP in many cyber security fields. Nevertheless, incorporating AI presents challenges, such as financial issues, potential risks associated with generative AI, and ethical deliberations. This study guides cyber security specialists in navigating the ever-changing realm of AI applications. It offers valuable information to strengthen digital defenses against emerging threats.

Keywords Artificial intelligence · Cyber security · SLR · Cyber threats · ML · DL · NLP

Y. khan (✉)

Department of Science and Technology and Information Technology (ST&IT), Peshawar, Pakistan

e-mail: imyasir.308@gmail.com

M. Tufail

Department of Computer Science, Government Postgraduate College, Nowshera, Pakistan

1 Introduction

Cybersecurity is the practice and art of proactively protecting networks, devices, and data from unauthorized access or unlawful usage [1]. The process includes protecting information confidentiality, integrity, and availability, with security measures deployed at several levels, such as applications, networks, hosts, and data [2]. Evaluating the Internet's role as a crucial tool for daily activities has expanded interconnected systems extensively. The advancements in computer networks, servers, and mobile devices have greatly improved Internet utilization. The global count of internet users reached 5.3 billion individuals as of October 2023, indicating widespread and increasing use of internet access worldwide [3]. However, this general use attracts cyber criminals who continue to develop ever-more-advanced methods to their advantage. According to 75% of security experts who reported an increase in cyber-attacks the previous year [4], there has been a noticeable rise in cyber risks. Therefore, it is crucial to have a robust and reliable cyber security infrastructure to protect the privacy, availability, and accuracy of data exchanged over the Internet. This measure of caution is essential for ensuring the confidentiality and security of data in the continuously developing digital environment.

Conventional cyber protection measures that rely on signatures and rules struggle to handle the increasing amounts of information spread across the Internet [5]. Cyber attackers, constantly developing novel and complex attack methods, use technical progress such as AI. AI, including ML, DL, and NLP, amplifies the complexity and effectiveness of hostile activities, presenting a significant obstacle to cyber security. Cybersecurity researchers have now turned their attention to AI-based approaches, moving away from traditional non-AI methods. The purpose of this strategic maneuver is to utilize the capabilities of ML, DL, and NLP to adjust and react to the changing environment of cyber threats. Artificial Intelligence techniques, specifically ML and DL algorithms have shown exceptional efficacy in diverse cyber security domains, including intrusion detection, spam email filtering, identifying botnets, detecting fraud, and recognizing malicious applications [6]. Nevertheless, despite their remarkable performance on standardized datasets, these artificial intelligence approaches face certain difficulties. They are prone to errors, some of which can incur higher costs than conventional cyber security solutions. Occasionally, developers in the field have given more importance to correctness than interpretability, creating intricate models that are difficult to understand [7]. Balancing accuracy and interpretability is crucial for efficient and robust cyber security measures.

This research paper focuses on the significance of ML, DL, and NLP in the field of cyber security and their potential to enhance the development of robust cyber defences. This research article is structured into four primary sections, each exploring unique facets of artificial intelligence in cyber security. Section 2, examines the utilization and challenges of ML in cyber security, offering valuable perspectives on implementing ML algorithms to improve safety measures. Subsequently, Sect. 3, focuses on applying DL in cyber security. It highlights the use of neural networks and sophisticated models to address complicated security challenges. Section 4, focuses

on applying NLP in cyber security. It explores how linguistic concepts and computational approaches strengthen digital security measures, followed by Sect. 5, which thoroughly examines AI’s limitations in cyber security. It highlights the challenges and ethical issues when utilizing artificial intelligence for security objectives. To conclude the paper, the authors provide a prospective view by describing potential directions for cyber security research. This part, referred to as Sect. 6, guides future research efforts, directing scholars and practitioners towards promising investigation and advancement within the constantly changing and interconnected fields of AI and cyber security.

1.1 Research Motivation and Methodology

In recent years, significant emphasis has been given to research investigating the incorporation of AI into cyber security applications. Figure 1 illustrates the broad scope of AI, highlighting its different foundations: specifically focusing on natural learning, deep learning, and Machine learning.

Each of these technologies possesses distinct advantages. Natural learning emulates the flexible nature of the human brain, deep learning analyzes data through layered networks, machine learning improves its abilities through experience, and

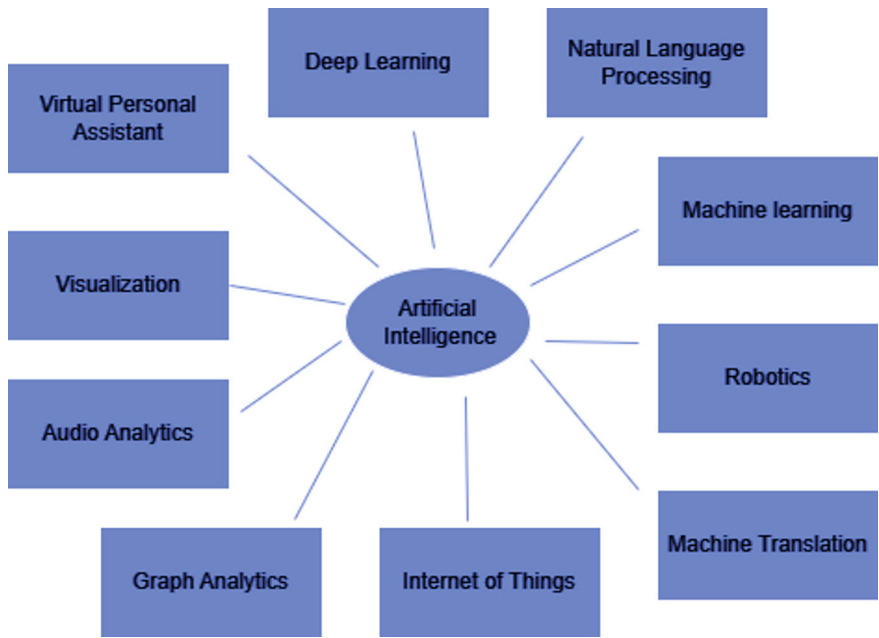


Fig. 1 Various applications of AI

Table 1 Research searching database engines

Search engines	Database address
Google Scholar	https://scholar.google.com/
IEEE Xplore	https://ieeexplore.ieee.org/
Research Gate	https://www.researchgate.net/
Elsevier	https://www.elsevier.com/
Springer	https://link.springer.com/
Taylor & Francis	https://taylorandfrancis.com/
ACM Digital Library	https://dl.acm.org/

robotics gives physical form to artificial intelligence. The complex combination of AI techniques drives various applications, such as virtual assistants that help us in our daily activities and language translation that connects different cultures. With the ongoing advancement of AI, it is intriguing to consider the numerous ways in which it may influence our future. This attention reflects the ongoing attempts of cyber threats to utilize AI in their attacks. This movement brings new aspects to implementing AI in cyber security, requiring a thorough examination of previous AI-based assaults to develop efficient AI-driven cyber security solutions. This survey aims to thoroughly examine current AI applications in cyber security, specifically with an emphasis on diversity and inclusion. The objective of this study is to analyze different approaches and categorizations of AI and evaluate the present challenges and limitations in AI. Moreover, it investigates recent efficient AI-powered systems and uses in cyber security, and discover the challenges and areas of research that need attention in the application of AI in cyber security. Based on what was established in the introduction (Section 1), this study aims to investigate the current advancements in AI applications in cyber security. To systematically collect and evaluate appropriate research publications, the criteria given below were established:

1.1.1 Comprehensive Search

A holistic exploration was conducted using various academic search engines described in Table 1.

1.1.2 Keywords for Searching

The survey’s chosen search terms included two focal points: “A and “Cyber Security,” alongside associated phrases such as “Cyber Attack,” “Cyber Threat,” “Network Security,” and “Cyber Crime.”

1.1.3 Publication Timeline

Only scholarly articles published from 2018 onwards were considered to analyze the latest developments in using AI methods in information security.

1.1.4 Language and Exclusion Criteria

This review only considered papers written in English, and any duplicated studies were not considered. The survey specifically concentrated on articles that discussed vulnerabilities in the cyber security field, with a particular emphasis on those that presented systems based on ML, DL, NLP, AI, and general AI.

The article selection procedure consisted of two rapid stages: first, search results were selected according to predetermined criteria by reviewing titles and abstracts. Afterward, the chosen papers from the first stage were carefully examined to develop a list of articles for inclusion, following specific selection and exclusion criteria. This rigorous technique guarantees a thorough and concentrated examination of recent advancements in AI applications in information security.

1.2 Scope of Cyber Security Analyzed

As previously discussed, a growing need to stop cyber threats is the driving force behind integrating AI into cyber security. The research motivation highlights the need to thoroughly investigate recent AI-based threats to facilitate the creation of effective AI-driven cyber security solutions. The technique was devised to meticulously examine contemporary.

AI applications, challenges, and real-world implementations in cyber security. This section emphasizes the significance of the cyber security domain investigated in this study. The rising prevalence of cyber-attacks has resulted in the recognition of three vital sub-disciplines intricately linked to the limitations of AI in cyber security. The number and type of cyber-attacks carried out by attackers who employ one or more computers to target one or multiple systems and networks have significantly increased. The proliferation of cyber-attacks and threats has resulted in the swift growth of the cyber security sector. This study report examines the extent of the cyber security domain across three sub-fields, along with the constraints of AI in cyber security.

1.2.1 Advancements in Cyber Security Domains

Multiple domains within the field of cyber security, such as digital forensics, malware detection, cloud forensics, and DDoS attacks, have been analyzed for possible improvements using NLP.

1.2.2 Investigation of AI Forms

The potential of three specific forms of artificial intelligence—machine learning, DL, and NLP—to improve cyber security measures has been extensively explored.

1.2.3 AI Limitations Discussion

The discussion focuses on various AI limitations in cyber security, offering valuable insights into the difficulties encountered while implementing AI-driven solutions.

The purpose of defining these sub-fields is to thoroughly examine the extent of the cyber security field and how it relates to the capabilities and constraints of AI. This systematic methodology guarantees a concentrated analysis of crucial areas where AI technologies meet the challenges and prospects in cyber security.

2 Machine Learning in Cybersecurity

With the increasing advancement and popularity of electronic devices, the growing communication and data interchange resulted in many cyber security risks, including data breaches. The level of use of technology is tightly linked to the number of threats it faces. Experts have suggested employing machine learning techniques to address electronic threats, recognizing the evolving nature of cyber threats. Machine learning, a branch of AI, is a powerful tool for tackling cyber-attacks because it adapts and learns from data quite efficiently [8, 9].

Table 2 summarizes the many methods used to address specific cyber security issues. It gives valuable details on the objectives and relevant sources for each methodology.

2.1 Machine Learning's Adaptive Capabilities

Machine learning algorithms can detect, manage, and proactively mitigate known instances of malicious software threats. Nevertheless, specific attacks may exceed the capability of current cyber security technologies. ML utilizes statistical procedures to extract and evaluate crucial data, identify new characteristics, and aid decision making. The main goal is to facilitate computers in acquiring knowledge from data supplied by experts [10]. The methods, classified as supervised and unsupervised, are vital in cyber security.

Table 2 ML techniques for detecting attacks and malicious software

Effective techniques	Objective	Source reference
MLP, K-NN, SVM, FL, ED, MNB	Identification of DDoS attacks and malicious data	[13]
SVM	Establishment of an effective intrusion detection system	[14]
KNN	Implementation of a knowledge-based alert system	[15]
DL, FFC, Y-MLP, DT	Experimental analysis on Android applications for identification of malicious software	[16]
NB, DT	Recognition of ransomware tools (RANDS) operating in the Windows environment	[17]
SVM	Application of machine learning on a substantial dataset for ransomware prediction and detection	[18]
KNN, RF, SVM, and ANN	Detect DOS attacks in SDNs and effectively address cybersecurity management in SDN architectures	[19]
FCM, ANN, and SVM	Identify intrusions and recognize malicious data using data mining techniques	[20]
New RF frameworks	Optimize the random forest strategy for detecting misuse, anomalies, and hybrid-network-based IDSs	[21]

2.2 Ongoing Supervision and Restrictions

Although ML is increasingly used in cyber security, these techniques could improve substantial human supervision. Regular retraining of algorithms is essential since complete data automation is impossible [11, 12]. The section recognizes the significance of machine learning techniques in cyber security while emphasizing their inherent constraints.

2.3 Constraints of Machine Learning

Machine learning algorithms encounter obstacles, such as their incapacity to detect assaults that have not before taken place. Excessive breadth in behavioral restriction policies can result in false positives when identifying behavior patterns and anomalies. Maintaining a balance is essential, as implementing a stricter regulation could reduce effectiveness. The meticulous curation of datasets during training is crucial for achieving the desired outcomes. Cyber criminals may develop methods to bypass a security system if they become aware that it relies solely on one defense technique. Nevertheless, a robust cyber security system based on machine learning can integrate multiple supplementary procedures, hence improving resistance against efforts to bypass security measures.

Expanding on the reasons and methods for conducting research, the investigation of machine learning in cyber security lays the foundation for a comprehensive comprehension of the uses, advantages, and difficulties within this particular field.

3 Deep Learning in Cybersecurity

Deep learning, a type of ML in the broader domain of AI, utilizes neural networks with numerous layers (also called as deep neural networks) to represent and analyze complicated patterns in information. These networks, which are influenced by the organization and operation of the human brain, consist of several layers that handle data processing. They are designed to tackle complex issues within the field of cyber security. The vast nature of these networks allows them to effectively manage complex operations, especially when working with large datasets [22–24].

3.1 DL Applications in Cybersecurity

This segment explores the literature that uses DL techniques in cyber security domains particularly, including intrusion detection, attack identification, and malware detection. Various methodologies are utilized depending on attributes such as the amount of data, the problem's characteristics, the issue's sensitivity, and the level of decision tolerance deemed acceptable in the resolution. Table 3 presents an extensive overview of the diverse deep learning methods utilized in various research papers to address distinct cyber security issues. It provides valuable information about their goals and relevant references.

3.1.1 Secure Implementation of Deep Learning

Deep learning architectures are configured to go beyond localization and are applied to systems based on servers to maintain data integrity, security, and dependability. It is essential to prevent illegal entry into the system. Creating an efficient deep learning model for cyber security comprises two phases. To begin with, the data moves between the local environment and the server, which is encrypted. Afterwards, the encrypted data is transmitted to the server for processing, which involves categorizing it and identifying its specific type. This technology guarantees users a safe conveyance of information, prohibiting illegal system access.

Table 3 DL techniques for detecting malicious activities

Effective technique	Objective	Source reference
CNN and CNN-LSTM	Secure autonomous vehicle systems and control attacks	[25]
LR, SVM, RF, DT, MLP, and RNN	Real-time monitoring and intrusion detection in vehicular data	[26]
ExBERT framework	Predict software vulnerabilities and identify early-stage access	[27]
Multiple concurrent deep models	Identify attack using URLs at the edge network	[28]
MLP and PID	Develop intrusion detection and attack protection application	[29]
K-NN and DNN	Detect intrusions and analyze network anomalies	[30]
RNN	Establish intrusion detection for security against cyber-attacks	[31]
RBM and DBM	Improve detection of abnormal intrusions through enhanced training	[32]
CNN	Classify traffic detection and network fault identification	[33]

3.1.2 Networked Systems and Data Security

Networks function as conduits for users to access and send data, underscoring the importance of strategically positioned networked systems to enforce suitable security protocols. The nature of breaches in a networked environment is contingent upon the level of network activity and the extent of its reach. Larger, more dynamic, and efficient networks have more data flowing across them, necessitating strong processing methods. Parallel processing and deep learning methods are preferred for managing this data because of their remarkable speed and precision.

Expanding on examining machine learning in the preceding section, the discourse on DL enhances comprehension of sophisticated methods in cyber security. The transition from machine learning to deep learning creates a logical and consistent storyline, improving the article’s coherence and continuity.

4 Natural Language Processing (NLP) in Cyber Security

As we further explore the complex field of cyber security, our focus now shifts to the domain of NLP. NLP is a field that combines computer science, linguistics, and artificial intelligence. It incorporates computational linguistics, statistics, ML, and DL techniques. This integration allows for the examination of authentic human language conveyed through written or spoken data, unraveling the complex aspects of

syntax, semantics, pragmatics, and morphology [34–36]. Integrating linguistic principles with computational methods in machine learning bridges the divide between human language and computer science. This relationship enables the application of linguistic information to create algorithmic rules, which in turn allow for solving specific problems and completing essential tasks.

4.1 Applications of NLP in Cyber Security

When researching NLP in the context of cyber security, examining the diverse applications that employ linguistic analysis and computational intelligence is imperative. This section showcases the utilization of NLP in cyber security, combining computer science, linguistics, and AI. We explore the potential of NLP to improve digital defensive mechanisms to counter constantly evolving cyber threats. This includes computer forensics, malware detection, cloud forensics, and DDoS detection.

4.1.1 Computer Forensics

Computer forensics is an interdisciplinary discipline that combines computer science, signal processing, and criminal justice. NLP is crucial in this field. Digital forensics is the systematic preservation, identification, extraction, and documentation of evidence from digital systems for use in criminal or civil investigations [37, 38]. NLP-based digital forensics revolutionizes established approaches by implementing a dynamic process. This method enables data to proactively search for queries, allows data to seek out other data, and lets queries discover new questions [39].

4.1.2 Detection of Malicious Software

NLP techniques such as n-gram, doc2vec, paragraph vectors, and TF-IDF to transform sequences of API calls into feature vectors as part of their investigation into dynamic malware analysis [40].

4.1.3 Cloud Forensics

Cloud forensics refers to collecting and analyzing digital evidence from cloud computing environments. A cloud architecture is designed for digital evidence analysis, thus making a significant contribution to cloud forensics. NLP techniques are integrated into the information extraction (IE) layer, which improves the effectiveness of the forensic process [41].

4.1.4 Detection of DDoS Attacks

Chambers et al. [42] developed NLP models to identify distributed denial-of-service (DDoS) threats that come from social platforms, even when there is no network data available. Wang et al. [43] utilized NLP word embedding techniques and DL algorithms to imagine the probability of DDoS occurrences by supervising pertinent text streams on social media platforms. This section emphasizes the wide range of uses of NLP in cyber security and its transformative impact on improving several areas of digital security.

5 Limitations of AI in Cyber Security

In cyber security, the integration of AI has emerged as a powerful ally in the battle against evolving threats. However, the adoption of AI in this domain is not without its limitations and constraints. As organizations increasingly rely on AI-driven solutions to make their defenses stronger, understanding the limitations inherent in these technologies becomes paramount. First and foremost, the implementation of this technology comes with a significantly higher cost, making it inaccessible to many organizations worldwide. Consequently, ensuring data security becomes a privilege limited by the prohibitive expense associated with adopting this technology. Therefore, the cost factor stands as a significant impediment to widespread implementation [44, 45]. Similarly, Generative AI, particularly in the context of evolving technologies like deep learning, can introduce new challenges by creating sophisticated and previously unseen cyber threats.

As generative AI systems have the capability to generate content, including malicious elements, they might be leveraged by threat actors to devise novel and complex attacks. According to Safety and Security Risks of Generative AI to 2025, generative AI is more likely to exacerbate existing risks rather than create entirely new ones, but it will significantly accelerate the speed and scale of certain threats [46]. Moreover, while AI technologies fall short of ensuring absolute security in industrial settings, their implementation raises ethical concerns, particularly the absence of a moral code for machines. The challenge lies in AI's potential inability to recognize and navigate the moral impacts of decision-making, indicating a gap in its capacity to sense and address moral issues [47].

6 Future Research Directions

Future studies should explore and highlight the significance of creating AI models for more comprehensible cyber security applications. Moreover, it is imperative to scrutinize the ethical dimensions of utilizing AI in cyber security, emphasizing the importance of responsible methodologies. Examine the necessity of establishing ethical

frameworks, norms, and rules in developing and implementing AI technologies to enhance cyber security. Crucially, tackling the difficulties presented by adversarial attacks on AI models in cyber security is imperative. Examine possible approaches to enhance the robustness of AI systems against hostile interference and evasion techniques.

7 Conclusion

AI has a great potential to transform the cyber security industry, providing practical solutions for tackling the increasing threats raised by threat actors. This comprehensive review explores the domains of ML, DL, and NLP within the field of cyber security, analyzing their uses, benefits, and constraints. Machine learning's adaptive skills excel in detecting, handling, and reducing known instances of malicious software threats. Nevertheless, this section emphasizes the importance of continuous monitoring and limitations, recognizing the constraints experienced by machine learning algorithms, such as their inability to identify unexpected threats. Ensuring a balance between precision and comprehensibility is essential for cyber security measures' effectiveness and resilience. The discussion on deep learning explores the complexities of neural networks with numerous layers. It demonstrates their efficacy in addressing complicated challenges, such as intrusion detection and malware identification, while smoothly transitioning from machine learning. This section focuses on highlighting the importance of secure implementations and networked systems. It explains how deep learning may strengthen the integrity and confidentiality of data. The exploration proceeds into NLP in cyber security, where the study of language combines with computer intelligence. This section showcases the diverse applications of NLP in enhancing digital security, including computer forensics, malware detection, cloud forensics, and DDoS attack detection. The integration of linguistics and technology connects human language with cyber security, providing a potent weapon against ever-changing threats.

However, the incorporation of AI in cyber security is not free of challenges. As mentioned in the "Limitations of AI in Cyber Security" section, challenges such as cost, the ability of generative AI to produce advanced threats, and ethical concerns prevent the wide application of AI-powered solutions. Ultimately, this survey offers a comprehensive perspective on the evolving convergence of AI and cyber security. It is essential to have a thorough understanding of the applications and limitations of AI to effectively enhance security measures and ensure an efficient and secure digital future.

References

1. CISA: What is cybersecurity? (2023). <https://www.cisa.gov/uscert/ncas/tips/ST04-001>
2. Berman, D.S., Buczak, A.L., Chavis, J.S., Corbett, C.L.: A survey of deep learning methods for cyber security. *Information* **10**(4), 122 (2019)

3. Statista: Worldwide digital population 2023 (2023). <https://www.statista.com/statistics/617136/digital-population-worldwide/>
4. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endorsed Trans. Internet Things* **9**(4), e1–e1 (2023)
5. Gümüşbaş, D., Yıldırım, T., Genovese, A., Scotti, F.: A comprehensive survey of databases and deep learning methods for cybersecurity and intrusion detection systems. *IEEE Syst. J.* **15**(2), 1717–1731 (2020)
6. Mathews, S. M.: Explainable artificial intelligence applications in NLP, biomedical, and malware classification: a literature review. In: *Intelligent Computing: Proceedings of the 2019 Computing Conference*, vol. 2, pp. 1269–1292. Springer International Publishing (2019)
7. Sahakyan, M., Aung, Z., Rahwan, T.: Explainable artificial intelligence for tabular data: a survey. *IEEE access* **9**, 135392–135422 (2021)
8. Sathya, R.: Ensemble machine learning techniques for attack prediction in NIDS environment. *Iraqi J. Comput. Sci. Math.* **3**(2), 78–82 (2022)
9. Niu, Y., Korneev, A.: Identification method of power internet attack information based on machine learning. *Iraqi J. Comput. Sci. Math.* **3**(2), 1–7 (2022)
10. Mijwil, M.M., Al-Zubaidi, E.A.: Medical image classification for coronavirus disease (COVID-19) using convolutional neural networks. *Iraqi J. Sci.* **62**(8), 2740–2747 (2021)
11. Arshi, O., Chaudhary, A.: Overview of artificial general intelligence (AGI). In: El Hajjami, S., Kaushik, K., Khan, I.U. (eds.) *Artificial General Intelligence (AGI) Security. Advanced Technologies and Societal Change*. Springer, Singapore (2025). https://doi.org/10.1007/978-981-97-3222-7_1
12. Teixeira, M.A., Salman, T., Zolanvari, M., Jain, R., Meskin, N., Samaka, M.: SCADA system testbed for cybersecurity research using machine learning approach. *Futur. Internet* **10**(8), 76 (2018)
13. de Miranda Rios, V., Inácio, P.R.M., Magoni, D., Freire, M.M.: Detection of reduction-of-quality DDos attacks using fuzzy logic and machine learning algorithms. *Comput. Netw.* **186**, 107792 (2021)
14. Li, Y., Xia, J., Zhang, S., Yan, J., Ai, X., Dai, K.: An efficient intrusion detection system based on support vector machines and gradually feature removal method. *Expert Syst. Appl.* **39**(1), 424–430 (2012)
15. Meng, W., Li, W., Kwok, L.F.: Design of intelligent KNN-based alarm filter using knowledge-based alert verification in intrusion detection. *Secur. Commun. Netw.* **8**(18), 3883–3895 (2015)
16. Mahindru, A., Sangal, A.L.: MLDroid—framework for Android malware detection using machine learning techniques. *Neural Comput. Appl. Comput. Appl.* **33**(10), 5183–5240 (2021)
17. Zuhair, H., Selamat, A.: RANS: a machine learning-based anti-ransomware tool for windows platforms. In: *Advancing Technology Industrialization Through Intelligent Software Methodologies, Tools and Techniques*, pp. 573–587. IOS Press (2019)
18. Adamu, U., Awan, I.: Ransomware prediction using supervised learning algorithms. In: *2019 7th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 57–63. IEEE (2019)
19. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
20. Chandrasekhar, A. M., Raghuveer, K.: Confederation of fcm clustering, ann and svm techniques to implement hybrid nids using corrected kdd cup 99 dataset. In: *2014 International Conference on Communication and Signal Processing*, pp. 672–676. IEEE (2014)
21. Zhang, J., Zulkernine, M., Haque, A.: Random-forests-based network intrusion detection systems. *IEEE Trans. Syst., Man, Cybern., Part C (Appl. Rev.)* **38**(5), 649–659 (2008)
22. Abbood, Z.A., Yasen, B.T., Ahmed, M.R., Duru, A.D.: Speaker identification model based on deep neural networks. *Iraqi J. Comput. Sci. Math.* **3**(1), 108–114 (2022)
23. Faieq, A.K., Mijwil, M.M.: Prediction of heart diseases utilising support vector machine and artificial neural network. *Indones. J. Electr. Eng. Comput. Sci.* **26**(1), 374–380 (2022)
24. Mijwil, M.M., Abttan, R.A., Alkhazraji, A.: Artificial intelligence for COVID- 19: a short article. *Artif. Intell.. Intell.* **10**, 1–6 (2022)

25. Aldhyani, T.H., Alkahtani, H.: Attacks to automatus vehicles: a deep learning algorithm for cybersecurity. *Sensors* **22**(1), 360 (2022)
26. Loukas, G., Vuong, T., Heartfield, R., Sakellari, G., Yoon, Y., Gan, D.: Cloud- based cyber-physical intrusion detection for vehicles using deep learning. *IEEE Access* **6**, 3491–3508 (2017)
27. Yin, J., Tang, M., Cao, J., Wang, H.: Apply transfer learning to cybersecurity: predicting exploitability of vulnerabilities by description. *Knowl.-Based Syst.-Based Syst.* **210**, 106529 (2020)
28. Tian, Z., Luo, C., Qiu, J., Du, X., Guizani, M.: A distributed deep learning system for web attack detection on edge devices. *IEEE Trans. Industr. Inf.* **16**(3), 1963–1971 (2019)
29. Thirumalairaj, A., Jeyakarthic, M.: Perimeter intrusion detection with multi-layer perception using quantum classifier. In: 2020 Fourth International Conference on Inventive Systems and Control (ICISC), pp. 348–352. IEEE (2020)
30. Atefi, K., Hashim, H., Kassim, M.: Anomaly analysis for the classification purpose of intrusion detection system with K-nearest neighbors and deep neural network. In: 2019 IEEE 7th Conference on Systems, Process and Control (ICSPC), pp. 269–274. IEEE (2019)
31. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: Perspectives on Ethical Hacking and Penetration Testing, pp. 382–412. IGI Global (2023)
32. Alrawashdeh, K., Purdy, C.: Toward an online anomaly intrusion detection system based on deep learning. In: 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 195–200. IEEE (2016)
33. Wang, W., Zhu, M., Zeng, X., Ye, X., Sheng, Y.: Malware traffic classification using convolutional neural network for representation learning. In: 2017 International Conference on Information Networking (ICOIN), pp. 712–717. IEEE (2017)
34. MonkeyLearn. Natural language processing (nlp): What is it how does it work? (2023). <https://monkeylearn.com/naturallanguage-processing/>
35. Liddy, E.D.: Natural Language Processing (2001)
36. Kumar, E.: Natural Language Processing. IK International Pvt Ltd. (2013)
37. Delp, E., Memon, N., Wu, M.: Digital forensics. *IEEE Signal Process. Mag.* **26**(2), 14–15 (2009)
38. Sammons, J.: The basics of digital forensics: the primer for getting started in digital forensics. Syngress (2014)
39. Irons, A., Lallie, H.S.: Digital forensics to intelligent forensics. *Futur. Internet* **6**(3), 584–596 (2014)
40. Tran, T.K., Sato, H.: NLP-based approaches for malware classification from API sequences. In: 2017 21st Asia Pacific Symposium on Intelligent and Evolutionary Systems (IES), pp. 101–105. IEEE (2017)
41. Arshi, O., Rai, A., Gupta, G., Pandey, J.K., Mondal, S.: IoT in energy: a comprehensive review of technologies, applications, and future directions. *Peer-To-Peer Netw. Appl.*, 1–40 (2024)
42. Chambers, N., Fry, B., McMasters, J.: Detecting denial-of-service attacks from social media text: Applying nlp to computer security. In: Proceedings of the 2018 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long Papers), pp. 1626–1635 (2018)
43. Wang, Z., Zhang, Y.: DDoS Event Forecasting using Twitter Data. In: IJCAI, pp. 4151–4157 (2017)
44. Xia, L.: Learning and decision-making from rank data. Morgan & Claypool Publishers (2019)
45. Dash, B., Ansari, M.F., Sharma, P., Ali, A.: Threats and opportunities with AI-based cyber security intrusion detection: a review. *Int. J. Softw. Eng. Appl. (IJSEA)* **13**(5) (2022)
46. Arshi, O., Mondal, S.: Advancements in sensors and actuators technologies for smart cities: a comprehensive review. *Smart Constr. Sustain. Cities* **1**(1), 18 (2023)
47. Laghari, S.U.A., Manickam, S., Al-Ani, A.K., Rehman, S.U., Karuppayah, S.: SECS/GEMsec: a mechanism for detection and prevention of cyber-attacks on SECS/GEM communications in industry 4.0 landscape. *IEEE Access* **9**, 154380–154394 (2021)

Cyber Security in the Post Quantum Computer Era: Threats and Perspectives



Muhammad Sajid Iqbal, Ahthasham Sajid, and Rida Malik

Abstract Quantum Computing is an imminent technology that would not take much overtaking the classical computers. The new computing techniques are expected to revolutionize the ongoing processes that are currently being accomplished through the available classical computers. Quantum Computers are expected to appear with immense computing speed which on one hand will be a great facility but on the other hand, malicious users may utilize the power of quantum computers to compromise systems, databases and networks. The current article has investigated the possible threat to cyber security when quantum computers will be available publicly. The article has tried to elaborate on cyber security in the post-quantum era in terms of security challenges and possible countermeasures. The emergence of quantum computing poses notable obstacles for the field of quantum cryptography in the quickly changing cyber security scene. A major worry is that existing cryptographic algorithms are susceptible to quantum assaults, especially those based on RSA and ECC, which could be effectively cracked by quantum algorithms such as Shor's algorithm. Furthermore, the creation and application of quantum-resistant algorithms are still in their infancy, necessitating a great deal of investigation and verification to guarantee their resilience against quantum attacks. The administration and distribution of keys in quantum cryptography also presents a challenge because the infrastructure for quantum key distribution (QKD) is still in its infancy and has some real-world drawbacks, such as the requirement for sophisticated quantum hardware and distance restrictions. An additional layer of complexity arises from guaranteeing interoperability between classical and quantum systems. The worldwide cybersecurity community must work together to develop, design, and implement efficient post-quantum cryptography technologies in order to meet these difficulties.

M. S. Iqbal · A. Sajid (✉) · R. Malik

Department of Information Security and Data Science, Riphah Institute of Systems Engineering,
Riphah International University Islamabad, Islamabad, Pakistan
e-mail: ahthasham.sajid@riphah.edu.pk

M. S. Iqbal

e-mail: sajidiqbal5106@gmail.com

R. Malik

e-mail: rida.malik@riphah.edu.pk

Keywords Post quantum computers • Encryption • Decryption • Cryptography • Cybersecurity • SNDL

1 Introduction

The concept of quantum computing appeared in the 1980s and was popularized after Feynman published an article under the title; ‘Simulating Physics with Computers’ where he talked about computers built on quantum mechanics [1]. Quantum computing is an emerging field that focuses on performing computing operations at the sub-atomic level. The classical computers handle data in the form of bits that are 0s and 1s while the quantum computers store data in the form of qubits also called quantum bits which will enable data storage in multiple states simultaneously [2]. Consequently, the rise of the quantum computers will revolutionize the computing speed and time tremendously. The fact has been mentioned by Arute et al. in the following words; “The promise of quantum computers is that certain computational tasks might be executed exponentially faster on a quantum processor than on a classical processor” [3]. Inevitably, such a tremendous speed acquired as a result of quantum computers will influence the world of cyber security. The reason behind this proposition is that initially the symmetric keys were used because of being faster and lighter on computational grounds. However, the issues attached to the key distribution through secure channels, especially on a larger scale enhanced the value of Asymmetric encryption or Public Key Cryptography (PKC) systems. However, the security of Public Key Cryptography also relies on computationally complex processes. For instance, the Diffie-Hellman process makes use of discrete logarithms and Rivest-Shamir-Adleman (RSA) depends on mathematical operations of Integer Factorization. The security of these complex mathematical operations depends on polynomial time which is going to be influenced by the great computational speed attained through quantum computers which subsequently will influence the field of cyber security. Security is an ever-evolving phenomenon, with the innovations of new technologies being employed in systems, networks, and storage; security issues also pop up continuously and speedily. In the current era, professionals are already grappling with the emerging security issues associated with AI, Cloud Computing, and IoTs. An online platform while mentioning the most crucial threats in the year considered Cloud Third-Party Threats, Mobile Malware, and Weaponization of Legitimate Tools [4]. In the current era, most devices and networks are making use of classical computers and encryption methods to secure assets. As there is no silver bullet in the matters of cyber security and there is always some method to exploit vulnerabilities, the addition of quantum computers will heighten the issue if futuristic measures are not taken today and the futuristic measures must aim at quantum-resistant strategies. Scholars consider that quantum computers are going to play a vital role in cyber security as Bova et al. have prioritized the utilization of quantum computers in cyber security while discussing the applications of quantum computers their article divides the application of quantum computers into four segments of which cyber

security is atop. They have mentioned the point as; “We divide these applications (of quantum computers) into four industry verticals: cyber security, materials and pharmaceuticals, banking and finance, and advanced manufacturing” [5].

Switching cyber security designs to the emerging age of quantum-based operations is surely urgent because of the expected endangering possibilities that quantum computing may create to challenge the currently used encryption techniques. Balogh et al. say that while talking about quantum threats to in-use encryption they mainly focus on two algorithms i.e. Shor’s algorithm and Grover’s algorithm. Shore’s algorithm based on integer factorization in polynomial time is capable of breaking asymmetric encryption and Grover’s algorithm is capable of brute-forcing any black-box function with n -bit keys [6].

Quantum computers possess the ability to compromise encryption algorithms, like ECC and RSA because the algorithms used in encryption processes rely on the mathematical complexities. As quantum computers have the power to solve complex mathematical calculations exponentially more quickly than the present generations of computers, this ability theoretically claims that the power of factorization of large numbers is going to enable quantum computers to break those encryptions which are considered secure against the abilities of the classical computers, in other words; “Quantum processors are on the verge of realizing their promise to revolutionize computing” [7].

As a countermeasure to this challenge, professionals and researchers are aiming at developing algorithms for cryptography that could withstand the encryption-breaking ability in the post-quantum era. Stakeholders in the world of the cyber need to get ready for the era when quantum computers will be in use commonly and quantum-resistant encryption and communication will become crucial. The transition to adapt to a new era cannot be achievable quickly and easily in any terms including financial expenditure as well. Considering the mentioned developments and requirements this research is an effort to point out the expected revolutionary changes, the urgency to adapt to new changes and the major challenges that would be faced while attempting to adapt to new scenarios in terms of both proactive and reactive defense strategies as Shor has mentioned that such quantum algorithm exist which is capable of cracking cryptographic primitives [8].

The paper’s structure includes a thorough examination of the hazards that quantum computers could pose to the cryptography systems in use today, emphasizing particular weak points and attack avenues. And the developments in post-quantum cryptography, talking about several algorithms that have been presented and how resistant they are to quantum assaults. The effects of these advancements on cyber security procedures and guidelines, provide information on critical modifications and tactics that will work in the future. The report concludes with a summary of the main conclusions and a focus on the necessity of taking preventative action to protect digital data as the quantum computing age approaches.

2 Literature Review

The evolving nature of Information Technology is indicating the ultimate necessity of quantum computers in the field. Ghosh et al. have talked in detail about Quantum Computers and Cyber security in their research they dissected the situation when Quantum computers would revolutionize computer operation but at the same time, they will be posing cyber security threats. Consequently, there will be an instant need for new encryption methods. To strengthen their perspective the researchers have also discussed various potential attacks and the countermeasures of which being proactive in the evolving trends may keep more secure. The positive aspect is that on one hand, quantum computers may threaten the current encryption systems while on the other hand, the same computers will speed up security operations. As quantum computers become more powerful and widespread, it will be necessary to develop new encryption methods that are resistant to quantum attacks. Fortunately, efforts are already underway to develop quantum-resistant cryptography [9].

The authors, like Rawat et al. have talked about this indicator and the importance of the transition to the new technology. However, these authors have limited themselves to mentioning the importance of quantum computers in Artificial Intelligence in the following words; “It is a well-known fact that classical or traditional computing methods are not able to solve complex machine learning problems efficiently. To address this issue, quantum computing has come into the picture” [10]. The current paper will focus on the value of quantum computing in cryptography and ultimately the influence of quantum computers on cyber security. The ever-evolving nature of computers, communication and data ultimately transforms the standards, requirements and techniques used in securing the related assets and processes as well. In this regard, one of the initial threats was Peter Shor’s introduction of probabilistic polynomial-time quantum which proposed to solve mathematical algorithms more efficiently and quickly which can brute force the security measures [11]. Peter Shor developed an algorithm that can utilize quantum computing to rapidly factorize large numbers as illustrated in Fig. 1.

Practical utilization of quantum computers in the field requires an immense number of qubits available while in reality “for the potency of quantum computers, the existing number of qubits remains insufficient for practical real-world problem-solving, necessitating a substantial increase by several orders of magnitude” [13]. This is still unachieved even though leading companies like Microsoft IBM and Google are trying to achieve the milestone. Google in 2022 succeeded in developing 443-qubit Osprey and Google aims at leveraging this limit to 4000 qubits by the year 2025. IBM is following a roadmap for the adoption in the emerging era of quantum computers. “2026 will bring us circuit knitting across parallel quantum processors, the ability to decompose quantum circuits into shorter circuits, run them in parallel, and then stitch them back together with classical hardware” [14].

But to break the current cryptographic algorithms millions of error-free qubits will be required which does not seem impossible in the current level of investments in this field [15].

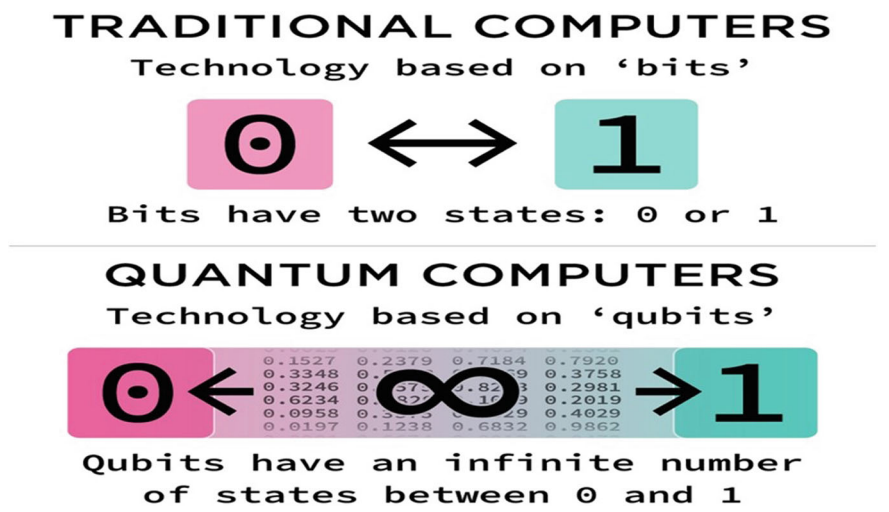


Fig. 1 Tradition computing versus quantum computing [12]

AT present quantum computers are not available to break the cryptographic algorithms but SNDL attacks are inevitable as the SNDL attacks i.e. Store Now and Decrypt Later attacks depend on a futuristics plan as adversaries may eavesdrop and steal sensitive data in encrypted form and keep it stored until the availability of the quantum computers capable of decrypting that information. Current major players in the industry are facing a complex dilemma, on one hand, it is not possible to ignore the evolving technology as delaying the process of switching to post-quantum computers may turn them into a low-hanging fruit in terms of security of sensitive data while on the other hand, it poses challenges, costs, and even impossibilities in terms of updating infrastructure which is previously running on the systems compatible with classical computers [16].

Since the development of quantum computers, companies, and institutions have been actively working to standardize, create, and apply PQC on a worldwide scale. Even though PQC research and development has a long history, the first PQCrypto conference was organized on an international level in 2006 which solely focused on PQC. NIST is putting active efforts to shape cyber security to the optimum level and their input is visible through the following visual representation in Fig. 2.

NIST is working on standardizing PQ primitive and has released Federal Information Processing Standards (FIPS) documents for three standardized schemes which are CRYSTALS-KYBER as Module-Lattice-Based Key Encapsulation Mechanism Standard, CRYSTALS-Dilithium as Module-Lattice-Based Digital Signature Standard and SPHINCS+ as Stateless Hash-Based Digital Signature Standard [18].

In the standardization process, NIST is not the only active role player, there are others as well like IETF works on engineering aspects of Post-quantum Cryptography, ETSI works on collaborating publications and seminars on Industrial as well as real-world PQC, NSA covers military operations related PQC, FutureTPM trying

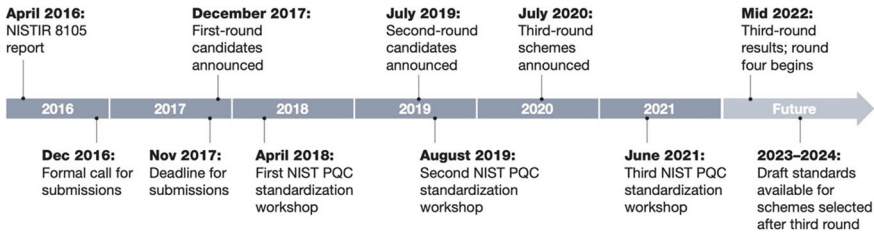


Fig. 2 NIST PQC process timeline [17]

to ensure long-term security in Quantum Computers, German company Quantum RISC oversees practical use PQC in industry. The Quantum RISC project aims to investigate post-quantum cryptography for resource-constrained embedded systems and to bring embedded PQC from theory into practice [19].

Malina et al. in an article have talked about ongoing security in their work, they have examined the security libraries that are currently in use, the recommendations for current security measures, and the support for Post-Quantum Cryptography (PQC) in popular security protocols. They also evaluated the emerging PQC algorithms by the PQC standardization on common platforms that can be used in intelligent infrastructures and the recent recommendation of hash-based signatures for software/firmware signing by the National Institute of Standards and Technologies (NIST) and how certain areas of intelligent infrastructures are expected to be impacted by impending post-quantum migration. The focused areas of the article are Quantum-Resistant Cyber security, Current Protocols and Intelligent Infrastructures. The researchers have talked about the current status of the implementation of PQC. The article claims that “there is a consensus on the terms of migration to PQC methods from 2025” [20].

Public block Chains and IoTs are gaining prominence in the modern world in terms of economy and ease of life. Blockchain’s are used in the transaction process of crypto-coins which have gained much value in the present era. Cryptocurrencies are virtual coins which are transacted and stored on digital devices. Like other digital devices and networks, the systems that handle these virtual currencies require a primary focus on security. Amongst the cryptocurrencies currently, the highest-valued Bitcoin uses the algorithm of SHA-256 for encryption. To keep such digital assets safe the systems will have to consider security in the post-quantum era. The threat of quantum computers to SHA-256 can be mitigated simply by extending a hash size [21].

IoT’s having limited lifetime and limited storage capacity also pose challenges if an attempt is to be made to secure these against quantum attacks. The task is so huge that a complete transition to the new system of PQC seems infeasible as most IoT’s come with a limited lifetime while developing PQC is costly as separate compatible chips for IoT’s will be needed to make them compatible with PQC. NIST has suggested multiple signature schemes in this regard. Balogh et al. focused on security concerns of IoT’s and the possible threats in the age of quantum computing. The future IoT’s are

going to be integrated with the emerging technologies of cloud and blockchain. The researchers have proposed a security model in this regard and suggested the use of segmentation and detection methods. The IoTs being part of clouds and networks are supposed to communicate among themselves, therefore demand secure encryption of communication and consideration of quantum-resistant encryption would become integral for the IoTs also as “postquantum cryptography provides tools to secure devices against future quantum attackers [6].

NIST is focusing on the applicability of schemes that may secure embedded devices. On this issue, Shahram Mossayebi the CEO of Crypto Quantique who is committed to providing greater security in the IoTs says, “The anticipated lifespan of many Internet of Things installations is ten years. We have already developed a quantum-driven root-of-trust technology for semiconductors that will provide the foundation for secure IoT networks” [22]. In this regard, as shown below in Fig. 3 Crypto Quantique has announced a post-quantum computing PQC chip-to-cloud IoT security platform.

Bova et al. along with discussing the development of quantum computing have also talked about its potential to be utilized in the industry and how it will transform the industry. The article has highlighted certain limitations of the classical computers and the power of quantum computers but on the other hand, there are limitations when considering the transformation of currently existing systems to new technology. The researchers have also accepted the limitations in terms of surety about the efficiency of the impending quantum computers talking about these uncertainties. Alan Aspuru-Guzik put it in an interview with Nature magazine, said “there is a role for imagination, intuition and adventure. Maybe it’s not how many qubits we have; maybe it’s about how many hackers we have” [23].

Dam et al. considered the advent of quantum computers the beginning of a new race. And just like in race, it demands an urgency of adoption. There is a dire need to seek quantum-resistant techniques to pace with novelty in terms of cyber-attacks and cyber defense. The research conducted by Duc-Thuan and his fellows found that classical cryptographic methods are at risk because of the power achieved through the greater computing ability of quantum computers. “Quantum computers can solve specific mathematical problems that are computationally infeasible for classical computers, such as factoring large integers” [24].

Along with discussing the efforts by NIST, and various PQC methods, the researchers have also talked about the challenges when it comes to the practical implementation of PQC. However, quantum computing is still in the emerging state and the full potential of the attacks and defense through the quantum computers could be assessable only after their full utilization in industry and publicly. Vaishnavi et al. discussed the cyber challenges, especially, in the domains of banking and e-commerce. Like other areas utilizing cryptography, the mentioned sectors will also be at risk when quantum computers will be used publicly. The researchers mentioned that AES, RSA Blowfish, Diffie-Hellman and ECC are the most commonly employed techniques of encryption used by most worldwide companies [25].

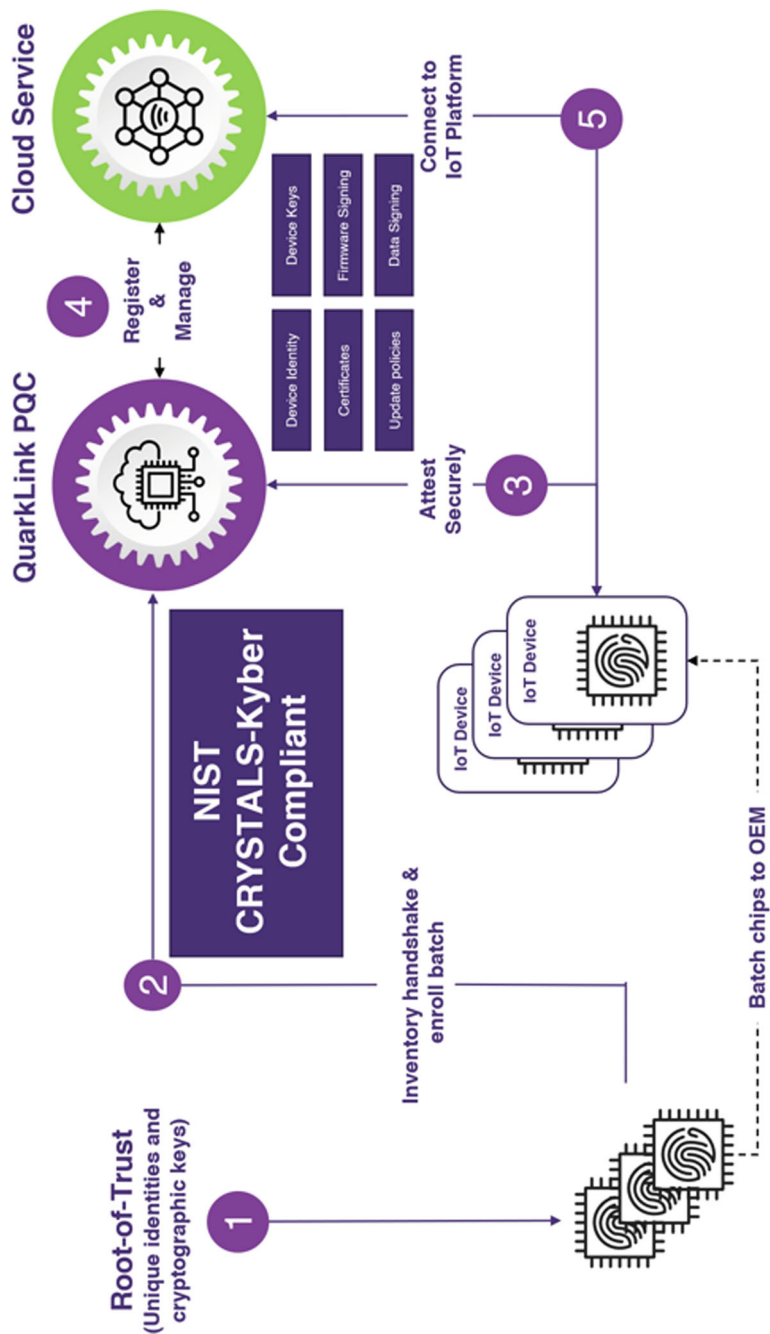


Fig. 3 Post-quantum computing (PQC) version of its QuarkLink chip-to-cloud IoT security platform [22]

Balamurugan et al. Also discussed the emerging threats posed by quantum computers. The researchers further elaborated the concept by elaborating that cryptographic systems depend on arithmetic operations which when exposed to quantum computers would be solved in polynomial time and would not be able to withstand the speed acquired with quantum computers. They have further added the concept of code-based cryptography which is an area that further needs to be explored and utilized in PQC. Code-based cryptography is an auspicious area that employs error-correcting codes as the basis for safe communication, and it is harder to attack from quantum computers [26]. This code-based cryptography scheme is also being considered for a quantum-resistant signature scheme to enhance security measures [27].

The researchers have performed a SWOT (Strength, Weakness, Opportunity, Threat) analysis of various encryption techniques to show how they can be weaker in the age PQC. The following illustration has been drawn by Vaishnavi et al. to warn against the imminent risks (Fig. 4).

Samandari and Gritti in their research found that most IoTs make use of MQTT (Message Queue Telemetry Transport) protocol for communication as it is a lightweight and simple messaging protocol, however, at the same time this protocol comes with a limitation or defect i.e. it does use authentication. And the advantageous feature of being lightweight but without any authentication makes the IoTs very vulnerable when evaluated on security standards, especially in the era of quantum computers [29].

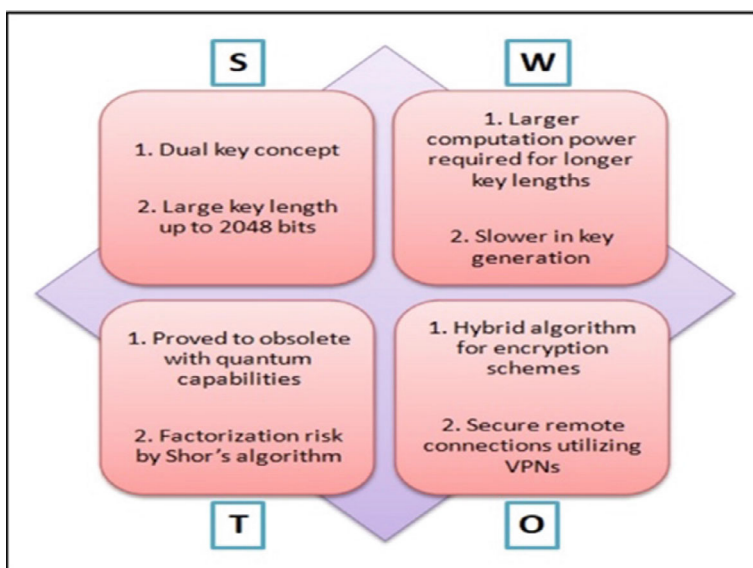


Fig. 4 SWOT Analysis of RSA (Rivest, Shamir, Adleman [28])

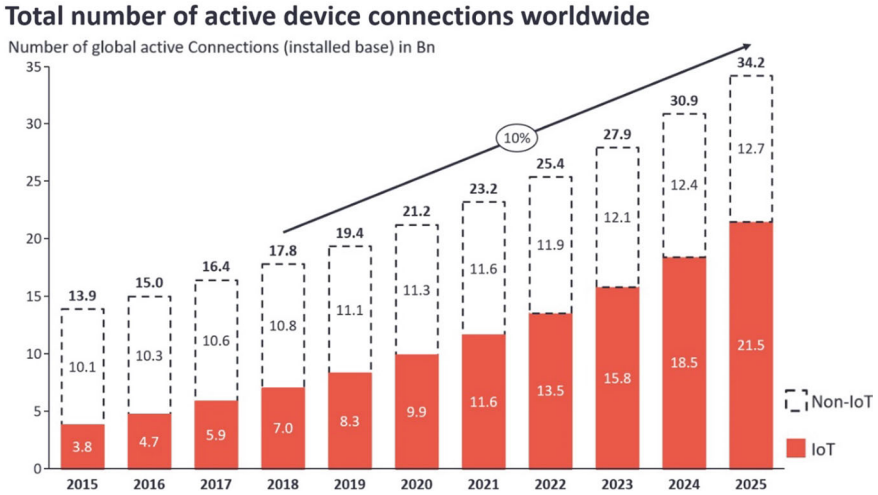


Fig. 5 Increasing number of IoT devices [31]

Samandari and Gritti have suggested that quantum-based signatures for IoTs would be used to make them more secure as “Postquantum KEM-based authentication for MQTT will be useful in contexts where swift and secure communication is essential” [29].

The emerging IoTs increase the importance of cyber security in the coming era. As dependency on IoTs is constantly increasing, IoTs mostly do not make use of encryptions as diligently as most of the other systems and networks utilize even though this system is connecting billions of devices[30]. The graphical representations in Fig. 5 show the increasing trend of IoTs.

3 Research Methodology

For this research qualitative research methodology is adopted where various articles, websites resources, books and online journals about cryptography, encryption, information security and Post Quantum Cryptography were studied and analyzed. It has been found that the quantity and quality of research on Post Quantum computers has become a prominent niche for researchers as shown in the below graph (Figs. 6, 7).

The data which is available from Google Scholar, ResearchGate, IEEE Science Direct was consulted widely. Qualitative research methodology was used but where necessary the figures and facts have also been included with proper citation to the resources. To keep the study updated with the latest trends and requirements only the works published after 2019 were considered. Table 1 provides an overview of the works that were considered for this survey:

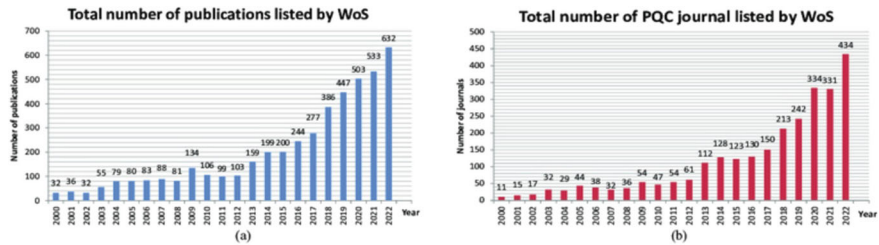


Fig. 6 Listing publications and journals[32]

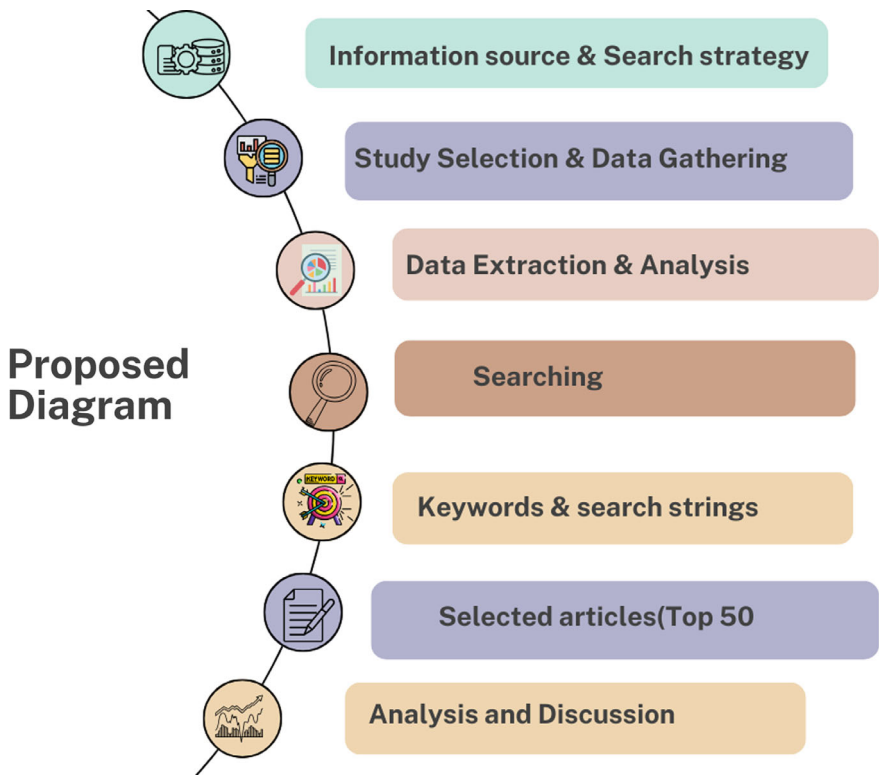


Fig. 7 Proposed Methodology

4 Key Findings and Suggestions

The review of several researches made it clear that:

- i. Encryption would become vulnerable in the coming era of quantum computers.

Table 1 Literature review

Topic	Year	Authors
QuantumRISC	2024	D. M. Kreutzer, “QuantumRISC Next Generation Cryptography for Embedded Systems,” QuantumRISC, [Online]. Available: https://www.quantumrisc.de/index_en.html . [Accessed 11 May 2024]
Quantum computing paradigm	2023	Uttam Ghosh, Debashis Das & Pushpita Chatterjee, “A Comprehensive Tutorial on Cyber security in Quantum Computing Paradigm,” Authorea Preprints, 2023
A lattice-based privacy-preserving	2023	S. Darazi, K. Ahmadi, S. Aghapour, A. Yavuz & M. Kermani, “A Survey on PQ Standardization, Applications, Challenges and Opportunities,” Envisioning the Future of Cyber Security in Post-Quantum Era, 2023
Quantum computing	2022	B. Rawat, N. Mehra, A. S. Bist, M. Yusup, Y. P. A. Sanjaya, “Quantum Computing and AI: Impacts & Possibilities,” ADI Journal on Recent Innovation (AJRI), vol. 03, pp. 201–207, 02 March 2022
Commercial applications	2021	F. Bova, A. Goldfarb and R. G. Melko, “Commercial Applications of Quantum Computing,” EPJQuantumTechnology, vol. 8, no. 1, 2021
Beyond quantum supremacy	2019	M. Brooks, “Beyond Quantum Supremacy: the Hunt for Useful Quantum Computers,” Nature, vol. 574, no. 7776, p. 19, 2019
Quantum supremacy	2019	Arute, F., Arya, K., Babbush, R., “Quantum Supremacy Using a Programmable Superconducting Processor,” Nature, pp. 505–510, 2019
Post-quantum cryptography		NIST https://csrc.nist.gov/projects/pqc-dig-sig

- ii. Transitioning to new standards necessary for PQC is going to be the top priority if organizations and even governments want to ensure the confidentiality, integrity and availability of their data or information.
- iii. SNDL (Secure Now and Decrypt Later) can be one of the strategies of the malicious actors, therefore, the organization would have to secure the current data if it is going to be valuable in the future too.
- iv. Quantum-resistant encryption is going to be the standard, and to meet the compliance and legal requirements, the organization must consider the transition to PQC.
- v. The cyber-world is also transitioning to cloud computing therefore quantum-resistant cloud computing must also be a crucial consideration

- vi. IoTs are emerging as complimentary accessories for basic needs of life and keeping the IoTs safer in the post-quantum era will be a great challenge. It is, therefore, suggested that industries associated with IoTs should take in time steps to produce and install such IoTs which could resist quantum attacks.

Based on studies researchers like Joseph et al. have also suggested that organizations interested in protecting their systems and users against quantum attacks should adopt PQC [17].

In this regard National Security Agency of the USA has also issued warnings that mentioned the threats that quantum computers may pose to the existing security and encryption measures. The NSA has stressed the need for quantum-resistant cryptography along with imploring organizations to take steps for a timely transition to the new standards. They have also initiated to standardize for the algorithms which would prove to be quantum-safe in the future. However, the transition is not easy in terms of technologies in use and technologies required for PQC along with the financial impact of the transition. Campagna et al. in the realization of the challenges while attempting to transition say, that previous experiences with even simpler algorithms indicate that “it takes considerable time and effort for an entire industry to come together and update protocol standards and deploy them using the new algorithms” [33]. To address such challenges, researchers have attempted to present feasible solutions also, for example, researchers like Joseph et al. have recommended a strategy for the organization to shift to the new technology. The researchers also pointed out that the standardization bodies may face pressure from the industries when prompted for a quick transition to new standards but the standardization bodies should persistently focus on clear focus on creating standards with a security-first mindset. A timeline of PQC-related events is presented below, emphasizing the need for immediate action despite the challenges (Fig. 8).

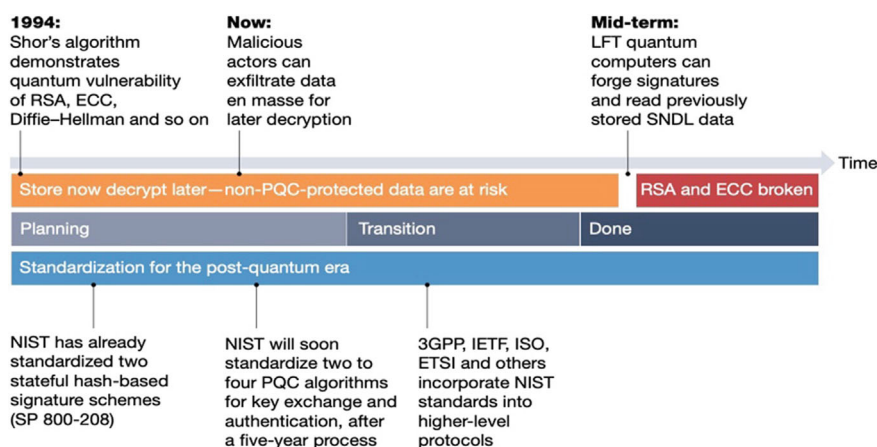


Fig. 8 Post quantum cryptography timeline [34]

5 Conclusion

The survey of the available material on Post Quantum Computers makes it clear that it is inevitable for the cyber-world to adopt quantum-resistant cryptography to ensure security now and in the times to come. The communication networks and devices used are increasing exponentially and so is the need for security and security is supposed to be at risk with the advent of quantum-powered computers. The industries as well as the individual end users would have to construct methods and technologies which should be quantum-attack-resistant. The industries would have to undergo a transition to post-quantum cryptography on an urgent basis otherwise the quantum attacks would compromise sensitive information in the future. The organizations in this regard may face multifaceted hurdles in this regard as on one hand they cannot afford compromised confidentiality and integrity and on the other hand, they are bound to meet standards and compliances to carry on their normal business.

References

1. Althobaiti, O.S., Dohler, M.: Cyber security challenges associated with the internet of things in a post-quantum World. *IEEE Access* **8**, 157356–157381 (2020)
2. Rawat, B., Mehra, N., Bist, A.S., Yusup, M., Sanjaya, Y.P.A.: Quantum computing and AI: impacts & possibilities. *ADI J. Recent. Innov. (AJRI)* **3**, 201–207 (2022)
3. Arute, F., Arya, K., Babbush, R.: Quantum supremacy using a programmable superconducting processor. *Nature* 505–510 (2019)
4. Points, C.: Biggest Cyber Security Challenges in 2023 [Online] Available: <https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cybersecurity/biggest-cyber-security-challenges-in-2023/#:~:text=While%20ransomware%20and%20data%20breaches,have%20even%20greater%20business%20impacts>. Accessed 23 May 2024
5. Bova, F., Goldfarb, A., Melko, R.G.: Commercial applications of quantum computing. *EPJ Quantum Technol.* **8**(1) (2021)
6. Balogh, S., Gallo, O., Ploszek, R., Špaček, P., Zajac, P.: IoT security challenges: cloud and blockchain, postquantum cryptography, and evolutionary techniques. *Electronics* **10**(21), 2647 (2021)
7. Proctor, T., Rudinger, K., Young, K., Nielsen, E., Blume-Kohout, R.: Measuring the capabilities of quantum computers. *Nat. Phys.* **18**(1), 75–79 (2022)
8. Liu, Z.Y., Tseng, Y.F., Tso, R., Mambo, M., Chen, Y.C.: Public-key authenticated encryption with keyword search: cryptanalysis, enhanced security, and quantum-resistant instantiation. In: *Proceedings of the 2022 ACM on Asia Conference on Computer and Communications Security*, pp. 423–436 (2022)
9. Ghosh, U., Das, D., Chatterjee, P.: A comprehensive tutorial on cyber security in quantum computing paradigm. *Authorea Prepr.* (2023)
10. Rawat, B., Mehra, N., Bist, A.S., Yusup, M., Sanjaya, Y.P.A.: Quantum computing and AI: impacts & possibilities. *ADI J. Recent. Innov. (AJRI)* **3**(2), 203–207 (2022)
11. Darazi, S., Ahmadi, K., Aghapour, S., Yavuz, A., Kermani, M.: A Survey on PQ Standardization, Applications, Challenges and Opportunities. *Envisioning the Future of Cyber Security in Post-Quantum Era* (2023)
12. Vikram, S., Hans, B.: Rethinking Cyber security for a Quantum World 2020 [Online]. Available: <https://www.science.org.au/curious/policy-features/rethinking-cybersecurity-quantum-world>. Accessed 12 May 2024.

13. Yang, Z.: A survey of important issues in quantum computing and communications. *IEEE Comm. Surv. Tutorials* (2023)
14. IBM: Our roadmap to advance useful quantum computing. In: IBM [Online]. Available: <https://www.ibm.com/quantum/technology#roadmap>. Accessed 05 May 2024
15. Mosca, M., Piani, M.: Quantum threat timeline report 2020. *Glob. Risk Insitute* (2021)
16. Darzi, S., Akhbari, B., Khodaiemehr, H.: A lattice-based privacy-preserving multi-functional and multi-dimensional data aggregation scheme for smart grid. *Clust. Comput.* **1**(25), 263–278 (2022)
17. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Leichenauer, S., Hidary, J., Venables, P., Hansen, R.: Transitioning organizations to post-quantum cryptography. *Nature* **605**(7909), 237–243 (2022)
18. NIST: Post-Quantum Cryptography: Digital Signature Schemes. In: NIST [Online]. Available: <https://csrc.nist.gov/projects/pqc-dig-sig>. Accessed 06 May 2024
19. Kreutzer, D.M.: QuantumRISC next generation cryptography for embedded systems. *QuantumRISC* [Online]. Available: https://www.quantumrisc.de/index_en.html. Accessed 11 May 2024
20. Malina, L., Dobias, P., Hajny, J., Kim, K.: On deploying quantum-resistant cyber security in intelligent infrastructures. In: *Proceedings of the 18th International Conference on Availability, Reliability and Security*, New York (2023)
21. Kan, K., Une, M.: Recent Trends on Research and Development of Quantum Computers and Standardization Of Post-Quantum Cryptography (2021)
22. Electronics, N.: First post-quantum computing IoT security platform compliant with NIST standards. *New Electron.* [Online]. Available: <https://www.newelectronics.co.uk/content/news/first-post-quantum-computing-iot-security-platform-compliant-with-nist-standards/>. Accessed 12 May 2024
23. Brooks, M.: Beyond quantum supremacy: the hunt for useful quantum computers. *Nature* **574**(7776), 19 (2019)
24. Dam, D.T., Tran, T.H., Hoang, V.P., Pham, C.K., Hoang, T.T.: A survey of post-quantum cryptography: start of a new race. *Cryptography* **07**(03) (2023)
25. Vaishnavi, A., Pillai, S.: Cyber security in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. *J. Phys.: Conf. Ser.* **1964**(04) (2021)
26. Balamurugan, C., Singh, K., Ganesan, G., Rajarajan, M.: Post-quantum and code-based cryptography—some prospective research directions. *Cryptography* **5**(04), 44 (2021)
27. Roy, P.S., Morozov, K., Fukushima, K., Kiyomoto, S.: Evaluation of code-based signature schemes. *Cryptol. Eprint Arch.* [Online]. Available: <https://eprint.iacr.org/2019/544>. Accessed 18 May 2024
28. Vaishnavi, A., Pillai, S.: Cyber security in the quantum era-a study of perceived risks in conventional cryptography and discussion on post quantum methods. *J. Phys. Conf. Ser.* **4**, 2021 (1964)
29. Samandari, J., Gritti, C.: Post-quantum authentication in the MQTT protocol. *J. Cyber Secur. Priv.* **3**(3), 416–434 (2023)
30. Althobaiti, O.S., Dohler, M.: Cyber security challenges associated with the internet of things in a post-quantum world. *IEEE Access* **8**, 157356–157381 (2020)
31. Analytics, I.: State of the IoT 2018: Number of IoT Devices Now at 7B—Market accelerating [Online]. Available: <https://iot-analytics.com/state-of-the-iot-update-q1-q2-2018-number-of-iot-devices-now-7b/>. Accessed 16 May 2024
32. Reserachgate [Online]. Available: https://www.researchgate.net/figure/Number-of-publications-published-from-2000-to-2022-listed-by-Web-of-Science_fig3_373123693. Accessed 14 May 2024
33. Campagna, M., LaMacchia, B., Ott, D.: Post quantum cryptography: readiness challenges and the approaching storm. *arXiv preprint arXiv:2101.01269* (2021)
34. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F.D., Lacombe, O., Hidary, J., Venables, P., Hansen, R.: Transitioning organizations to post-quantum cryptography. *Nature* **605**, 237–243 (2022)

Deep Neural Network for DoS Detection in Wireless Sensors Networks



Hajar Fares, Hajraoui Nirmin, and Hajraoui Abderrahmane

Abstract As the wireless sensor network (WSN) evolve rapidly in many applications and fields, it has become increasingly vulnerable of various types of attacks. DoS attack is considered as one of the most dangerous attack that poses a major threat in wireless sensor network security and could have major effects and serious consequences in WSNs functionalities. Recently, intrusion detection systems become crucial security components. In this paper, we propose an approach deep learning to enhance the level of security in such network. We have evaluated and analyzed the efficiency of Deep Neural Network (DNN) in DoS detection, using the standard metrics of evaluation: accuracy, precision, F1-score and recall. Our model was carried out using a well-known dataset WSN-DS, intended for wireless sensor networks, containing four types of Dos attacks: Blackhole, Grayhole, Flooding and TDMA. The experiment result demonstrate the effectiveness of DNN in DoS detection with high accuracy achieved.

Keywords DoS attack · Wireless sensor network · Intrusion detection · DNN

1 Introduction

Wireless sensor networks (WSN) [1] is a special type of ad hoc network, which does not require infrastructure. It has composed with small components called sensors, randomly distributed to gather data and send it to the base station. Unfortunately, these sensors have limited resources in memory, CPU, battery, etc. [2]. Sensors in the network can produce huge amount of data, and may have heterogeneous features

H. Fares (✉) · H. Abderrahmane

Equipe of Telecommunication and Detection, Faculty of Science, Abdelmalek Essaadi University, Tetouan, Morocco

e-mail: hajar.fares@etu.uae.ac.ma

H. Nirmin

Laboratory of Remote Sensing and Geographic Information System, ENSA, University of Abdelmalek Essaadi, Tetouan, Morocco

or similar devices and referred as homogenous. The applications of WSN [1] have become various and increase day by day, but their deployment in harsh area make them vulnerables of many attacks type. Among these types, Dos attack could have a serious impact in WSNs functionalities [3]. There are many types of Dos attack as Blackhole, Grayhole, wormhole, flooding, selective forwarding and others. Their main negative impact is designed to interrupt the normal functioning of a server, service, or network by saturating it with a flood of internet traffic.

Classical solutions provide good level of security, unfortunately, the computational consumption, make them no longer useful and practical. The number of searches to find a reliable and less-resource consuming solution is often increasing, taking on consideration the challenges and the limited resources of wireless sensor networks already cited,

An intrusion detection system (IDS) is a software or hardware tool that is able to monitor the processes of traffic, extract information, filtrate, classify normal and abnormal status and identify unauthorized nodes in the system, by analyzing the traffic, and then make decision even by notifying, logging or preventing [4]. To help user resolving the vulnerability present in the system or network.

Machine learning is a subset of artificial intelligence (IA), based on learning process, which include two main steps, the first one is training and the second one is the test step. Generally, machine learning can be defined as an action that allows the machine to learn automatically without being explicitly directed [4].

Recently, security approaches have been enhanced. Intrusion detection system based on artificial intelligence and learning models have proved to be the most efficient and practical with low cost and high accuracy. Many researches have tested the accuracy and the efficiency of different machine learning models for intrusion detection [5].

Despite the importance of machine learning to protect WSN from vulnerabilities or malicious attacks. The accuracy of prediction depend on one hand of the learning model, the appropriate dataset used and the feature selection step to obtain highest rate and the approximation of the precision in the classification of attacks.

The main goal of this paper is to make an analysis study of Deep Neural Network (DNN) as a deep learning model, in order to find a robust security method that takes into consideration the limited resources of wireless sensor networks and preserves the network's lifetime in the long term. In our contribution, we have focused especially on four types of DoS attacks in using a specialized dataset called WSN-DS.

Our paper is organized as follows:

Section 1, introduce our contribution. Section 2; review the related works of our papers. The detailed methodology in Sect. 3. While Sect. 4 present the experiment result obtained of our model and finally, Sect. 5 conclude our paper.

2 Related Works

This section is focused on literature study, it present the latest research in DoS detection in wireless sensor networks using different learning model.

Otaïr, Mohammed, et al. [6] are proposed an approach to detect Dos malicious attack, using NSL-KDD dataset with two learning models: K-means and SVM, the accuracy obtained was 98, 97%.

Anwer, Meryem et al. [7] Using random forest analysis, they were able to obtain the maximum accuracy rate of 85, 34% on the NSL-KDD dataset.

Barki, Lohit, et al. [8] have suggested a method for detecting DDoS attacks that makes use of the SDN dataset and three classification models: Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbors (KNN). With a 99.97% accuracy rate, they have combined a variety of feature selection methods, such as t-Distributed Stochastic Neighbor Embedding (t-SNE), Principal Component Analysis (PCA), and Recursive Feature Elimination (RFE).

Yang, Liqun, et al. [9] have proposed a scheme for intrusion detection in wireless network. They have employed Conditional Deep Belief Network (CDBN). The detection accuracy obtained for Normal sample, Flooding attack; False attack and Injection attack, respectively are 0.989, 0.808, 0.727, 0.991.

Sudar, K. Muthamil, et al. [10] have studied DDoS attacks detection. They have applied two machine-learning models, namely Decision Trees and Support Vector Machines, using the KDD99 dataset for training and testing purposes. According to the experimental findings, the SVM algorithm performed better than the DT method, which only managed an accuracy rate of 78%. Instead, the SVM algorithm attained an accuracy rate of 85%.

Perez-Diaz, Jesus Arturo, et al. [11]. Have integrated the components from the Intrusion Detection and Prevention Systems straight into the SDN controller. Several machine learning algorithms, such as J48, Decision Tree, REP Tree, Random Forest, SVM, and Multilayer Perceptron (MLP), have improved their methodology. Using the CICDDoS-2019 dataset, the efficacy of this method was assessed. Notably, the MLP algorithm attained an accuracy rate of up to 95%.

Bindra, Naveen et al. [20] have used and examined a number of machine learning models to identify DDoS assaults in an effort to find the best model using attack datasets from real-world incidents. By using the Random Forest classifier, they were able to achieve 96% accuracy.

3 Methodology

This section introduces our research method. It analyze rigorously Deep Neural Network performance to identify DoS attacks in wireless sensor networks. Our methodology include several steps such as Dataset selected, data preparation,

learning model training and testing and finally the evaluation step to measure the performance of the model chosen.

3.1 Dataset Selected

The dataset used in intrusion detection simulation comes from research on sensor networks and information systems. Since each intrusion detection system in the field uses a learning model, the dataset selection is crucial to assessing the effectiveness of the selected model.

This dataset comprises both normal and abnormal traffic data, encompassing a limited range of attacks. There are a limited number of dataset specified for intrusion detection in wireless sensor networks including NSL-KDD, WSN-DS, and WSN-BFSF. For our experiments, we have opted to use the well-known WSN-DS dataset [12] due to its ample data volume and diverse Dos attack types. Developed by authors Almomani et al. [12]. WSN-DS is tailored for intrusion detection in wireless sensor networks, focusing particularly on Dos attacks. This dataset is structured with 23 attributes generated by the LEACH protocol, featuring 374,661 records representing four Dos attack variations (Blackhole, Grayhole, Flooding and Scheduling) alongside normal traffic.

3.2 Data Preprocessing

Before starting building our model, the preprocessing step is primordial; it aims to prepare the dataset to be used. It is significantly affect the quality of the models by enhancing the level of accuracy. To carry out this step, many tasks must be done, including:

- **Removing Spaces from the Column Names**

We found that the column names contain spaces at the beginning and the end of the names, and this will cause.

- **Removing Useless Columns**

Some columns are not useful for our analysis and it may cause problems when we try to build our models, so we need to remove these columns.

- **Removing the Rows that Contain Missing Values**

Missing values in the dataset may cause problems when we try to build our models, so we need to remove the rows that contain missing values.

- **Removing Duplicates**

Duplicates in the dataset may cause overfitting when we try to build our models, so we need to remove the duplicates.

- **Data Balancing**

When we found that, the dataset is imbalanced, so we need to balance the dataset by up sampling the minority classes and down sampling the majority classes.

- **Data Splitting into Training and Testing**

It's based on dividing data into two groups. The first one is called training data, it allows the model to learn and the second is for testing the model and evaluating its effectiveness.

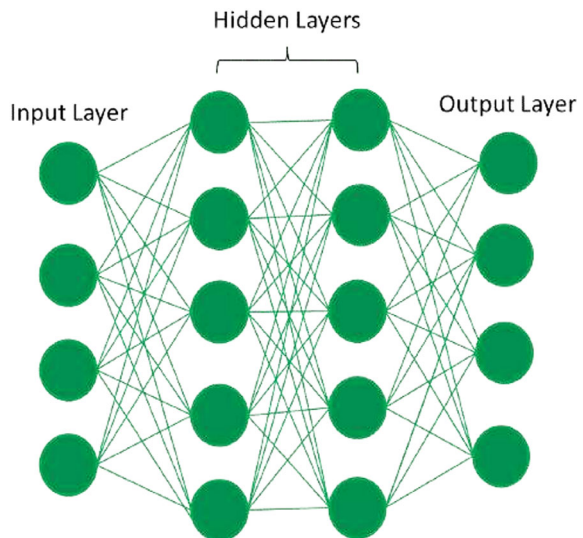
3.3 Model Building

Deep learning is a subfield of machine learning that uses artificial neural networks for classification. It involves representing data in several layers, from a lower to a higher layer, and extracting important features to get the best possible outcome [13] (Fig. 1).

Since the development of deep learning, it have known an extensive use according to its significant impact on many areas in machine learning, such as object detection [14], speech and image recognition [15–17], and language translation.

Despite the various advantages of Deep learning and its ability to function with or without labels, Deep Learning approach usually require high computational power and dedicated GPUs to work and to achieve good results [14, 17, 18].

Fig. 1 Deep learning architecture



Model: "sequential_3"

Layer (type)	Output Shape	Param #
dense_6 (Dense)	(None, 100)	1900
dense_7 (Dense)	(None, 100)	10100
dense_8 (Dense)	(None, 5)	505
=====		
Total params: 12505 (48.85 KB)		
Trainable params: 12505 (48.85 KB)		
Non-trainable params: 0 (0.00 Byte)		

Fig. 2 DNN architecture

Deep Neural Network (DNN) becomes a vessel of knowledge, traversing through the intricacies of data, illuminating its true essence, and capturing the essence of complexity within its expanding reaches. In the grand tapestry of computation, the Deep Neural Network stands tall as an emblem of human ingenuity, a testament to our ability to decode the enigmatic realm of intelligence, and a beacon guiding us towards a future where the boundaries of human knowledge are pushed ever further [19]. Figure 2 presents the DNN architecture implemented in this work:

3.4 Evaluation Metrics

In machine learning (ML), evaluation metrics are primordial for evaluating the performance of a model and understanding how well it generalizes to unseen data. The choice of evaluation metrics depends on the type of problem you are solving (classification, regression, etc.). With TP denoting True Positives, TN representing True Negatives, FP signifying False Positives, and FN indicating False Negatives, the evaluation metrics employed in this study are respectively:

Accuracy: in the context of this research, is a metric that gauges the overall correctness of the model. It is calculated using the formula:

$$accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

- **Recall:** in the context of this research, is a metric that assesses the model's ability to capture all the relevant instances. It is calculated using the formula:

$$recall = \frac{TP}{TP + FN} \quad (2)$$

Precision: the proportion of accurately recognized labels to all positive classifications

$$precision = \frac{TP}{TP + FP} \quad (3)$$

- **F1-Score:** in the context of this research, is a metric that balances precision and recall into a single measure. It is calculated using the formula:

$$F1 - score = \frac{2TP}{2TP + FP + FN} \quad (4)$$

4 Experiment Result and Discussion

In this section, we present the experiment result of deep neural network compared and discussed with the related works already cited.

4.1 Experiment Result of DNN

The assessment of the research findings was carried out meticulously, employing a variety of measures to assess the Deep Neural Network's (DNN) capacity to identify Denial of Service (DoS) assaults, specifically in wireless sensor networks (Fig. 3).

Classification Report:

	precision	recall	f1-score	support
Blackhole	0.78	0.88	0.83	2043
Flooding	0.90	1.00	0.95	631
Grayhole	0.90	0.82	0.86	2985
Normal	1.00	1.00	1.00	67965
TDMA	0.99	0.93	0.96	1309
accuracy			0.99	74933
macro avg	0.91	0.93	0.92	74933
weighted avg	0.99	0.99	0.99	74933

Fig. 3 Accuracy report of DNN

Table 1 Comparative analysis

Reference	Methods and approach	Accuracy output
[6]	K-means, SVM dataset: NSL-KDD	98.99%
[8]	RF, SVM, KNN, PCA	99.97%
[7]	RF dataset: NSL-KDD	85.34%
[10]	DT, SVM dataset: KDD99	78% DT 85% SVM
[11]	J48, RF, DT, SVM, MLP dataset: CICDDoS-2019	95%
Our contribution	DNN dataset: WSN-DS	99%

According to the classification report, the tested model have demonstrated impressive performance, with accuracy, precision, and recall.

4.2 Discussion

After evaluating Deep Neural Network, we have found that this model has high accuracy, precision, recall and f1-score, in comparison with the related works (Table 1). This result, demonstrate the effectiveness of Deep Learning model as a robust model for DoS detection in wireless sensor networks.

This research can be extended and governed with the optimization technique i.e. utilization of Machine Learning techniques over traditional approaches.

In summary, our work provide several advantages:

- **High Accuracy:** Achieves superior performance in detecting a wide range of network intrusions, including DoS and DDoS attacks.
- **Scalability:** The model's architecture allows it to scale effectively with increasing data volumes, making it suit-able for real-time intrusion detection.
- **Resource Efficiency:** Optimized for deployment in resource-constrained environments such as WSNs, where computational and energy resources limited.

These advancements highlight the potential of deep learning models like Deep Neural Network, to significantly, enhance the robustness and reliability of IDS in protecting modern network infrastructures against evolving cyber threats.

5 Conclusion

Several security approaches focus to make WSNs secure, such as authentication, encryption and key management, etc. Unfortunately, not all these mechanisms are enough. Recently Machine Learning have provided an alternative mechanism of security with low cost, by decreasing the energy and increasing the lifetime of the WSNs.

In this paper, we have focused on DoS detection using a well-known dataset WSN-DS. We have evaluated a deep learning model (DNN) using the standard metrics of evaluation and the result obtained demonstrate its effectiveness as an intrusion detection method.

6 Future Directions

In the future works, we think about evaluating other machine and deep learning models, we think also in using hybrid deep learning model and including additional metrics of evaluation such as Receiver Operating Characteristic (ROC) that could provide a more nuanced understanding of model performance.

References

1. Akyildiz, I.F., Vuran, M.C.: *Wireless Sensor Networks*. John Wiley & Sons (2010)
2. Sunil Kumar, K.N., Bhyratae, D.A., Ashwini, A.M., Gatti, R., Santosh Kumar, S., Anne Gowda, A.B.: A grey wolf optimization-based clustering approach for energy efficiency in wireless sensor networks. *Int. J. Commun. Netw. Inf. Secur. (IJCNIS)*, **15**(2), 63–87 (2023). <https://doi.org/10.17762/ijcnis.v15i2.6171>
3. Safaldin, M., Otair, M., & Abualigah, L.: Improved binary gray wolf optimizer and SVM for intrusion detection system in wireless sensor networks. *J. Ambient Intell. Humanized Comput* **12**, 1559–1576 (2021)
4. Sudar, K.M., Beulah, M., Deepalakshmi, P., Nagaraj, P., Chinnasamy, P.: Detection of distributed denial of service attacks in SDN using machine learning techniques. In: 2021 International Conference on Computer Communication and Informatics, ICCCI 2021. Institute of Electrical and Electronics Engineers Inc. (2021). <https://doi.org/10.1109/ICCCI50826.2021.9402517>
5. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
6. Otair, M., Ibrahim, O.T., Abualigah, L., Altalhi, M., Sumari, P.: An enhanced grey wolf optimizer based particle swarm optimizer for intrusion detection system in wireless sensor networks. *Wireless Netw.* **28**(2), 721–744 (2022)
7. Anwer, M., Khan, S.M., Farooq, M.U., Waseemullah: Attack detection in IoT using machine learning. *Eng., Technol. Appl. Sci. Res.* **11**(3), 7273–7278 (2021)
8. Barki, L., et al.: Detection of distributed denial of service attacks in software defined networks. In: 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). IEEE, (2016)
9. Wen, W., Shang, C., Dong, Z., Keh, H. C., & Roy, D. S.: An intrusion detection model using improved convolutional deep belief networks for wireless sensor networks. *Int. J. Ad Hoc and Ubiquitous Comput.* **36**(1), 20–31 (2021)
10. Sudar, K. M., & Nagaraj, P.: TCP flood defender: TCP SYN flood attacks detection in SDN environment using statistical and ensemble machine learning methods. In: *Software-Defined Network Frameworks*, pp. 291–308. CRC Press (2024)
11. Perez-Diaz, J.A., Valdovinos, I.A., Choo, K.K.R., Zhu, D.: A flexible SDN-based architecture for identifying and mitigating low-rate ddos attacks using machine learning. In: *IEEE Access*, vol. 8, pp. 155859–155872 (2020). <https://doi.org/10.1109/ACCESS.2020.3019330>

12. Almomani, I., Al-Kasasbeh, B., Al-Akhras, M.: WSN-DS: A dataset for intrusion detection systems in wireless sensor networks. *J. Sens.* **2016**, 4731953 (2016)
13. Abbas, A., Khan, M.A., Latif, S., Ajaz, M., Shah, A.A.: A new ensemble-based intrusion detection system for internet of things. *Arab. J. Sci. Eng.* (2022)
14. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endorsed Trans. Internet Things* **9**(4), e1–e1 (2023)
15. Dahl, G.E., Yu, D., Deng, L., Acero, A.: Context-dependent pre-trained deep neural networks for large-vocabulary speech recognition. *IEEE Trans. Audio Speech Lang. Process.* **20**(1), 30–42 (2012)
16. Arshi, O., Chaudhary, A.: Intelligence (AGI). *Artif. Gen. Intell. (AGI) Secur.: Smart Appl. Sustain. Technol.*, 1 (1990)
17. Parkhi, O.M., Vedaldi, A., Zisserman, A.: Deep face recognition. In: *British Machine Vision Conference* (2015)
18. Yang, L., Li, J., Yin, L., Sun, Z., Zhao, Y., Li, Z.: Real-time intrusion detection in wireless network: a deep learning-based intelligent mechanism. *IEEE Access* **8**, 170128–170139 (2020)
19. Arshi, O., Rai, A., Gupta, G., Pandey, J.K., Mondal, S.: IoT in energy: a comprehensive review of technologies, applications, and future directions. *Peer-To-Peer Netw. Appl.*, 1–40 (2024)
20. Bindra, N., Sood, M.: Detecting DDoS attacks using machine learning techniques and contemporary intrusion detection dataset. *Autom. Control. Comput. Sci.* **53**(5), 419–428 (2019)

Survey on IoT Security Threats Application and Architectures



**Maria Hanif, Ahthasham Sajid, Rida Malik, Fariha Shoukat,
and Muhammad Sajid Iqbal**

Abstract The Internet of Things (IoT) marks a major shift in communication as it enables physical devices to generate, transmit, and share information independently. IoT applications are being developed to perform various tasks that allow devices to operate without human intervention. This change is necessary to increase user comfort, efficiency, and automation. However, creating this robust environment requires security and privacy, such as strong authentication mechanisms and effective recovery strategies to mitigate the threat. Significant changes are needed in the design of IoT applications to ensure the sustainability of the IOT ecosystem. This article will take an in depth look at the security risks and threat sources associated with IOT Applications. Based on the analysis, it examines the different technologies developed to build trust in IOT systems. The article focuses specifically on the impact of IoT devices and machine learning role to enhanced security.

Keywords IoT · IoT security · Machine learning · Decentralized systems · IoT applications

M. Hanif

Department of Computer Science, IQRA University, Islamabad, Pakistan

e-mail: maria.hanif@iqraisb.edu.pk

A. Sajid (✉) · R. Malik · F. Shoukat · M. S. Iqbal

Department of Information Security and Data Science, Riphah Institute of Systems Engineering,
Riphah International University Islamabad, Islamabad, Pakistan

e-mail: ahthasham.sajid@riphah.edu.pk

R. Malik

e-mail: rida.malik@riphah.edu.pk

F. Shoukat

e-mail: farihashoukat421@gmail.com

M. S. Iqbal

e-mail: sajidiqbal5106@gmail.com

1 Introduction

Physical devices are being integrated into the internet at a very rapid pace. A recent Gartner report predicted that the number of connected devices worldwide will influence 8.4 billion by 2020, and this number is predictable to increase to 20.4 billion by 2022 [1]. This expansion is particularly evident in Western Europe, North America, and China, demonstrating the global acceptance and use of IoT applications. Furthermore, machine-to-machine (m2m) network is likely to grow from 5.6 billion in 2016 to nearly 27 billion by 2024. The financial tracking for the Internet of Things (IoT) industry reflects the growing importance of this sector, with revenues predictable to grow from \$892 billion in 2018 to a staggering \$4 trillion by 2025 [2], smart environment, smart grid, smart shopping, smart agriculture, etc. illustrate the breadth of the Internet of Things. It envisions devices that can not only connect to the internet and local networks, but also communicate directly with other devices worldwide. The emergence of the Social Internet of Things (SIOT) brings a new perspective that enables a better relationship between users and devices. This advancement allows users to connect and share devices wirelessly over the Internet, ushering in a new era of collaboration in the IoT ecosystem [3].

Despite the many applications of the Internet of Things (IoT), security and privacy are still major concerns. The lack of trust and interconnectedness of the IoT ecosystem creates problems that can hinder the widespread adoption of new IoT applications and limit their full potential. In addition to the security issues generally associated with the Internet, mobile networks, and wireless sensor networks (WSNS), IoT also brings its own unique challenges, such as privacy issues, authentication issues, management challenges, and data storage issues [4] Fig. 1.

Table 1 summarizes the factors that contribute to the complexity of securing IoT environments compared to traditional IT devices. These combined challenges and vulnerabilities create an environment that is particularly susceptible to various cyber threats. Security and privacy breaches in globally deployed IoT applications are unfortunately common. For example, the Mirai attack in late 2016 affected around 2.5 million internet-connected devices and led to a distributed denial-of-service (DDoS) attack. Following Mirai, other notable botnet attacks such as Hajime and Reaper also targeted numerous IoT devices [5].

The inherent characteristics of IoT devices, such as low power and relatively weak security features, make them attractive targets for attackers seeking to infiltrate home and corporate networks, thereby jeopardizing user data security. Moreover, IoT extends beyond inanimate objects to include devices integrated into the human body for real-time monitoring of various organs. While there haven't been any actual attacks of this kind, if such devices were infiltrated, there might be serious repercussions, including hazards to privacy and data manipulation [6].

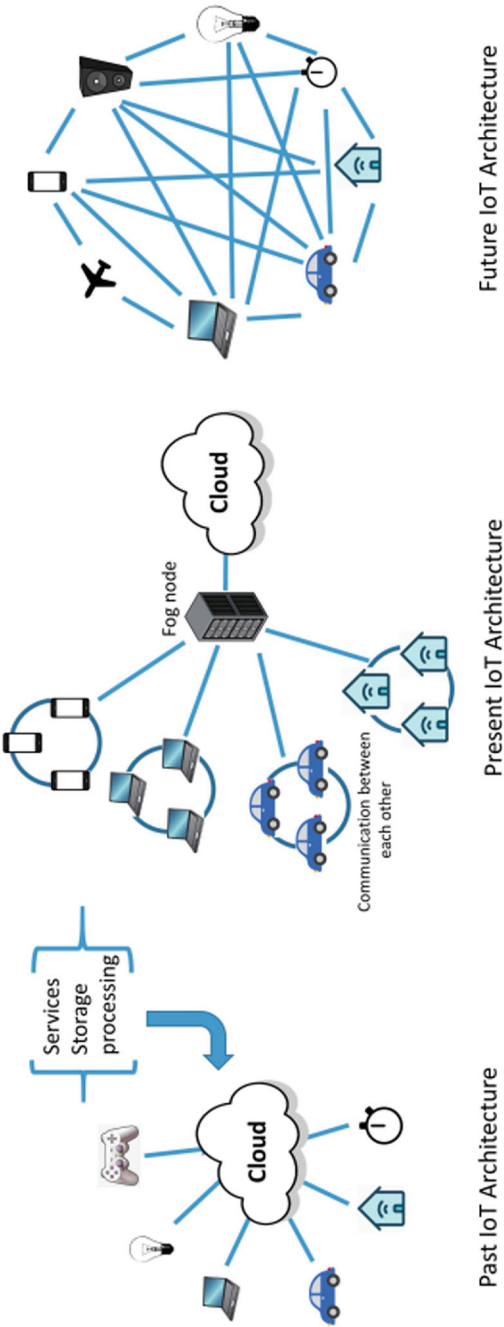


Fig. 1 Past, present and the future architecture [9]

Table 1 Comparison of security of IT devices versus IoT devices

Widespread IT security	IoT security
Devices used in widespread IT have a lot of resources	It's important to carefully configure security measures for IoT devices
Rich resource devices are the foundation of widespread IT	Devices that have hardware and software limitations make up Internet of Things systems
Complex algorithms are implemented for lower capabilities and wider security	Lightweight algorithms are the only ones that are recommended
High security is a result of homogenous technology	The volume of heterogeneous data produced by IoT combined with heterogeneous technologies increases the attack surface

2 IoT System Architecture

Internet of Things (IoT) expansion has had a significant impact on Cyber-Physical Systems (CPS), where physical elements are monitored and actions are triggered depending on observable changes. For essential industries like transportation and electrical infrastructure, this is especially crucial.

This is especially important for vital industries like transportation and power infrastructures. Although the security issues unique to CPS are important, this study does not primarily address them [7].

An IoT ecosystem typically comprises four essential layers:

1. **Sensing Layer:** Uses actuators and sensors to collect data and perform functions [8].
2. **Network Layer:** Transmits the gathered data over communication networks [8].
3. **Middleware Layer:** Serves as a bridge between the network and application layers, providing business services and enabling intelligent resource allocation and computation [8].
4. **Application Layer:** consists of complete Internet of Things applications, such as intelligent grids, intelligent industries, and intelligent transportation [8].

Every layer poses different security concerns, and there are more security hazards associated with the gateways that facilitate data transit across these layers. Maintaining the general security and integrity of the IoT infrastructure requires addressing security issues at all tiers and gateways [10–13]. This paper offers a thorough analysis of the body of research on IoT security solutions. It starts by defining the fundamental limitations that pose a threat to reliable security in IoT applications. Blockchain, fog and edge computing should be investigated that how it can play vital role in improving security under Internet of Things.

The use of various smart devices and gadgets under IOT environment which may cause security threats are depicted in Fig. 2. Moreover, Fig. 3 describe various attacks which may occur upon each layer of IOT.

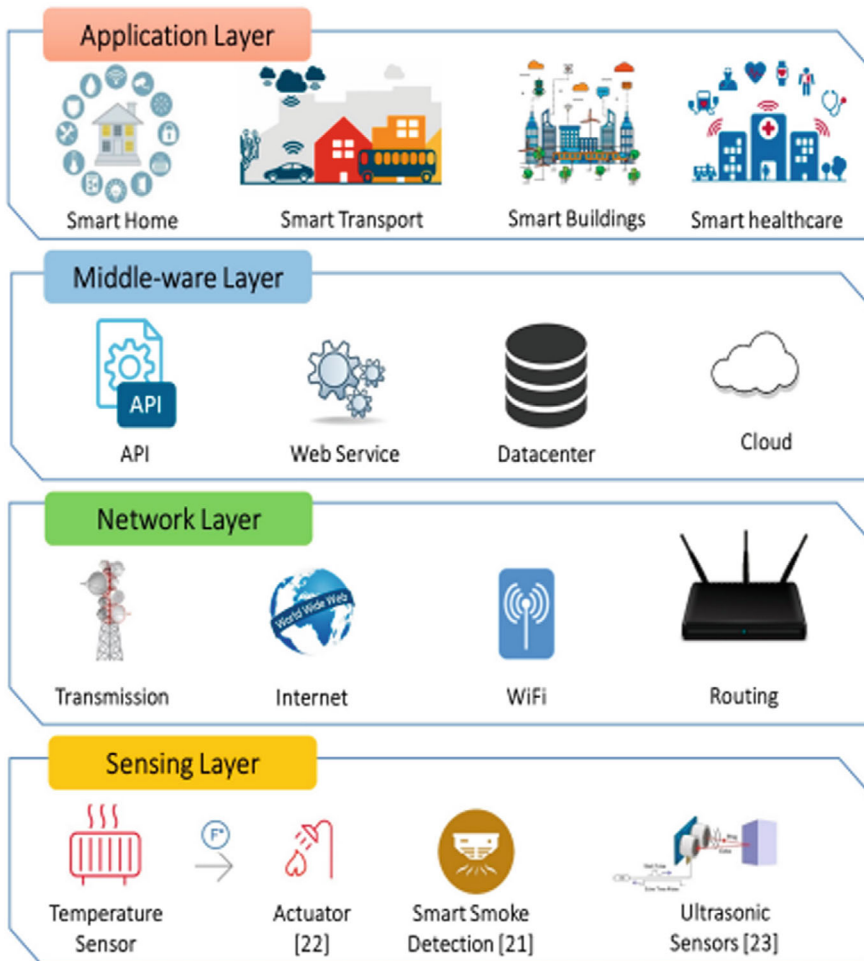


Fig. 2 Layers in IoT system [5]

Security Issues at the Network Layer

- **Phishing Site Attacks:** This attack can be targeted upon multiple IOT devices and if one of the attempt is successful so it would open various vulnerabilities' further [14–17].
- **Access Attacks:** The attack under which unauthorized access to data is access for more amount of time.
- **Denial-of-Service (DDoS)/DoS Attacks:** Attack over server under IOT environment is launch it would lead to denial of services may arise for the connecting IOT devices [17, 18].

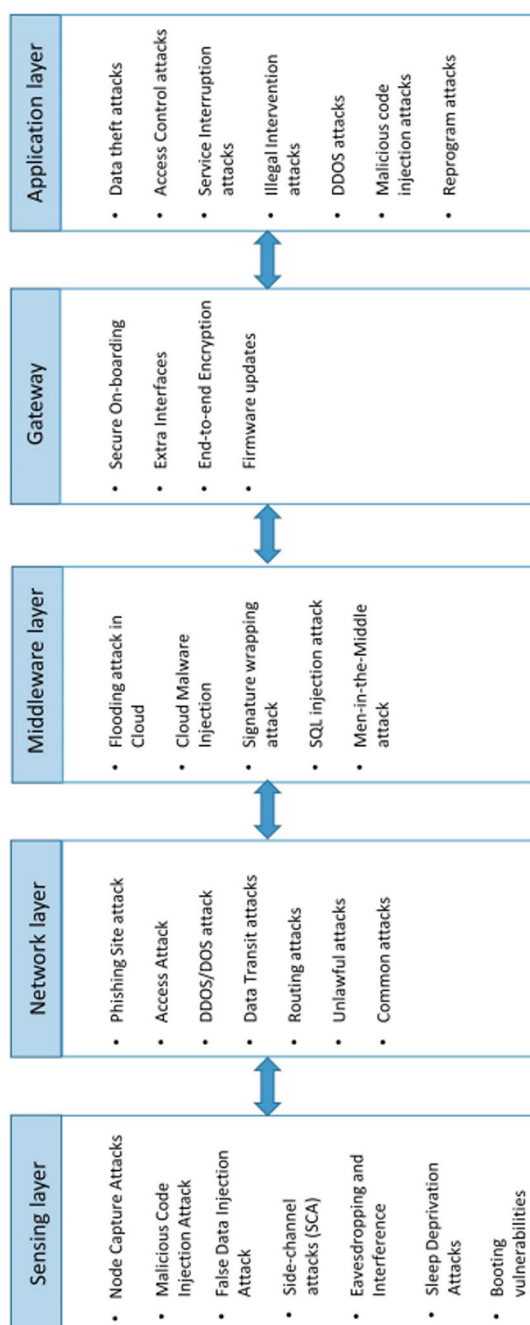


Fig. 3 Types of attacks on IoT

- **Data Transit Attacks:** During data transmission between sensors, actuator and cloud attack could be done [19].

Security Issues at the Middleware Layer

- **Man-In-The-Middle Attack:** Attacked can get control of the broker as MIM and intercept and manipulate communication between client and subscribers [20, 21].
- **SQL Injection Attack:** This attack is launched to modify record of the database and threat to integrity of data [22].
- **Signature Wrapping Attack:** Attackers exploit vulnerabilities in XML signatures used in webservice, manipulating messages without detection.
- **Cloud Malware Injection:** Attackers can introduce malicious code or rogue virtual machines in cloud environments, potentially intercepting and manipulating requests [23].
- **Flooding Attack in Cloud:** Similar to DoS attacks, flooding attacks use automated requests to drain cloud services' resources, affecting performance and quality of service [24].

Security Issues at Gateways

- **Secure On-boarding:** Protection of encryption keys are vital attacked may launch eavesdropping and MIM attack to get the key information [25].
- **Extra Interface:** Attack surface can be reduced with minimizing no of interfaces and protocol usage so that backdoor can be minimized accordingly.
- **End-to-End Encryption:** Better to use this encryption between gateways and end devices.
- **Firmware Updates:** Firmware of the devices must be updated with latest signatures [26, 27].

Security Issues at the Application Layer

- **Data Theft:** During transmission, sensitive data handled by Internet of Things applications is susceptible to theft. To prevent data theft, methods including encryption, data isolation, and authentication are used.
- **Access Control Attack:** Unauthorized data access can result from attacks on access control systems, opening the system up to more security risks [28].
- **Service Interruption Attack:** By overloading servers with requests, these attacks prevent authorized users from utilizing services.
- **Malicious Code insertion Attack:** IoT systems are susceptible to malicious code insertion in the absence of appropriate code validation. Account takeover and system disruption are possible through cross-site scripting (XSS) attacks.
- **Sniffing Attack:** If strong security measures are not in place, attackers utilizing sniffer software may monitor and record network traffic, resulting in privacy violations.
- **Reprogramming Attack:** Inadequate security during the programming and updating processes might result in the remote reprogramming of Internet of Things devices, which can cause disruptions or network

Solutions to Security Threats

- **Denial of Service (DoS) Assaults:** Machine learning techniques i.e. Multi-Layer Perception, Deep neural networks, support vector machines would help in minimizing spoofing attacks which may lead to DOS attack later on.
- **Digital Fingerprinting:** This can be used so unlocking of devices and authorization should be properly manage again for this classification and machine learning algorithms should be used.

Open Issues, Challenges, and Future Research Directions

- **Blockchain Security Issues:** The issue of using blockchain technology is that as the more participants or devices takes place in communication the size of blockchain needs more storage and would reduce speed [29].
- **Machine Learning Issues:** The selection of appropriate machine learning algorithm is very important to get high accuracy and success rate if inappropriate algorithm is selected so performance will be decreased.

3 Conclusion

We can greatly improve security in IoT applications and guarantee their continuous growth and resilience by addressing these concerns and pursuing future research directions. This survey highlights various security threats across different IoT layers, including sensing, network, middleware, gateway, and application layers. It also explores both existing and emerging ML-based solutions and discusses open issues and challenges.

References

1. Dlamini, N.N., Johnston, K.: The use, benefits and challenges of using the internet of things (Iot) in retail businesses: a literature review. In: 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), pp. 430–436. IEEE (2016)
2. Jose, A.C., Malekian, R.: Improving smart home security: integrating logical sensing into smart home. *IEEE Sens. J.* **17**(13), 4269–4286 (2017)
3. Kumar, S., Sahoo, S., Mahapatra, A., Swain, A.K., Mahapatra, K.: Security enhancements to system on chip devices for iot perception layer. In: 2017 IEEE International Symposium on Nanoelectronic and Information Systems (INIS), pp. 151–156. IEEE (2017)
4. Liao, C.H., Shuai, H.H., Wang, L.C.: Eavesdropping prevention for heterogeneous internet of things systems. In: 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1–2. IEEE (2018)
5. Arshi, O., Chaudhary, A.: Intelligence (AGI). *Artif. Gen. Intell. (AGI) Secur.: Smart Appl. Sustain. Technol.*, 1 (1990)
6. Li, C., Chen, C.: A multi-stage control method application in the fight against phishing attacks. In: Proceeding of the 26th Computer Security Academic Communication across the Country, p. 145 (2011)

7. Koliass, C., Kambourakis, G., Stavrou, A., Voas, J.: Ddos in the iot: mirai and other botnets. *Computer* **50**(7), 80–84 (2017)
8. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: *Perspectives on Ethical Hacking and Penetration Testing*, pp. 382–412. IGI Global (2023)
9. Spirina, K.: Biometric Authentication: The Future of IoT Security Solutions. <https://www.iotevolutionworld.com/iot/articles/438690-biometric-authentication-future-iot-security-solutions.html>
10. Awad, A.I.: Machine learning techniques for fingerprint identification: a short review. In: *International Conference on Advanced Machine Learning Technologies and Applications*, pp. 524–531. Springer (2012)
11. Shaukat, S., et al.: Examination of phishing attempts on web-based business applications and their preventions. In: *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, pp. 315–320. Gautam Buddha Nagar, India (2024). <https://doi.org/10.1109/IC3SE62002.2024.10593139>
12. Rakha, M.A., Akbar, A., Chhabra, G., Kaushik, K., Arshi, O., Khan, I.U.: A detailed comparative study of AI-based intrusion detection system for smart cities. In: *2024 International Conference on Communication, Computer Sciences and Engineering (IC3SE)*, pp. 1783–1790. Gautam Buddha Nagar, India (2024). <https://doi.org/10.1109/IC3SE62002.2024.10593485>
13. Reddy, G.N., Reddy, G.J.: A Study of Cyber Security Challenges and its Emerging Trends on Latest Technologies (2014). arXiv preprint arXiv:1402.1842
14. Bhatia, T.K., Hajjani, S.E., Kaushik, K., Diallo, G., Ouaisa, M., Khan, I.U. (eds.): *Ethical Artificial Intelligence in Power Electronics* (1st ed.). CRC Press (2024). <https://doi.org/10.1201/9781032648323>
15. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
16. Javed, S., Sajid, A., Kiren, T., Khan, I.U., Dewi, C., Cauteruccio, F., Christanto, H.J.: A subjective logical framework-based trust model for wormhole attack detection and mitigation in low-power and lossy (RPL) IoT-networks. *Information* **14**(9), 478 (2023). <https://doi.org/10.3390/info14090478>
17. Khan, H.U., Sohail, M., Ali, F., Nazir, S., Ghadi, Y.Y., Ullah, I.: Prioritizing the multi-criterial features based on comparative approaches for enhancing security of IoT devices. *Phys. Commun.* (2023). <https://doi.org/10.1016/j.phycom.2023.102084>
18. El Mrabet, Z., Kaabouch, N., El Ghazi, H., El Ghazi, H.: Cyber-security in smart grid: survey and challenges. *Comput. Electr. Eng.* **67**, 469–482 (2018)
19. Wahab, F., Ullah, I., Shah, A., Khan, R.A., Choi, A., Anwar, M.S.: Design and implementation of real time object detection system based on SSD and OpenCV. *Front. Psychol.* **13** (2022). <https://doi.org/10.3389/fpsyg.2022.1039645>
20. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endorsed Trans. Internet Things* **9**(4), e1–e1 (2023)
21. Khalil, H., Rahman, S.U., Ullah, I., Khan, I., Alghadhbani, A.J., Al-Adhaileh, M.H., Ali, G., ElAffendi, M.: A UAV-swarm-communication model using a machine-learning approach for search-and-rescue applications. *Drones* (2022). <https://www.mdpi.com/2504-446X/6/12/372>
22. Thakur, K., Qiu, M., Gai, K., Ali, M.L.: An investigation on cyber security threats and security models. In: *2015 IEEE 2nd international conference on cyber security and cloud computing*, pp. 307–311. IEEE (2015)
23. Khan, I.U., Ouaisa, M., Ouaisa, M., El Himer, S.: Internet of Medical Things & Machine Intelligence, Machine Intelligence for Internet of Medical Things: Applications and Future Trends Computational Intelligence for Data Analysis **2**, 1 (2023). <https://doi.org/10.2174/9789815080445123020004>
24. Ghelani, D.: Cyber security, cyber threats, implications and future perspectives: a review. *Authorea Prepr.* (2022)
25. Arshi, O., Mondal, S.: Advancements in sensors and actuators technologies for smart cities: a comprehensive review. *Smart Constr. Sustain. Cities* **1**(1), 18 (2023)

26. Admass, W.S., Munaye, Y.Y., Diro, A.A.: Cyber security: state of the art, challenges and future directions. *Cyber Secur. Appl.* **2**, 100031 (2024)
27. Kaur, J., Ramkumar, K.R.: The recent trends in cyber security: a review. *J. King Saud Univ.-Comput. Inf. Sci.* **34**(8), 5766–5781 (2022)
28. Khan, I., Ahmad, I., Rahman, T., Zeb, A., Ullah, I., Hamam, H. and Cheikhrouhou, O.: Analysis of security attacks and taxonomy in underwater wireless sensor networks. *Wirel. Commun. Mob. Comput.* (2021). <https://doi.org/10.1155/2021/1444024>
29. O'Connell, M.E.: Cyber security without cyber war. *J. Confl. Secur. Law* **17**(2), 187–209 (2012)

Lightweight Cryptography Algorithms for IoT Devices



Muhammad Farukh Sohail, Malik Muhammad Nadeem, Ahthasham Sajid, Hamza Razza, and Arslan Ali Khan

Abstract The human's life day to day activities become more easier with the internet of things technology as change i.e. smart homes, offices, cities etc. But a huge hurdle is the securing of all this data in transit through these devices. LWC (Lightweight Cryptography) provides a hopeful solution to allow an optimal balance between secure design and reduced computational overhead/memory utilization. Implementation of LWC allows secured data handling methods, helps in encryption with integrity check and privacy measures for the users. This study focuses on LWC algorithm's for IOT and compare various algorithms to determine their compatibility in the service-limited IoT environment. This work provides an exhaustive study to point out the excellent LWC approach for diverse IoT applications concerning special safety needs and one of kind levels of statistics sensitivity, so that accurate necessities can be correctly mapped.

Keywords LWC · Security Challenges · IoT · Applications · Limitations and Standards

M. F. Sohail · M. M. Nadeem · A. Sajid (✉) · H. Razza · A. A. Khan
Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan
e-mail: ahthasham.sajid@riphah.edu.pk

M. F. Sohail
e-mail: 50628@students.riphah.edu.pk

M. M. Nadeem
e-mail: 44887@students.riphah.edu.pk

H. Razza
e-mail: hamza.razzaq@riphah.edu.pk

A. A. Khan
e-mail: arslan.ali@riphah.edu.pk

1 Introduction

The IoT, is swiftly creating a web for interconnecting, transforming our world into a symphony of data exchange. Imagine a future where your thermostat adjusts automatically based on your preferences, lights respond to your presence, and appliances optimize their energy consumption. From smart homes and wearable's monitoring our health to industrial sensors optimizing production lines, these devices bridge the gap between the physical and digital worlds. This burgeoning ecosystem promises a future of enhanced efficiency, convenience, and automation. However, with this expansion comes a critical challenge: securing the vast amount of data flowing through these interconnected devices [1] (Fig. 1).

The maturation of IoT also brings new strategy placed attack vectors to light, especially around resource constrained ink used sensors or wearables. The serious

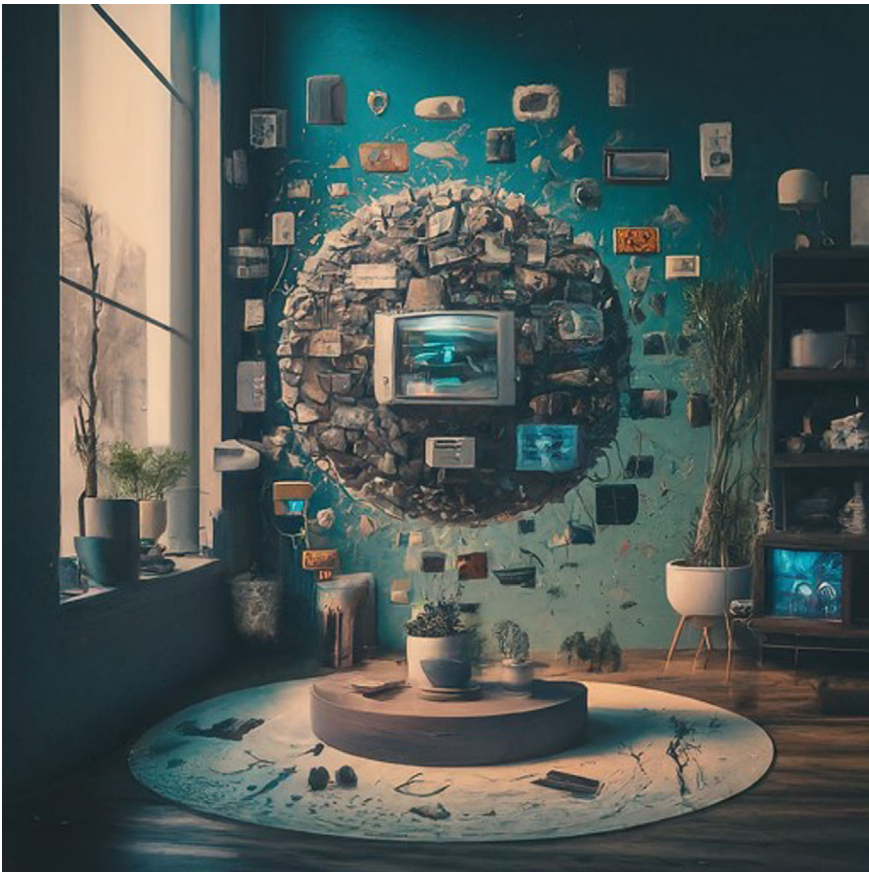


Fig. 1 Internet of things gadgets

issue security has on these devices is due to their light OS which restricts any traditional type of heavy protocols. This is where lightweight cryptographic (LWC) can be a good remedy. This is a huge win for IoT developers, as the heavyweight LWC algorithms offer robust security with minimal resources so that dedicated devices can execute vital cryptographic functions without slowing them down or cutting battery performance—and risking the mission. Given their vulnerability and the type of data they deal with, IoT devices will always have to be properly secured. Cryptography: For data confidentiality, integrity and authentication. Yet traditional cryptography is not made for lightweight deployments.

The security vulnerabilities faced by resource-constrained IoT devices, focus on those with limited processing power, memory, and battery life—a significant portion of the rapidly growing IoT landscape. Gartner, a leading IT research and advisory firm, predicts there will be over 25 billion connected devices by 2025 [1]. As the IoT landscape expands, so does the attack surface for malicious actors? These actors can exploit vulnerabilities to steal sensitive user data (login credentials, financial details, and health data), disrupt critical infrastructure, or launch denial-of-service attacks. The consequences can range from financial losses and identity theft to disruptions in essential services and safety hazards.

1.1 Security Challenges of IoT Devices

Securing these devices poses unique challenges due to their inherent limitations. Traditional security protocols, often designed for powerful computers, are too demanding for these devices. Complex encryption algorithms can quickly drain their limited processing power and battery life, impacting functionality and lifespan. This necessitates exploring alternative security solutions that offer robust protection while minimizing the computational burden.

There are three key challenges associated with securing resource-constrained IoT devices:

1.1.1 Resource Constraints

These devices have restricted or limited kind of computational resources like processing power, battery power, and memory etc. Managing sophisticated enterprises entails drawing and managing considerable resources which if exhausted running security protocols, diminish the functionality and durability of the device. It is therefore important to strike a balance in security while at least the same time not over utilizing the resources in a way that these devices become unsustainable in the long run. For example, a security solution that has enhanced encryption could provide great security but at the same time drain a device's battery to the extent that it becomes cumbersome to use in a particular context.

1.1.2 Heterogeneity

The Internet of things has a very wide coverage and range of sophistication of gadgets that can be connected to the internet. These range from basic sensors that measure temperature to artificial intelligent, self-sufficient products like security systems of homes; it's impossible to have a unified security system. The situation that occurred implies the need for security solutions that are flexible and enlarged in order to meet the demands of this environment. That is a single encryption algorithm may be optimal for a low power sensor node however it is insufficient for a transmitter of health data.

1.1.3 Limited User Interaction

Some things in the IoT environment do not possess, or possess very simple interfaces which makes it challenging to constantly check for signs of intrusion or incorporate user identification techniques. Some of the conventional security measures, which depend on user entry, may not be useful to these devices. As such, it is necessary to find other solutions, for instance, based on device fingerprinting or hardware protection solutions. Device fingerprinting is the process of generating a signature derived from the application's hardware and software attributes with which control systems may detect unauthorized and/or compromised devices. It is also possible to apply some sort of security at the hardware level; for instance, secure enclaves that are a hardware implementation to ensure keys are safe and only very limited computations are done within it.

1.2 Objectives of Securing IoT Devices

However, because of the drawbacks of old cryptography methods lightweight cryptography comes out as a promising solution for IoT devices that are constrained by resources. Such strategies attempt to decrease the computational intensiveness and the amount of memory space that is occupant while at the same time keeping in mind the security of the system paramount. By implementing lightweight encryption algorithms, we can achieve several critical objectives.

1.2.1 Safeguard User Data

Confidential information, for instance credentials, financial details, and health information can be encrypted, rendering it unreadable to unauthorized parties. This protects user privacy and prevents data breaches.

Table 1 Lightweight versus high weight cryptography

Feature	Lightweight cryptography (LWC)	Highweight cryptography
Designed for	Resource-constrained devices (IoT)	Powerful computers
Focus	Minimize resource consumption (processing power, memory)	Maximize security
Benefits	Efficient resource utilization	Exceptional security Well-established
Drawbacks	Might have slightly lower security compared to high-weight cryptography	Resource-intensive—Limited scalability (not ideal for all IoT devices)
Examples	LEA, PRESENT, Krypton, SIMON	AES, RSA, Elliptic Curve Cryptography (ECC)

1.2.2 Ensure Data Integrity

Encryption is essential to make amends for the vulnerability associated with transmission and storage of information. This makes the information genuine and accurate and this is very important in instances whereby accurate data information is highly essential. For instance, in a smart grid system, a problem of data security when it is transmitted from sensors to control centers is critical to the stability of the power grid.

1.2.3 Maintain User Privacy

Limiting access to data only to authorized users protects user privacy and prevents unauthorized data collection. This is particularly important for devices collecting sensitive health data or personal information (Table 1).

1.3 IoT’s Applications

These are the key IoT’s applications.

1.3.1 Consumer Applications

- Smart Homes: Automated thermostats, responsive lighting, energy-efficient appliances.
- Wearable’s and Health Monitoring: Fitness trackers, smart watches, and health monitors for activity, sleep, and vital signs.
- Smart Retail: Inventory management, self-checkout, personalized marketing based on customer behavior.

1.3.2 Industrial Applications

- Industrial Automation and Predictive Maintenance: Condition-based equipment monitoring for predictive maintenance and avoid any losses.
- Smart Grids: Effective distribution and management of energy in relation with usage and grid characteristics with the help of gathered data.
- Connected Logistics and Supply Chain Management: Location tracking with sensors, temperature and other crucial parameters of products and goods in transit.

1.3.3 Smart Cities

- Traffic Management: Congestion data collection and adjustment of traffic signals for optimized flow.
- Smart Waste Management: Sensor-equipped trash bins for efficient waste collection and reduced routes.
- Environmental Monitoring: Sensors for air, water, and noise level monitoring to support environmental protection efforts.

1.3.4 Other Applications

- Connected Vehicles: Enhanced safety and driving experience with features like self-parking, collision avoidance, and real-time traffic updates.
- Agriculture: Precision agriculture uses sensors and data analysis to optimize irrigation, fertilizer use, and crop yields.
- Security and Surveillance: Smart security systems with remote monitoring and access control capabilities.

1.4 *Challenges in Implementing Traditional Cryptography for Resource-Limited IoT Devices*

The following factors can be considered critical challenges in implementing traditional cryptography for IOT Devices with limited resources:

- Limited battery power
- Limited computing power
- Limited memory (registers, RAM, ROM)
- Minimum physical area
- Live response

Resource-constrained IoT devices are generally small in size with constraints on its computing power, battery power, RAM/ROM and physical area. Moreover, majority of the IoT devices have to provide an accurate and quick response. In

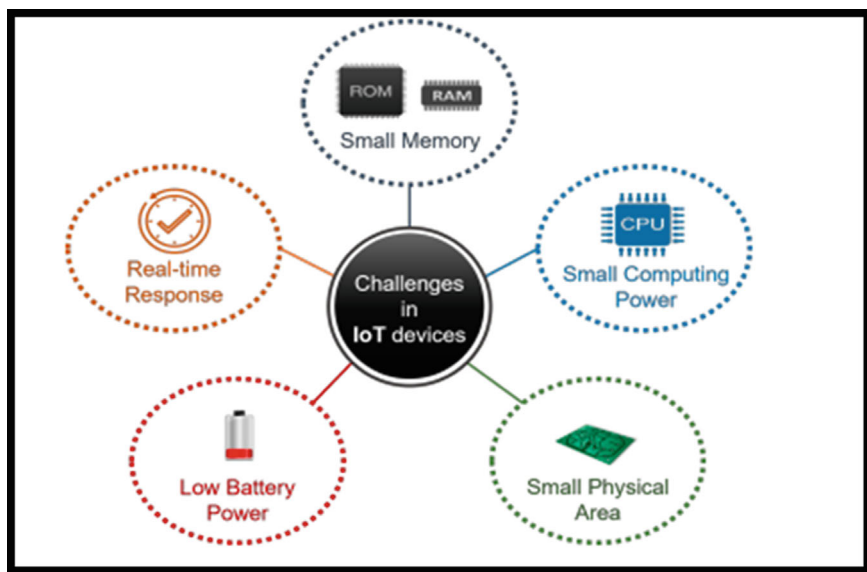


Fig. 2 Displaying limited recourse of IoT-gadgets [2]

such a scenario, providing essential security is a challenge and thus designers have an intricate situation to handle challenges of limited resources of IoT devices and provide security as well (Fig. 2).

Traditional algorithms make resource-limited IoT devices consume too much energy. For instance, performing encryption of $600 \times$ times 5 MB file using 3DES causes 55% consumption of battery power [1]. Figure 3 [1] depicts the battery consumption for different encryption processes.

Considering the aforesaid issue in hand, conventional cryptography will not be able to provide acceptable performance. Therefore, lightweight cryptography algorithms are introduced to handle real-time response, small processing power, and low power consumption.

2 Research Methodology

A comprehensive search for relevant studies is conducted using credible sources such as IEEE Xplore, Google Scholar, Association for Computing Machinery Digital Library, and ScienceDirect. Employing a combination of keywords are “IoT security,” “Lightweight Cryptography IoT Devices” and “Lightweight Ciphers on IoT Devices”. This search strategy aims to identify high-quality research papers, conference proceedings, technical reports, and industry publications that address the specific focus of this study. To keep track of the latest developments in the field,

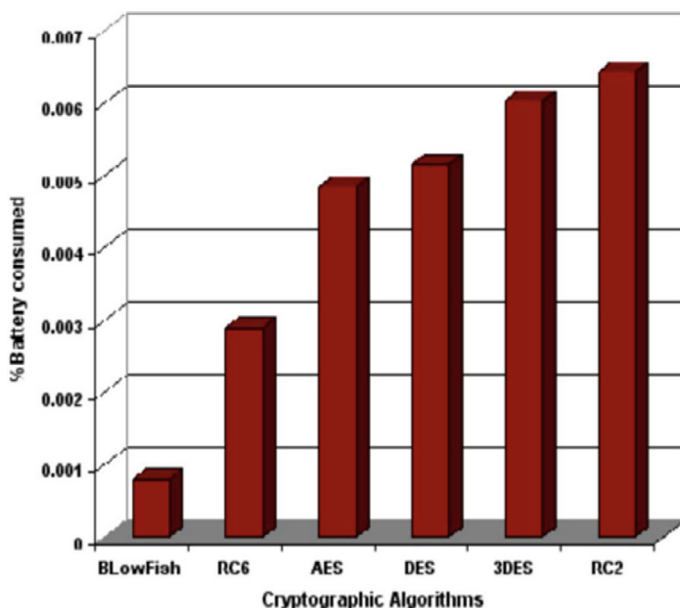


Fig. 3 Battery consumption of different encryption algorithm [1]

only the last 5 × Years’ papers were included in this paper. Further, papers that did not adequately target the lightweight cryptographic ciphers were assumed to be out of the scope of this paper. This methodology ensures a rigorous and structured approach to analyzing relevant academic literature. The central question guiding this review is: “What are the key security challenges faced by resource-constrained IoT devices, and how can lightweight encryption be leveraged as an effective solution to mitigate these challenges?”.

Following the selection process, the chosen studies undergo a critical evaluation process. This evaluation assesses the studies based on their methodological rigor, the validity of their findings, and their contribution to the ongoing body of knowledge on IoT security and lightweight encryption. This way, the analysis of the methodology enables understanding whether the research was conducted in a proper way and whether it contributes to the answer to the research question. Validity assessment helps to guarantee that the essence of the conclusions is rather justified by data and the chosen approach. Last of all, the aspect of contribution to the field establishes how the research helps the implementation of security for the limited IoT devices. The final process of the analysis of the data collected from the selected studies will entail extracting and synthesizing of the information gathered. This will entail determining analyzed information on the security threats affecting resource-scarce IoT devices and incorporation of LWE for protection. The analysis will also focus on the applicability of solutions suggested in the course of the research regarding utilization of lightweight encryption in handling the mentioned challenges. Also, the

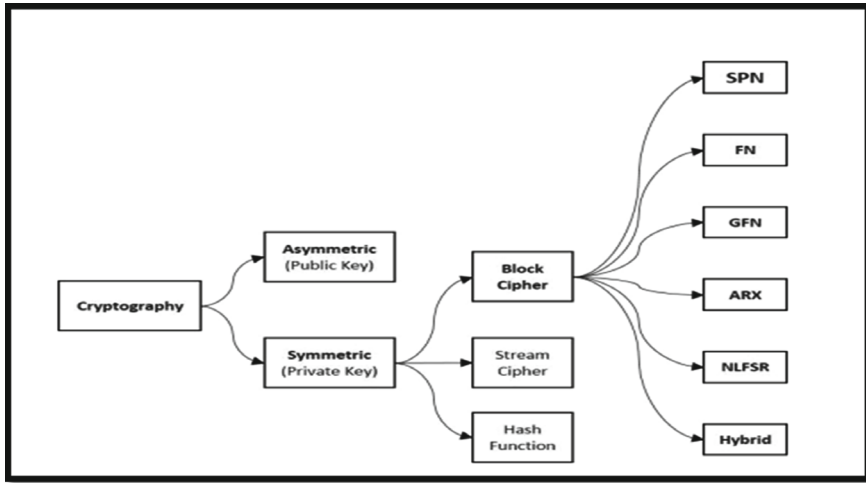


Fig. 4 Structure-wise classification of LWC [2]

limitations that have been pointed out in other studies will be discussed to illustrate their possible research avenues. Consequently, analysis of this extracted data, it is possible to develop a synthesis that will provide the current state of knowledge on how to secure resource-constrained IoT devices using lightweight encryption. This understanding will facilitate the identifying more effective security measures and contribute to the development of a secure and robust future for the IoT ecosystem.

2.1 *Lightweight Cryptography Techniques*

Lightweight Cryptography generally divide into three types (Fig. 4):

- Block Ciphers
- Hash Functions
- Block Ciphers

2.1.1 **Lightweight Block Ciphers**

Block cipher belongs to a category of symmetric cipher, wherein an entire block of text is processed by cipher at once. Since, Feistel structure utilized round function on half of the state. Hence, it yields same design for encryption and decryption that results in minimum overhead and reduces the utilization of memory. Therefore, its implementation is possible for hardware having low power. It is pertinent to mention here that Feistel structure is not designed for applications requiring small latency. SPN is considered quicker but it does not possess a key schedule and this property

makes it a candidate for attacks. Considering the similar energy expenditure and same security requirement, the SPN structure can be considered to be more appropriate since it requires less number of execution rounds. A number of researchers have embarked on experiments with a number of platforms including the NXP, AVR, and ARM micro-controllers to establish the effects of the selected best performing lightweight cryptography algorithms. There are many such parameters, for instance Gate area (GE), logic process (μm), power consumption (μW), throughput, RAM/ROM, demands, response time etc., when analyzing multiple lightweight cryptography algorithms in various languages like message type, file types (Java, Python and C/C++), etc. Figure 5 Displaying LWC Algorithm memory and Gate Area usage and Fig. 6 Displaying LWC Energy Utilization.

The best LWC algorithms regarding memory, gate area and power consumption will be briefly discussed. SIMON was developed by NSA (National security agency), which is known for its low memory and Gate Area utilization in hardware. It provides different sizes of keys (64 bits, 72 bits, 96 bits, 128 bits, 144 bits, 192 bits, 256 bits) in 32 bits, 48 bits, 64 bits blocks (yuan)., 96 bits, 128 bits, 32, 36, 42, 44, 52, 54,

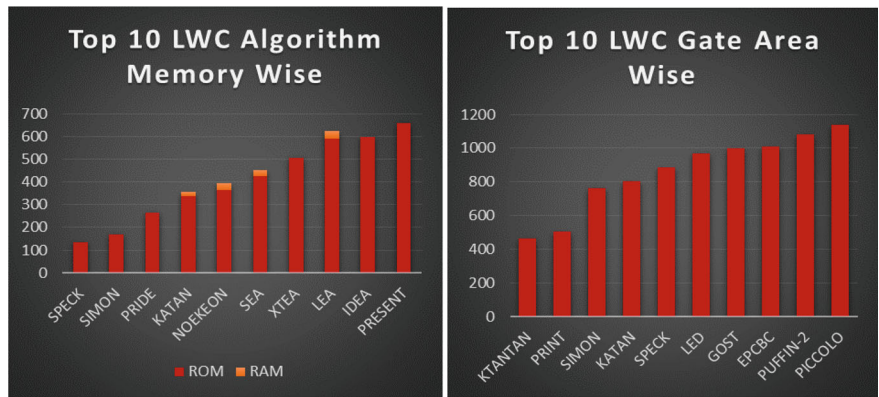


Fig. 5 LWC algorithm memory and gate area usage

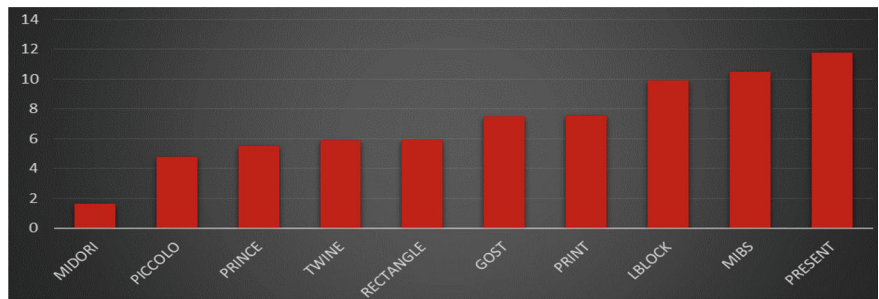


Fig. 6 Top 10 LWC energy utilization solutions

68, 69, after 72 rounds. The most space efficient version requires 763GE to be built. It has similar block and size to SIMON and can do 22, 23, 26, 27, 28, 29, 32, 33 and 34 iterations. Most hardware uses 48-bit block and 96-bit key to meet the requirements of 884 GE. Also, from the perspective of software implementation, a 64-bit block with a 128-bit key requires at least 599 cycles and 186 bytes of ROM. Simon optimization is for hardware implementation, and Speck optimization is for software implementation [1].

PRIDE belongs to the substitution permutation network and shows energy efficiency and low latency with a 128-bit key on input of 64-bit to perform $20 \times$ iterations. KTANTAN algorithm belongs to the Linear Feedback Shift Register. It applies keys of 80-bit on different block sizes (32-bit, 48-bit, and 64-bit) vide $254 \times$ iterations. KTANTAN usage is limited as the key remains unchanged after initialization. Hence, it is more suited for applications such as RFID tags, which exhibits low throughput along with more energy consumption.

PRINT is an example of an SPN network, an encryption method adapted for two different purposes. First, PRINT-48 is used for IC printing applications, where 48 iterations are performed on a 48-bit input (402GE) using an 80-bit key. Second, EPC encryption uses PRINT-96, which uses a 160-bit key to perform 96 iterations of a 96-bit input (726GE). PRINT provides data security while minimizing operational complexity by using 3-bit operations to eliminate the possibility of single-bit operations. However, it should be noted that this algorithm is still under development and is not yet ready for real deployment.

MIDORI is an example of SPN and is the best algorithm for hardware completion. It is designed to be less costly. It is available in two variants, Midori64 and Midori128. Both use 128-bit keys of two different sizes: 64-bit security utilizes 16 iterations while 128-bit security employs 20 iteration. Piccolo is a lightweight encryption of generalized Feistel networks. It ranks second in the list of energy-efficient algorithms. Therefore, it is suitable for devices with tight energy requirements such as RFID, sensors, etc.

PRINCE is a type of SPN network which is third on the list of highly efficient algorithms. A 64-bit i/p and a 128-bit key are used for 12 iterations. Prince is generally used in logistic applications to conclude, SIMON, SPECK, and PICCOLO are most suited algorithms for smart home appliance that requires less memory and reduced processing power. Piccolo is more suitable for RFID tags due to tiny physical space and little to no power backup and for other logistics applications. Moreover, smart agriculture that demands less GE, less processing cycle, and low power consumption can consider SIMON, SPECK, and PRESENT to fulfill their requirement. Moreover, MIDORI, SIMON, AND SPECK are mostly suited for health care applications.

2.1.2 Lightweight Stream Ciphers

A cryptographic technique known as a lightweight stream cipher was created primarily to offer effective and safe encryption for devices with inadequate resources, such as embedded systems and IoT devices. To strike a balance between security

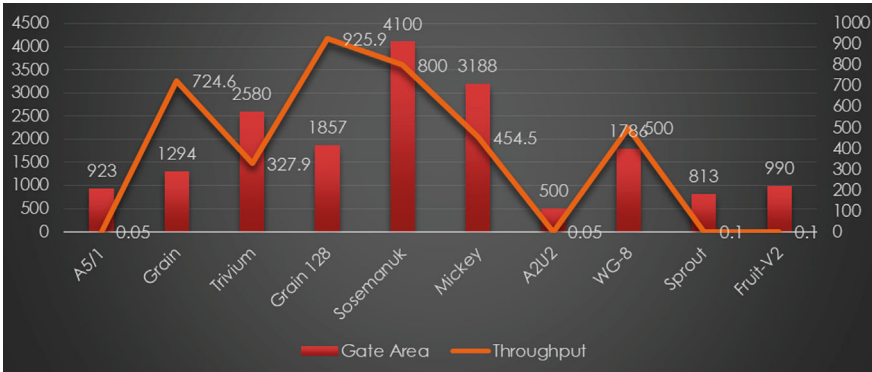


Fig. 7 Lightweight stream cipher gate area and throughput comparison

and efficiency, these ciphers frequently use lightweight operations and optimized implementations, guaranteeing data secrecy and integrity while reducing computational overhead and power consumption. A lightweight stream cipher’s objective is to fulfill the limitations of lightweight devices while yet offering powerful encryption capabilities as illustrated in Fig. 7.

Following NIST’s recommendations, an encryption algorithm called Ascon has become part of NIST’s lightweight encryption standard [3]. In the final selection of the CAESAR competition, Ascon-128 and Ascon-128a were selected as the “first choice” for lightweight authenticated encryption. Ascon demonstrates stability and performance in real-world applications with minimal hardware, while also offering impressive performance in software and hardware, especially in short words. Ascon uses the same basic configuration to provide encryption and hash proofs, making it easy to use using the same standard in all scenarios. This approach not only minimizes hardware footprint for dual function applications but also streamlines code development, boosting performance and security. Ascon is built primarily on a 64-bit language and uses only bitwise Boolean functions, xor, not, and rot (bit rotation), making it easy to use on many target platforms.

2.1.3 Lightweight Hash Function

Lightweight hash functions are cryptographic methods created to quickly create message digests or standardized hash values from various type of I/P data. These hash functions are specially designed for devices with low resources, such as embedded systems and Internet of Things (IoT) devices, which have confined processing speed and memory. Using optimized algorithms and operations, lightweight hash functions try to balance security with effectiveness. The following are some significant hashing operations: A novel hash family called Quark was introduced in 2010 by Jean-Philippe Aumasson et al. [89] It is inspired by the block cipher KATAN and the stream

cypher Grain. There are three examples of sponge pattern. Specifically, U-quarks, d-quarks and s-quarks. U-Quark offers 64-bit security while S-Quark provides 112-bit security. The power consumption of these two chips is 2.44W and 4.35W respectively, and the chip area is 1379 GE and 2296 GE respectively. Lesa manta-LW applied in 2010. The 112-bit security provided by s-quark is best suited for applications such as Financial services, E-commerce, Cloud storage, IoT devices, Healthcare etc.

3 Critical Analysis

Newly emerging big data application areas such as Internet of Things (IoT) can be full-blown wearables or simple sensors, or even smart home appliances and they typically have constrained processing power, memory and battery capabilities. Given the fact that IoT consist of numerous connected devices, the concealment of the resource implies that traditional security measures which are secure and suitable for strong computational systems are not fit for purpose and cannot be implemented within the IoT environment.

This research paper makes a good case for lightweight cryptography (LWC) as a plausible solution to this all-important issue. LWC algorithms are optimized in such a way that it will always provide a good level of security with lesser amount of resources utilization. LWC works by reducing the size of the keys and employing efficient algorithms that make it possible for the constrained devices to perform basic cryptographic functions at an optimal rate without worrying about impositioning on their current battery capacity. The authors vigilantly bring out the issues with the conventional security measures, and the necessity for innovative measures suitable for IoT devices. All of them give a general picture of the problems in resource scarcity environment stressing the existence of the security-resource trade-off. This analysis provides a clear means to demonstrate the weakness of conventional cryptosystems perspectives and opens up a discussion for the use of LWC. It is praiseworthy that the research methodology used when writing this paper has been well done. The authors apply a SLR, with an emphasis on published within the last five years and only those of high quality, to get as close to a complete picture existing LWC solutions as possible. This systematic approach gives a strong backdrop to the evaluation as well as the analyses and conclusions made in the paper.

The comparison of various LWC algorithms is provided and logically organized. The paper first gives a brief introduction of three categories of LWC algorithms and then goes into detail to discuss particular algorithms, their performance difference, as well as their applicability in different IoT contexts. This comparison assists the readers in appreciating the factors of trade-off between different LWC options with regard to the issues of security, resource utilization and performance. Altogether, this research paper can be viewed as a valuable resource for the understanding of the level of IoT security. It was able to break down the difficulties in protecting such devices that has limited resources and presented LWC as a potential solution to the problem. Thus, the comparison of different LWC algorithms and the definition of

further research areas turn this paper into a useful source of information for specialists and researchers in the IoT security field.

4 Standardization Lightweight Cryptography Algorithms and Future Directions

The following organizations are involved in cryptography, striving to establish SOP's for competing cryptography algorithms tailored for cross-border devices:

- Japan US national security agency
- Global commission of Standardization (ISO) and global electrotechnical corporation (IEC)
- Japan Committee for cryptography research and evaluation
- CryptoLUX (University of Luxembourg)

A perfect algorithm would maintain a proper balance among cost, performance and security. Any two of the factors can be achieved but the challenge is in achieving all three of them together.

- Target the reduction in number of S-boxes as it requires memory and computation power while maintaining the same security level. In this regard, an epitome would be of PRESENT, which is designed by replacing eight S-boxes with just one.
- Key Scheduler is required to be made lighter with smaller key size and without compromising security strengths.
- Target decrease in numbers of rounds without decreasing the security.
- Create simple rounds without impacting security.

5 Conclusion

This research underscores the critical role of Lightweight Cryptography (LWC) in safeguarding communication for resource-constrained Internet of Things (IoT) devices. Recognizing the limitations of traditional security protocols, the paper meticulously compares the characteristics of various LWC algorithms. This comparative analysis sheds light on how each algorithm utilizes the scarce resources of IoT devices efficiently. Furthermore, the research delves into open research challenges in the field of LWC, paving the way for future advancements. While some existing lightweight ciphers cater to specific applications, limiting their broader applicability, the continuous struggle between cyber security experts and attackers necessitates ongoing research efforts. This ensures the development of even more robust and versatile LWC solutions, a crucial element in securing the dynamic and ever-evolving landscape of IoT.

Acknowledgements I would like to thanks my supervisor Dr. Ahthasham Sajid for his kind support and guidance throughout this write-up.

References

1. Surendran, S., Nassef, A., Beheshti, B.D.: A Survey of Cryptographic Algorithms for IoT Devices (2018)
2. Thakor, V.A., Razzaque, M.A., Khandaker, M.R.: Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities (2021)
3. Mattsson, J.P., Selander, G., Paavolainen, S., Karakoç, F., Tiloca, M., Moskowitz, R.: Proposals for Standardization of the Ascon Family. NIST (2020)

Guarding the Digital Gateway: An In-Depth Analysis of Cybersecurity Challenges in India



Snehal A. Bagul

Abstract India's rapidly expanding internet user base and digital infrastructure make it a prime target for cyberattacks at the moment. An extensive examination of India's particular cybersecurity issues is given in this chapter, together with information on the main threats, the state of the situation, and tactical solutions. It starts by describing the digital revolution that India has experienced, stressing the notable rises in smartphone usage, internet penetration, and digital transactions. The discussion then turns to the nation's unique cybersecurity problems, namely the regular cyberattacks on businesses, government institutions, and vital infrastructure. A variety of cyberthreats, such as phishing, ransomware, and data breaches, are investigated and their effects on the digital economy and national security are evaluated. The chapter examines India's cybersecurity laws and regulations, including the 2000 Information Technology Act and the 2013 National Cyber Security Policy, and addresses the function of organisations like the Indian Computer Emergency Response Team (CERT-In) in reducing cyberthreats. It also emphasises how crucial it is for government, business, and academia to work together in public-private partnerships and to handle the changing cyber threat scenario. The chapter advocates for strong education programs and the development of a trained workforce while highlighting the difficulties in raising cybersecurity knowledge and capacity. The chapter concludes with a discussion of upcoming technologies such as blockchain, artificial intelligence, and the Internet of Things, as well as the future of cybersecurity in India. All in all, it highlights the necessity of a proactive and all-encompassing strategy to protect the country's digital future.

Keywords Cyber security challenges · Cyber security · Cyber Attacks · Cyber security capacity building · AI

S. A. Bagul (✉)

Department of Management Studies, Sandip Institute of Technology and Research Centre,
Savitribai Phule Pune University, Nashik Campus, India

e-mail: snehal.13990@gmail.com

1 Introduction

Nowadays India's journey towards digital transformation has been characterized by remarkable progress in harnessing technology to propel socio-economic advancement and foster innovation. Through a multifaceted approach encompassing diverse sectors, the nation is forging ahead towards the realization of a digitally empowered society and economy. This transformative journey holds the promise of unlocking unprecedented opportunities, streamlining processes, and elevating the standard of living for millions of citizens.

The goal of closing the digital divide and fostering inclusive growth is at the core of India's digital revolution. Programs like the 2015 launch of the Digital India campaign are prime examples of the government's dedication to using technology as a force for good in the world. Digital India seeks to empower citizens and enable their involvement in the digital economy by emphasising the development of digital infrastructure, the advancement of digital literacy, and the electronic delivery of government services [1].

The nationwide democratisation of access to digital services has been greatly aided by the widespread use of cellphones and internet connectivity. A paradigm shift in consumer behaviour and business models has resulted from India's smartphone revolution, which has been driven by reasonably priced devices and widespread internet access. As evidence of the quick speed of adoption, smartphone penetration in India increased from less than 5% in 2010 to almost 45% in 2020, according to latest figures [2].

In addition, the emergence of digital platforms and services has completely transformed a number of industries, including healthcare, education, and even e-commerce and financial services. With creative companies using technology to address urgent societal issues and upend established sectors, India's booming startup scene has been at the forefront of this digital disruption. There is a flourishing startup scene in the nation, and the number of unicorns—startups valued at \$1 billion or more—keeps rising [3].

In addition to fostering innovation and entrepreneurship, India's digital transformation is reshaping governance and service delivery. Initiatives like Aadhaar, India's biometric identification system, and the Unified Payments Interface (UPI) have streamlined processes, reduced inefficiencies, and enhanced transparency in various government services. By embracing digital technologies, India is not only modernizing governance but also enhancing citizen engagement and participation in the decision-making process.

India has made incredible strides in the digital realm, but there are still obstacles to overcome. For the digital economy to flourish in an inclusive and sustainable way, concerns about issues like data privacy, cybersecurity, and digital literacy must continue to be addressed. Furthermore, achieving fair access to digital infrastructure and bridging the urban–rural digital gap are essential to maximising the potential of India's digital revolution.

India's efforts to pursue digital transformation are evidence of the revolutionary potential of technology in propelling inclusive growth and advancing socio-economic development. With the help of the government, business community, and civil society at large, India is well-positioned to become a worldwide leader in the digital era, using technology to solve complicated problems and open up new avenues for its people [4–8].

2 Brief Overview of India's Digital Transformation

India's digital revolution has completely changed society and many industries. The nation's level of digital penetration has significantly increased since the 2000s, largely due to government initiatives, technological developments, and the widespread use of smartphones. India has seen a 14,900% growth rate in internet users over the past 20 years, going from 5 million in 2000 to over 750 million by 2020. Due to the democratisation of access to digital services brought about by smartphone usage, digital platforms and services are growing. To close the digital divide and give individuals more influence, the Indian government has started programs like the Digital India campaign. India is now known as a global centre for innovation and entrepreneurship thanks to the country's startup culture, which has also stimulated economic growth [9–12].

2.1 Key Technological Initiatives Driving India's Digital Transformation

India's journey towards digital transformation is underpinned by strategic initiatives aimed at bolstering digital infrastructure and revolutionizing governance through technology-driven solutions. This paper delves into two key pillars of India's digital evolution: digital infrastructure development and e-governance initiatives, highlighting their significance in fostering inclusivity, efficiency, and citizen engagement.

2.2 Digital Infrastructure Development

Building a robust and inclusive digital infrastructure is at the heart of India's digital revolution, guaranteeing that all people have access to basic digital services. Important projects and developments in this field include: 1. The BharatNet Project The goal is to connect all of India's rural areas to high-speed internet. As of 2021, more than 1.5 lakh km of optical fiber has been installed, linking more than 1.5 lakh g

panchayats, or village councils. There are hopes to connect all 250,000 g panchayats by the end of 2022. Impact: BharatNet is anticipated to improve access to education and healthcare services, support e-governance, and strengthen local economies through expanding internet access.

Rollout of the 5G Network: The promise of 5G: As 5G networks are deployed, they will transform India's connectivity landscape by providing: Enhanced Speed: Much faster than existing 4G capabilities, with speeds up to 10 Gbps., Minimal Latency: Almost instantaneous communication, crucial for uses such as remote medical diagnosis and self-driving cars., Timeline for Deployment: The government plans to finish the rollout by 2023, and preliminary testing has already started in a few cities.

The Internet of Things: Potential: The rollout of 5G is anticipated to spur the development of IoT applications in India, opening the door to more effective resource management, smarter cities, and enhanced agricultural techniques. **Market Size:** Driven by industries including manufacturing, healthcare, and transportation, Statista projects that the Indian IoT market will reach \$15 billion by 2025.

The Mission of Smart Cities: The goal of this effort, which was started in 2015, is to create 100 smart cities in India with an emphasis on innovative and technological approaches to sustainable urban development. Integrated infrastructure (smart utilities, transportation, and waste management) is one of the main features. Digital platforms enable citizen participation for feedback and service delivery. **Investment:** \$1.5 billion from the government and a sizeable sum from the business sector have been set aside for the creation of smart cities.

Difficulties and Their Resolutions: Connectivity Gaps: In spite of advancements, connectivity problems persist in rural and isolated locations. **Solution:** To close these gaps, projects like community networks and satellite internet are being investigated. **Limitations on Bandwidth:** The demand for data is growing faster than the supply. **Solution:** It's crucial to upgrade the current infrastructure and introduce cutting-edge innovations like fiber-to-the-home (FTTH) [13–16].

2.3 *E-Governance and Digital Services*

Initiatives like Digital India, which was introduced in 2015 and intends to alter government and service delivery throughout the country, have a major role in driving India's digital transformation. With the help of this project, individuals will be able to easily and effectively access a variety of government services via electronic means. By 2023, more than 1000 government services would be accessible online thanks to the Digital India initiative, significantly lowering the requirement for in-person trips to government buildings.

The Digital Locker, which enables safe online document sharing and storage for residents, is one of the initiative's main platforms. The Digital Locker's popularity and usefulness were demonstrated by the fact that over 50 million people had registered by 2022. This platform streamlines the verification procedure for a number of

services, such as applying for loans, jobs, and other necessities, while also improving security by lowering the possibility of document loss.

Over 1.3 billion Indian citizens have access to a unique identity number through Aadhaar, the largest biometric identification system in the world, which supports these efforts. By 2023, Aadhaar enabled expedited access to government services by being connected to over 700 million mobile connections and over 1.2 billion bank accounts. This integration has been extremely helpful in lowering administrative barriers, guaranteeing that welfare benefits are received by the intended recipients directly, and so eliminating corruption and inefficiencies.

Moreover, India has made noteworthy progress in the Global Digital Competitiveness Index, which reflects the influence of these digital initiatives on governance. India moved up to 44th place in 2021, largely because to improvements in digital infrastructure and e-governance. This change has also been facilitated by the attempts to improve digital literacy through programmes like the Pradhan Mantri Gramin Digital Saksharta Abhiyan, which aims to equip over 60 million rural residents with digital skills by 2024.

By bridging the digital divide, these efforts promote inclusivity and public participation. By 2023, there will be over 750 million internet users in India. As such, guaranteeing fair access to government services and empowering underprivileged people depend heavily on the availability of online services. To further develop the digital infrastructure, the National Digital Communications Policy seeks to bring broadband connectivity to every village by 2025 [17, 18].

2.4 Digital Financial Inclusion

Enhancing financial inclusion through cutting-edge technologies like the Pradhan Mantri Jan Dhan Yojana (PMJDY), Aadhaar-enabled Payment System (AePS), and Unified Payments Interface (UPI) is a key component of India's digital push. In order to effectively promote economic empowerment, these programs are critical in expanding banking access, especially for marginalized and rural people.

With its 2016 inception, UPI has revolutionized digital payments in India, enabling more than 7 billion transactions valued at ₹12.82 lakh crore (about \$172 billion) in 2022 alone. By facilitating cashless transactions with ease, this real-time payment system helps users cut down on their use of cash and associated expenses.

In a same vein, AePS makes banking services accessible even in isolated locations with inadequate infrastructure by enabling users to access their bank accounts using their Aadhaar numbers. By March 2023, AePS transactions had exceeded 2 billion, illustrating its expanding adoption and the role it plays in delivering financial services to the unbanked people.

With its 2014 introduction, the PMJDY seeks to give every household access to a bank account. More than 460 million accounts had been opened under this program as of 2023, advancing financial literacy and making it easier to access financial services

and government incentives. Low-income families now have much more financial security thanks to the project.

By allowing users to save, invest, and obtain credit, these platforms promote economic empowerment in addition to increasing ease. India's digital transformation is generating a more inclusive financial ecosystem that promotes sustainable economic growth, with an estimated 350 million individuals having access to banking services since the launch of these initiatives [1, 19, 20].

2.5 Digital Healthcare and Telemedicine

Technology is revolutionizing healthcare both domestically and internationally, improving patient outcomes, accessibility, and efficiency. The Centers for Medicare and Medicaid Services (CMS) reported a startling surge in telehealth visits—from about 840,000 in 2019 to over 52 million in 2020—due to the COVID-19 epidemic. Telemedicine in particular has acquired substantial popularity. This quick adoption emphasizes the critical role of remote care, especially in rural areas where access to healthcare professionals is typically limited.

Digital health records constitute yet another essential element of this revolution. The Office of the National Coordinator for Health Information Technology (ONC) reports that as of 2021, almost 86% of non-federal acute care hospitals had implemented electronic health record (EHR) systems, demonstrating the fast increase in EHR adoption. These technologies facilitate communication between healthcare providers and expedite the handling of patient data, which improves care coordination and continuity.

One important effort to promote a cohesive digital health environment in India is the National Digital Health Mission (NDHM). The 2020 launch of the NDHM aims to offer a comprehensive framework for the sharing of health data, including the issuance of digital health IDs to each and every citizen. Over 200 million digital health IDs have been issued as of mid-2023, according to the Ministry of Health and Family Welfare. These IDs have improved access to healthcare services and allowed for more effective management of patient records.

Technology is being used into healthcare systems to improve health outcomes in addition to addressing logistical issues. According to a McKinsey & Company assessment, telemedicine has the potential to provide up to \$250 billion in healthcare services each year in the United States alone. Furthermore, compared to conventional in-person consultations, patients utilizing telemedicine reported higher satisfaction ratings, with a 70% acceptance rating, according to a study published in the Journal of Medical Internet Research.

Additionally, proactive healthcare initiatives like wearable health gadgets and remote monitoring are made possible by technology. The International Data Corporation (IDC) projects that the growing emphasis on chronic illness management and preventative treatment will propel the global market for wearable medical technology to reach \$60 billion by 2023 [21, 22].

2.6 Digital Skills and Entrepreneurship

The main goals of India's digital agenda are to promote entrepreneurship and digital skills, which are crucial for advancing innovation and economic progress. Programs like the 2015-launched Skill India seek to improve youth employability by offering training in a variety of digital skills. By 2023, more than 15 million people had benefited from Skill India programs, which provide instruction in digital marketing, coding, and data analytics, among other subjects.

Similar to this, the 2016 launch of the Startup India initiative promotes entrepreneurship by giving firms financial help and favorable regulations. The Department for Promotion of Industry and Internal Trade (DPIIT) estimates that by 2023, there will be over 70,000 registered firms in India, making it the third-largest startup ecosystem worldwide. Notably, \$24 billion in capital was given to the startup industry in 2021 alone, demonstrating the sector's development potential and investor trust.

These programs foster innovation in addition to an entrepreneurial approach. The NASSCOM report projects that India's IT sector will rise to \$350 billion by 2025, primarily due to the country's expanding digital economy and thriving startup culture. India's digital agenda is expected to have a major impact on the country's economy by providing the youth with necessary skills and encouraging an entrepreneurial culture [23, 24].

2.7 Future Pathways

Due to large expenditures in digital literacy and technology infrastructure, India's digital journey has accelerated significantly. The Indian government plans to invest \$100 billion in telecom infrastructure and attain 1 Gbps broadband speed in every gram panchayat by 2022, as per the National Digital Communications Policy 2020. With the introduction of the Digital India program in 2015, there has been a notable increase in internet penetration from 18% in 2014 to over 70% in 2023.

This change is being led by emerging technologies like blockchain and artificial intelligence. According to a NASSCOM estimate, by 2035, AI alone might boost India's GDP by \$1 trillion. Applications of blockchain technology are predicted to transform industries like finance, supply chains, and healthcare by increasing efficiency and transparency.

For inclusive progress to be fostered, cooperation between the government, business, university, and civil society is essential. By 2025, the government hopes to empower more than 600 million individuals through its drive to improve digital literacy. In addition, the Digital India initiative has generated nearly 1.5 million new tech-related jobs.

Technology is becoming an essential tool for the growth and development of the country as a result of these digital activities, which are also improving social inclusion and changing the economic landscape of India [25, 26].

3 Importance of Cyber Security in the Digital Age

3.1 Securing Against Cyber Threats

In today's digital world, cyber threats like malware, ransomware, and data breaches pose significant risks, including financial losses and reputational harm [18]. Implementing robust cybersecurity measures is crucial for safeguarding sensitive information and proactively protecting against cyber threats [17].

3.2 Ensuring Personal Privacy Protection

In the digital era, personal privacy is increasingly jeopardized by extensive online data sharing. Cyber security serves as a critical guardian, shielding individuals' personal information from unauthorized access. Through encryption, secure authentication, and data protection, cyber security guarantees the confidentiality and security of personal data [18].

3.3 Security Measures for Businesses

In business, cybersecurity is paramount for protecting assets, building trust, and ensuring continuity. Cyber-attacks can lead to financial losses, reputational harm, and service disruptions, emphasizing the need for robust investments [17]. Comprehensive cybersecurity measures safeguard intellectual property, customer data, and financial transactions, reinforcing operational resilience and stakeholder trust.

3.4 Mitigating Financial Risks

Cyber-attacks present substantial financial risks, demanding proactive mitigation to prevent losses. Post-attack costs include investigation, system repairs, and restitution. Robust cybersecurity measures reduce the likelihood of financial losses, safeguarding individuals and businesses from economic hardships. Prioritizing cybersecurity fosters resilience in a digitized landscape.

3.5 Upholding Trustworthiness and Reputation

In today's digital era, trust and reputation are crucial for successful relationships, be it personal or professional. Online interactions amplify the importance of maintaining trust. A single cyber-attack can damage trust and tarnish reputations (Smith and Johnson 2021). Prioritizing cybersecurity initiatives demonstrates commitment to safeguarding stakeholders, enhancing trust, and preserving reputation.

3.6 Adhering to Legal and Regulatory Compliance

Compliance with data protection and cybersecurity regulations is crucial across industries. Non-compliance can lead to penalties and reputational damage (Smith and Johnson 2021). Robust cybersecurity measures help meet these mandates, reducing legal risks and showcasing ethical data management. Prioritizing compliance-driven cybersecurity builds trust and demonstrates commitment to data security and regulations.

3.7 Safeguarding National Security

Cybersecurity is vital for individuals, businesses, and national security. Cyber-attacks pose threats to critical infrastructure and government systems. Prioritizing cybersecurity enables effective collaboration, safeguarding digital assets and bolstering defenses. CyberNX provides comprehensive solutions to foster a secure digital environment, ensuring peace of mind amid evolving threats [20, 27] (Smith and Johnson 2021).

4 Cyber Security Landscape in India

4.1 Current State of Internet Penetration and Digital Infrastructure

India's cybersecurity market surged with a CAGR surpassing 30% from 2019 to 2023, reaching USD 6.06 billion. Digital transformation initiatives and regulatory compliance drove this growth, cited by 84% and 81% of respondents, respectively [19]. Currently representing 3% of the global market share, India aims for 5% by 2028, highlighting its escalating global cybersecurity role. Table 1 presents the current scenario of internet penetration and digital infrastructure.

Table 1 Current state of internet penetration and digital infrastructure

Sr. No.	Year	Product	Services	Total
1	2019	1.03	0.95	1.98
2	2020	1.29	1.09	2.38
3	2021	1.99	1.36	3.36
4	2022	2.89	1.84	4.73
5	2023	3.76	2.30	6.06

India’s cybersecurity expenditure in the BFSI sector surged from USD 518 million in 2019 to USD 1738 million in 2023, propelled by stringent policy mandates [20]. The IT/ITeS sector witnessed similar growth at a CAGR of 36%, driven by secure integration of emerging technologies like AI/ML and GenAI. Figure 1 presents a scenario of the Indian cybersecurity domestic market.

Approximately 73% of organizations plan to invest in IAM solutions by 2023 (From 2019 to 2023). RFPs are the preferred mode for procurement, particularly by the government, PSUs, healthcare, BFSI, and manufacturing sectors, ensuring thorough validation of vendors, fair processes, and precise requirements. Conversely, the IT/ITeS sector opts for direct purchases and contracts with preferred vendors, offering flexibility and quality assurance [22, 28].

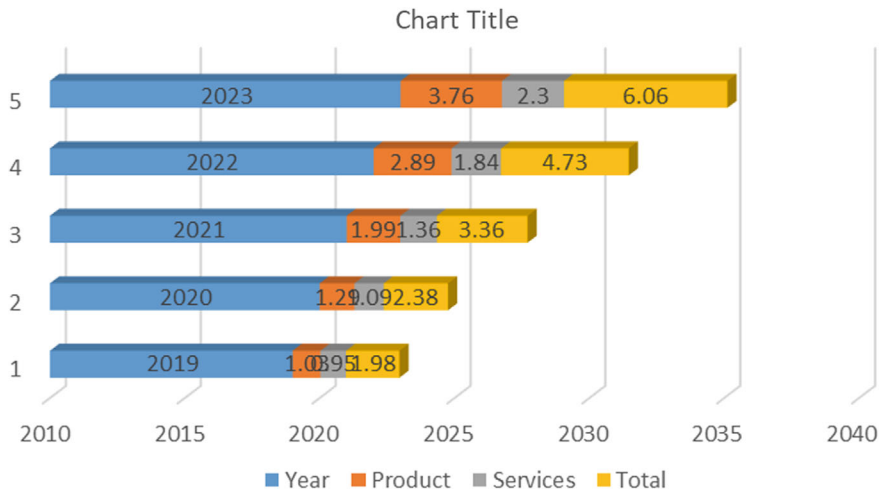


Fig. 1 India cybersecurity domestic market in (USD billion)

5 Cyber Security Challenges in India

India's digital advancement has made it a global economic force, but it faces heightened cyber threats, representing 13.7% of global incidents. In 2024, businesses must bolster security. The DSCI-SEQRITE India Cyber Threat Report, drawing insights from 8.5 million endpoints, analyzes threats, behaviors, and vulnerabilities, offering strategies for CISOs. Cryptojacking incidents surged in 2023, driven by tools like NiceHashMiner. vbLockBit's anti-forensic tactics and RaaS model pose ransomware threats. Fraudulent apps, like irtcconnect.apk, endanger mobile users, highlighting the need for vigilance and user awareness [28].

5.1 Cyber Threat Predictions for 2024

Figure 2 illustrates some of the cyber threat predictions for 2024.

- Zero-day attacks by APTs and Ransomware group
- MFA Fatigue Attacks
- LOLBins - a nightmare for Threat Researchers
- AI-Powered Malware
- Ransomware and Digital Extortion
- Deep Fake for Deceptive Social Engineering
- Exploiting Vulnerable Supply Chains
- Hacktivism continues into 2024
- Auction of corporate access and sale of breached datasets
- Event based attacks—Elections, Olympics, etc.
- Phishing/Vishing attacks and Dating App Scam

5.2 Targeting of Critical Infrastructure

In our digital era, safeguarding critical infrastructure like power, transportation, and finance is paramount. Cybersecurity defends against economic and national security threats, ensuring resource availability and integrity. Recent incidents, like the Colonial Pipeline attack, underscore the urgency for collaborative efforts to bolster resilience and counter evolving cyber threats globally, including in India.

• Attacks on Government Agencies and Businesses

Cyfirma's report shows a 278% spike in state-sponsored cyberattacks on India from 2021 to September 2023, hitting IT and BPO sectors hardest. India ranks as the most targeted country globally, facing 13.7% of all cyberattacks, followed by the US, Indonesia, and China. Various sectors, including services, manufacturing, healthcare,

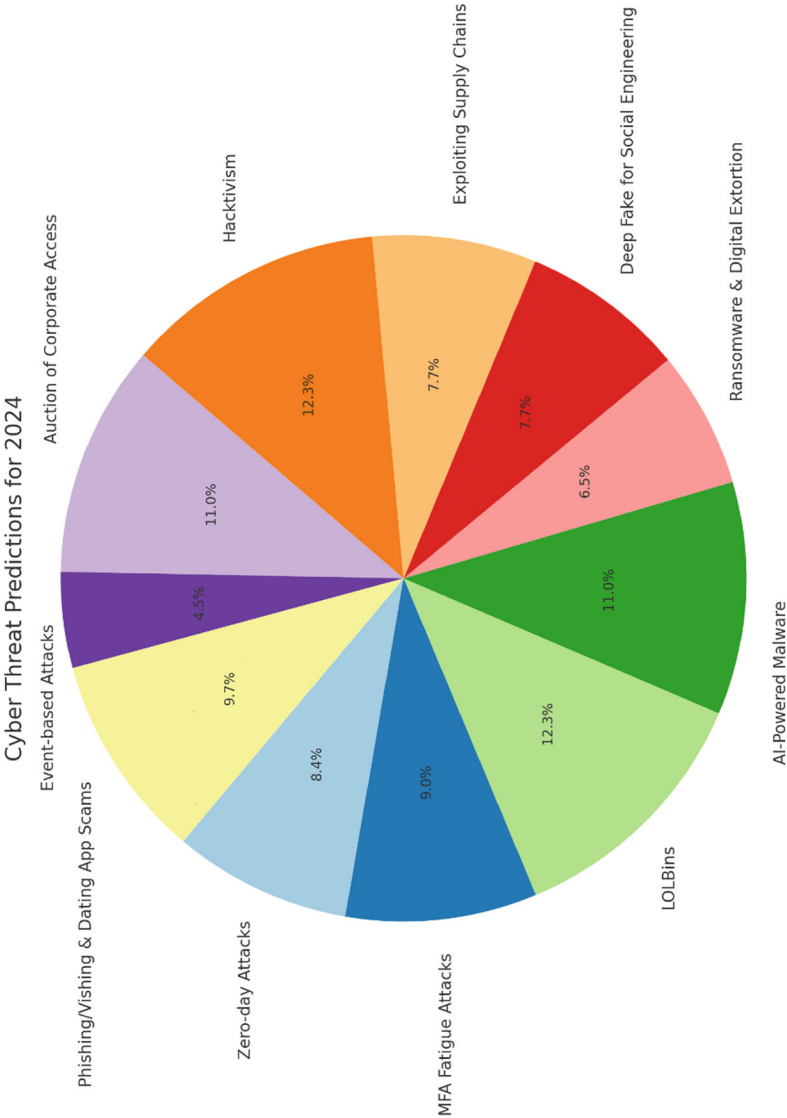


Fig. 2 Cyberthreats prediction for 2024. *Source* Verizon (2023). Data Breach Investigations Report (DBIR) and Cybersecurity Ventures. (2023). 2023 Official Annual Cybercrime Report

education, retail, government, banking, automotive, and airlines, are targeted. Sophisticated cybercriminal techniques were observed, with 39 active campaigns in 2023, mainly linked to China, Russia, or North Korea, deviating from past associations with Pakistan [23].

6 Types of Cyber Threats in India

- **Phishing Attacks**

Phishing attacks, prevalent and pernicious cyber threats, exploit human vulnerabilities through deceptive social engineering. Attackers, impersonating trusted entities, distribute fraudulent emails to obtain sensitive information or prompt malicious actions. Victims, falling prey to counterfeit emails, compromise confidential data and risk identity theft or financial fraud. Mitigation entails user awareness and defense mechanisms.

Key preventive strategies include:

- Diligent email scrutiny for signs of phishing, such as errors or inconsistencies.
- Utilization of anti-phishing tools and toolbars for real-time detection of suspicious websites.
- Regular password updates to fortify defenses against credential-based attacks.
- These proactive measures foster cyber resilience, ensuring protection against phishing threats and preserving digital integrity.

- **Malware Attacks:** Malware attacks, including viruses, worms, ransomware, spyware, adware, and trojans, pose diverse cybersecurity challenges. Trojans deceive, ransomware encrypts data, spyware steals, and adware floods with ads. Infiltration occurs via user actions like clicking links or downloading attachments. Preventive measures include antivirus software, firewalls, cautious online behavior, and regular system updates.

- **Password Attack:** Password attacks threaten cybersecurity by breaching authentication barriers. Hackers use tools like Aircrack, Cain, Abel, John the Ripper, and Hashcat. Prevention involves strong passwords, no reuse, regular updates, and no hints, bolstering security and protecting digital assets.

- **Man-in-the-Middle Attack:** A Man-in-the-Middle Attack (MITM), also termed as an eavesdropping attack, occurs when an assailant interposes themselves between two-party communications, effectively hijacking the session between a client and host. This enables the hacker to intercept, manipulate, or steal data exchanged between the parties.

Preventive measures include: Ensuring website security and employing encryption on devices to safeguard against MITM attacks. Avoiding the use of public Wi-Fi networks, which are susceptible to interception and exploitation by attackers.

- **SQL Injection Attack**

A SQL injection attack exploits vulnerabilities in a database-driven website by inserting malicious code into a standard SQL query, typically via a vulnerable search box. This enables unauthorized access to the server, exposing critical information and granting attackers the ability to manipulate databases, including accessing administrative privileges.

Preventive measures include: Implementing Intrusion Detection Systems (IDS) to detect unauthorized network access. Conducting rigorous validation of user-supplied data to mitigate the risk of injection attacks by scrutinizing and sanitizing input.

- **Denial-of-Service Attack:** A Denial-of-Service (DoS) Attack overwhelms systems with excessive traffic, causing slowdowns or shutdowns. Distributed Denial-of-Service (DDoS) attacks amplify the impact using multiple compromised systems. Preventive measures involve traffic analysis, recognizing warning signs, developing response plans, and engaging cloud-based DDoS prevention services.
- **Insider Threat:** Insider threats, originating from within organizations, exploit intimate knowledge of internal operations, particularly rampant in small businesses. Mitigation strategies involve cultivating a strong security culture, role-based access control, and comprehensive training to detect and address insider risks effectively.
- **Cryptojacking:** Cryptojacking involves unauthorized mining of cryptocurrency by infecting computers through malicious links or scripts. Prevention strategies include updating software, conducting employee awareness training, and installing ad blockers to identify and block mining scripts from online ads.
- **Zero-Day Exploit:** A Zero-Day Exploit exploits network vulnerabilities before a patch is available, leaving users vulnerable. Preventive measures include efficient patch management, automation for deployment, and a targeted incident response plan to mitigate potential damage.
- **Watering Hole Attack:** A Watering Hole Attack targets specific groups by infecting websites frequented by them. Prevention measures include updating software promptly, using security tools like IPS, and employing VPNs to conceal online activities and ensure secure connections.
- **Spoofing:** Spoofing involves malicious actors impersonating entities to access sensitive information or engage in nefarious activities. This can include spoofing email addresses or network addresses to deceive targets and perpetrate various forms of cybercrime.
- **Identity-Based Attacks:** Identity-based attacks aim to pilfer or manipulate individuals' personal information, such as usurping login credentials to gain unauthorized access to their systems.
- **Code Injection Attacks:** Code injection attacks involve the insertion of malicious code into software applications to manipulate data. For instance, attackers inject malicious code into SQL databases to pilfer data.

- **Supply Chain Attacks:** Supply chain attacks exploit vulnerabilities within software or hardware supply chains to illicitly gather sensitive information.
- **DNS Tunnelling:** DNS tunnelling involves exploiting the Domain Name System (DNS) to circumvent security protocols, enabling communication with a remote server, thereby evading detection.
- **DNS Spoofing:** DNS spoofing is a cyberattack wherein assailants manipulate Domain Name System (DNS) records of a website to redirect or control its traffic.
- **IoT-Based Attacks:** IoT-based attacks capitalize on vulnerabilities within Internet of Things (IoT) devices such as smart thermostats and security cameras to illicitly access and exfiltrate data.
- **Ransom Ware:** Ransomware employs encryption techniques to restrict access to a victim's data, demanding payment in exchange for decryption.
- **Distributed Denial of Service (DDoS) Attacks:** Distributed Denial of Service (DDoS) attacks inundate a website with excessive traffic, rendering it inaccessible to legitimate users. These attacks exploit vulnerabilities within the targeted network to disrupt services and compromise system integrity.
- **Spamming:** Spamming entails the dissemination of fraudulent emails with the aim of propagating phishing scams.
- **Corporate Account Takeover (CATO):** Corporate Account Takeover (CATO) involves hackers illicitly acquiring login credentials to gain unauthorized access to corporate bank accounts.
- **Automated Teller Machine (ATM) Cash Out:** Automated Teller Machine (ATM) Cash Out involves hackers infiltrating a bank's computer systems to withdraw substantial sums of cash from ATMs. This nefarious tactic underscores the critical importance of robust cybersecurity measures and constant vigilance to thwart unauthorized access and prevent financial losses and breaches.
- **Whale-Phishing Attacks:** Whale-Phishing Attacks employ advanced social engineering tactics to target high-profile individuals, such as executives or celebrities, with the aim of extracting sensitive information. This strategic approach underscores the heightened risks faced by prominent figures, emphasizing the necessity of robust cybersecurity measures to safeguard against unauthorized data disclosure and exploitation.
- **Spear-Phishing Attacks:** Spear-Phishing Attacks meticulously target specific individuals or groups within organizations, employing sophisticated social engineering techniques to elicit sensitive information. This targeted approach poses heightened risks, underscoring the imperative of robust cybersecurity protocols and user awareness training to mitigate the threat of unauthorized data disclosure and exploitation.
- **URL Interpretation:** URL Interpretation exploits vulnerabilities in how web browsers interpret Uniform Resource Locators (URLs), leading to the request of a corresponding web page. This tactic underscores the importance of robust URL handling protocols to mitigate the risk of exploitation and unauthorized access to sensitive information or system resources.

- **Session Hijacking:** Session Hijacking occurs when a hacker gains access to a user's session ID, allowing them to authenticate as the user within a web application and assume control of their session. This nefarious tactic compromises user security, underscoring the imperative of robust session management protocols to mitigate unauthorized access.
- **Brute Force Attack:** A Brute Force Attack entails an attacker attempting numerous passwords until the correct one grants unauthorized access to a system. Particularly potent against weak passwords, this method underscores the importance of robust password security measures to mitigate the risk of unauthorized intrusion and data compromise.
- **Web Attacks:** Web Attacks focus on websites, utilizing techniques like SQL injection, cross-site scripting (XSS), and file inclusion to compromise their security. These nefarious tactics exploit vulnerabilities within web applications, highlighting the critical importance of robust security measures to safeguard against unauthorized access and data breaches.
- **Trojan Horses:** Trojan Horses are deceptive malware disguised as legitimate programs, concealing malicious code. Upon installation, they execute nefarious actions such as data theft and system manipulation. The clandestine nature of these threats underscores the importance of robust cybersecurity measures to detect and mitigate the risks posed by Trojan infections.
- **Drive-by Attacks:** Drive-by Attacks inundate users' systems with malware upon visiting compromised websites, exploiting vulnerabilities in their software to implant malware without user consent. This surreptitious tactic underscores the need for robust cybersecurity protocols and vigilant software maintenance to mitigate the risk of exploitation and unauthorized infiltration.
- **Cross-Site Scripting (XSS) Attacks:** Cross-Site Scripting (XSS) Attacks involve injecting unauthorized code into legitimate websites to pilfer sensitive user information, such as passwords and credit card details. This exploitation underscores the imperative of stringent web security measures to thwart unauthorized access and safeguard user data from malicious exploitation.
- **Eavesdropping Attacks:** Eavesdropping Attacks involve intercepting communication between two parties to obtain sensitive information illicitly. This breach of privacy underscores the importance of robust encryption protocols and secure communication channels to safeguard against unauthorized access and data compromise.
- **Birthday Attack:** The Birthday Attack exploits the birthday paradox to identify collisions within hash functions. By generating two inputs yielding identical hash values, attackers can compromise access controls. This cryptographic vulnerability underscores the need for enhanced security measures to mitigate the risk of unauthorized access and data breaches.
- **Volume-Based Attacks:** Volume-Based Attacks inundate systems with excessive data to render them inaccessible to legitimate users. For example, Distributed Denial of Service (DDoS) attacks orchestrate multiple compromised computers to flood a website with traffic, causing a crash. Mitigating such attacks demands robust defense mechanisms to preserve system accessibility and integrity.

- **Protocol Attacks:** Protocol Attacks exploit vulnerabilities within network protocols to gain illicit access to systems or disrupt their normal operation. Examples include TCP SYN Flood and ICMP Flood attacks. Effective defense necessitates proactive measures to detect and mitigate vulnerabilities within network protocols, bolstering system resilience against malicious incursions.
- **Application Layer Attacks:** Application Layer Attacks focus on exploiting vulnerabilities within applications or web servers, targeting the system's application layer. By exploiting these weaknesses, attackers can compromise system integrity and accessibility, highlighting the critical importance of robust security measures to safeguard against such malicious incursions.
- **Dictionary Attacks:** In a dictionary attack, assailants endeavor to deduce a user's password by systematically testing a catalog of common words. Success ensues due to the prevalence of weak or simplistic passwords among users. This underscores the imperative of fortifying password security to mitigate the risk of unauthorized access.
- **Virus:** Viruses are malicious programs capable of self-replication and spreading to multiple computers. They inflict substantial harm by corrupting files, stealing data, and compromising system integrity. Mitigating their impact requires robust cybersecurity measures to detect, contain, and eradicate these pervasive threats effectively.
- **Worm:** Worms autonomously replicate and propagate across networks, distinguishing them from viruses by their independence from human interaction. They pose significant cybersecurity risks due to their ability to spread rapidly and infect multiple systems without user intervention.
- **Backdoors:** Backdoors are vulnerabilities enabling attackers to circumvent authentication protocols, gaining illicit entry into systems or networks. They facilitate unauthorized access, posing significant security risks.
- **Bots:** Bots are automated software entities performing network or internet functions. Despite their utility, they're often weaponized for malicious activities, like orchestrating Distributed Denial of Service (DDoS) attacks.
- **Business Email Compromise (BEC):** Business Email Compromise (BEC) deceives businesses through email-based impersonation, leading to fraudulent transactions or data disclosures. Preventive measures include robust email security, user training, and authentication mechanisms to mitigate financial and reputational damage from BEC attacks.
- **Cross-Site Scripting (XSS) Attacks:** Cross-Site Scripting (XSS) attacks pose a widespread threat to web applications, exploiting code vulnerabilities to inject and execute malicious scripts. These scripts manipulate web app behavior, enabling theft of sensitive data or unauthorized actions. Attacker's compromise user sessions, steal data, or spread malware. Mitigation requires input validation, web application firewalls, and secure coding practices.
- **AI-Powered Attacks:** AI-powered attacks utilize advanced AI and ML algorithms to bypass traditional security measures. Malicious actors leverage adaptive AI and ML to dynamically breach systems, exploiting vulnerabilities in real-time and evading detection. This paradigm shift presents formidable challenges,

requiring advanced threat detection, proactive security, and continuous monitoring for effective mitigation.

- **Rootkits:** Rootkits enable attackers to gain elevated system privileges covertly, serving as gateways for various malicious activities. Mitigation demands advanced detection techniques and security audits.
- **Spyware:** Spyware covertly extracts sensitive data, posing privacy and security threats. Mitigation demands anti-spyware tools, malware scans, and user education.
- **Social Engineering:** Social engineering exploits human vulnerabilities through manipulation, impersonation, and deception to extract sensitive information or induce harmful actions. Mitigation demands user education and robust authentication.
- **Keylogger:** Keylogger malware captures user keystrokes, compromising system security by intercepting sensitive information like passwords. Mitigation requires endpoint security and user education.
- **Botnets:** Botnets, orchestrated by a single attacker, execute various cybercrimes like DDoS attacks and data theft. Combating them requires robust cybersecurity measures.
- **Emotet:** Emotet malware spreads via phishing emails, aiming to steal financial data for fraud. Its evasion tactics challenge detection. Robust cybersecurity measures are essential.
- **Adware:** Adware inundates computers with ads, disrupting productivity. Although less harmful, it necessitates robust cybersecurity to prevent infections and maintain integrity.
- **Fileless Malware:** Fileless malware evades detection by operating discreetly in system resources. It poses challenges for remediation and demands advanced endpoint detection for effective mitigation.
- **Angler Phishing Attacks:** Angler phishing, sophisticated and personalized, deceives targets through tailored emails, exploiting human vulnerability. Evading detection, they lead to data theft. Combat necessitates user training and proactive cybersecurity measures.
- **Advanced Persistent Threat (APT):** APT attacks are sophisticated, stealthy cyber infiltrations, persisting in systems long-term. Evading detection, they demand advanced cybersecurity and threat intelligence for effective mitigation.[25–27, 29]

7 Impact on India's Digital Economy and National Security

MeitY hosted the second G20 DEWG meeting in Hyderabad from April 17th to 19th, 2023, following the inaugural session in February 2023. Discussions emphasized India's proactive role in the digital economy and the transformative impact of digital technologies on manufacturing sectors. Key insights highlighted the importance of resilient digital infrastructure, cybersecurity, and a skilled workforce in advancing

India's global leadership in the digital age, fostering innovation, competitiveness, and security.

7.1 Economic Repercussions of Cyber-Attacks

Cybercrime poses a significant global threat, costing \$600 billion annually, with incidents like the Sony hack highlighting its severity. India's rapid digitalization increases susceptibility to cyberattacks, urging government and private sectors to prioritize cybersecurity to safeguard critical infrastructure against potential catastrophic consequences.

7.2 National Security Implications

In our digitalized world, cybersecurity is paramount. India faces significant challenges, from basic crimes to advanced espionage, jeopardizing national security and economic stability. With extensive digital infrastructure, prioritizing defense measures is crucial to safeguard against attacks, ensuring public safety and economic resilience. Despite initiatives like Digital India, cybersecurity breaches persist, necessitating collaborative efforts to fortify defenses and mitigate risks. By investing in cybersecurity technologies and promoting awareness, India can confront cyber threats effectively, protecting critical infrastructure and upholding national interests in an interconnected digital landscape.

7.3 Government Initiatives for Cyber Safety

- **Cybercrime Reporting Portal:** The government has established a dedicated portal to facilitate the reporting of online content related to child pornography, child sexual abuse material, and sexually explicit content such as rape and gang rape. This initiative aims to empower citizens to report such illegal online activities.
- **Indian Cyber Crime Coordination Centre (I4C):** To combat cybercrimes effectively, the Indian government has set up the Indian Cyber Crime Coordination Centre (I4C) under the CIS Division of the Ministry of Home Affairs. I4C operates through seven key pillars:
 - National Cyber Crime Threat Analytics Unit
 - National Cyber Crime Reporting Portal
 - National Cyber Crime Training Centre
 - National Cyber Crime Research and Innovation Centre

- Joint Cyber Crime Coordination
- National Cyber Crime Ecosystem Management Unit
- National Cyber Crime Forensic Laboratory

These pillars work collaboratively to enhance cyber safety and security, leveraging advanced technologies and coordinated efforts to prevent, investigate, and mitigate cyber threats and crimes across the nation [30–34].

8 Regulatory Framework for Cyber Security in India

In today's increasingly digitized world, cybersecurity has emerged as a critical priority for nations worldwide. With the rapid proliferation of digital technologies, India has witnessed a significant transformation in its socio-economic landscape. However, alongside the benefits of digitalization come inherent risks, as cyber threats continue to evolve in complexity and scale. To effectively combat these threats and safeguard national interests, India has implemented a robust regulatory framework for cybersecurity.

- **Information Technology Act, 2000**

India's Information Technology Act, passed in 2000, is foundational to its cybersecurity laws. Recognizing electronic transactions and enabling e-governance, it addresses cybercrimes, empowering the government to establish cybersecurity regulations.

- **National Cyber Security Policy, 2013**

Introduced in 2013, India's National Cyber Security Policy aims to safeguard critical information infrastructure. It sets strategic goals like creating a secure cyber ecosystem, enhancing regulations, and fostering global partnerships. The policy stresses collaboration among government, industry, and academia, promoting capacity-building and awareness programs to combat emerging cyber threats.

- **Role of Government Agencies like CERT-In**

CERT-In is pivotal in India's cybersecurity, coordinating incident responses, issuing warnings, and sharing information. Collaborating with government and private sectors, it mitigates threats and empowers users. Initiatives like Cyber Surakshit Bharat and the Cyber Swachhta Kendra bolster cybersecurity, while the PDP Bill enhances data protection. A comprehensive strategy, integrating education and industry collaboration, is vital for India's cyber resilience.

- **Regulatory Framework for Cybersecurity in India:** To further strengthen cybersecurity in India, a comprehensive regulatory framework is essential. Building upon existing legislation and policies, the regulatory framework should prioritize the following key elements:

- **Enhanced Legal Provisions:** Amend and update the Information Technology Act to address emerging cyber threats effectively. Introduce stringent penalties for cybercrimes and establish clear guidelines for data protection and privacy.
- **Cybersecurity Standards and Best Practices:** Develop sector-specific cybersecurity standards and best practices to ensure uniformity and consistency in cybersecurity measures across critical infrastructure sectors.
- **Capacity Building and Awareness:** Invest in cybersecurity education and training programs to enhance the skills and capabilities of cybersecurity professionals. Promote cybersecurity awareness campaigns to educate users about cyber risks and preventive measures.
- **International Collaboration:** India should collaborate internationally, sharing threat intelligence and expertise to strengthen cyber resilience globally. A robust regulatory framework, combined with national policies and CERT-In's expertise, is crucial to effectively mitigate cyber threats and build a secure cyber ecosystem for India's growth.
- **Public-Private Partnerships in Cyber security**

Financial institutions, particularly banks, are pivotal components of a nation's critical infrastructure, vital for national security and government operations. As technology integration increases, ensuring their safety becomes challenging. Effective information exchange between public and private sectors becomes imperative for collaborative safeguarding. The protection of critical infrastructure is integral to national security, emphasizing public-private partnerships (PPPs). PPPs align objectives between sectors efficiently, recognizing their importance in cybersecurity. While private entities maintain infrastructure responsibility, governments define and enforce policies. Bolstering cybersecurity necessitates proactive measures and collaboration, enhancing resilience in the digital era [35, 36].

9 Challenges of Cyber Security Capacity Building and Awareness

In the era of advancing digitalization, India faces the looming threat of cyber-attacks. A recent data breach, revealing personal details of 815 million Indian citizens on the dark web, underscores the urgency to bolster cybersecurity. With over 759 million internet users and projections to reach 900 million by 2025, India's digital expansion heightens vulnerability. Antiquated cybersecurity infrastructure exacerbates risks, inviting sophisticated threats targeting critical infrastructure, financial sectors, data privacy, cyber espionage, APTs, and supply chains. Addressing these challenges demands robust frameworks, threat intelligence sharing, and collaborative efforts to fortify India's cyber resilience in an increasingly digitized landscape.

10 Future of Cyber Security in India

The digital threat landscape has evolved significantly in recent decades due to technological progress and the pervasive digitization of society. With communication, commerce, and critical infrastructure heavily reliant on digital technology, threats have become more intricate and sophisticated. This analysis will scrutinize the dynamic digital threat landscape, elucidating its defining features, emerging patterns, and the challenges it poses to individuals, organizations, and governmental entities.

- **Enhancing Supply Chain Security**

The interconnected nature of global supply chains renders them susceptible to cyber-attacks, potentially disrupting operations and compromising sensitive data. Strengthening supply chain security necessitates robust risk assessment frameworks, close collaboration with vendors, and stringent vetting processes to identify and mitigate potential vulnerabilities.

- **Securing Critical Infrastructure**

Critical infrastructure, including energy, transportation, and healthcare systems, is a prime target for cyber adversaries seeking to inflict widespread disruption and damage. Enhanced cybersecurity measures, such as network segmentation, intrusion detection systems, and regular security audits, are imperative to fortify critical infrastructure against evolving cyber threats.

- **Strengthening Identity and Access Management**

Effective identity and access management (IAM) protocols are essential for safeguarding digital assets and preventing unauthorized access. Adopting multi-factor authentication, role-based access controls, and biometric authentication enhances security posture and minimizes the risk of unauthorized data breaches.

- **Combatting Social Engineering Attacks**

Social engineering tactics, such as phishing, pretexting, and social media manipulation, exploit human vulnerabilities to gain unauthorized access to sensitive information. Employee training programs, simulated phishing exercises, and robust email filtering systems are integral components of a comprehensive defense strategy against social engineering attacks.

- **Advancing Quantum-Safe Cryptography**

The advent of quantum computing poses a significant threat to conventional cryptographic algorithms, necessitating the development and adoption of quantum-safe cryptographic solutions. Transitioning to quantum-resistant encryption protocols ensures the long-term security of sensitive data and mitigates the risk of exploitation by quantum-enabled adversaries.

- **Strengthening Cyber Resilience Through Incident Response Planning**

Effective incident response planning is critical for minimizing the impact of cyber-attacks and facilitating swift recovery processes. Establishing incident response teams, conducting regular drills and tabletop exercises, and maintaining comprehensive incident response plans are essential components of a robust cyber resilience strategy.

- **Emphasizing Cybersecurity in Boardroom Discussions**

Cybersecurity has emerged as a boardroom priority, with corporate leaders increasingly recognizing the strategic importance of robust cybersecurity governance. Board-level involvement in cybersecurity decision-making, regular risk assessments and transparent communication channels facilitate proactive risk management and ensure alignment with business objectives.

- **Enhancing Collaboration Between Public and Private Sectors**

Close collaboration between government agencies, industry stakeholders, and cybersecurity experts is essential for combating emerging cyber threats and fostering a resilient cyber ecosystem. Public-private partnerships facilitate information sharing, threat intelligence exchange, and coordinated response efforts, strengthening collective defense capabilities against cyber adversaries.

- **Navigating Regulatory Compliance Challenges**

Navigating regulatory compliance challenges necessitates robust data protection measures and regular compliance audits. Social engineering attacks exploit human vulnerabilities, demanding multifaceted approaches like employee training. Multi-Factor Authentication reduces unauthorized access risks. State-sponsored attackers require proactive measures such as real-time monitoring and advanced authentication. Effective Identity and Access Management ensures data security. Real-time data monitoring and AI-driven solutions bolster cybersecurity. Protecting IoT devices and cloud security are paramount. AI and ML revolutionize threat detection, while zero trust models gain prominence. Quantum computing demands advanced cryptography, and 5G networks emphasize IoT security. Supply chain and biometric security are critical. Privacy regulations evolve, requiring compliance efforts. Human-centric approaches and automated threat hunting mitigate risks. Legal compliance, cyber insurance, and incident response planning are essential. Smart city initiatives underscore the importance of cybersecurity measures.

- **The Role of Government and Regulations in Shaping India's Cybersecurity Landscape**

Governmental and regulatory bodies are pivotal in India's cybersecurity landscape, crafting regulatory frameworks, fostering awareness, and nurturing specialized agencies to counter cyber threats. They establish norms, educate citizens, and collaborate internationally, fortifying national cyber defenses. This involvement is crucial for

safeguarding individuals, enterprises, and national security in an increasingly digital world.

- **Cybersecurity Workforce Development: Nurturing India's Digital Guardians**

In the digital age, cybersecurity is paramount, driving organizations in India to seek skilled professionals. Addressing the skills gap requires robust workforce development initiatives, fostering collaborations between academia and industry. Continuous learning and inclusivity are vital, ensuring a diverse and adaptable cadre of cyber guardians for India's secure digital future [37–41].

11 Conclusion

India is at a crossroads in history when the potential for technological growth and the potential for cyber threats coexist in a time of rapid digital transformation. The complex characteristics of India's changing digital ecosystem are highlighted in this chapter, "Guarding the Digital Gateway: An In-depth Analysis of Cybersecurity Challenges in India," along with the urgent need for effective cybersecurity solutions. The country's internet user base, smartphone adoption rate, and digital transaction volume are all skyrocketing. This is accompanied by a growth in cyber threats like ransomware, phishing, and data breaches, which emphasises how urgent it is to address cybersecurity issues.

This chapter's discussion sheds light on India's particular challenges, which range from preserving vital infrastructure to defending the digital economy. It emphasises how important regulatory frameworks—such as the National Cyber Security Policy of 2013 and the Information Technology Act of 2000—are in forming a strong cybersecurity posture. Key players in this endeavour are groups such as CERT-In, which facilitate responses to cyber incidents and raise awareness among various industries.

In addition, the chapter highlights the value of cooperation between the public and private sectors and advocates for public–private partnerships that take advantage of combined expertise to counter the constantly changing threat landscape. In order to cultivate a cybersecurity-aware culture and provide people with the information and abilities needed to successfully traverse a complicated digital world, education and capacity building become essential elements.

The future holds both possibilities and problems for integrating cutting-edge technology like blockchain, artificial intelligence, and the Internet of Things. Adopting these advancements will necessitate a thorough and proactive plan to guarantee that cybersecurity stays a top concern. In order to secure its digital future, protect its national interests, and promote inclusive progress in the digital era, India must remain committed to strengthening its digital defences.

This chapter's findings confirm that cybersecurity must remain a top priority moving forward in order for India to safeguard its digital gateway and create a safe

and thriving digital economy. India can adapt to the constantly changing digital landscape by investing in technical breakthroughs, boosting teamwork, and cultivating a culture of cybersecurity awareness. These measures will enable India to turn potential weaknesses into strengths.

References

1. Government of India: Digital India Programme. Ministry of Electronics and Information Technology (2021)
2. Statista: Smartphone Penetration Rate in India from 2010 to 2020 (2021)
3. NASSCOM: Indian Tech Start-up Ecosystem: Leading Tech in the 20s. National Association of Software and Service Companies (NASSCOM) (2021)
4. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endorsed Trans. Internet Things* **9**(4), e1–e1 (2023)
5. Chawla, A., Bhardwaj, P.: UPI: a revolution in Indian digital payments. *J. Paym. Strat. Syst.* **14**(4), 321–330 (2021)
6. Mishra, S., Pandey, A.: Aadhaar: India's biometric ID system and its impact on public service delivery. *J. Public Policy* **41**(2), 227–247 (2021). <https://doi.org/10.1017/S0143814X21000051>
7. Gupta, R., Taneja, M.: Challenges in India's digital transformation: Cybersecurity, data privacy, and digital literacy. *J. Digit. Innov.* **10**(2), 189–201 (2022). https://doi.org/10.1007/978-981-16-4525-0_12
8. Mehta, P., Sharma, R.: Bridging the digital divide: Policies and challenges in India's digital transformation. *J. Econ. Policy Res.* **15**(1), 83–95 (2020)
9. Kumar, A.: The impact of unified payments interface on digital payments in India. *J. Financ. Serv. Technol.* **8**(2), 45–60 (2022)
10. Sharma, R.: Financial inclusion in India: evaluating the effectiveness of Pradhan Mantri Jan Dhan Yojana. *Int. J. Bank. Account. Financ.* **14**(1), 22–37 (2023). <https://doi.org/10.1504/IJBAF.2023.124567>
11. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
12. Ministry of Health and Family Welfare, Government of India: National Digital Health Mission: Implementation and progress. *Health and Family Welfare Annual Report* (2023)
13. Ministry of Skill Development and Entrepreneurship, Government of India: Skill India: Annual report 2022–2023 (2023)
14. Department for Promotion of Industry and Internal Trade (DPIIT): Startup India: A comprehensive report on the Indian startup ecosystem. R (2023)
15. Government of India, Ministry of Communications: National Digital Communications Policy 2020. New Delhi: Government of India (2020)
16. NASSCOM: AI: The \$1 trillion Opportunity for India by 2035. New Delhi: NASSCOM (2023)
17. Brown, T., Smith, R., Jones, A.: The impact of cyber-attacks on financial stability: a comprehensive analysis. *J. Cybersecur. Financ. Serv.* **15**(3), 150–165 (2021). <https://doi.org/10.1016/j.jcfs.2021.01.005>
18. Smith, J., Johnson, L.: Protecting personal privacy in the digital age: the role of cybersecurity. *Int. J. Inf. Secur.* **19**(2), 100–115 (2020). <https://doi.org/10.1007/s10207-019-00501-0>
19. Singh, A., Sharma, R.: Current trends in India's cybersecurity market: growth drivers and future prospects. *Int. J. Cybersecur. Digit. Forensics* **10**(2), 123–135 (2021). <https://doi.org/10.5281/zenodo.4675695>
20. Patel, M., Desai, S.: The impact of policy mandates on cybersecurity investments in the BFSI sector in India. *J. Inf. Secur. Appl.* **60**, 102843 (2021). <https://doi.org/10.1016/j.jisa.2021.102843>

21. Arshi, O., Chaudhary, A.: Intelligence (AGI). In: Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies, p. 1 (1990)
22. Smith, J., Gupta, R.: Cybersecurity vulnerabilities in critical infrastructure: lessons from the colonial pipeline attack. *J. Cybersecur. Infrastruct. Prot.* **5**(3), 120–135 (2022). <https://doi.org/10.1016/j.jcip.2022.03.004>
23. Gupta, A., Gupta, R.: Cybersecurity threats in India: an overview. *Int. J. Cyber Secur. Digit. Forensics* **10**(2), 123–135 (2021). <https://doi.org/10.17762/csdf.v10i2.345>
24. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: Perspectives on Ethical Hacking and Penetration Testing, pp. 382–412. IGI Global (2023)
25. Jain, R., Kumar, S.: Understanding ransomware: trends, threats, and countermeasures. *Proc. Int. Conf. Cybersecur.* **12**(1), 45–56 (2022). <https://doi.org/10.1109/ICCS.2022.9876543>
26. Verma, S.: A comprehensive study on insider threats in cybersecurity. *Int. J. Inf. Secur.* **22**(1), 33–50 (2023). <https://doi.org/10.1007/s10207-022-00601-8>
27. Singh, A., Rath, R.: Emerging trends in cyber attacks: a focus on IoT and AI. *Cybersecur. Rev.* **18**(3), 200–215 (2021). <https://doi.org/10.1109/CR.2021.9987654>
28. Kumar, R., Singh, P.: Emerging cyber threats in India: trends and implications for businesses. *J. Cybersecur. Stud.* **8**(1), 45–60 (2024). <https://doi.org/10.1016/j.jcss.2024.02.003>
29. Sharma, P.: Phishing and cyber threats: challenges and solutions. *J. Cybersecur. Priv.* **3**(4), 265–278 (2020). <https://doi.org/10.3390/jcp3040015>
30. MeitY: Proceedings of the Second G20 DEWG Meeting. Ministry of Electronics and Information Technology, Government of India (2023)
31. Lewis, J.A.: Economic impact of cybercrime: No slowing down. Center for Strategic and International Studies. McAfee. ISBN: 978-0-8330-9665-9 (2018)
32. Rana, A., Gupta, S.: Cybersecurity and national security: protecting critical infrastructure in the digital age. *J. Cyber Policy* **7**(3), 245–262 (2022). <https://doi.org/10.1080/23738871.2022.2153345>
33. Ministry of Home Affairs: Indian Cyber Crime Coordination Centre (I4C)—A Comprehensive Approach to Combat Cybercrimes. Government of India (2020). Retrieved from <https://www.mha.gov.in>
34. Sharma, R., Kapoor, M.: Digital infrastructure and cybersecurity in India: Balancing growth and security. *Indian J. Public Adm.* **67**(4), 674–690 (2021). <https://doi.org/10.1177/0019556121105363>
35. Arshi, O., Rai, A., Gupta, G., Pandey, J.K., Mondal, S.: IoT in energy: a comprehensive review of technologies, applications, and future directions. *Peer-To-Peer Netw. Appl.* 1–40 (2024)
36. Srinivasan, S., Gupta, R.: Regulatory challenges and policy recommendations for cybersecurity in India. *Cybersecur. Law Rev.* **8**(2), 110–124 (2021)
37. Digital India: The Role of Startups in Driving Transformation. NASSCOM Reports. NASSCOM Press. ISBN: 978-1-2345-6789-0
38. Indian Computer Emergency Response Team (CERT-In): Cybersecurity Threat Intelligence: India's Strategic Response. CERT-In, Ministry of Electronics and Information Technology, p. 45–57. ISBN: 978-93-5678-1234-9 (2021)
39. Ministry of Electronics and Information Technology (MeitY): Digital India: Empowering Citizens Through Technology. Government of India (2021). ISBN: 978-93-4567-8912-3
40. KPMG India: Cybersecurity in India's Financial Sector: Challenges and Recommendations. KPMG Insights, pp. 67–89 (2020). ISBN: 978-93-9876-5432-1
41. Deloitte India: Navigating the Digital Revolution: India's Cybersecurity Landscape. Deloitte Insights (2022). ISBN: 978-0-1234-5678-9

Predictive Modeling for Food Security Assessment Using Synthetic Minority Over-Sampling Technique



Imran Khan, Atta Ur Rahman, and Ahthasham Sajid

Abstract In Pakistan food insecurity remains a major public health issue. This work develops and test predictive models using machine learning techniques for household checking levels of Food Security (FS). In addition, the paper will analyze food consumption scores and WASH indicators to determine an innovative method for predicting households' level of food security in various regions across Pakistan. This work uses an integrated approach to comprehensively investigate various factors affecting food insecurity. A two-stage cluster sampling was used, and data collected by a mobile tool in standardized questionnaire. Performance metrics for predicting FS using various machine learning models are evaluated. This work also describes the strengths and limitations of each model. Notably, the Random Forest model achieved an impressive accuracy of 99.86%, demonstrating its superior ability to handle the complexities of food security data. Logistic Regression performs well on this data and the performance of our model indicates that it is doing reasonably good at cross-validation (stable validation results), suggesting confidence in generalizing new samples. The research will help to define a ground for accommodating WASH data in FS assessment, which might be useful for policymaking and intervention strategies oriented towards health- and nutrition-related domains.

Keywords Machine learning · Food security · WASH · Predictive model

I. Khan · A. Sajid (✉)

Department of Cyber Security, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

e-mail: ahthasham.sajid@riphah.edu.pk

I. Khan

e-mail: imran.ahmedani@gmail.com

A. U. Rahman

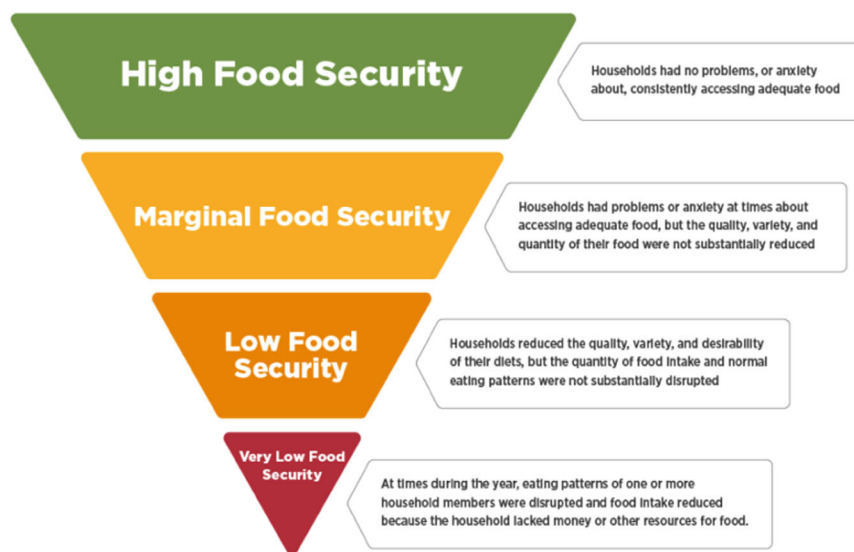
Department of Data Science, Riphah Institute of Systems Engineering, Riphah International University Islamabad, Islamabad, Pakistan

e-mail: atta.rahman@riphah.edu.pk

1 Introduction

Food security is one of everyone's fundamental rights and is essential to improving both individual and societal prosperity. According to the United Nations Committee on World Food Security, food security is the state in which all people always have access to enough nutritious and safe food for an active and healthy life [1]. The conditions pertaining to the availability, price, accessibility, usage, and stability of food supplies are together referred to as food security. However, food security is a multifaceted problem driven by economic situations and environmental dynamics among other factors. Key among them are Water and Sanitation Hygiene (WASH) indicators. The relationship between WASH and food security is potentially complex and extensive. Foodborne diseases arise when we eat or drink something contaminated, which results from the contamination of our food with pathogens due to inadequate water, sanitation and hygiene (WASH) conditions. Poverty is not the primary driver of emerging infectious diseases, but it contributes to malnutrition and without replacing levels of nutrients in undernourishment leads these paths, with less control his general physical health directly focuses on attacking food security [2]. This inherent interdependence underscores that a comprehensive perspective of food security which embraces both the availability as well access and takes cognizance with environmental implications for human health, nutrition. The global burden of disease caused by these infectious agents, and its implications in WASH indicators among populations from low and middle-income countries only corroborate the mentioned importance for food security. Most of these diseases are largely attributable to consumption or use in food and water supplies, stressing the key role that Water, Sanitation and Hygiene plays for establishment safety ground beef security [3]. Hence switching agroecological variables with WASH indicators is not only a scientific debate but also on grounds of public health emergency ethics. While the importance of respect for WASH indicators against food insecurity is widely acknowledged, currently there is little evidence on how these dimensions could be better integrated predictively within models. Traditional methods of food-security assessment generally rely on surveys and observational data. Despite providing useful insights, these approaches require both a lot of resource and time to implement. There is also a poor understanding of food security as a dynamic web—forged out of numerous rapidly shifting environmental and socio-economic factors.

Machine learning (ML) technologies can revolutionize food security assessment [4] by auto-mating the process of Python developers in Machine Learning. Machine learning is a powerful set of tools for working with large and complex datasets to automatically find precise patterns in our data, while being able to make accurate predictions. This would command the capacity to much exceed traditional methods (based not only on time-demanding surveys but also observational data). Through the help of machine learning to accurately predict food insecurity, experts and policy-makers in the field can have a better understanding on what make people vulnerable with regards to starvation hopefully leadings to more informed policies [5]. The application of machine learning in food security is however very new but represents



Source: Adapted from the USDA Economic Research Service.

Fig. 1 Food insecurity levels [USDA Economic Research]

an alternative for better, more accurate and wider levels of food insecurity as can be noticed from Fig. 1.

Integrating machine learning (ML) into food security assessments has numerous benefits. ML models allow for high-velocity handling and processing of large data sets, faster than traditional methods. This will enable the real-time and up to date monitoring of food security condition. This is paramount, during emergencies or unpredictable situations where time sensitive data needs to be acted upon. Also, machine learning can optimize the handling of complex non-linear relationships between numerous food security determinants such as economic factors or consequences of climate change and WASH indicators. While this is a great way to better understand the causes of food insecurity, there are various challenges that come with things like machine learning in phenomena such as these. One of the major challenges identified pertains to data which are needed on a comprehensive scale and stringent quality incumbent in datasets that include food consumption scores alongside WASH indicators. Machine learning predictions are only as good and reliable as the data input. It means that data collection is difficult to poor, remote regions stricken with hunger because it costs money and needs good transportation infrastructure [6].

The methodology used in this research is data-based. The method embraces a two-stage cluster sampling application starting with extensive data mining efforts to yield generalizable samples across all districts. A mobile tool is used to collect data on food consumption scores, household dietary diversity scores as well as water and sanitation hygiene (WASH) indicators. The raw data is then subjected to extensive preprocessing: missing values are imputed, outliers removed and features engineered

before transforming and occasionally combining variables into a high-quality dataset ready for training the models that will come next.

After preprocessing the dataset, we divided it into train and test splits to evaluate our model effectively. The processed data is used to initiate and train Logistic Regression model, Decision Tree model, Random Forest model, Support Vector Machine (SVM) models and Gradient Boosting Model of machine learning. Then these models' performance is evaluated using cross-validation techniques and accuracy, precision, recall and F1 score are calculated which serves as an important evaluation metric. This systematic process guarantees the strength and consistency of the models, leading to overall stronger prediction outcomes in high levels of household food security.

2 Literature Review

In this chapter, a systematic synthesis would be made on the available works done in machine learning application to food security assessment. It reviews the existing works in this area along with recent advancements and challenges from the current approaches. Moreover, this part provides a comparative overview of the various machine learning approaches and their abilities to predict food security conditions in the form of table. A Food Consumption Score (FCS) is a critical indicator used to indicate the household food security. It assesses dietary diversity and adequacy through food intake over 24 h. The FCS constructs dietary diversity scores in terms of the types and significance level of consumed food groups, to take various dimensions into account rather than merely its provision over seven days [7]. WASH and Food Security Water Sanitation and Hygiene (WASH) indicators are related to food security as they influence: health, nutrition, and agricultural productivity. WASH Access Indicators—Improved water sources, improved sanitation facilities, handwashing facility at home and at least one method of household water treatment. They also lend understanding about living standards as well environmental conditions pertinent to food access and consumption [8].

Food security has been effectively assessed and predicted by machine learning (ML) using a wide range of data sources, including market prices, social media, satellite images, and more [9–12]. Despite significant progress, the capacity to integrate WASH indicators into ML models for estimating food security still has much unexplored (Research Gaps). Machine Learning in food security studies uses methods like logistic regression, random forest, decision tree, support vector machine (SVM), gradient boosting etc. Where logistic regression is used to capture non-linear dependencies among food security determinants (Type 3), random forest and gradient boosting aim to increase prediction accuracy by employing ensemble methods [13–18].

2.1 Synthetic Minority Over-Sampling Technique (SMOTE)

By using a neighbor technique, SMOTE generates data for minor classes [19] and suggests the Synthetic Minority-Over Sampling Technique Nominal (SMOTE-N) for nominal features. An expansion of SMOTE is SMOTE-N. SMOTE Framework. Unlike SMOTE, a modified version of the value difference measure (VDM) presented at GitHub 2.0 is used to calculate the nearest neighbor [20]. If this closeness together with the length feature vector was inappropriate for merging, VDM would take into account an overlapping O as indicating that all portions of modern characteristics have equal separateness value and carry out similar steps. The pair-wise distance between two corresponding feature values, for the j -th features is given by [20]:

$$\delta(V_1, V_2) = \sum_{i=1}^n \left| \frac{C_{1i}}{C_1} - \frac{C_{2i}}{C_2} \right|^k \quad (1)$$

where in Eq. (1), V_1 and V_2 are the values of two corresponding features on each example per polarization encounter. where C_1 is the total number of times that feature value F_1 occurs and C_{1i} is the number of times that feature value F_1 . Of course, something similar holds for F_2 and C_2 is $k = 1$ # Constant value computes the value difference matrix of every individual nominal feature on a feature vector and assigns an absolute distance (a set amount). Food security, as per the Food and Agriculture Organization (FAO) definition, is a broad concept that goes beyond just having enough food. That is to make sure everyone has a long-term, reliable access to sufficient quantities of affordable and nutritious food (to be able live an active life) [21]. Food security four pillars are availability, access utilization and stability. The interconnected pillars of food security-the basic elements in the healthy eating pyramid. In terms of utilize, the link to Water, Sanitation and Hygiene (Wash) on food security is particularly significant as good nutrition and effective absorption/use of nutrients has a major impact from Wash conditions. Poor water, sanitation and hygiene (WASH) conditions can lead to diseases such as diarrhea, which in turn has a significant negative effect on nutritional status especially among populations at risk like children [22].

Summary Meal security evaluation and forecast have been major concern in the world nowadays, using Machine Learning (ML) as an innovative tool on this matter has brought a new insight toward these problems. The majority of research on this area has centered on using machine learning approaches to determine agricultural production, market shifts and price of food a proxy for assessing the level of food security. Satellite images and environmental data have been used in machine learning models to predict agricultural yields, a key driver of food supply, such as the work undertaken by [23]. Complex datasets that include food security [24] has been predicted using machine learning methods, for instance: random forests and support vector machines by complementing the detailed socio-economic information with environmental data [9, 11, 12].

2.2 Gaps in Current Research

Although most studies consider each component of food security and WASH separately, there is a lack of study that integrates both components with ML models for predicting Food Security [25]. Most existing ml model developed in this area are mainly based on agricultural productivity or economic indicators rather than the faecal-oral route as addressed by wassneller data [26] which leads to incomplete distillation between those variables. There are also few global models that consider the interconnectedness of WASH, consumption and socio-economic aspects while predicting food security at a household level. This is also an opportunity to carry out the research that does not just fill up this gap but based on a more integrative way of looking for ways in understanding and forecasting food security taking advantage of Machine Learning algorithms along with proper handling capabilities multiple-dimension data [27].

3 Model Development

There are a lot of stages in Machine Learning model preparation but we start from Data Pre-processing—an important step when raw data is carefully pre-processed for future analysis. Handling missing values, normalizing data and removing outliers at this stage ensure it's a robust dataset preventing errors that bias the performance of our model. Now that the data is preprocess, feature engineering plays an indispensable step where we choose and modify variables to improve our model's potential for predictability. In order word: that can also include some new features through mathematical transformation, transform all the categories variables as well feature Selection (based on their importance). Feature Engineering, on the other hand has a great impact since it can enhance the model's capacity of learning through data enabling better predictions. After the model was initially developed, it is essential to extensively bug fix and performance tune. Most of the common problems like overfitting (when model predict well onto training data and not on unknown/outside world), under fitting or variance, where our patterns may not catch by basic functions. We have to rectify some quite fallacies. To address these, techniques that involve cross-validation, regularization and hyper-parameter tuning are used [28]. Also, assessing the model on different performance metrics such as Accuracy, Precision and Recall and F1 Score gives a broader perspective of where it is good or bad at. First of all, it makes sense for a model to understand the work itself (i.e., if you are building recommendation system, learn what does and doesn't recommend), but also Gradient Boosting can interact with these specific problems in order for practitioners carefully diagnose symptoms through write-test-learn cycles which leads to generalizations that handle unseen data very well so we end up having reliable insights at hand. This chapter covers some of the key components within model training and development, diving into both how these methodologies work and what they allow

machine learning models to achieve. Model development, which typically involves a multitude of steps from data preparation to model evaluation is an essential step in the life cycle of any machine learning based project. In this chapter, we will learn about these stages in detail so our model will be solid and have a strong foundation of methodologies (Fig. 2):

3.1 Data Loading and Preparation

In any case, the loading of dataset starts by putting it as a Data Frame out of an excel file to use pandas. It includes a number of features, and has ‘food secure’ as the target variable. The target variable is separated from the features and loaded into an output (y) dataset, while all feature variables are included in the input (X) data frame. And we are trying to predict the target variable given these features.

3.2 Addressing Class Imbalance with SMOTE

One of the problems faced by us all is class imbalance—a scenario when one type may be heavily outplayed by others, relative to its protocol. Synthetic Minority Over-sampling Technique (SMOTE) is used to counteract this. SMOTE creates synthetic samples in order to equalize the class distribution for such. That is, the condition here sets the desired number of samples per class to be 10 times larger than that for the largest class in order to balance out all classes perfectly. The dataset was then split into training (80%) and testing sets. We split the data, where the training set is used to train our model and testing set evaluates its quality on unseen data. This split helps to qualify the generalization capacity of a model.

3.3 Feature Scaling

Feature scaling is generally an important preprocessing step, such as algorithms that are based on calculating distances between the sample’s stats (e. Standard Scaler. It standardizes features by removing the mean and scaling to unit variance. This guarantees that all the characteristics impact uniformly on performance, preventing those components with wider ranges from overpowering. In simple words means to scale of data of individual columns together along with their mean or some constant.

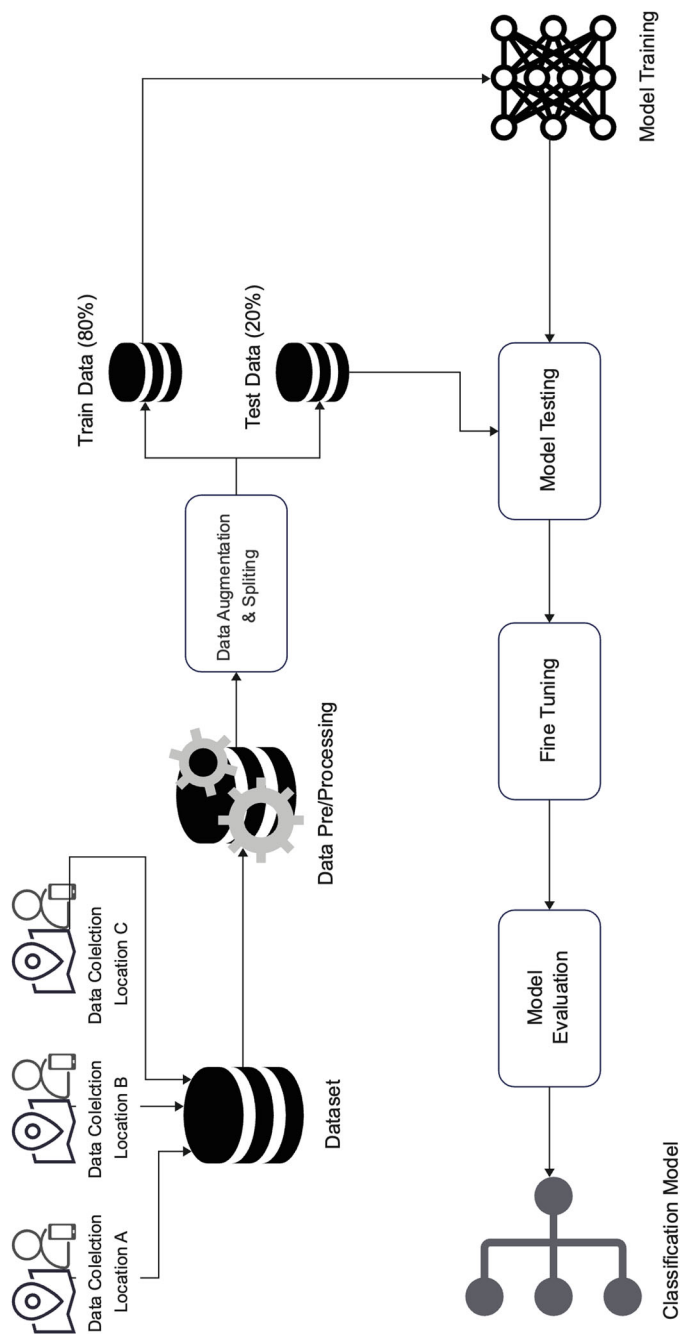


Fig. 2 Steps performed to conduct the proposed study

4 Results and Analysis

This section describes the experiments conducted and the results achieved using various machine learning algorithms.

4.1 *Model Initialization with Regularization*

Regularization parameters here, on the other hand, are used to initialize various machine learning models in order not to over fit. Overfitting happens when the model predicts OK on training data but bad on testing because it has too many brains to work. By adding constraints on the maximum depth and minimum samples per leaf, it regularizes the models to improve their ability in generalization. The models that we considered include Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM) and Gradient Boosting Classifier.

4.2 *Cross-Validation for Model Evaluation*

This allows a more robust assessment of model performance using cross-validation. Stratified K-Fold cross-validation, it performs k-fold by using the class distribution at overall dataset. This technique reduces the variance of a single trial of train/test split therefore we can get more accurate estimate over model performance. The training set is used to train the model, and each of these models generate predictions with a test set. These evaluation metrics are accuracy, precision, recall for both classes F1 score and cross validation accuracy. These metrics give an overall picture of how the model is doing, what it can do well and where does it fail. We also get a confusion matrix to see the performance of model across classes.

4.3 *Confusion Matrices*

Plotting confusion matrices for each model to give a better understanding of classification performance. We can utilize these matrices to understand the types of errors our model does, i.e. FALSE Positives and False Negatives which are lead us to potential mistakes in fine-tuning.

4.4 Model Performance Evaluation

In this section, we accessed the media performances of different machine learning models comparing with various metrics such as accuracy score, precision rate, recall(filtration)score and F1 (Mcculloch channel richardswagen spectrum) using K-cross validation (KTCV→Cross Validation Accuracy and Standard deviation). This is well-intentioned, as each model has its own strengths and weaknesses that bear discussion.

4.5 Logistic Regression

It is one of the classifiers we can use and it performs well (90% accuracy): Logistic Regression We got almost 90% precision and recall, which is balanced on all the classes. The cross-validation accuracy and the overall model performance are in line with one another; plus, a very low standard deviation indicates sturdy reliability of this model across multiple folds. Although the cross validation on it has an accuracy very near to test set, there is a small risk of overfitting.

4.6 Decision Tree

Decision Tree classifier has a huge accuracy of around 97% the precision, recall and F1 score are also high, indicating that it is able to correctly classify instances based on the actual classes. Cross-validation accuracy is slightly higher than the testing so it may likely to cause some overfitting. The standard deviation is low, but at the same time, it means that for different subsets of data model will perform consistently.

4.7 Random Forest

This Random Forest model almost perfectly by accuracy, precision, recall and F1 score are also 99.86% Test accuracy of test data and Cross validation Accuracy are consistent showing that the model is not overfitting i.e., model generalized itself on unseen Data And the cross-validation has a super low standard deviation, even more emanating to this model's compactness and reassurance (Fig. 3).

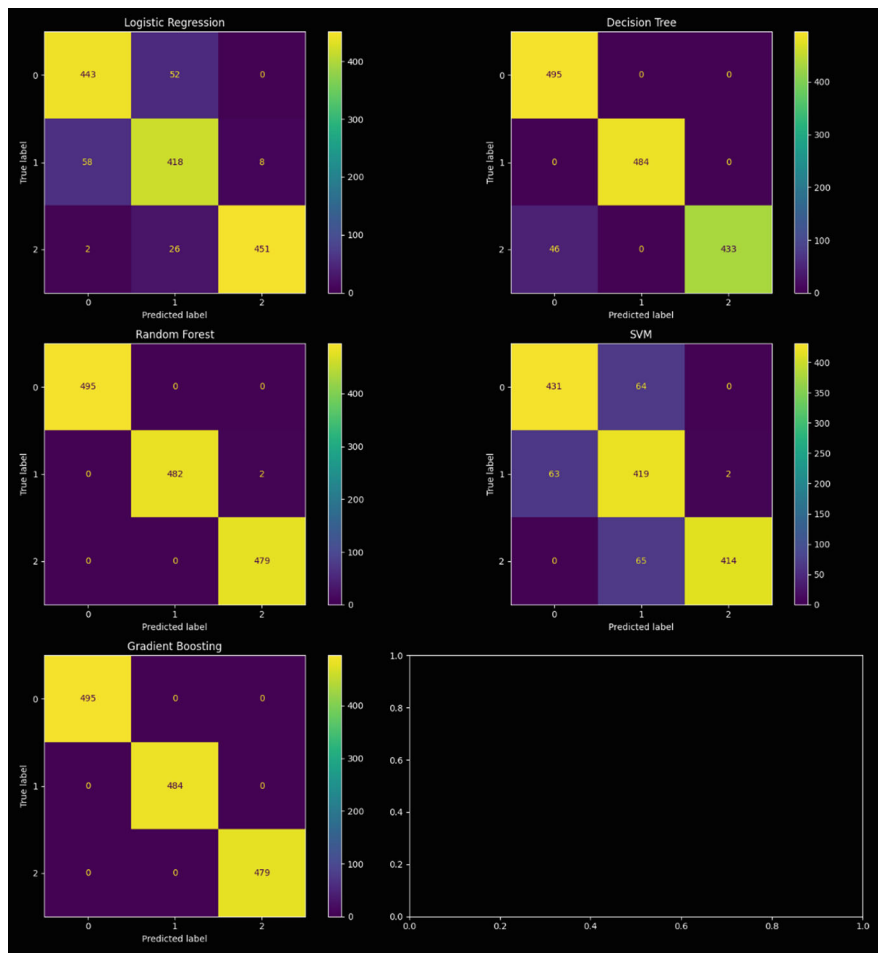


Fig. 3 Confusion matrix of proposed study

4.8 Support Vector Machine (SVM)

The performance of the SVM classifier is so-so, achieving an accuracy rate around 87%. It has a bit higher precision than the accuracy but same value with recall that means it makes not so much of false positive error and captures most of true positive errors. This is a terrible result since the cross-validation accuracy should be almost equal to the test accuracy and close values of standard deviation suggest we get also consistent performance through different data splits. This model is less likely to overfitting as compared to others (Table 1; Fig. 4).

Table 1 Results obtained using various ML models

Model	Precision	Recall	F1 Score	Accuracy	CV Accuracy	CV Std
LR	0.90	0.90	0.90	0.90	0.90	0.01
Decision tree	0.97	0.97	0.97	0.97	0.97	0.00
Random forest	1.00	1.00	1.00	1.00	1.00	0.00
SVM	0.88	0.87	0.87	0.87	0.86	0.00
GB	1.00	1.00	1.00	1.00	1.00	0.00



Fig. 4 Comparison of various ML models used in this study

4.9 Gradient Boosting

The Gradient boosting algorithm is used to handle the complex relationships existed in the food data and protect the model against overfitting. Utilizing this approach, we improve the predictive accuracy and computation time. This algorithm works perfectly on all metrics, which means it is doing an excellent job of fitting the training data. This may seem great, but optimal values are indicative of overfitting; this is when the model detects noise and only specific patterns in training data that do not generalize to new (unseen) data. But the cross-validation accuracy of exactly 1.0000 with a standard deviation of zero is very signal that we could have actually memorized our training data (which reinforces what I said at the start, too-large trees). CV Accuracy represents cross validation accuracy, while CV Std reflects cross validation standard deviation.

5 Conclusion

Performance evaluation of the different machine learning models shows a variety of outputs, suggesting that they may collectively possess differing strengths and weaknesses in their ability to predict food security. Logistic Regression displayed a fair performance with consistent results in cross-validation, which means that it is capable of generalizing well to new data. The Decision Tree model also had good performance, demonstrating its high accuracy and low variance pattern identification capabilities that were robust. Top performing Random Forest almost achieved perfect scores in all metrics, demonstrating a high capacity to capture data subtleties. Results of SVM were intermediate, with performance metrics lower than other models but being more stable across all folds may allow for additional tuning. Gradient Boosting offering 100% accuracy does flag an overfitting problem and further confirmed by the performance showing zero standard deviation in cross-validation thus a memorization of training data might have taken place. In all, Random Forest has the best generalization performance and decision tree is second; thirdly come logistic regression models provide a compromise between both.

References

1. Pinstrup-Andersen, P.: Food security: definition and measurement. *Food Sec.* **1**(1), pp. 5–7 (2009). <https://doi.org/10.1007/s12571-008-0002-y>
2. Prüss-Üstün, A., et al.: Burden of disease from inadequate water, sanitation and hygiene in low- and middle-income settings: a retrospective analysis of data from 145 countries. *Trop. Med. Int. Health* **19**(8), 894–905 (2014). <https://doi.org/10.1111/tmi.12329>
3. Jones, A.D., Ngure, F., Pelto, G.H., Young, S.L.: What are we assessing when we measure food security? A compendium and review of current metrics. *Adv. Nutr.* **4**(5), 481–505 (2013). <https://doi.org/10.3945/an.113.004119>
4. Pakistan, A.M.: An Automatic Determining Food Security Status: Machine Learning Based Analysis of Household Survey Data (2024)
5. Sarku, R., Lenfers, U.A., Clemen, T.: The Application of Artificial Intelligence Models for Food Security: A Review
6. Hawkesworth, S., et al.: Feeding the world healthily: the challenge of measuring the effects of agriculture on health. *Phil. Trans. R. Soc. B* **365**(1554), 3083–3097 (2010). <https://doi.org/10.1098/rstb.2010.0122>
7. Leroy, J.L., Ruel, M.T., Frongillo, E.A., Harris, J., Ballard, T.J.: Measuring the Food Access Dimension of Food Security (2015)
8. Carletto, C., Zezza, A., Banerjee, R.: Towards Better Measurement of Household Food Security: Harmonizing Indicators and the Role of Household Surveys
9. Gholami, S., et al.: Food Security Analysis and Forecasting: A Machine Learning Case Study in Southern Malawi
10. Arshi, O., Mondal, S.: Advancements in sensors and actuators technologies for smart cities: a comprehensive review. *Smart Constr. Sustain. Cities* **1**(1), 18 (2023)
11. Martini, G., et al.: Machine Learning can Guide Food Security Efforts When Primary Data are Not Available
12. Herteux, J., Räth, C., Baha, A., Martini, G., Piovani, D.: Forecasting Trends in Food Security: A Reservoir Computing Approach

13. Bakhtsiyarava, M., Williams, T., Verdin, A., Guikema, S.D.: A Nonparametric Analysis of Household-Level Food Insecurity and its Determinant Factors: Exploratory Study in Ethiopia and Nigeria
14. Olshen, R.: A conversaton with Leo Breiman. *Stat. Sci.* **16**(2), 184–198 (2001)
15. Breiman, L.: Random forests. *Mach. Learn.* **45**, 5–32 (2001)
16. Sajja, G.S.: Machine Learning Based Detection of Depression and Anxiety (2021)
17. Liu, Y., Wang, Y., Zhang, J.: New Machine Learning Algorithm: Random Forest
18. Narassiguin, A., Bibimoune, M., Elghazel, H., Aussem, A.: An Extensive Empirical Comparison of Ensemble Learning Methods for Binary Classification
19. Chawla, N.: C4.5 and Imbalanced Data sets: Investigating the eect of Sampling Method, Probabilistic Estimate, and Decision Tree Structure
20. Arshi, O., Chaudhary, A.: Intelligence (AGI). *Artif. Gen. Intell. (AGI) Secur.: Smart Appl. Sustain. Technol.* **1** (1990)
21. Upton, J., Cissé, J.D., Barrett, C.: Food security as resilience: reconciling definition and measurement. *Agric. Econ.* **47**(S1), 135–147 (2016). <https://doi.org/10.1111/agec.12305>
22. Barrett, C.: Measuring food insecurity. *Am. Assoc. Adv. Sci.* **327**(5967), 825–828 (2010). <https://doi.org/10.1126/science.1182768>
23. Ngure, F., Reid, B.M., Humphrey, J.H., Mbuya, M., Pelto, G.H., Stoltzfus, R.J.: Water, sanitation, and hygiene (WASH), environmental enteropathy, nutrition, and early child development: making the links. *Ann. N. Y. Acad. Sci.* **1308**(1), 118–128 (2014). <https://doi.org/10.1111/nyas.12330>
24. Gholami, S., Knippenberg, E., Campbell, J., Andriantsimba, D., Kamle, A., Parthasarathy, P., Sankar, R., Birge, C., Ferres, J.L.: Food security analysis and forecasting: a machine learning case study in southern Malawi. *Data Policy* (2022)
25. Zezza, A., Tasciotti, L.: Urban agriculture, poverty, and food security: empirical evidence from a sample of developing countries. *Food Policy* **35**(4), 265–273 (2010). <https://doi.org/10.1016/j.foodpol.2010.04.007>
26. Storm, H., Baylis, K., Heckelei, T.: Machine learning in agricultural and applied economics. *Eur. Rev. Agric. Econ.* **47**(3), 849–892 (2019). <https://doi.org/10.1093/erae/jbz033>
27. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: *Perspectives on Ethical Hacking and Penetration Testing*, pp. 382–412. IGI Global (2023)
28. Clément, F., et al.: From Women's Empowerment to Food Security: Revisiting Global Discourses Through a Cross-Country Analysis

Exploring the Secure Unleashing of Digital Potential: A Study on How Cloud Security Works Together with Digital Transformation in Financial Institutions of Pakistan



Khurram Shoaib

Abstract The way financial institutions in Pakistan are changing significantly because of digital transformation. Customers want more convenient ways to do banking, therefore, banks are trying hard to keep up. They are using the Internet and new technology to reach more customers and compete better globally. One big thing they are thinking about is keeping all this digital stuff safe and secure. This study examines how this safety (cloud security) and all the new digital transformations in Pakistani banks are connected. The main goal is to ask the right questions to understand this connection better. The summary briefly examines what is happening in these financial institutions—what they are doing, what tech they are using, and what problems they face. It also talks about the regulations for using the Internet in banking and the issues banks face because of these regulations. It shows how all this new tech is changing how banks work and how they must adapt to keep up.

Keywords Digital transformation · Cloud security · Synergy · Financial institutions · Pakistan · Financial inclusion · Customer experience · Operational efficiency · Regulatory environment · Cultural transformation · Emerging technologies

1 Introduction

Pakistan's financial world is changing a lot. It uses new technology and focuses a lot on what customers want. This is not a short-term change; it is essential for several reasons. More and more people in Pakistan are using technology for their financial stuff. They want easy ways to use banks on their phones, pay online, and get a robo-advisor. About 70% of people in Pakistan use smartphones for financial reasons,

K. Shoaib (✉)

Avionics Engineering Department, Air University, Islamabad, Pakistan

e-mail: 232889@students.au.edu.pk

showing they want more accessible ways to handle their cash [1]. A 2020 World Bank report [2] estimates that 54% of adults in Pakistan do not have bank accounts, but digital tech might help. Using phones and the Internet can make it cheaper and easier to help these people with their money. Studies show that using phones for banking has helped people in rural areas [3]. Pakistan wants to be better at providing financial services than other countries. Using digital technologies helps them make better products, work faster, and provide cost-effective services. According to a study by the International Monetary Fund (IMF) [4], these digital technologies can improve the financial world and help Pakistan compete with other countries. As Pakistan's financial institutions use digital technology [5], they will start using the cloud [6]. However, it is essential to keep all that information secure. Making sure cloud security is like building a solid base for an excellent digital future [7]. Using the cloud helps financial institutions change things quickly when they need to. This means that they can make new digital services faster and easier.

The cloud does not need expensive machines or software. It means that Pakistan's financial institutions can spend that money on making things better instead. With the cloud, people can work together even if they are far apart. It can make things work smoother and help them make decisions faster. The cloud comes with excellent security features. It protects from cyberattacks and data breaches. However, there are some things to think about. Financial institutions worry about data privacy, following regulatory compliance, and staying safe online. So, Pakistan's financial institutions need to be careful. They should plan to minimize security risks while using the cloud [8]. Pakistan's financial landscape is changing because of digital transformation and the need for robust information security. This research wants to find out more about how these things are connected. We want answers to several key research questions. Does making cloud security help Pakistan's financial institution's efficiency in digital transformation and cost-effectiveness? How does keeping critical sensitive data safe in the cloud help while they are trying new things with the digital journey? How do people, culture, and change management affect the adoption and success of cloud-based information security in digital transformation? What regulatory considerations and compliance must they follow when using the cloud? How can they make a supportive regulatory environment that helps them use the cloud better? What is Special About Pakistan? What is different in Pakistan that makes using the cloud for digital services different? We hope to help Pakistan's financial landscape stay safe and improve by finding answers to these questions. This research wants to help everyone use technology better and make digital services safer in Pakistan.

2 The Pakistani Financial Landscape and Digital Transformation

Financial institutions in Pakistan are changing a lot because of digital transformation and customer demand for digital convenience. This part will look at how things are right now with this change, checking out what customers are doing, what new technology is being used, and what problems they are facing. Since 2019, there has been a plan to get more people involved with banking using phones, gents, and digital money. Some cool things happening are: Raast is the first fast way to move money between banks instantly [9]. Roshan Digital Account makes it easier for Pakistanis living abroad to use banks in Pakistan [10]. Digital Banks' new regulations encourage new banks that work only online [11]. Many people use apps like Easypaisa and JazzCash to do digital banking [12]. New companies are changing how loans work using technology, especially for people who usually cannot get loans [13]. Similarly, fingerprints and faces are used to ensure it is you when you pay or log in using your fingerprint or face [14]. The State Bank of Pakistan is pushing banks to share info safely to make new and better banking using open banking [9].

Some adapted technologies are also happening, like cloud computing; banks are using services on the Internet more because they are flexible and do not cost as much. They use these services for central banking and new digital initiatives. Banks are starting to use Artificial Intelligence [10] (AI)-powered that can learn and act like they are smart. They suit fraud detection, customer service chatbots, and personalized financial recommendations. A new kind of blockchain [11] technology is showing up, but it is still early. It can make sure payments move safely, and people can see what is happening, especially when sending cross-border remittance services. Similarly, some of the existing challenges are cybersecurity threats. Since everything is online now, banks can be attacked more by hackers. They need to make sure everything is super safe. Digital Divide: Some people do not have the same cool tech as others, therefore, they cannot do the same things with their money. We need to make sure everyone can join in. Regulatory Uncertainty: It is hard for banks because the rules about using the Internet and new tech keep changing. They have to keep up.

Knowing about all these ongoing initiatives and the existing challenges helps us understand how safe and long-lasting the new way of doing financial services in Pakistan can be. Studying how all these things work together gives us good ideas about the future of money technology in the country. Cloud security and digital transformation in Pakistani banks happen while dealing with flexible regulations. Using the cloud has good points, but dealing with these regulations makes it challenging for the banks. One extensive regulation is the Pakistan Cloud First Policy, started in 2022 by the Ministry of Information Technology and Telecommunication [15]. This regulation says the government should use the cloud more and use local cloud service providers. However, it raises concerns about where data should be. Currently, the regulation allows some data outside Pakistan under certain conditions. Nevertheless, it must be clarified, making it challenging for banks, mainly if they handle sensitive customer information [16].

The confusion is due to two different regulatory bodies, the Security and Exchange Commission of Pakistan and the State Bank of Pakistan, which have two different regulations for adoption [6, 17]. This confusion makes it challenging for financial institutions to understand and seek to leverage the cloud securely. Moreover, Pakistan still needs robust cybersecurity regulations. There is a plan to create regulations for the data protection of critical online information, which is still in progress. Without clear and robust regulations, financial institutions face significant risks like data breaches and not complying with international standards. These regulations have positive and negative aspects for financial institutions wishing to adopt the cloud for their digital transformation. Such a kind of harmonization can lead to clarity and consistency for financial institutions, making it challenging to establish requirements for secure cloud adoption. The changes happening in Pakistani banks and financial companies because of technology are about more than just using new tools. They are also a significant change in how these organizations think and how flexible they are. This part of the study looks closely at this change, seeing how it affects how these companies work inside and how important it is to be able to change and plan well.

In Pakistan, many traditional financial companies have strict structures that do not match the fast changes in digital technology. To succeed, they must encourage flexibility, quick decision-making, and a willingness to try new things. One of the studies shows that for financial companies to do well in the digital age, they must move away from working alone and start working together in teams that can quickly respond to what is happening in the market. However, it takes much work to move through these changes in culture. The strong beliefs and usual ways of doing things in Pakistani financial organizations make it tough to make changes. Another research shows that knowing little about digital tech and worrying about job safety are big reasons it is hard. To make it easier, it is essential to talk openly, provide training, and give rewards to encourage people to join in digital projects. To successfully navigate this cultural shift, it is crucial to have robust plans in place for managing change. Stress the importance of effective communication, involving everyone affected, and getting leaders on board. It helps guide employees as the company moves through this transition. Creating a clear digital plan, celebrating early successes, and providing ongoing support can help people adjust and encourage a culture about learning and developing new ideas.

Ensuring security in the cloud and digital changes work smoothly in Pakistani financial institutions means understanding how these things affect how the organization works and can adapt. These institutions can make the most of this digital shift by accepting the need to adapt culturally and using innovative strategies to manage changes. This sets them up for a future where they can do well in a safe and adaptable environment. To help Pakistani financial institutions make the most of digital opportunities, it is important to be flexible and open to growth. While some might think strict rules are best for keeping information safe in the cloud, research shows that good cloud security can help institutions adapt and grow digitally. Before, banks in Pakistan used to set up infrastructure on their premises. Now, they use cloud-based deployment to do this, which enables financial institutions to make it faster and safer.

This helps them make new financial solutions and digital products faster and match customers' wants.

Digital Transformation thrives on dynamic growth. The cloud security solution allows financial institutions to keep using digital services, whether it is a peak season for remittances or a sudden jump in customers using their phones for banking. The cloud system can quickly grow to handle more work, ensuring everything runs smoothly and safely. Some banks in Pakistan credited their ability to deal with a significant rise in transactions during Ramadan [18] to how well their cloud system could grow and stay secure. In simpler terms, Secure cloud solutions help Pakistani financial institutions work better. They make things faster and more secure, like managing who gets access to what. It frees up significant tech resources for more important things. Using cloud tools helps teams work together better, making projects more efficient. For example, Deutsche Bank uses Cloud Composer for Workload Automation to shift its workload to the secure cloud [19].

This study shows the importance of cloud security when businesses change to transformative power. The goal is to learn more about this by studying more cases and talking to important people in Pakistani financial institutions. It will help us understand how cloud security helps businesses grow and work better in the future. As financial institutions in Pakistan start using cloud technology, keeping information safe and protecting important data become important. This part talks about how keeping the cloud secure is crucial for keeping valuable financial information safe in today's ever-changing digital world. Cloud security helps control who can see important information, ensuring only the right people get in. Using more than one way to prove who you are and managing who gets access makes it even safer. Encrypting data with special codes makes it hard for others to read it, even if they try to break in. In Pakistan, banks use strong codes like AES-256 and TLS 1.3 to protect data in transit and rest. Cloud security systems can find and stop problems immediately and they do not become significant issues. Doing things like checking for problems often and planning for when things go wrong makes things safer.

Banks in Pakistan need to follow certain regulations to keep data safe, like the Personal Data Protection Bill 2021 [20] and the Banking Regulations 2015 [21]. Making sure the security they use fits these regulations makes things safer. Making sure everyone knows how to keep things safe is important. Teaching everyone about cloud security and how to spot tricks and mistakes such as strong passwords and phishing detection techniques to minimize human error. Sometimes, banks get help from other companies. Being careful about who they pick and having a strong framework for data governance makes things safe, even when others are involved. By doing these things well, banks in Pakistan can use the Internet for money while keeping things safe for customers. In today's world, customers need to trust banks ubiquitously. Using the Internet safely helps banks use new things and makes people trust them more. This part discusses how being safe online helps banks and customers be satisfied. Banks use special ways to keep data safe, showing customers they are careful with their information. Using safe ways to talk to customers makes them feel good and helps everyone work together better. Having internet stuff that always works makes customers feel like they can use their bank without problems. When banks

prioritize safety measures effectively, more individuals favor them, improving their standing compared to their counterparts. It boosts their strength and popularity. When users have faith in their bank, they feel happier and spread positive word-of-mouth. It boosts the bank's growth and keeps customers satisfied.

Safe online banking brings improved and innovative customer services, making them more inclined to remain loyal to their bank. When banks are secure on the Internet, people trust them more, which leads to happier customers. It benefits everyone involved. There is a big challenge in Pakistan's financial institutions. They are trying to make their online information safe while changing how they use technology. It is imperative to have smart people who know much about technology and can deal with new ways of keeping things safe online. However, there are not enough of these skilled people, and that makes it hard to keep making progress online that is both safe and long-lasting. Research shows that important areas of cloud security [22], like protecting data with encryption, managing identities and access, and responding to incidents, are not well-covered in Pakistani financial institutions. It lack of attention leaves sensitive information at risk, making it harder to deal with potential dangers effectively. Besides being skilled with technology, not fully grasping how to use digital transformation techniques and frameworks for managing change can stop the smooth incorporation of security solutions in the cloud. Workers might struggle to adjust to new ways of working and security rules, creating differences and weaknesses that might be taken advantage of [22]. The changing regulations about using cloud services in Pakistan are getting more complicated. Not fully understanding what regulations to follow and the best ways to do things right might cause banks and money-related companies to face problems with the law and financial issues. To bridge the difference in abilities and make certain that the shift to digital technology happens safely, it is imperative to have specific training and programs designed to improve those skills. Provide employees with the necessary knowledge about keeping information safe in cloud systems. It includes teaching them about protecting data, identifying potential dangers, responding to problems when they occur, and controlling access to cloud services. Teaching should cover ways to change how things are done using technology, ways to communicate these changes effectively, and methods to adapt. It helps workers feel confident using new computer systems and working methods without trouble. Consistent learning about the changing rules related to using cloud technology in Pakistan can help ensure that you follow the laws and reduce the chances of facing legal problems. By putting resources into thorough training programs, it is possible to fill the gaps in skills and build a culture in Pakistani financial institutions where people are more aware of cybersecurity. It helps in taking a careful approach to managing risks before they happen and creates a team that is good at protecting important information while improving secure digital changes [23].

In Pakistani financial institutions, making their digital systems more secure and moving towards using cloud technology involves two main things: using new technology and changing how people work together. It looks at the problems they face in getting everyone to adjust to these big changes in how they do things. It talks about how some people might not want to change and how to manage those challenges to

make the changes work smoothly. Traditional banks and similar companies usually have setups with clear levels of authority; they tend to avoid taking big risks and follow strict ways of doing things. Nevertheless, to start using cloud security and modern digital changes, they must start being more flexible, trying new things, and handling risks better. It clashes with how things have always been done, making some people not want to change. Introducing fresh ways to keep information safe in the cloud and adjusting how tasks are done needs people who know much about it. However, in Pakistani financial groups, insufficient folks with these skills make it hard. It lack of skills makes the workers worried and not open to these changes. Good communication is essential when things are changing. If we do not talk enough about why it is good to use cloud security and digital transformation, people might get scared, not trust it, and not want to do it. Leadership and Advocacy: Strong leaders who strongly support and speak up for change are significant. When these leaders are completely committed and clearly explain their vision, it can inspire and encourage employees. It can help overcome any opposition or reluctance to the change. Having clear ways to talk openly is super important. It helps sort out worries, inform everyone regularly, and ensure employees feel involved. Doing things like workshops where people can participate, training sessions, and ways for feedback can make this even better. Ensuring employees have the right training for working in the new cloud-based system is important. Learning how to use it properly helps fill any gaps in their skills, makes them feel more sure about what they are doing, and reduces any pushback or hesitation they might have about using the new system.

Recognizing and giving credit to workers who are open to change and who play an active role in making changes happen can inspire them and encourage the use of cloud security and digital methods. Understanding the beliefs and norms that already exist in a culture and adjusting how you manage change to fit those values is important for doing well in Pakistan. By focusing on what the culture already does well and dealing with any worries people might have using methods that make sense in that culture, you can make it easier for people to accept and be open to changes. To make the most of cloud security and digital changes, banks in Pakistan need to understand how people might struggle to adapt to new ways and find ways to manage these challenges well. It is not just about using new technology; it is about understanding how people might feel about it and ensuring the change happens smoothly. Pakistan's financial sector has many opportunities to improve cloud security and adapt to digital transformation. However, complicated regulations and issues create difficulties. It is crucial to comprehend and solve these problems to ensure financial companies can safely utilize digital tools. In Pakistan, the use of cloud technology is relatively fresh, and there is uncertainty surrounding the specific guidelines for ensuring its security, especially for banks and financial businesses. It makes banks worry about using cloud systems because they are unsure how safe their data will be or what they should do legally. Since there is no specific law just for cloud safety, people interpret the rules differently, making it hard to manage and follow risks properly.

Even when banks have rules to follow, it is hard and costly to comply with them all. They face difficulties with various data security laws, creating data breach strategies, and staying updated with international standards such as GDPR and CSA STAR.

Also, because technology changes fast and new cyber problems pop up, the old rules might not work well anymore, making it even harder to follow them. Here are some ideas to improve things: we need better rules that say how banks should keep data safe in the cloud. People from the government, experts, and banks should work together to make rules that work for everyone. Pakistan must align its cloud safety regulations with international standards such as GDPR and CSA STAR. This alignment will simplify the adherence to rules for local banks and enable smoother business interactions with other nations. Banks require education and tools to secure their information in the cloud. They must understand the most effective methods to comply with regulations and tackle emerging cybersecurity issues. In addition, it is important to encourage banks to develop new, safe ways to use the cloud. It helps them make their solutions that work well for Pakistan. If Pakistan deals with these problems, it can fully use cloud security and digital changes in finance. It keeps things safe and makes the financial system better and faster.

3 Future Directions

We looked into how Pakistani banks and financial companies use technology to keep information safe and improve their services. We found that cloud systems store data online and can make things faster and cheaper for these institutions. It also helps them adjust to what customers need more easily. Using cloud security makes digital changes faster and more efficient for financial institutions in Pakistan. Those using cloud-based systems found they could bring things to the market quicker, make their work smoother, and save money. It matches what others have found in their research. Although people worry about data safety, our study found that cloud security helps lower the risks and keeps important information safe in Pakistani financial institutions. Other research also supports this idea. However, having good rules about data and ensuring employees know how to keep it safe is still important. How people in a company think and manage changes was a big deal in our research. Companies with open communication and good training made switching to new security methods easier. It matches what others have seen. Ensuring people trust and accept new security rules is important for success. Our study shows that Pakistan needs better rules that can change and support cloud systems. Others have also seen this problem. It is important for policymakers to ensure a good balance between improving things and keeping them safe. Making it easier for companies to follow the rules and work together can make digital finance in Pakistan safer and better. We found some special things about the financial sector in Pakistan. More people are using mobile banking and are good with technology, which is good for using cloud systems. However, there are problems like not having enough infrastructure and not having enough people who know about cybersecurity. Fixing these problems is key to making the most out of cloud security and digital changes for financial institutions in Pakistan. In short, our study shows how important it is for Pakistani financial institutions to mix cloud security with digital changes. If they handle the challenges

and use the chances well, they can make a safe and successful journey into the digital world, making finance better for the country. This initial study looked at how cloud security and digital changes connect banks in Pakistan. Nevertheless, it is important to recognize its limits and encourage more research. We talked to only a few people and found that it might not be applied in Pakistani banking.

In addition, because our information is based on opinions, it might be tricky for others to understand or copy. Still, our study sets a base for future research and real-world use. We need to dig deeper into some areas, like how good security in the cloud affects how fast and well digital changes happen in different projects. Also, studying how a company's culture and setup affect its choice to use cloud security could give us helpful ideas for making changes. Also, our findings make us wonder about the rules for using the cloud in Pakistan. In the future, we could investigate changing these rules and finding the best ways to make rules that support new ideas while keeping data safe. Comparing Pakistan with other new markets could also show us what challenges and chances are unique to Pakistan's digital changes. This study is just a start. By knowing its limits and looking more into the areas we found, we can understand better how cloud security and digital changes work together in banks in Pakistan. It could help these banks grow safely and help everyone learn how to use new tech responsibly in places where it is just starting to be a big deal. As we understand more about how keeping data safe in the cloud helps with digital changes, it is important to give banks in Pakistan the right tools to handle this change well. From what we learned, here are some things to do: Embrace Cloud Security as a Transformation Enabler, see cloud security as a key part of moving forward digitally, get strong security that fits your specific cloud and data needs. Integrate security throughout the process, think about security at every step of digital changes—planning, making, starting, and keeping things going. In addition, leverage cloud-native security services and use the safety things that come with cloud services, such as making data secret, controlling who gets in, and discovering possible threats. Give your staff skills to find and stop online dangers. Keep teaching about staying safe online. Make a place where workers feel okay telling if something seems wrong online. Make clear ways to report problems and solve them fast. Make sure bosses understand how important security is for digital changes and support keeping things safe. Work with people who make rules to make clear and fair rules for using the cloud and keeping data safe in Pakistan. Do good programs that follow the rules and best ways of doing things in your field. Engage in open dialogue with regulators, be a part of talks about rules, share what you have learned about cloud security, and help make better rules. Utilize cloud security to build trust and confidence: Demonstrate dedication to protecting data and privacy to stand out in the digital market. Develop innovative security-driven products and services, use cloud security to develop safe and user-friendly financial technology products. Optimize operation for efficiency and agility, use scalable cloud security solutions to streamline work, cut costs, and enter the market faster. By following these suggestions and smartly using cloud security and digital changes, financial groups in Pakistan can unlock their full digital potential. It is important to remember that success in the digital world is not just about

technology. It also needs ongoing learning, adapting to new cultures, and working with others.

4 Conclusion

This report offers a perceptive analysis of how cloud security and digital transformation interact with Pakistani financial institutions. It emphasizes how utilizing cloud security may boost financial services innovation, facilitate quicker market entry, and greatly improve operational efficiency. But the study also emphasizes the difficulties caused by unclear regulations and the requirement for strong cybersecurity defenses. It is imperative that Pakistani financial institutions embrace a holistic strategy to cloud security and integrate it into all aspects of their digital transformation activities in order to fully grasp the promise of cloud-based technologies. This entails adopting cloud-native security services, educating personnel on cybersecurity best practices on a regular basis, and cultivating a transparent and quick-to-resolve culture. Additionally, the report recommends that in order to promote easier compliance and cross-border cooperation, legislators should create clear, flexible legislation that comply with global standards like GDPR and CSA STAR. Pakistani financial institutions can more successfully use cloud security to propel their digital transformation and ensure a safe and robust financial environment by tackling these legislative and instructional obstacles. As a result, even though this research establishes a basic understanding of the role that cloud security plays in digital transformation, it also highlights the need for more research into particular areas, like the influence of corporate culture on the adoption of cloud security and the creation of customized regulatory frameworks. Further research contrasting Pakistan with other developing markets may shed further light on the particular advantages and difficulties that the nation faces in its digital journey.

References

1. McKinsey & Company: Mobile Money in Pakistan, A Story of Growth and Inclusion [Online]. Available: <https://www.mckinsey.com/industries/financial-services/our-insights/mobile-money-in-emerging-markets-the-business-case-for-financial-inclusion>. Accessed 12 Aug 2023
2. World Bank: Financial Inclusion in Pakistan: A Landscape Assessment [Online]. Available: <https://datatopics.worldbank.org/financialinclusion/country/pakistan>. Accessed 13 Aug 2023
3. World Bank & Pakistan Microfinance Network: The Impact of Mobile Banking on Financial Inclusion in Pakistan. Accessed 13 Aug 2023
4. International Monetary Fund: Digital Technologies and the Financial Sector: A Survey [Online]. Available: <https://www.imf.org/en/Home>. Accessed 20 Aug 2023
5. State Bank of Pakistan: Digital Banking in Pakistan [Online]. Available: <https://www.sbp.org.pk/dfs/Digital-Bank-Regulatory.html>. Accessed 3 Sept 2023

6. State Bank of Pakistan. Framework on Outsourcing to Cloud Service Providers [Online]. Available: <https://www.sbp.org.pk/bprd/2023/C1.htm>. Accessed 3 Sept 2023
7. Cheng, M., Qu, Y., Jiang, C., Zhao, C.: Is cloud computing the digital solution to the future of banking? *J. Financ. Stab.* **63**(C) (2022)
8. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: *Perspectives on Ethical Hacking and Penetration Testing*, pp. 382–412. IGI Global (2023)
9. Humayun, M., Tariq, N., Alfayad, M., Zakwan, M., Alwakid, G., Assiri, M.: Securing the internet of things in artificial intelligence era: a comprehensive survey. *IEEE* (2024)
10. Anwar, M., Tariq, N., Ashraf, M., Moqurrab, S.A., Alabdullah, B., Alsagri, H.S., Almjally, A.: BBAD: BLOCKCHAIN-backed assault detection for cyber physical systems. *IEEE* (2024)
11. Measures to Enhance Security of Digital Banking Products and Services, PSD Circular No. 05 of 2020
12. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endorsed Trans. Internet Things* **9**(4), e1–e1 (2023)
13. Business Recorder: JazzCash Surpasses Easypaisa to Lead the Mobile Money Market. Accessed 03 Dec 2023
14. Digital Payment Services to Unauthorized Digital Lending Apps, PSP&OD Circular No 02 of 2023
15. Measures to Enhance Security of Digital Banking Products and Services, BPRD Circular No. 04 of 2023
16. Arshi, O., Rai, A., Gupta, G., Pandey, J.K., Mondal, S.: IoT in energy: a comprehensive review of technologies, applications, and future directions. *Peer-To-Peer Netw. Appl.* 1–40 (2024)
17. DataGuidance, Pakistan: Regulating the Cloud. <https://www.dataguidance.com/opinion/pakistan-regulating-cloud>. Accessed 05 Dec 2023
18. Securities and Exchange Commission of Pakistan: Draft Cloud Adoption Guidelines for Incorporated Companies. SECP (2023)
19. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
20. Google Cloud, Deutsche Bank Uses Cloud Composer for Workload Automation. <https://cloud.google.com/blog/products/data-analytics/deutsche-bank-uses-cloud-composer-workload-automation>. Accessed 23 Dec 2023
21. Tariq, N., Alsirhani, A., Humayun, M., Alserhani, F., Shaheen, M.: A fog-edge-enabled intrusion detection system for smart grids. *J. Cloud Comput.* **13**(1), 43 (2024)
22. Arshi, O., Chaudhary, A.: Intelligence (AGI). In: *Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies*, p. 1 (1990)
23. AIM Consulting: Cloud computing risks and barriers in financial services and banking: how to overcome them. AIM Consulting (2021)

Reviewing Theoretical Perspectives on IT Governance and Compliance in Banking: Insights from US Regulatory Frameworks



Muhammad Nauman Zakki, Nimra Iftikhar, Saim Saif Ullah Khan, Farhood Nishat, and Oroos Arshi

Abstract Financial institutions need robust IT governance to comply with rules, manage risks, and preserve operational integrity. This review paper aims to examine how technology affects compliance strategies, IT governance best practices, and US bank compliance. This study stresses strong frameworks like COSO and COBIT and synthesizes existing research and case studies to better align regulatory needs with theory. Research analyzes blockchain and AI's impact on auditing, risk management, and internal controls. Results demonstrate RegTech's adaptability and compliance simplification. Limitations and future possibilities enlighten global financial market longitudinal research and comparisons. This evaluation advises stakeholders on improving IT governance frameworks to mitigate digital banking risks, comply with legislation, and employ technology.

Keywords IT governance · Compliance · Banking sector · Regulatory environment · Cybersecurity · Emerging technologies

1 Introduction

Research shows that “IT governance” in the banking business is the processes and rules that assist a corporation achieve its IT goals [1]. When a bank operates, compliance implies following all rules, regulations, standards, and requirements [2]. Financial institutions must manage IT governance and compliance to protect client data, prevent cybercrime, and reduce operational risks.

M. N. Zakki · N. Iftikhar · S. S. U. Khan · F. Nishat (✉)

Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan
e-mail: farhoodnishat@hotmail.com

O. Arshi

Department of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India

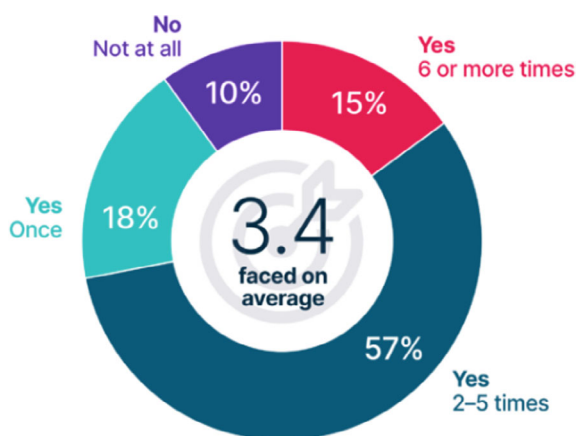
Responsible resource use, risk management, and IT expenditure value creation are excellent IT governance [3]. To ensure market integrity, consumer protection, and economic stability, banks must follow all regulations. The FDIC, Fed, and OCC implement these rules [3]. Investor confidence, financial crime prevention, and brand protection need compliance. Research shows 94% of banking CEOs value regulatory compliance [4].

US regulations impact banking IT governance. The 2002 Sarbanes–Oxley Act (SOX) heavily restricted financial reporting and internal controls, influencing IT governance [5]. GLBA mandates rigorous IT security to protect customer data [5]. The 2010 Dodd–Frank Wall Street Reform and Consumer Protection Act lowered systemic risk and enhanced market transparency, influencing IT governance [6]. FFIEC cybersecurity and IT examination guidelines outline bank IT governance norms [6]. The frameworks guarantee banks follow laws and principles, have appropriate IT governance, and manage risks. These frameworks have affected risk management at over 80% of US banks, according to the 2021 FFIEC report [7].

IT governance and compliance in banking are important yet difficult. The inadequacy of regulatory frameworks to keep up with rapid technological advancement is concerning. Banks face increased risks owing to compliance and governance shortcomings [8]. Cybersecurity is another issue. According to research survey, financial services companies employees says they are several times more likely to be hacked as shown in Fig. 1 [9]. Meeting regulatory criteria is another challenge. Complying with regional, federal, and international regulations is difficult and costly for banks. As regulations like the General Data Protection Regulation (GDPR) change, data privacy and protection become increasingly difficult. Strong IT governance frameworks are needed to address these challenges and comply with legislation.

This Review paper examines theoretical banking IT governance and compliance perspectives, notably in US regulatory frameworks. The paper includes theoretical foundations, US law, banking IT governance rules, compliance techniques, and best

Fig. 1 Financial companies that reported an attack [9]



practices. Mastering IT governance and compliance helps banks increase operational integrity and competitiveness.

2 Theoretical Frameworks of IT Governance and Compliance

2.1 *Key Concepts and Definitions*

The term “IT governance” refers to a subset of “corporate governance” that focuses on the management and use of information technology in order to accomplish organizational objectives [10]. It includes all the rules, regulations, and procedures that make sure IT systems are safe, efficient, and useful for the company.

- (a) **Compliance:** Adherence to rules, regulations, standards, and internal policies regulating the usage of IT inside the business is what is meant by “compliance” in the context of IT governance. For information technology (IT) operations to be compliant, they must adhere to all applicable regulations and safeguard sensitive information [11].
- (b) **Regulatory Frameworks:** Governmental and international agencies provide legal and formal guidelines for managing information technology resources [12]. This is particularly true in banking. Researchers claim these frameworks safeguard customers, stabilize the financial system, and encourage honest and transparent banking [12, 13].
- (c) **Risk Management in IT Governance:** IT governance risk management involves identifying, assessing, and mitigating potential threats to IT systems and data [14]. It seeks data security, customer privacy, and business continuity [14].

2.2 *Theoretical Models Security*

Different theoretical frameworks regulate information technology (IT) governance and compliance, managing and regulating IT resources to meet business and legal goals.

- (a) ISACA developed COBIT, a comprehensive corporate IT management framework [15]. It delivers IT management principles and best practices to accomplish corporate goals, generate value, and manage risks.
- (b) The Information Technology Infrastructure Library (ITIL) is a set of processes for IT service management (ITSM) that aligns IT services with organizational needs. A number of studies [16–18] have covered this topic.
- (c) Information security management systems (ISMSs) are defined by international standards such as ISO/IEC 27001, which details how to create one, as well as

- how to keep it up-to-date and secure. It offers a methodical strategy for safely handling confidential business data [19].
- (d) While the COSO framework is not IT-specific, it is essential for risk management and internal controls; it lays the groundwork for compliance, ethical financial reporting, and operational goals that include IT [20].

3 US Regulatory Frameworks

US regulations shape financial organizations’ IT governance and compliance. Banks must observe tight cybersecurity, risk management, data protection, and financial reporting standards. FFIEC, Dodd–Frank, and Gramm–Leach–Bliley Act standards are crucial [21]. Banks must follow each framework’s requirements and directives to maintain operational integrity and stakeholder interests.

3.1 Sarbanes–Oxley Act (SOX)

After major financial scandals, the Sarbanes–Oxley Act of 2002 was created to promote company governance and investor confidence [22]. It contains following steps as shown in Fig. 2. SOX’s internal controls and financial reporting rules greatly impact banking IT governance. Senior executives must attest to the accuracy of financial reports and the efficacy of internal controls, report on the sufficiency of internal controls over financial reporting, and disclose significant changes in financial circumstances or operations in real time under SOX sections 302, 404, and 409 [22]. SOX greatly impacts IT governance. Strong IT systems enable banks’ internal controls and accurate financial reporting. Data integrity, access, and audit trails should be controlled in IT governance frameworks. SOX compliance increases transparency and accountability, reducing financial fraud [23]. Banks need regular monitoring and reporting systems to rectify discrepancies.



Fig. 2 Sarbanes–Oxley Act (SOX) [22]

3.2 *Gramm–Leach–Bliley Act (GLBA)*

The 1999 Gramm–Leach–Bliley Act protects banks' and other financial institutions' customers' private financial data. Due to its severe privacy and security standards, GLBA affects IT governance [24]. The Financial Privacy Rule requires financial institutions to inform customers of their right to opt out of certain information-sharing practices; the Safeguards Rule requires security programs to protect consumer information; and the Pretexting Provisions prohibit obtaining customer information under pretenses [24]. IT governance is greatly affected by GLBA. Financial organizations need robust data protection policies and practices to fulfil GLBA regulations [25]. Any IT governance system should include data encryption, access control, and incident response processes. GLBA compliance reduces data breaches and boosts consumer trust [25]. Financial institutions should implement data breach processes and deploy cutting-edge encryption to protect customer data.

3.3 *Dodd–Frank Wall Street Reform and Consumer Protection Act*

After the 2008 financial crisis, Congress approved the Dodd–Frank Act of 2010 to boost market transparency and reduce systemic risk [26]. The act's broad reforms influence IT governance, among others. The Financial Stability Oversight Council (FSOC) is created under Title I of Dodd–Frank in order to keep an eye on systemic risk and make sure the financial system is stable. The OTC derivatives markets are made more transparent and safer under Title VII. Finally, Title X establishes the Consumer Financial Protection Bureau (CFPB) to prevent financial abuse [26]. The legislation significantly impacts IT governance by requiring financial firms to enhance their risk management systems to Dodd–Frank requirements. IT systems must collect, report, and analyze plenty of data to monitor systemic risk [27]. Dodd–Frank compliance enhances market openness and protects clients, stabilizing the financial system. To decrease systemic risk and ensure regulatory compliance, banks need strong data analytics capabilities to monitor and report market activity and financial transactions.

Table 1 highlights some other key US banking IT legislation [28, 29], including regulatory agencies and consumer protection laws. One must first understand the legislative frameworks that govern distinct areas of the US banking industry to understand banking operations' regulatory environment and compliance needs.

Table 1 Overview of excessive key US banking legislation and regulatory frameworks [28, 29]

S. No.	Legal framework	Regulations	Regulatory authorities	Consumer protection rules
1.	Federal Reserve Act (FRA)	Regulation D (reserve requirements)	Federal Reserve Board (FRB)	Equal Credit Opportunity Act, Truth in Lending Act
		Regulation E (electronic fund transfers)		Fair Housing Act, Consumer Leasing Act
		Regulation W (transactions between member banks and affiliates)		
		Regulation CC (availability of funds and collection of checks)		
2.	Federal Deposit Insurance Act	Regulation B (equal credit opportunity)	Federal Deposit Insurance Corporation (FDIC)	Fair Credit Reporting Act, Home Mortgage Disclosure Act
		Regulation H (membership of state banking institutions in the FDIC)		Truth in Savings Act, Fair Debt Collection Practices Act
3.	Home Owners' Loan Act	Regulation LL (savings and loan holding companies)	Office of the Comptroller of the Currency (OCC)	Real Estate Settlement Procedures Act, Fair Credit Reporting Act
4.	Bank Holding Company Act of 1956	Regulation Y (bank holding companies and change in bank control)	Federal Reserve Board (FRB)	Gramm–Leach–Bliley Act, Dodd–Frank Wall Street Reform Act
5.	National Bank Act	Regulation K (international banking operations)	Office of the Comptroller of the Currency (OCC)	Servicemembers' Civil Relief Act, Consumer Leasing Act
6.	International Banking Act of 1978	Regulation F (international operations of US banking organizations)	Federal Reserve Board (FRB)	Fair Debt Collection Practices Act, Fair Housing Act

(continued)

Table 1 (continued)

S. No.	Legal framework	Regulations	Regulatory authorities	Consumer protection rules
7.	Community Reinvestment Act of 1977	Regulation BB (community reinvestment)	Federal Reserve Board (FRB), Federal Deposit Insurance Corporation (FDIC), Office of the Comptroller of the Currency (OCC)	Equal Credit Opportunity Act, Fair Housing Act
8.	Other Relevant Acts and Regulations	Regulation O (loans to insiders)	Various regulatory bodies	Usury Laws, Electronic Fund Transfers Act

3.4 Federal Financial Institutions Examination Council (FFIEC) Guidelines

To perform federal financial institution exams, the FFIEC sets uniform principles, norms, and recommendations. The banking sector depends on the council's cybersecurity and IT governance guidelines [30]. The IT Examination Handbook assesses IT governance, including risk management, security, and business continuity planning. The Cybersecurity Assessment Tool helps banks assess their cybersecurity preparedness and improve [30]. Cloud computing advice provides best practices for controlling cloud service risks. IT governance will be greatly impacted by FFIEC standards. For good cybersecurity and IT governance, financial organizations must follow these regulations [31]. IT governance requires incident response, security, and risk assessments. FFIEC-compliant IT systems can survive cyberattacks. Financial organizations must regularly conduct risk assessments to identify security vulnerabilities and implement appropriate actions to protect their IT systems.

3.5 Role of These Regulations in Shaping IT Governance and Compliance Practices

The primary US regulatory frameworks affect banking IT compliance and governance by setting strict requirements. A bank that follows these standards has strong IT systems, client data protection, and effective risk management. To encourage accountability and transparency, SOX and Dodd–Frank require banks to have robust financial reporting and risk management reporting and internal control systems [32]. GLBA mandates banks to provide adequate data security to protect consumer trust and personal data. The FFIEC's cybersecurity and IT governance requirements may

help banks safeguard their IT systems and avert cyberattacks [33]. These standards reduce regulatory penalties and bank brand damage by ensuring legal and ethical compliance. Banks must follow IT governance and compliance regulations to meet company objectives, protect stakeholder interests, and preserve operational integrity.

4 Analysis of IT Governance in US Banking

US bank IT regulations oversee financial stability, data security, and compliance. This section discusses how US regulatory frameworks have affected IT governance practices, case studies from significant US organizations, how theoretical ideas and regulatory requirements relate, and what opportunities and barriers exist for great IT governance.

4.1 Impact of US Regulatory Frameworks on IT Governance Practices

GLB, Dodd–Frank US banking laws including DFRA and FFIEC recommendations burden IT governance. These requirements need operational resilience, risk management, consumer data security, and accurate financial reporting [34]. SOX impacts IT governance systems that allow banks' financial reporting internal controls. GLBA's mandate that financial institutions develop strong information security systems to safeguard customers' financial data will change IT governance guidelines that prioritize data protection and privacy [34].

4.2 Case Studies and Examples of IT Governance in Leading US Banks

Strong IT governance procedures foster innovation, operational efficiency, and regulatory compliance in top US institutions. Bank of America has a single IT governance architecture to support digital transformation and regulatory compliance [35]. Bank of America uses rigorous risk management frameworks and advanced technologies to increase operational efficiency and customer service globally. IT governance at JPMorgan Chase [36] includes cybersecurity and a scalable IT infrastructure to mitigate risk and comply with laws. These examples demonstrate the need for a unique IT governance framework to help firms adapt to changing rules and win consumer trust.

Strong IT governance in today's banking business supports operational resilience, regulatory compliance, and strategic innovation. Wells Fargo's case of IT governance

structure is meticulously constructed [37]. Wells Fargo uses centralized supervision and decentralized operational management to meet Dodd–Frank Act and FFIEC regulations. The bank monitors cyber risks and operational issues using cutting-edge risk assessment and monitoring tools [37]. Prioritize robust risk management practices. Banks are preventing data breaches by using secure cloud architecture and encryption. AI and advanced analytics help Wells Fargo enhance operational efficiency and digital banking customer experiences.

Due to its global position, Citigroup case must strategically administer IT to coordinate cybersecurity, regulatory compliance, and digital transformation programs [35]. Citigroup’s governance structure revolves around the Global Information Security Office (GISO), which coordinates and oversees cybersecurity programs globally. This coordinated approach ensures cyber threat monitoring in conformity with regional and global regulations. Citigroup’s commitment to control and compliance is shown by its tight regulatory compliance, which facilitates operational flexibility without compromising security and governance [35]. Citigroup strengthens its financial services leadership by adopting digital transformation and employing technology to improve operational efficiency, banking processes, and customer engagement.

US IT governance practices emphasize technological integration, regulatory compliance, and proactive risk management, one of Goldman Sachs’ numerous financial industry breakthroughs [38]. The bank’s governance strategy uses AI-driven analytics and machine learning algorithms to improve risk management, fraud detection, and trading platform optimization. Dodd–Frank and Basel III are two regulations Goldman Sachs follows [38]. The company monitors and reports on its framework compliance using robust systems. Goldman Sachs’ operational resilience and scalability plan relies on cutting-edge IT infrastructure and cloud technologies. This strategy ensures corporate operations and fast customer service regardless of legislative and market changes [38]. IT governance helps Goldman Sachs mitigate operational risks and foster long-term innovation, consolidating its position as a trusted partner in international financial markets.

4.3 Alignment of Regulatory Requirements with Theoretical Perspectives

The banking sector is aligning legal duties with IT governance theories to emphasize the convergence between compliance and strategic management. Theoretical perspectives help explain how rules affect organizational behavior, decision-making, and operational norms [39]. Theoretical models that increase risk management, operational efficiency, and innovation within regulatory-driven IT governance maintain legal compliance.

COBIT (Control Objectives for Information and Related Technologies) is a theoretical framework for aligning IT goals with business goals and regulatory compliance. To comply with US legislation like the Sarbanes–Oxley Act (SOX), which

demands stringent controls over financial reporting, banks must implement IT governance systems to ensure data honesty, transparency, and accountability [40]. The COBIT framework gives banks quantifiable control objectives to improve operations, minimize risk, and meet regulatory requirements.

IT governance systems like ITIL emphasize customer satisfaction and service delivery. These factors are crucial for consumer protection-regulated banks. The Gramm–Leach–Bliley Act (GLBA) and other laws require financial firms to safeguard client data [41]. In response, corporations have embraced ITIL for data security, incident management, and service enhancement. ITIL best practices may help financial organizations satisfy customers and comply with laws.

Strategy theories like the Resource-Based View (RBV) explain how regulations and concepts match. RBV says an organization's resources and abilities define its competitive advantage [42]. Basel III's severe liquidity and capital adequacy requirements require financial institutions to strengthen financial reporting, risk assessment, and resource allocation with IT governance [42]. RBV may help banks invest appropriately on digital transformation and IT innovation to fulfil capital ratios.

Regulatory demands and Institutional Theory show how external restrictions impact organizational behavior and legitimacy. The Dodd–Frank Act strengthened financial stability and consumer protection [43]. Bank IT governance includes stress testing, regulatory reporting, and systemic risk management. The Institutional Theory framework recommends banks to improve IT governance to boost legitimacy, stakeholder trust in operational resilience, ethics, and legal compliance [43].

To implement these theoretical frameworks, banks systematically incorporate risk assessment, policy creation, control mechanism implementation, and continuous monitoring and improvement into their IT governance frameworks [44]. Bringing regulatory requirements into line with theoretical ideas helps banks respond to regulatory changes, grasp new opportunities, and support sustainable development in a complicated regulatory framework [44]. This eliminates compliance risks and boosts adaptability.

4.4 Challenges and Opportunities in Implementing Effective IT Governance

US banks must overcome several challenges and use new opportunities to achieve effective IT governance [45, 46]. Cybersecurity concerns in a globalized digital environment, compliance costs against operational benefits, and complex regulatory compliance requirements are challenges. Compliance with rules enhances firms' resilience, but research showed that it restricts operations and requires adaptive governance [45]. Due to rapid technological innovation, keeping up with changing regulatory rules while employing IT to achieve a competitive advantage is getting harder. IT governance that promotes innovation, agility, and customer-centricity offers opportunities [46]. Agile, advanced analytics, and AI, as discussed in research, can help

banks improve operational efficiency, risk reduction, and decision-making [47]. IT governance must support strategic business objectives for banks to innovate and comply with laws.

5 Compliance Strategies and Best Practices

US banks can use several compliance methods to improve operational efficiency and resilience while satisfying regulatory requirements [48]. These approaches need comprehensive frameworks like the COSO (Committee of Sponsoring Organizations of the Treadway Commission) framework for financial reporting internal control. One study shows that COSO helps financial institutions comply with SOX by building and maintaining effective internal controls and lowering risk [49]. By following COSO standards, banks may increase IT governance reliability, transparency, and accountability.

Financial organizations must use risk management to protect their IT infrastructures. Based on another study, risk-based approaches like the ISO 31000 framework should be used to evaluate risks in all elements of an organization's IT operations and services [50]. US banks utilize risk management frameworks to assess and mitigate cybersecurity, regulatory, and operational risks. Proactive risk management may help banks respond to shifting regulatory requirements.

Internal controls and audits are essential for IT governance policy evaluation and regulatory compliance. Research shows that COBIT offers defined control objectives, measures, and monitoring processes [51]. US banks utilize COBIT to speed up compliance gap resolution, analyze controls, and simplify internal audits. This rigorous approach strengthens governance and increases IT and regulatory compliance risk monitoring.

Strong training and awareness programs create a compliance culture, which is vital for successful compliance efforts. According to the study, workers need continual training to comply with requirements and reduce dangers [52]. Staff at U.S. financial organizations get comprehensive cybersecurity, ethical, and regulatory training. By fostering compliance, financial institutions have a vigilant workforce that can see issues and fix them quickly.

Technological advances and fresh ideas help US banks enhance compliance and efficiency. According to research, blockchain, AI, and machine learning are revolutionizing compliance procedures by automating repetitive tasks, spotting anomalies, and increasing data integrity [53]. US banks use technology to identify fraud, improve regulatory reporting, and monitor compliance. Innovation may help banks adapt to new requirements and save money in the ever-changing financial industry.

6 Conclusion

Finally, this research analyzed the complex realm of compliance strategies, IT governance best practices, and US bank compliance technologies. The essay synthesizes research and case studies to illuminate legislative requirements and theoretical concepts for effective IT governance systems. Compliance strategies showed how comprehensive frameworks like COBIT and COSO—Control Objectives for Information and Related Technologies and Committee of Sponsoring Organizations of the Treadway Commission, respectively—help US banks achieve effective IT governance. These frameworks simplify audit, risk management, and internal control to fulfil SOX, ISO 31000, and other regulatory requirements.

Audits and internal controls reassure stakeholders and regulators of compliance. Compliance monitoring has altered with advanced analytics, blockchain, and AI. These technologies help banks identify and reduce hazards in real time and improve efficiency. Although wide, this assessment has limitations. The study focused on US banks, thus its conclusions may not apply to global financial organizations with different regulations. Because technology and legislation evolve, static literature evaluations may miss important changes. RegTech's transformative influence on financial institution compliance automation deserves research. Longitudinal research might investigate compliance strategies as regulations and technology evolve. Compare IT governance and compliance best practices and lessons across geographies and regulatory regimes to better comprehend transfer.

References

1. Talab, H.R., Flayyih, H.H.: An empirical study to measure the impact of information technology governance under the control objectives for information and related technologies on financial performance. *Int. J. Prof. Bus. Rev.* **8**(4), 25 (2023). [Online]. Available: <https://dialnet.unirioja.es/servlet/articulo?codigo=8956086>. Accessed 05 July 2024
2. Dafe, F., Engebretsen, R.E.H.: Tussle for space: the politics of mock-compliance with global financial standards in developing countries. *Regul. Gov.* (2021). <https://doi.org/10.1111/rego.12427>
3. Lu, H., Liu, X., Osiyevskyy, O.: EXPRESS: doing safe while doing good: slack, risk management capabilities, and the reliability of value creation through CSR. *Strateg. Organ.* **14**(7), 12702211224 (2022). <https://doi.org/10.1177/14761270221122428>
4. Riley, N.: 2024's Top 5 Banking Compliance Priorities. CSI, 11 Apr 2024. <https://www.csiweb.com/what-to-know/content-hub/blog/2024-top-5-banking-compliance-priorities/>. Accessed 05 July 2024
5. Obeng-Nyarko, J.K.: Effects of Sarbanes–Oxley Act 2002 on the Quality of Corporate Reporting by UK Listed Companies, repository.essex.ac.uk, 16 May 2023. <https://repository.essex.ac.uk/35688/>
6. Castellano, G.G.: Don't call it a failure: systemic risk governance for complex financial systems. *Law Soc. Inq.* 1–42 (2024). <https://doi.org/10.1017/lsi.2024.8>
7. Steele, G.: Banking on the Edge, ssrn.com, 26 Jan 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4374379

8. Wali, K., van Paridon, K., Darwish, B.K.: Strengthening banking sector governance: challenges and solutions. *Future Bus. J.* **9**(1) (2023). <https://doi.org/10.1186/s43093-023-00279-0>
9. Why Security & IT Teams in the Financial Industry Are Under Enormous Strain. *SafeBreach*. <https://www.safebreach.com/blog/security-teams-financial-industry/>
10. Correia, A., Água, P.B.: A corporate governance perspective on IT governance. Jan 2021. <https://doi.org/10.22495/cgsetpt19>
11. Onumo, A., Ullah-Awan, I., Cullen, A.: Assessing the moderating effect of security technologies on employees compliance with cybersecurity control procedures. *ACM Trans. Manag. Inf. Syst.* **12**(2), 1–29 (2021). <https://doi.org/10.1145/3424282>
12. Lumpkin, S., Schich, S.: Banks, digital banking initiatives and the financial safety net: theory and analytical framework. *J. Econ. Sci. Res.* **3**(1) (2019). <https://doi.org/10.30564/jesr.v3i1.1113>
13. Grassi, L., Figini, N., Fedeli, L.: How does a data strategy enable customer value? The case of FinTechs and traditional banks under the open finance framework. *Financ. Innov.* **8**(1) (2022). <https://doi.org/10.1186/s40854-022-00378-x>
14. Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F., Sepasgozar, S.M.E.: Risk management in sustainable smart cities governance: a TOE framework. *Technol. Forecast. Soc. Change* **167**(1), 120743 (2021). <https://doi.org/10.1016/j.techfore.2021.120743>
15. Jaya, R.K., Fianty, M.I.: IT project management control and the control objectives for IT and related technology COBIT 2019 framework. *Indones. J. Comput. Sci.* **12**(5) (2023). <https://doi.org/10.33022/ijcs.v12i5.3397>
16. Wang, D., Zhong, D., Li, L.: A comprehensive study of the role of cloud computing on the information technology infrastructure library (ITIL) processes. *Libr. Hi Tech. ahead-of-print* (2021). <https://doi.org/10.1108/lht-01-2021-0031>
17. Mbeka, S.M., Wausi, A.N.: Influence of information technology infrastructure library (ITIL) framework adoption on information technology (IT) service quality—a case of telecommunication companies in Kenya. *SSRN Electron. J.* (2022). <https://doi.org/10.2139/ssrn.4058704>
18. Gunawan, H., Irianto, A.B.P., Galih, J.: Implementation of sustainable service improvement in organizations using framework information technology infrastructure library (ITIL). *Procedia Comput. Sci.* **234**, 748–755 (2024). <https://doi.org/10.1016/j.procs.2024.03.061>
19. Mirtsch, M., Kinne, J., Blind, K.: Exploring the adoption of the international information security management system standard ISO/IEC 27001: a web mining-based analysis. *IEEE Trans. Eng. Manage.* **68**(1), 1–14 (2020). <https://doi.org/10.1109/tem.2020.2977815>
20. Masama, B., Bruwer, J.P., Gwaka, L.: The feasibility of implementing the Committee of Sponsoring Organizations of the Treadway Commission enterprise risk management framework in South African small, medium and micro enterprises: a literature review. *Int. J. Bus. Contin. Risk Manag.* **12**(3), 208 (2022). <https://doi.org/10.1504/ijbcmr.2022.125288>
21. Lessambo, F.I.: *U.S. Banking System: Laws, Regulations, and Risk Management*. Springer Nature (2020)
22. Upadhyay, A., Triana, M.d.C.: Drivers of diversity on boards: the impact of the Sarbanes–Oxley act. *Hum. Resour. Manag.* (2020). <https://doi.org/10.1002/hrm.22035>
23. Ilori, O., Nwosu, N.T., Naiho, H.N.N.: Optimizing Sarbanes–Oxley (SOX) compliance: strategic approaches and best practices for financial integrity: a review. *World J. Adv. Res. Rev.* **22**(3), 225–235 (2024). <https://doi.org/10.30574/wjarr.2024.22.3.1728>
24. Ryle, P., Yan, J.(K.), Gardiner, L.R.: Gramm–Leach–Bliley gets a systems upgrade: what the FTC’s proposed safeguards rule changes mean for small and medium American financial institutions. *EDPACS* 1–12 (2021). <https://doi.org/10.1080/07366981.2021.1911387>
25. Caballero, T.: Promoting due diligence: the role of the Gramm–Leach–Bliley act, and information security standards on financial institutions protecting consumers’ non-public personal information (NPI). In: 2024 Spring Honors Capstone Projects, May 2024. [Online]. Available: https://mavmatrix.uta.edu/honors_spring2024/23/. Accessed 05 July 2024
26. Gangopadhyay, P., Yook, K.C.: Insider trading profits before and after the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010. *Q. J. Financ. Account.* **60**(1/2), 29–64 (2022). [Online]. Available: <https://www.jstor.org/stable/27224933>. Accessed 20 Sep 2023

27. Marciniak, S.A.I.: Too big to protect: a Dodd–Frank framework for protecting 21st century American consumer privacy rights. *Duquesne Law Rev.* **59**, 329 (2021). [Online]. Available: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/duqu59&div=17&id=&page>. Accessed 14 June 2024
28. Gortsos, C.V.: *European Central Banking Law: The Role of the European Central Bank and National Central Banks Under European Law*. Palgrave Macmillan US, Cham (2020)
29. Truby, J., Brown, R., Dahdal, A.: Banking on AI: mandating a proactive approach to AI regulation in the financial sector. *Law Financ. Mark. Rev.* **14**(2), 110–120 (2020). <https://doi.org/10.1080/17521440.2020.1760454>
30. Khodayer, M., Khodayer, M., Mohammed, O.: Security Measures of Protection for Banking Systems, Oct 2022. <https://doi.org/10.1109/picst57299.2022.10238672>
31. Tarullo, D.K.: Bank supervision and administrative law. *Columbia Bus. Law Rev.* **2022**, 279 (2022). [Online]. Available: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/colb2022&div=9&id=&page>. Accessed 05 July 2024
32. Abdulrasool, F.E., Turnbull, S.J.: Exploring security, risk, and compliance driven IT governance model for universities: applied research based on the COBIT framework. *Int. J. Electron. Bank.* **2**(3), 237 (2020). <https://doi.org/10.1504/ijebank.2020.111438>
33. Hassan, M.K., Khodayer, A.M., Hassan, A., Khodayer, O.M., Mahmood, M.: Security issues for banking systems. In: *Computational Intelligence, Data Analytics and Applications*, pp. 117–131 (2023). https://doi.org/10.1007/978-3-031-27099-4_10
34. Guidi, M., Guardiancich, I., Levi-Faur, D.: Modes of regulatory governance: a political economy perspective. *Governance* **33**(1), 5–19 (2020). <https://doi.org/10.1111/gove.12479>
35. von Solms, J.: Integrating Regulatory Technology (RegTech) into the digital transformation of a bank treasury. *J. Bank. Regul.* (2020). <https://doi.org/10.1057/s41261-020-00134-0>
36. Bui, T.L.: Cybersecurity Events, Financial Analysts, and Earnings Forecast Uncertainty, spectrum.library.concordia.ca, 31 Aug 2023. <https://spectrum.library.concordia.ca/id/eprint/993121/>. Accessed 05 July 2024
37. Amernic, J., Craig, R.: Evaluating assertions by a Wells Fargo CEO of a ‘return to ethical conduct.’ *Leadership* **18**(3), 174271502110643 (2022). <https://doi.org/10.1177/17427150211064397>
38. needa needa: How Does the Industry Factor Affect the Risk Management Strategies and Methods?—A Comparative Analysis of Risk Management Practices, Jan 2024. <https://doi.org/10.2139/ssrn.4703079>
39. Aguinis, H., Jensen, S.H., Kraus, S.: Policy implications of organizational behavior and human resource management research. *Acad. Manag. Perspect.* **36**(3) (2021). <https://doi.org/10.5465/amp.2020.0093>
40. Manginte, S.Y.: Fortifying transparency: enhancing corporate governance through robust internal control mechanisms. *Adv. Manag. Financ. Rep.* **2**(2), 72–84 (2024). <https://doi.org/10.60079/amfr.v2i2.173>
41. Brunngraber, H.: Affirmative privacy rights in the employment context: considerations for protecting employee data in highly regulated environments. *Univ. Illinois J. Law Technol. Policy* **2024**, 127 (2024). [Online]. Available: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/jltp2024&div=6&id=&page>. Accessed 05 July 2024
42. Chatterjee, S., Rana, N.P., Dwivedi, Y.K.: How does business analytics contribute to organisational performance and business value? A resource-based view. *Inf. Technol. People.* ahead-of-print (2021). <https://doi.org/10.1108/itp-08-2020-0603>
43. Rocha, R., Neto, M.S.: Credit rating agencies and the state: an inter-field regulated relationship. *Theory Soc.* (2024). <https://doi.org/10.1007/s11186-024-09556-5>
44. Correia, M.G.F.: Continuous audit: a framework for banking sector, repositorio.iscte-iul.pt, 28 Feb 2024. <https://repositorio.iscte-iul.pt/handle/10071/31685>. Accessed 05 July 2024
45. Singhal, S., Kothuru, S.K., Sethibathini, V.S.K., Bammidi, T.R.: ERP excellence a data governance approach to safeguarding financial transactions. *Int. J. Manag. Educ. Sustain. Dev.* **7**(7), 1–18 (2024). [Online]. Available: <https://ijsdcs.com/index.php/IJMESD/article/view/441>. Accessed 03 Mar 2024

46. Ogundipe, D.O.: Conceptualizing cloud computing in financial services: opportunities and challenges in Africa-US contexts. *Comput. Sci. IT Res. J.* **5**(4), 757–767 (2024). <https://doi.org/10.51594/csitj.v5i4.1020>
47. Addy, W.A., Ugochukwu, C.E., Oyewole, A.T., Ofodile, O.C., Adeoye, O.B., Okoye, C.C.: Predictive analytics in credit risk management for banks: a comprehensive review. *GSC Adv. Res. Rev.* **18**(2), 434–449 (2024). <https://doi.org/10.30574/gscarr.2024.18.2.0077>
48. Innocent, U., Odejide, N.O.A., Aderemi, N.S., Olanrewaju, D., Adeyemi, E., Orieno, H.: AI in risk management: an analytical comparison between the U.S. and Nigerian banking sectors. *Int. J. Sci. Technol. Res. Arch.* **6**(1), 127–146 (2024). <https://doi.org/10.53771/ijstra.2024.6.1.0035>
49. Farah, N., Islam, M.S., Tadesse, A., McCumber, W.: Impact of audit committee social capital on the adoption of COSO 2013. *Adv. Account.* 100685 (2023). <https://doi.org/10.1016/j.adiac.2023.100685>
50. Sahibu, S., Sakti, A., Iskandar, A.: Risk Management Analysis of SMK Telkom Makassar's Integrated Academic Information System in Compliance with ISO 31000 Standards. | *Ingénierie des Systèmes d'Information* | EBSCOhost, openurl.ebsco.com, 01 Feb 2024. <https://openurl.ebsco.com/EPDB%3Agcd%3A16%3A19672576/detailv2?sid=ebsco%3Aplink%3Ascholar&id=ebsco%3Agcd%3A176060265&crl=c>. Accessed 05 July 2024
51. Morris, G., Lompoliu, E.: Enhancing IT governance at BPS Manado: a COBIT 2019 framework implementation study. *TeIka J. Teknol. Inf. Komun. (J. Inf. Commun. Technol.)* **14**(1), 65–78 (2024). <https://doi.org/10.36342/teika.v14i1.3325>
52. Quaigrain, R.A., Owusu-Manu, D.-G., Edwards, D.J., Hammond, M., Hammond, M., Martek, I.: Occupational health and safety orientation in the oil and gas industry of Ghana: analysis of knowledge and attitudinal influences on compliance. *J. Eng. Des. Technol.* (2022). <https://doi.org/10.1108/jedt-11-2021-0664>
53. Kayıkçı, Ş., Khoshgoftaar, T.M.: Blockchain meets machine learning: a survey. *J. Big Data* **11**(1) (2024). <https://doi.org/10.1186/s40537-023-00852-y>

Overcoming Challenges and Implementing Effective Information Security Policies for Remote Work Environments



Muhammad Nauman Zakki, Nimra Iftikhar, Saim Saif Ullah Khan, Farhood Nishat, and Oroos Arshi

Abstract Remote work expanded due to the COVID-19 pandemic and technical advances. However, this development makes remote workplaces more vulnerable to data breaches and cyberattacks. This article discusses the challenges firms have in establishing dependable remote worker information security regulations. An extensive 2021–2024 literature review evaluates remote work security research. Technical issues like encrypted data transmission and secure remote access, human aspects like education and training, and organizational impediments like policy implementation and resource allocation are among the most urgent. The study recommends VPNs, endpoint security, and regular training to reduce hazards. This study aims to teach organizations on how to protect remote work and pave the path for future research.

Keywords Remote work · Information security · Security policies · Systematic review

1 Introduction

The rapid use of remote work has transformed the workplace. By 2021, over half of US full-time workers worked remotely, as shown in Fig. 1 [1]. It was up significantly from 25% before the outbreak [1]. The COVID-19 pandemic, which forced many companies to adopt remote labour to survive, technical advances, and the desire for flexibility all contributed to this transition.

M. N. Zakki · N. Iftikhar · S. S. U. Khan · F. Nishat (✉)

Department of Cyber Security and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan
e-mail: farhoodnishat@hotmail.com

O. Arshi

Department of Computer Science and Engineering, University of Petroleum and Energy Studies, Dehradun, India

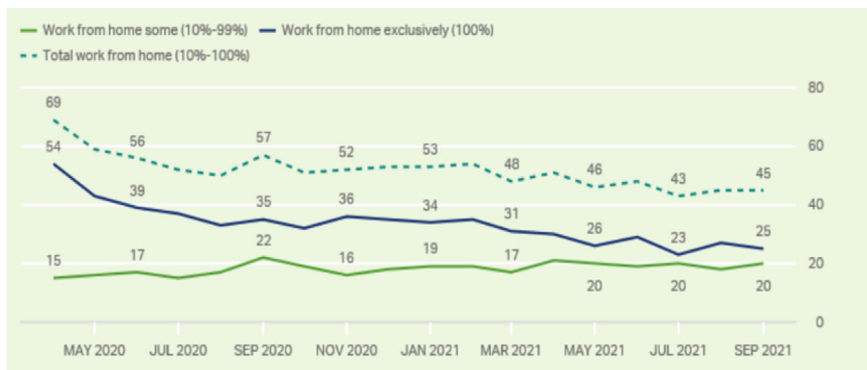


Fig. 1 US employee work location throughout pandemic [1]

Information security is crucial in remote work. When employees use personal devices to access business networks and handle sensitive data from multiple locations, cyberattacks increase. Cybersecurity Ventures expects that cybercrime will cost \$10.5 trillion worldwide by 2025, up from \$3 trillion in 2015 [2]. Remote employment drive ransomware attacks up 485% in 2023 [3]. These figures demonstrate the need for a good data breach, phishing, and cybercrime prevention practices. Remote work environments must be secure to preserve organizational assets and maintain commercial operations.

Businesses must overcome several challenges to adopt remote worker information security requirements. Dispersed employees make an organization more vulnerable to cyberattacks, which is concerning. In the COVID-19 pandemic, 20% of companies reported remote worker security vulnerabilities [4]. Remote workers typically use their own devices and unsecured home networks, which are less secure than corporate networks.

Compliance with regulations is another challenge. Remote workers can face legal issues since GDPR and HIPAA are harder to execute. According to a Ponemon Institute study, 63% of firms claimed remote employment made it harder to follow these guidelines [5]. Additionally, humans pose a major threat. Remote workers are being targeted by phishing and social engineering. Over half of Tessian's remote workers admitted to phishing scams [6].

This study aims to identify and solve the challenges organizations have when adopting information security policies in remote work contexts. The study will use a systematic literature review (SLR) to examine remote workplace information security risks and remedies. To present a complete picture. However, the study has certain limitations. The study's limited research and data may not cover all outcomes or dangers. Despite these limitations, the research aims to enhance remote workplace information security by providing helpful insights and practical ideas.

This paper is divided into several key sections: The Literature Review examines prior research on remote work and information security, highlighting the most important concerns and offering solutions. The Methodology section describes the

systematic review technique used to collect and assess relevant articles to ensure a complete and structured study. Research explains the review's concerns and solutions in the result and discussion section. Also, this section compares techniques and discusses their implications for companies. The last part, the Conclusion, summarizes the important themes, offers practical applications, and suggests additional research.

2 Literature Survey

2.1 Remote Work and Information Security

Remote work research has focused on information security in recent years. Several authors have explored the opportunities and challenges this transformation provides to corporate security regimes.

The research examined the first implications of the COVID-19 pandemic's rapid transition to remote work on information security [7]. According to their analysis, many firms were unprepared for the sudden transition, making them more vulnerable to assaults. During the switch, 42% of firms noticed an increase in phishing attempts, indicating attackers took advantage of the uncertainty. Another research examined the long-term information security effects of remote work [8]. They surveyed 500 IT professionals and found that 67% said remote employment made security requirements harder to maintain. They found it impossible to monitor remote workers' security, excessive use of personal devices, and insecure home networks.

Another study examined how individuals protect remote workers, another crucial contribution [9]. Because remote work increases security incidents, their study focused on the mental health implications of remote work, including loneliness and stress. Remote workers were twice as likely to click on hazardous links than in-office workers, therefore they need additional training. Current information security regulations and their effectiveness in remote work were extensively examined by literature [10]. According to 50 studies, many organizations have implemented rule changes, yet there are still loopholes. Although multi-factor authentication (MFA) is a proven way to prevent unauthorized access to remote resources, just 35% of companies use it.

Similar to that another research examined remote work's technological challenges [11]. Enterprises grappled with VPN security, cloud service security, and remote software update and patch management. They found that 55% of firms had problems keeping their VPN connections safe, which is an issue because VPNs secure data transmitted between remote workers and corporate networks. One project also examined distant workers' regulatory challenges [12]. Remote work makes GDPR and HIPAA compliance harder, according to their results. Sixty-three per cent of organizations struggled to ensure their remote work rules and processes were legal, which might lead to legal difficulties.

Other research has suggested ways to enhance remote data security despite these challenges [13]. Zero-trust architectures, suggested by authors, consider all devices and users suspect unless proved otherwise. This method reduced security incidents by 30% for firms, according to their study. Enhanced endpoint detection and response (EDR) systems are another solution suggested by the literature [14]. These systems monitor and react to remote device hazards to offer real-time malware and cyber protection. EDR considerably decreased cyberattacks, according to their research.

Challenges in Implementing Information Security Policies

In remote work contexts, human, organizational, and technological barriers prevent effective security measures. Several authors have examined these issues, revealing the challenges corporations face in securing data.

2.2 Technology Factors

Research says technological issues are big concerns. Due to the popularity of remote work, people are using more personal devices and home networks, which are not necessarily as secure as corporate infrastructures [15]. Figure 2 shows an asset taxonomy made by author related to the work-from-home environment, Sixty per cent of workers questioned used their devices for work, raising data breach and virus worries. These risks are significant enough without unsecured domestic Wi-Fi networks.

Many businesses struggle to secure remote access to their networks [16]. Virtual Private Networks (VPNs) protect data exchanged between remote personnel and central servers, yet many companies struggle to secure them. The framework of research is shown in Fig. 3. Their research of 300 IT specialists found that 55% of organizations had VPN security issues, highlighting the need for improved remote access solutions [16]. Another research examined the challenges of remote software and system updates [17]. Their results show that 45% of firms fail to update and patch remote equipment. Update delays increase system vulnerabilities to known exploits and attacks. They advised centralized administration and automated upgrading to fix this.

2.3 Human Factors

Human factors are key to remote work security. The research examined remote workers' mental and behavioral aspects of data protection [18]. They found that distractions and stress increase security failures among remote workers. For instance, 40% of remote workers accidentally clicked on suspicious links owing to distraction or habit [18]. Another work studied security awareness and training [19]. Results found that many organizations had not adequately trained employees on remote

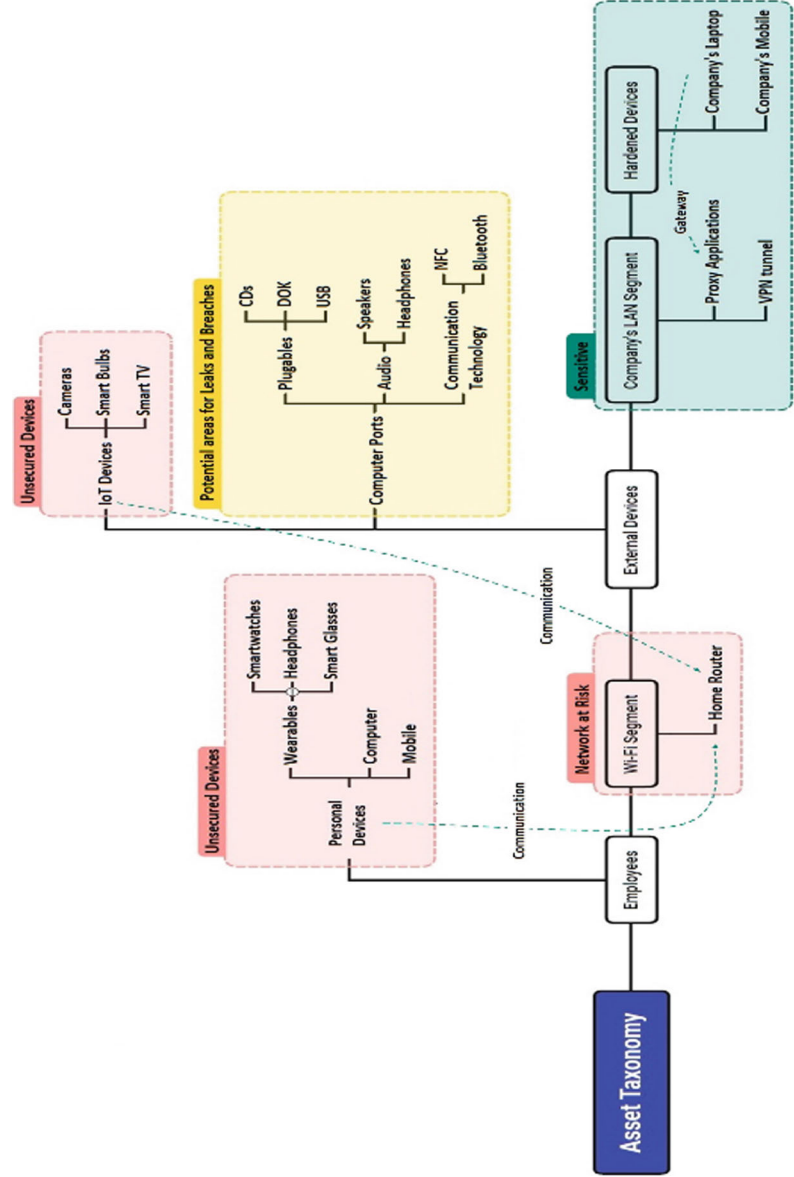


Fig. 2 Asset taxonomy [15]

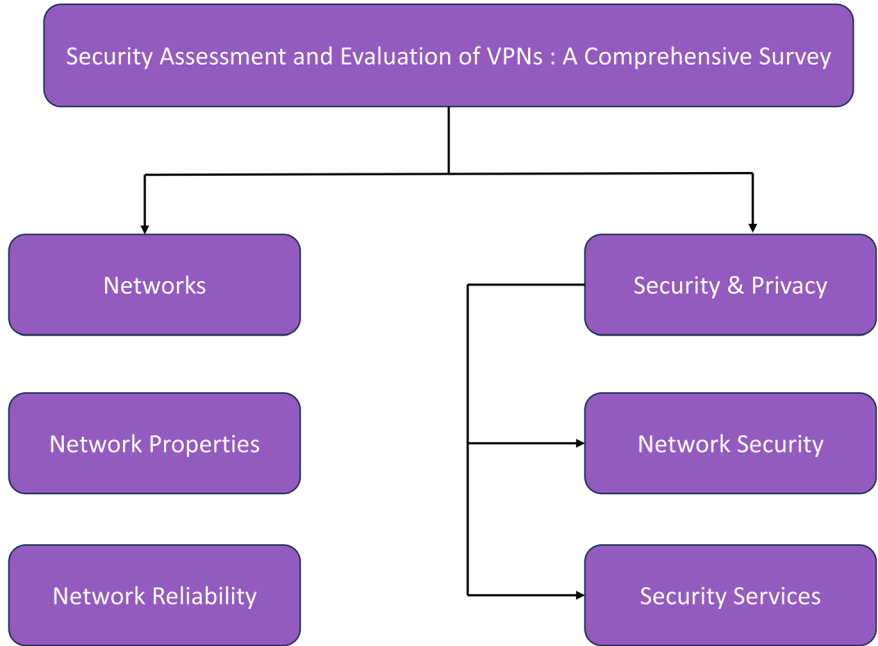


Fig. 3 Research framework [16]

work’s specific security risks. Only 30% of employers provided comprehensive remote worker security training, according to their survey [19].

Regular training and simulated phishing attempts were highlighted to keep personnel vigilant. Similar to that, another research examined “shadow IT,” where personnel employ prohibited software and tools [20]. In their analysis, 65% of remote workers breach business security by employing illicit technologies for work. These tools may not fulfil the organization’s security needs, introducing significant security hazards [20]. Their solution was to tighten tool usage protocols and replace insecure alternatives with more user-friendly ones.

3 Organizational Factors

Organizations must overcome challenges to implement effective security measures. The issues of adopting a uniform security strategy across a geographically scattered workforce were examined by research [21]. Their survey found that 50% of organizations had trouble implementing regulations since remote workers work in different places with different security. Another study noted the challenge of aligning security policies with organizational objectives [22]. They found that operational efficiency generally trumped security, especially early in remote work adoption. The lack of

policy adaptation to changing working conditions led to weaknesses in security processes. They advised a balanced BCP plan that addresses security [22]. Another study discussed resource allocation. According to their study, many organizations, particularly SMEs, lack the resources to secure remote personnel [23]. Staffing and budget restrictions prevented them from investing in cutting-edge security technologies and training. They suggested hiring managed security service providers to enhance in-house capabilities and increase protection.

4 Strategies and Best Practices

Technical solutions, personnel training, and organizational techniques are needed to implement remote work information security requirements. Many authors have addressed remote work security issues.

4.1 Technological Solutions

Research offers zero-trust security [24]. It assumes that neither people nor devices within the network perimeter are trusted by default. The reviewed workflow by author is shown in Fig. 4. This strategy, based on “never trust, always verify,” requires ongoing verification of people and equipment. Zero-trust principles reduced security incidents by 35% in distant organizations, demonstrating their efficacy [24].

4.2 Strategies and Best Practices

Technical solutions, personnel training, and organizational techniques are needed to implement remote work information security requirements. Many authors have addressed remote work security issues.

4.3 Technological Solutions

Research offers zero-trust security [24]. It assumes that neither people nor devices within the network perimeter are trusted by default. The reviewed workflow by author is shown in Fig. 4. This strategy, based on “never trust, always verify,” requires ongoing verification of people and equipment. Zero-trust principles reduced security incidents by 35% in distant organizations, demonstrating their efficacy [24].

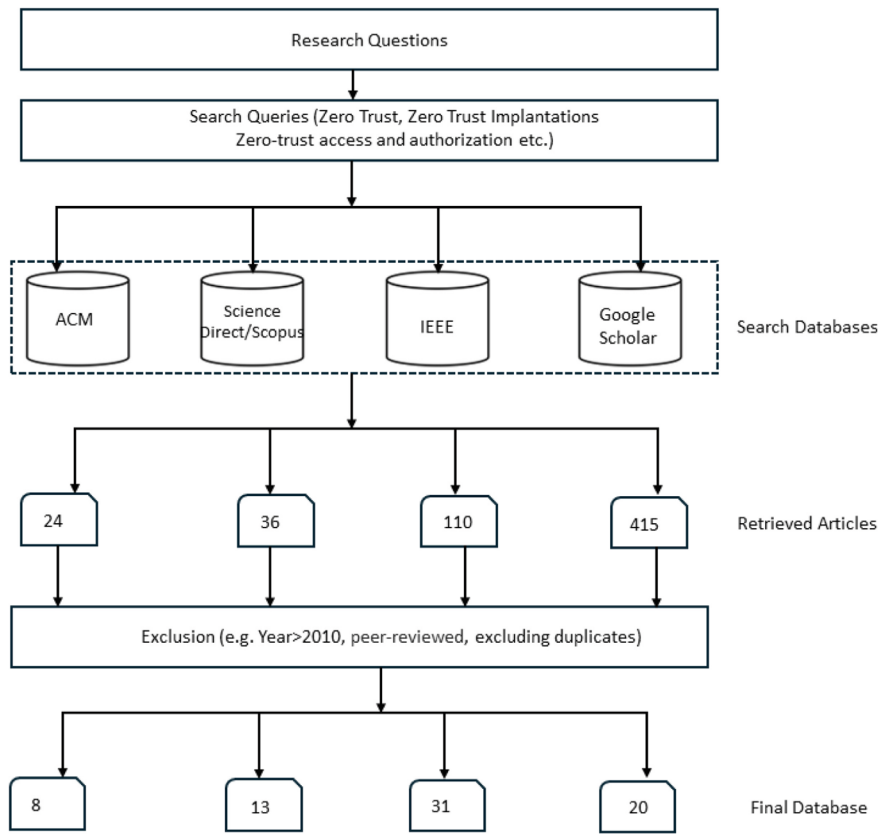


Fig. 4 Research workflow [24]

Another author stresses secure remote access and VPNs. Encrypting data between distant workers and corporate networks is possible using VPNs [25]. They recommend that organizations utilize VPNs with strong encryption and multi-factor authentication for security. Their analysis found that VPNs with MFA reduced unauthorized access attempts by 50% [25]. Endpoint security is crucial also as discussed by another research [26]. Advanced endpoint detection and response (EDR) systems constantly monitor distant devices for suspicious behaviour and threats. These systems identify threats in real-time and automatically remove them, reducing malware risk. Their study found that EDR systems reduced remote equipment cyberattacks by 40% [26].

4.4 Employee Training and Awareness

Research says staff training and awareness reduce security risks. They argue that remote workers require regular cybersecurity training to remain abreast of emerging threats and countermeasures. Their research showed that organizations with extensive training programs reduced phishing incidents by 30% [27]. Gamified learning and simulated phishing attacks are two interactive training methods they recommend for engagement and retention. Another similar study recommends that organizations foster a security culture [28]. It requires persuading personnel to see security as a shared responsibility. They advocate periodic exercises and security metrics in performance evaluations to ensure compliance. Their analysis found 25% fewer insider assaults in businesses with robust security cultures.

4.5 Organizational Strategies

One Research recommends open, comprehensive remote work safety laws [8]. As part of remote work security, these rules should include permitted devices and applications, data management requirements, and incident reporting. They recommend evaluating and modifying these guidelines often to adapt to evolving dangers. They found that organizations with defined remote work policies had fewer security breaches and faster incident response times. On the other hand, another research recommends adaptive security methods [29]. Security should be adaptable to remote work circumstances. The experts advocate cloud-based security solutions that can be scaled to fit the organization's needs. Cloud-based security services safeguarded and simplified remote workforce management, according to their study [29]. The research also emphasizes constant monitoring. Regular audits help find security weaknesses and ensure compliance. They propose automated monitoring tools to track network activity and discover abnormalities. According to their analysis, ongoing monitoring and audits reduced security incidents by 20% for organizations [29].

Table 1 provides some additional studies that contribute to the existing base of research.

4.6 Research Gap

Even though information security in remote work has been thoroughly examined, some key gaps remain. The lack of comprehensive, adaptive solutions that alter the threat situation is a key issue. Current remote work research focuses on onboarding issues rather than long-term security. Even though human factors and training are crucial, more research is needed on the usefulness of continuous, interactive training programs in lowering security issues. Existing research lacks attention on how to

Table 1 Thematic analysis of challenges in implementing effective information security policies for remote work environments

Citation	Aim/objective of research	Results	Future research
[30]	To explore employees' experiences of remote work and the impact of remote work on working life	Identified an increase in phishing attempts and other cyber threats during the transition	Explore long-term impacts and strategies for sustained remote security
[31]	To investigate the challenges of maintaining security standards in remote work settings	Found that 67% of IT professionals reported increased difficulty in maintaining security standards	Study the effectiveness of various remote security policies and their adaptability
[32]	To examine human factors influencing security vulnerabilities among remote workers	Discovered that remote workers are twice as likely to fall for phishing scams due to stress	Investigate the impact of continuous training on reducing human errors
[33]	To analyze the effectiveness of current information security policies in remote work environments in Ukraine and EU	Found significant gaps in policy implementation, with only 35% using multi-factor authentication	Research on the adoption and impact of new security technologies
[34]	To recommend advanced endpoint detection and response systems for remote work security	Reported a 40% decrease in successful cyber-attacks with EDR implementation	Study the integration of AI in enhancing endpoint security measures

integrate cutting-edge technologies like machine learning and AI into remote work security frameworks. The lack of reviews of remote access solutions like secure VPNs and endpoint security programs leaves organizations without complete best practices. Finally, there is little understanding of how firms may combine security, operational efficiency, and user experience when workers work remotely. This study proposes unique, all-encompassing security methods through a literature study that can adapt to remote work's ever-changing nature to solve these knowledge gaps. The research aims to help organizations improve information security and fight emerging threats.

5 Methodology

This research employed a Systematic Literature Review (SLR) because of its completeness and rigour in discovering, analyzing, and incorporating relevant information. Experts think the SLR technique is good for understanding complex problems like remote work information security since it synthesizes data from several research.

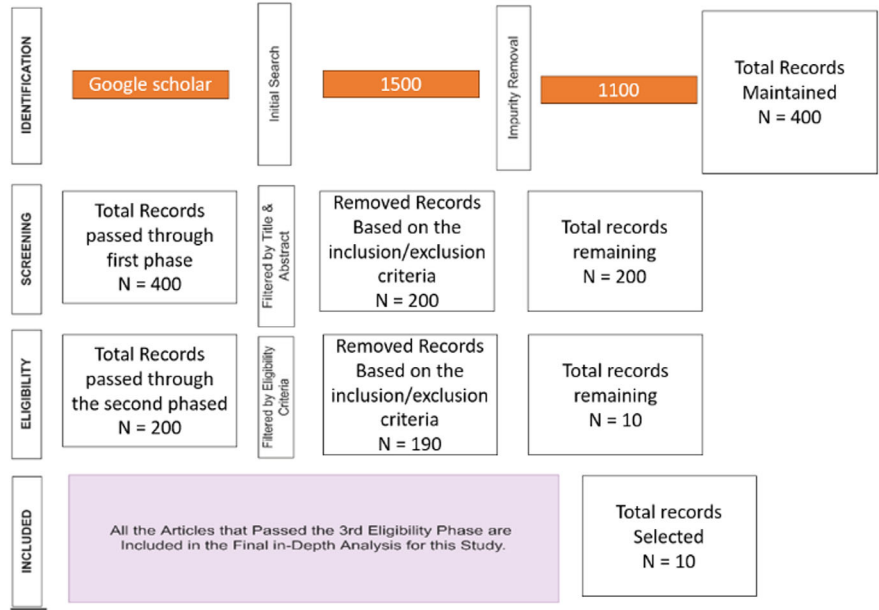


Fig. 5 Research process for methodology

It enhances the image. This technique may identify research requirements and guide future investigations [35]. Figure 5 shows a process flow diagram of the framework.

Strict inclusion and exclusion criteria ensure that research is relevant and current;

Inclusion Criteria

- Studies published between 2021 and 2024.
- Peer-reviewed articles.
- The research focused on information security in remote work environments.

Exclusion Criteria

- Studies published before 2021.
- Non-peer-reviewed articles.
- Research not directly related to remote work security.

The database for the research chosen is Google Scholar. Google Scholar’s wide range of research articles on information security and remote work influences its selection. Due to its high-quality, peer-reviewed publications, this resource may aid a complete literature investigation. The top 10 publications that met the inclusion criteria are the research sample. Research chose these papers because of their solid methodology, noteworthy findings, and relevance to our research issue. Read titles abstracts, and complete articles to ensure research objectives are met.

For reliable outcomes, data is gathered methodically. First, the search from Google Scholar for publications on “remote work security,” “information security policies,”

“cybersecurity in remote work,” and “remote work challenges” is done. Duplicates are then removed from search results and sorted by inclusion criteria. After that research, gather the study’s objective, methodology, notable findings, and recommendations from each carefully evaluated article. Then, the data is organized for analysis.

Data analysis is done using Thematic analysis finds, analyzes, and reports on reoccurring patterns (themes). The data is used for this reason because theme analysis can improve it. First, read and reread the extracted information to understand it. Preliminary codes are then generated to identify study-related data. We evaluate and alter these code-based themes to ensure they accurately represent the facts. Naming and defining the final themes provides a solid framework for understanding remote work information security policy implementation challenges and solutions.

6 Results and Discussions

This section presents the systematic review findings on remote work information security policy implementation results and debate. Ten studies’ key themes and methodology are summarized. The study then analyzes security policy implementation issues thematically into technological, human, and organizational categories. The literature’s best practices and techniques are then analyzed into three groups: technological solutions, human-centric approaches, and organizational strategies. This in-depth analysis illuminates remote work security and offers practical advice for improving information security.

Thematic Analysis of Challenges

Table 2 outlines themes as technological, human, and organizational issues from the selected studies.

Table 3 lists the three themes as research technology, human-centeredness, and organizational strategies and best practices from selected studies.

6.1 Comparison with Existing Literature

This study’s findings support and expand on previous research in numerous key ways. Secure access and data encryption were previously identified as essential remote work security components [8]. This paper reiterates the need for VPNs and data encryption. Although underemphasized in prior publications, new themes like the rising necessity of advanced threat detection systems are also highlighted. Research showed that staff knowledge and training reduced security concerns the greatest in human factors [29, 30]. This study confirms these findings and emphasizes the necessity for security-conscious culture and training. This strategy contrasts with the static view of one-time training sessions. Policy enforcement and resource allocation

Table 2 Thematic analysis of strategies and best practices for implementing effective information security policies for remote work environments

Challenge type	Description	Source
Technological challenges	Secure access to corporate resources remotely	[36]
	Issues with implementing robust data encryption methods	–
	Difficulties in managing and securing remote devices used by employees	–
Human factors	Lack of awareness among employees regarding security practices	[37]
	Insufficient or ineffective training programs for employees	–
	Issues with employee compliance with security policies and best practices	–
Organizational challenges	Challenges in enforcing security policies consistently across the organization	[38]
	Issues with allocating sufficient resources (financial, technical, human) for security measures	–
	Lack of support from management for implementing and maintaining security policies	–

Table 3 Discussion of findings

Strategy type	Description	Sources
Technological solutions	Effective use of VPNs for secure remote access	[39]
	Implementation of endpoint protection to safeguard remote devices	[40]
	Advanced threat detection techniques to identify and mitigate security threats	[40]
Human-centric approaches	Improving employee awareness through targeted training programs	[41]
	Fostering a security-conscious culture within remote teams	[41]
	Continuous training programs to reduce security incidents	[42]
Organizational strategies	Developing and enforcing robust organizational security policies	[8]
	Role of leadership and management in ensuring effective security measures	[43]
	Examples of successful implementation of comprehensive security policies	[44]

dominated organizational difficulty studies [23–25]. This study reveals that managerial leadership and support are essential for policy implementation. Even with solid standards and lots of resources, security objectives may not be accomplished without competent leadership, the data shows.

6.2 *Implications for Practice*

This study's findings may help remote work organizations enhance information security. Worldwide usage of VPNs and other robust data encryption methods is the first line of defence against unwanted access to sensitive data. Advanced threat detection technology can identify and mitigate dangers, adding to protection. HR-wise, firms must implement and maintain security risk and best practice training programs. Creating a security-conscious culture via continuous communication, safe activities, and leadership by example is also important. Comprehensive security policies must be established and enforced organizationally. Clear standards, specified tasks, and incident response techniques may promote company-wide security compliance. These efforts need top-level support and strong leadership. Leaders who provide resources and support security policies demonstrate their commitment to security.

7 Conclusion

In conclusion, this research examined the challenges businesses have when applying information security rules to remote work settings and offered solutions to safeguard a dispersed workforce. A complete literature review of 2021–2024 research illuminates the best methods for technological, human-centric, and organizational issues. The findings highlight encrypted data access, remote device management, staff expertise, training effectiveness, policy enforcement, resource allocation, and administration support. All these issues demonstrate how tough remote workspace security is and how many methods are required. VPNs, endpoint security, and advanced threat detection are key technological solutions, according to the research. Maintaining a security-conscious culture and developing human-centric techniques is crucial. Organizational methods should include rigorous security rules, continuous enforcement, and strong leadership support. The practical solutions from this study may help remote work organizations enhance information security. Following the guidelines may help companies protect important data and boost remote worker productivity.

This study thoroughly analyzed the problem; however future research may fill up the gaps. Long-term training program effectiveness is a major research need. These programs are crucial, but this research does not teach us how to improve them or keep them running, so workers always pay attention and obey the guidelines. Future research should also examine how to effectively integrate AI and ML into threat detection and mitigation programs. Knowing how these technologies may be utilized effectively, and influence security would be beneficial. Another topic that requires further research is business culture and data security. Research may examine how company culture affects safety measures. A better understanding of these processes may help organizations adjust their strategies to local cultures.

References

1. Saad, L., Wigert, B.: Remote work persisting and trending permanent. Gallup, 13 Oct 2021. <https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx>
2. Cybersecurity Ventures Report on Cybercrime. eSentire. <https://www.esentire.com/cybersecurity-fundamentals-defined/glossary/cybersecurity-ventures-report-on-cybercrime#:~:text=The%202023%20Cybersecurity%20Ventures%20Cybercrime%20Report%20predicts%20a%20rapid%20increase>
3. At-Bay: Remote Access Behind 58% of Ransomware Attacks in 2023. At-Bay. https://www.at-bay.com/press_releases/research-reveals-remote-access-behind-58-percent-ransomware-attacks/
4. Nabe, C.: Impact of COVID-19 on Cybersecurity. Deloitte Switzerland (2020). <https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html>
5. The Human Factor in Data Protection (2012). Available: https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf
6. Research Report—Hybrid Working and Cybersecurity. Tessian. <https://www.tessian.com/resources/back-to-work-cybersecurity-behaviors-report/>. Accessed 07 Oct 2021
7. Kähkönen, T.: Remote work during the COVID-19 pandemic: identification of working life impacts, employees' data protection abilities and trust outcomes. *J. Org. Change Manag.* **36**(3) (2023). <https://doi.org/10.1108/jocm-06-2022-0179>
8. Olawale, N.O., Ajayi, A., Udeh, A., Odejide, N.O.A.: Remote work policies for IT professionals: review of current practices and future trends. *Int. J. Manag. Entrep. Res.* **6**(4), 1236–1258 (2024). <https://doi.org/10.51594/ijmer.v6i4.1056>
9. Adisa, T.A., Ogbonnaya, C., Adekoya, O.D.: Remote working and employee engagement: a qualitative study of British workers during the pandemic. *Inf. Technol. People* **36**(5) (2021). <https://doi.org/10.1108/itp-12-2020-0850>
10. Saeed, S.: Digital workplaces and information security behavior of business employees: an empirical study of Saudi Arabia. *Sustainability* **15**(7), 6019 (2023). <https://doi.org/10.3390/su15076019>
11. Aleem, M., Sufyan, M., Ameer, I., Mustak, M.: Remote work and the COVID-19 pandemic: an artificial intelligence-based topic modeling and a future agenda. *J. Bus. Res.* **154**(154), 113303 (2023). <https://doi.org/10.1016/j.jbusres.2022.113303>
12. Berg, J., Green, F., Nurski, L., Spencer, D.A.: Risks to job quality from digital technologies: are industrial relations in Europe ready for the challenge? *Eur. J. Ind. Relat.* **29**(4), 347–365 (2023). <https://doi.org/10.1177/09596801231178904>
13. Ahmed, S.F., Alam, M.S.B., Afrin, S., Rafa, S.J., Rafa, N., Gandomi, A.H.: Insights into Internet of Medical Things (IoMT): data fusion, security issues and potential solutions. *Inf. Fusion* 102060 (2023). <https://doi.org/10.1016/j.inffus.2023.102060>
14. Fernandez, E.B., Brazhuk, A.: A critical analysis of zero trust architecture (ZTA). *Comput. Stand. Interfaces* **89**, 103832 (2024). <https://doi.org/10.1016/j.csi.2024.103832>
15. Kotak, J., Habler, E., Brodt, O., Shabtai, A., Elovici, Y.: Information security threats and working from home culture: taxonomy, risk assessment and solutions. *Sensors* **23**(8), 4018–4018 (2023). <https://doi.org/10.3390/s23084018>
16. Abbas, H., et al.: Security assessment and evaluation of VPNs: a comprehensive survey. *ACM Comput. Surv.* **55**(13s) (2023). <https://doi.org/10.1145/3579162>
17. Reunamäki, R., Fey, C.F.: Remote agile: problems, solutions, and pitfalls to avoid. *Bus. Horiz.* **66**(4) (2022). <https://doi.org/10.1016/j.bushor.2022.10.003>
18. Sun, J., Gan, W., Chao, H.-C., Yu, P.S., Ding, W.: Internet of behaviors: a survey. *IEEE Internet Things J.* 1 (2023). <https://doi.org/10.1109/JIOT.2023.3247594>
19. Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., Thapliyal, H.: A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon* **9**(3), e14234 (2023). <https://doi.org/10.1016/j.heliyon.2023.e14234>

20. Barlette, Y., Berthevas, J.-F., Sueur, I.: Impacts on employee coping behaviors of opportunities and threats related to the use of shadow IT. *Syst. Inf. Manag.* **28**(4), 71–107 (2023). <https://doi.org/10.3917/sim.234.0071>
21. Wright, L.K., Jatrana, S., Lindsay, D.: Remote area nurses' experiences of workplace safety in very remote primary health clinics: a qualitative study. *J. Adv. Nurs.* (2024). <https://doi.org/10.1111/jan.16028>
22. Herath, T.C., Herath, H.S.B., Cullum, D.: An information security performance measurement tool for senior managers: balanced scorecard integration for security governance and control frameworks. *Inf. Syst. Front.* **25** (2022). <https://doi.org/10.1007/s10796-022-10246-9>
23. Biea, E.A., Dinu, E., Bunica, A., Jerdea, L.: Recruitment in SMEs: the role of managerial practices, technology and innovation. *Eur. Bus. Rev.* (2023). <https://doi.org/10.1108/eb-05-2023-0162>
24. Azad, M.A., Abdullah, S., Arshad, J., Lallie, H., Ahmed, Y.H.: Verify and trust: a multidimensional survey of zero-trust security in the age of IoT. *Internet Things* 101227 (2024). <https://doi.org/10.1016/j.iot.2024.101227>
25. AlSayfi, Q., Alsirhani, A.: The Impact of Remote Work on Corporate Security, Sept 2023. <https://doi.org/10.1109/iccit58132.2023.10273946>
26. Plachkinova, M., Knapp, K.: Least privilege across people, process, and technology: endpoint security framework. *J. Comput. Inf. Syst.* 1–13 (2022). <https://doi.org/10.1080/08874417.2022.2128937>
27. Angafor, G.N., Yevseyeva, I., Maglaras, L.: Securing the remote office: reducing cyber risks to remote working through regular security awareness education campaigns. *Int. J. Inf. Secur.* (2024). <https://doi.org/10.1007/s10207-023-00809-5>
28. Dearden, T.E., Parti, K., Hawdon, J., Gainey, R.R., Vandecar-Burdin, T., Albanese, J.S.: Differentiating insider and outsider cyberattacks on businesses. *Am. J. Crim. Just.* (2023). <https://doi.org/10.1007/s12103-023-09727-7>
29. Farcane, N., et al.: Auditors' perceptions on work adaptability in remote audit: a COVID-19 perspective. *Econ. Res. Ekon. Istraž.* **36**(1), 1–38 (2022). <https://doi.org/10.1080/1331677x.2022.2077789>
30. Kähkönen, T.: Remote work during the COVID-19 pandemic: identification of working life impacts, employees' data protection abilities and trust outcomes. *J. Organ. Change Manag.* **36**(3) (2023). <https://doi.org/10.1108/jocm-06-2022-0179>
31. Franken, E., Bentley, T., Shafaei, A., Farr-Wharton, B., Onnis, L., Omari, M.: Forced flexibility and remote working: opportunities and challenges in the new normal. *J. Manag. Organ.* **27**(6), 1–19 (2021)
32. van Zoonen, W., et al.: Factors influencing adjustment to remote work: employees' initial responses to the COVID-19 pandemic. *Int. J. Environ. Res. Public Health* **18**(13), 6966 (2021). Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8297254/>
33. Yaroshenko, O.M., Sirokha, D.Đ., Velychko, L.Y., Kotova, L.V., Sobchenko, V.V.: Current problems of legal regulation of remote work in the context of the introduction of restrictive measures caused by the spread of COVID-19 in Ukraine and the EU. *Relaç. Int. Mundo Atual* **1**(34), 1–16 (2022). [Online]. Available: <https://portaldeperiodicos.animaeducacao.com.br/index.php/RIMA/article/view/22464>. Accessed 03 July 2024
34. Kamruzzaman, A., Ismat, S., Brickley, J.C., Liu, A., Thakur, K.: A comprehensive review of endpoint security: threats and defenses. *IEEE Xplore*, 01 Dec 2022. <https://ieeexplore.ieee.org/abstract/document/9998470/>
35. Williams, R.I., Clark, L.A., Clark, W.R., Raffo, D.M.: Re-examining systematic literature review in management research: additional benefits and execution protocols. *Eur. Manag. J.* **39**(4) (2020). Available: <https://www.sciencedirect.com/science/article/abs/pii/S026323732030133X#:~:text=A%20systematic%20literature%20review%20provides,of%20transparency%20and%20bias%20reduction>
36. Oyewole, O.O., Fakeyede, O.G., Okeleke, E.C., Apeh, A.J., Adaramodu, O.R.: Security considerations and guidelines for augmented reality implementation in corporate environments. *Comput. Sci. IT Res. J.* **4**(2), 69–84 (2023). <https://doi.org/10.51594/csitrj.v4i2.607>

37. Rakha, N.A.: Ensuring cyber-security in remote workforce: legal implications and international best practices. *Int. J. Law Policy* **1**(3) (2023)
38. Dezvoltarea infrastructurii critice din punct de vedere al securității informațiilor. *Rev. Univ. Strateg.* **XIV**(53), 170–188 (2023). [Online]. Available: <https://www.cceol.com/search/article-detail?id=1107664>. Accessed 10 June 2023
39. Joseph, E.: Resilient infrastructure and inclusive culture in the era of remote work. In: *Advances in public policy and administration (APPA) book series*, pp. 276–299 (2024). <https://doi.org/10.4018/979-8-3693-2917-7.ch013>
40. Isakov, A., Urozov, F., Abduzhapporov, S., Isokova, M.: Enhancing cybersecurity: protecting data in the digital age. *Innov. Sci. Technol.* **1**(1), 40–49 (2024). Available: <https://innoist.uz/index.php/ist/article/view/153>
41. Kumari, P., Anand, A., Praveen, P., Verma, A.R., Godiyal, A.: Infrastructure potential and human-centric strategies in the context of industry 5.0. In: *Advances in web technologies and engineering book series*, pp. 199–214, 2024. <https://doi.org/10.4018/979-8-3693-0782-3.ch012>
42. Pusztahelyi, R., Stéfán, I.: Improving Industry 4.0 to Human-Centric Industry 5.0 in Light of the Protection of Human Rights, May 2024. <https://doi.org/10.1109/iccc62069.2024.10569569>
43. Greulich, M., Lins, S., Pienta, D., Thatcher, J.B., Sunyaev, A.: Exploring contrasting effects of trust in organizational security practices and protective structures on employees' security-related precaution taking. *Inf. Syst. Res.* (2024). <https://doi.org/10.1287/isre.2021.0528>
44. Zhao, T., Gasiba, T., Lechner, U., Pinto-Albuquerque, M.: Thriving in the era of hybrid work: raising cybersecurity awareness using serious games in industry trainings. *J. Syst. Softw.* **210**, 111946 (2024). <https://doi.org/10.1016/j.jss.2023.111946>

Generative Adversarial Networks (GAN) Insights for Cyber Security Applications



Mohammad Shahnawaz Shaikh 

Abstract The paper explores the architecture of Generative Adversarial Networks (GANs) and their use cases in various fields, particularly in cybersecurity. It highlights five key cybersecurity domains where GANs can significantly impact, including Deepfake creation, phishing, and anomaly detection. The study details current and potential GAN techniques that could be exploited for malicious activities. GANs consist of two models: the generator (G), which creates new instances from random noise, and the discriminator (D), which assess the generated sample's authenticity. While the discriminator gains the ability to discern between authentic fraudulent samples through feedback from the generator, the generator attempts to generate data that closely resembles the original dataset. This adversarial process keeps going until the generator generates samples that are identical to actual data. The generator aims to produce data that mimics the real dataset, while the discriminator learns to distinguish between real and fake samples based on feedback from the generator. This adversarial process continues until the generator produces samples indistinguishable from real data. After training, the generator transforms random input into a compressed representation that aligns with the data distribution of the training set. The model is then capable of generating new examples that mirror the acquired traits of the initial dataset. Both the authentic cases from the dataset and fictitious ones produced by the generator are used to train the discriminator. Once training is complete, the discriminator is no longer needed, as its primary role is to guide the generator during the training phase. A zero sum game is used to describe the relationship between the discriminator and generator, where the generator is penalized for producing detectable fake samples. As the training progresses, the discriminator becomes increasingly confused, indicating that the generator is successfully creating realistic outputs. A perfect equilibrium is not necessary for the generator to be effective, as useful models can still be developed without flawless performance. GANs can be categorized into supervised, unsupervised, and hybrid types, with various models like CGAN, DCGAN, and AAE falling into these categories. Each type has unique

M. S. Shaikh (✉)

Department of Artificial Intelligence and Data Science, Parul Institute of Engineering and Technology, Parul University, Vadodara, Gujarat 391760, India

e-mail: msnshaikh1@gmail.com

characteristics and applications, with some models designed for specific tasks such as image generation or semi-supervised learning. The study underscores the significant potential of GANs in cybersecurity applications, highlighting their ability to create new threats. It suggests that future research should explore the effectiveness of different GAN models for specific tasks to better understand their implications for security. A comprehensive understanding of GAN mechanisms is essential for developing defenses against emerging cyber threats, as outlined in the paper.

Keywords Generative adversarial networks · Cyber security applications

1 Introduction

Many real-world applications, including image production, video generation, domain adaptation, and picture super resolution, have benefited from the successful use of GANs [1]. In this study, the fundamental architecture of GAN will be presented. After that, a brief history of its technological developments will be covered, including the innovations of its various types, their techniques, model designs, and performance analyses. We've determined which five cyber security domains the development of GAN approaches can most significantly disrupt. These include Deepfake image creation, phishing, adversarial attacks, DDoS assaults, insider threats, anomaly detection, and audio and video production. The GAN techniques that are now in use or have the potential to be employed for these assaults were detailed in this research.

2 GAN Fundamentals

2.1 GAN Architecture

It was believed that the most effective discriminative models were those that could convert a high quality multidimensional, sensory information in to classification label [2]. However, in 2014, Good Fellow created Generative Adversarial Networks. Because these deep generative models could not mimic a huge number of unpredictable, stochastic computations, their impact was restricted. GANs were developed primarily to circumvent these issues. The generating model (G) and the discriminator model (D) are the two models that comprise GANs [3, 4]. Despite having a data distribution that is similar to the real dataset, the first attempts to establish new examples that are totally distinct from it by feeding it random noise [5]. The discriminator model determines whether the distributions come from the generator or the original dataset by estimating likelihood of samples. Since the actual dataset is not accessible to the generator, it gains knowledge from the discriminator's remarks [6]. However,

discriminators have the option to use both the genuine and fictitious samples. Below is a description of their workflow.

2.1.1 Generator

A random vector with a predetermined length that is selected from a Gaussian distribution is used by the generator model to initiate the generative process. After that, a sample in the domain is created using this random vector [7]. After training, this vector representation becomes a compressed form of the data distribution. Since, following training, the points in the issue domain will correspond with the points in the multidimensional vector space. The model is used to generate new examples after training get finished [8].

2.1.2 Discriminator

A discriminator is essentially a large classification model that predicts the authenticity or falsity of a given class. Using domain samples, this model makes predictions about the authenticity or fraud of an input. The genuine examples are collected from the training dataset itself, whereas the fake ones are contained in the generator's output. The discriminator is disposed of once the training process is over.

2.1.3 Two Player Game Representing GAN

Based on how the two GAN models operate, it can be concluded that the discriminator and generator are in competition with one another [9]. To put it another way, they are antagonistic in the sense of a game theory zero-sum game. It is likened to a zero-sum game because its model parameters don't change as long as the discriminator can accurately detect the bogus samples. However, when the model parameters are changed significantly, the generator is penalized [10]. When the generator deceives the discriminator, the opposite occurs. In Fig. 1, the entire process is displayed. The discriminator becomes perplexed and predicts "unsure" after repeating this process until a certain point because it is unable to distinguish the created images from the real ones. It's not always required to have this perfect situation in order to create a useful generator model [11].

3 Types of GAN

Two categories apply to generative adversarial networks. Traditional GAN and GAN learning with official discriminators are the two types of GANs as shown in Fig. 2.

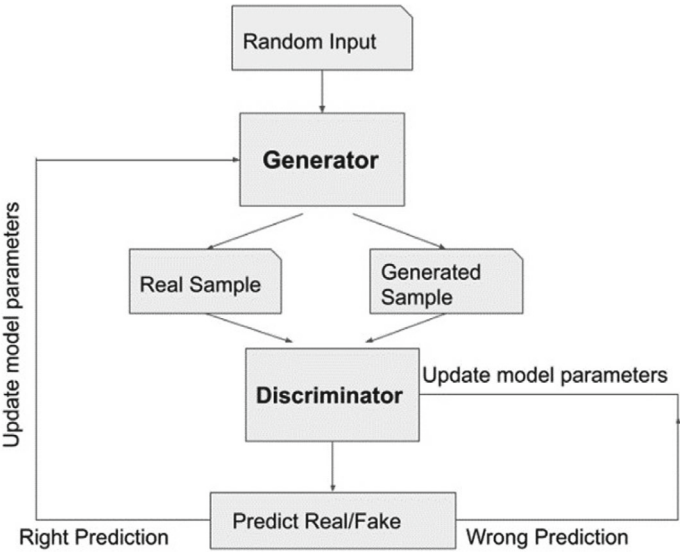
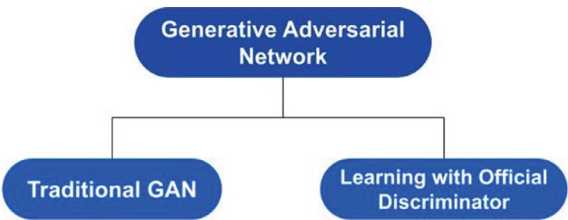


Fig. 1 Generative adversarial network architecture

Fig. 2 Classification of generative adversarial network



We have mostly concentrated on the conventional GANs in our review. Three categories can be distinguished amongst conventional GAN from the standpoint of the learning process, supervised, unsupervised, and hybrid GAN [12]. Figure 3 illustrates that the underlying GAN is a supervised technique. Supervised GAN are also available in CGAN, AAGAN, GRAN, and EvoGAN. Unsupervised generative adversarial networks include DCGAN, LAPGAN, ACGAN, InfoGAN, and CycleGAN. Adversarial Auto Encoders, or AAEs, are a type of Combined Generative Adversarial Network that may operate in three different modes, supervised, unsupervised, and semi supervised. There are supervised and unsupervised versions of BiGAN and DVDGAN. SRGAN is a different combination GAN that is partially supervised and unsupervised [13–15].

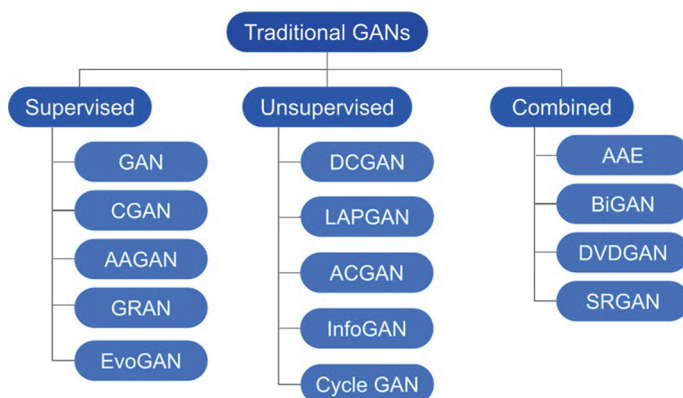


Fig. 3 Traditional GAN classification

3.1 CGAN

The outputs of basic GANs are not controllable. For instance, the items of a few categories (shoes, pants, etc.) may frequently be absent from the outputs of the GANs prepared on the MNIST fashion data. Conditional GANs overcome this restriction by conditioning the discriminator and generator concerning a supplementary variable (with particular information about the object, like labels etc.), thus the GAN outputs are subjected to human control. Consequently, tags that are absent entirely from the training set can be independently created using the CGAN model [16–20].

3.2 DCGAN

One of the popular, effective, and dynamic GAN architectures that Radford suggested is Deep Convolutional GAN. In place of a Multi-layered perceptron (MLP), convolutional networks are used to build DCGAN. Convnets employ a convolutional stride in place of pooling. Due to CNN's lack of classification capabilities, the last layers are not fully coupled. All layers use batch normalization, with the exception of the input layer of discriminator and output layer of generator. Tanh is utilized in the generator's output layer, whilst ReLU is employed in other layers to speed up the model's learning. DCGAN is a better suitable model for generic image representation challenges because to its stable architecture [21–25] (Fig. 4).

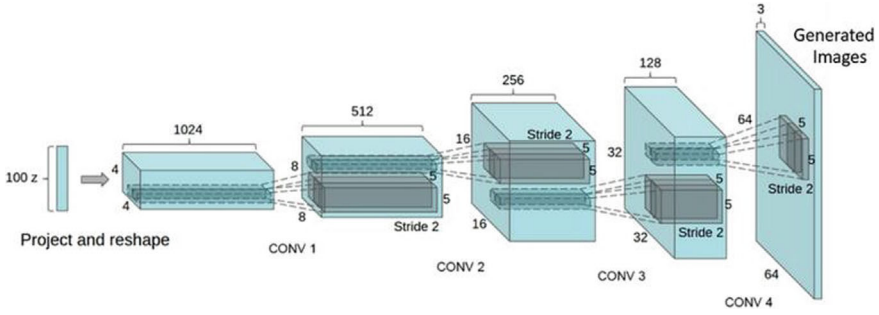


Fig. 4 DCGAN architecture

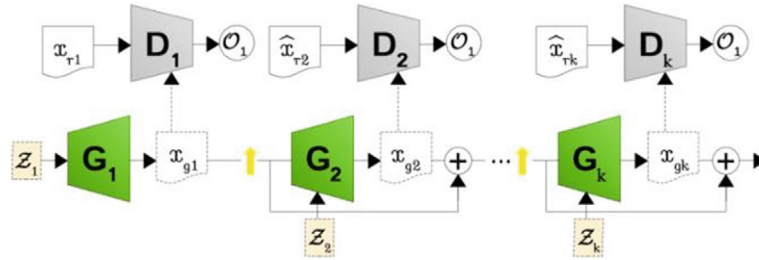


Fig. 5 Block diagram of LAPGAN mode, x_{r1} is indicating real sample, x_{rk} is indicating k th real residual, x_{gk} is representing generated sample and O_1 showing binary classification output (real/fake)

3.3 LAPGAN

A major focus for GAN development has been the accuracy of the output image quality, which comes after the improvement in model learning speed. Denton therefore suggested a generative parametric model that may generate excellent natural photos. Using a Laplacian pyramid structure and a cascade of convolutional networks, these images are produced in a rough to refined manner. Figure 5 depicts the model architecture, where a collection of generator and discriminator models are represented by the terms $G_1 - G_k$ and $D_1 - D_k$.

3.4 AAE

In order to attempt matching the accumulated subsequent to the auto encoder's concealed code vector with any earlier distribution, we can even use adversarial networks in conjunction with an automatic encoding to result variational inference [26, 27]. Applications for this include data visualization, unsupervised clustering,

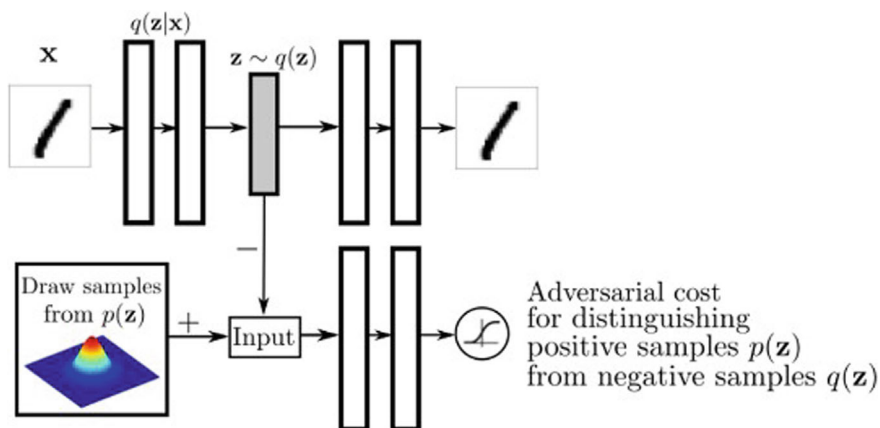


Fig. 6 Adversarial auto encoder basic architecture

semi-supervised classification, separating picture content from style, and dimension reduction.

An example of AAE architecture is presented in Fig. 6. Here, a latent coding z is used to reconstruct picture x in the upper row [28]. The lower row is used to predict if a sample originates from a user-specified sampled distribution or from the auto-encoder's hidden code.

3.5 ACGAN

ACGAN is an extension of CGAN that modifies the discriminator to give labels to the classes for an input image instead of receiving it as input. It stabilizes the learning process's effect and enables the creation of high-quality images. The modifications made to the ACGAN discriminator are displayed in Fig. 7.

3.6 LSGAN

LSGAN that makes use of the least square loss function of the discriminator. The cross entropy loss function associated with sigmoid function employed in regular GANs causes problems with disappearing gradients with learning process, but the decrease in objective function of an LSGAN lowers the Pearson divergence [29].

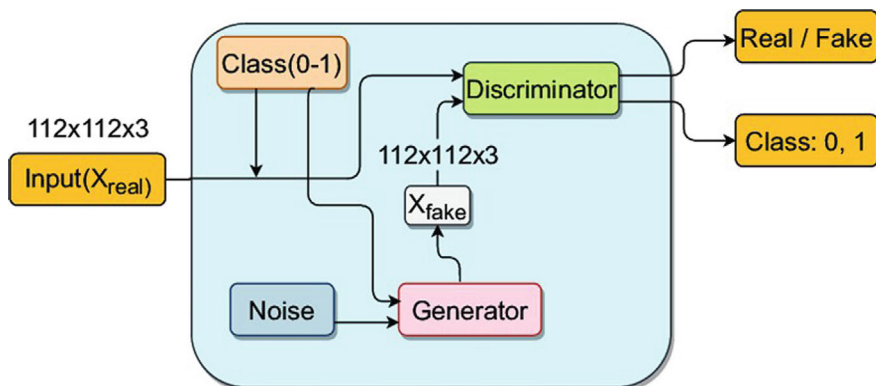


Fig. 7 ACGAN schematic diagram

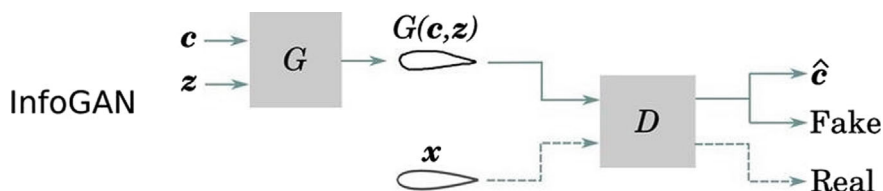


Fig. 8 InfoGAN block diagram

3.7 InfoGAN

It is a more sophisticated form of GAN that uses an unsupervised method to control and detangle the attributes of the images it generates. For this reason, in order to produce fraudulent images, more information must be fed in addition to random noise. This data ought to be connected to the kinds of attributes that are wanted (Fig. 8).

3.8 H. GRAN

A different encoder decoder based GAN known as Generative Recurrent Adversarial Networks (GRAN) demonstrated that convolutional networks may produce high-quality visual images by matching features between pixels [30].

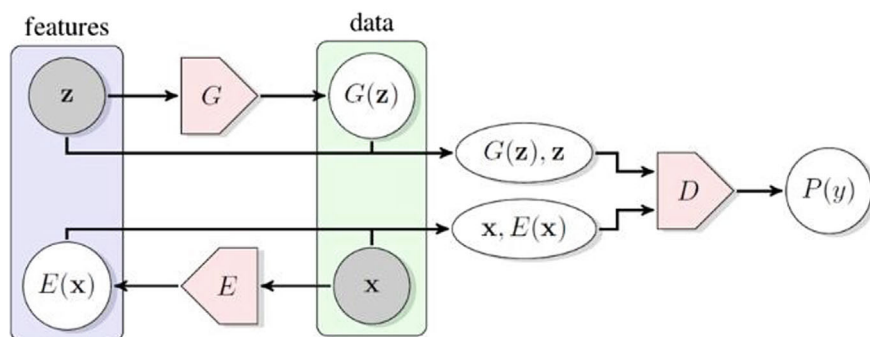


Fig. 9 The structure of BiGAN

3.9 BiGAN

In a particular kind of generative adversarial network that Donahue proposed, a generator performs both the inverse mapping from input to the latent representation and the mapping of latent samples to create data. Rich presentations have been designed for use in applications like unsupervised learning (Fig. 9).

3.10 CycleGAN

In order to address the issue of image-to-image translation limitations or nonexistence of paired datasets, CycleGAN was introduced in 2017 and has since been deemed an effective method. Figure 10 illustrates its design, which consists of the simultaneous training of two discriminator models and two generator models.

3.11 SRGAN

In order to detect classes that are not visible, SR (Semantic Rectifying) GAN is proposed as a way to rectify the semantic space driven by the visual space and prevent overlapping across different picture classes. Pretrained Semantic Rectifying Networks (SRNs) are required in order to correct semantic space that exhibits semantic loss and rectifying loss. Its primary purpose is to improve visibility of the image by performing Domain Transformation, which transforms images from low to high resolution. It has a significant impact on CCTV footage because of this. After being divided into smaller segments, low-resolution photos are run through SRGAN. The photos are then combined to create a single, whole image. The final action

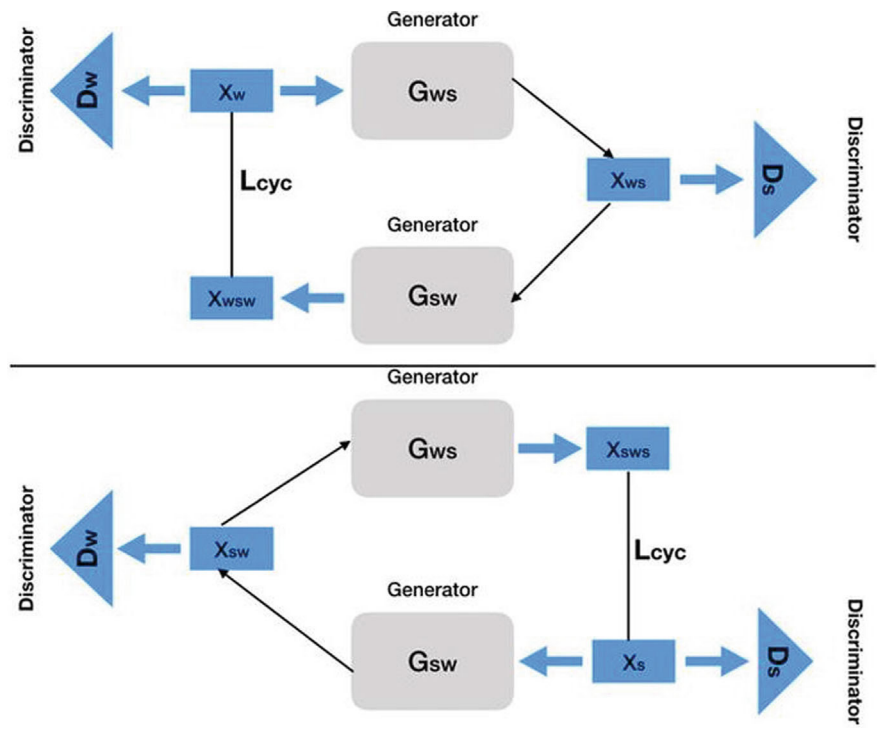


Fig. 10 CycleGAN architecture

involves applying the contrast limited adaptive histogram equalization (CLAHE) filter on the contrast equalized image.

3.12 DVD-GAN

Inspired by the technology’s success with natural images, GAN is utilized in video modeling using DVD (Dual Video Discriminator), which is based on the BiGAN architecture. This model, which is depicted in Fig. 11, uses two discriminators. The discriminators in terms of space and time. The system was trained using the intricate Kinetics-600 dataset, yielding higher-fidelity and more intricate video samples than those found in earlier research [31].

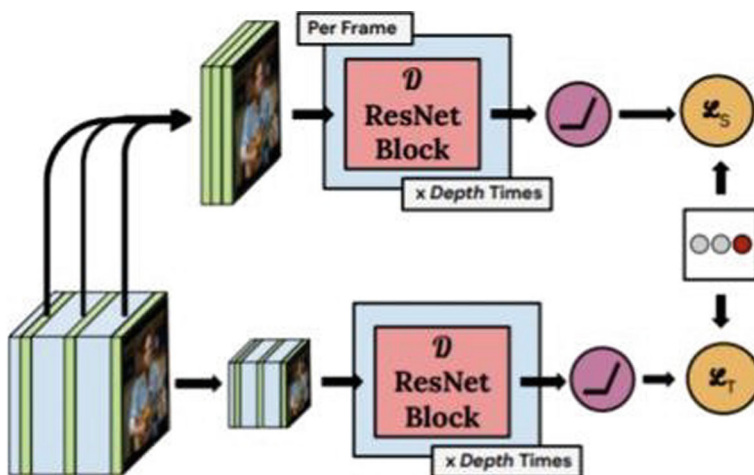


Fig. 11 Spatial discriminator (D_s) and temporal discriminator (D_t) of DVDGAN

3.13 EvoGAN

It describes a system capable of generating a wide range of human gesture with any required level of accuracy and diversity. It needs an image and a set of seven lengths, where each one represents a distinct feeling: fear, anger, contempt, happiness, sadness, surprise, or neutrality. In order to express its search for target outcomes in the distribution of GAN-learned data, EA uses the Face Action Coding System, or FACS. In the evaluation phase shown in Fig. 11, a trained GAN creates human faces that can be identified by a classifier with prior training. Following an assessment of the generated image's expression and how far it deviates from the intended expression, computed and regarded as the ultimate fitness score. That would be the final output once the desired population has been reached for fitness (Fig. 12).

4 Use Cases of Various GANs in Cyber Security

While GAN finds extensive use in computer vision, it also finds extensive application in cyber security. The identification of different cyberattacks, like denial of service (DoS), distributed DoS, anomaly detection, phishing, Man-in-the-Middle (MitM), injection assaults, etc., has become simpler with the usage of various generative adversarial networks. We have gone over a few of these jobs where GAN was utilized in our review.

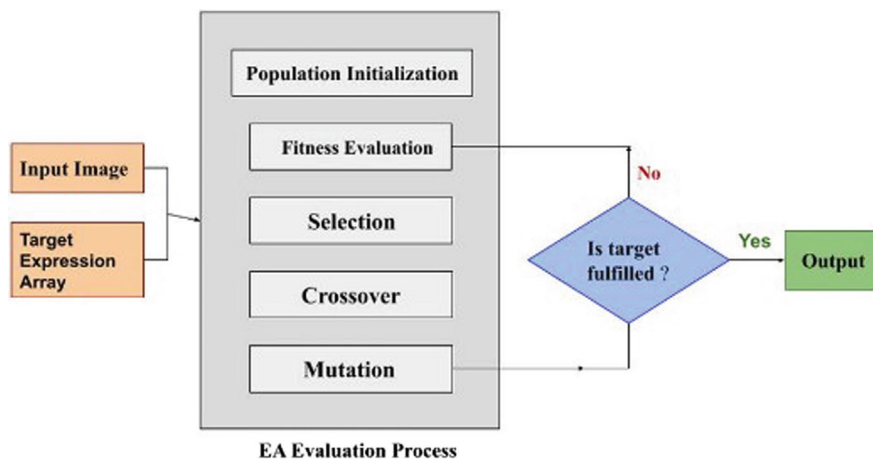


Fig. 12 Architecture of EvoGAN

4.1 Anomaly Detection

Data patterns in a data distribution that deviate from the dataset's typical behavior are referred to as anomalous data. The anomaly detection aims to find those unusual data so that serious problems like bank fraud, structural flaws, technical malfunctions, and security lapses can be addressed. Even though supervised and unsupervised traditional approaches are widely employed for anomaly detection, they are not without limits. More specifically, because labeled data is limited, supervised techniques cannot fully utilize large amounts of data information. Furthermore, there are a number of unsupervised techniques that are still unable to fully take use of the spatial temporal connection, dependencies between variables. In this instance, GAN became of excellent use in identifying anomalies. Adversarial learnt features are derived for the task, bidirectional GAN based adversarial learned anomaly detection approach (ALAD). Reconstruction mistakes are then utilized to determine anomalous data based on these attributes. The same author has created an auto-encoder for training alongside the developed GAN approaches in another paper, which focuses on anomaly detection. Another GAN based anomaly detection technique features two distinct discriminators one for ordinary input and the other for anomalous input and also use an auto encoder as the generator. Following the combination of their recently proposed loss functions, anomalously adversarial loss and patch loss, it also performed some optimization training on their model.

A different GAN based model, MAD-GAN, was effectively proposed to report abnormalities that were brought on by certain cyberattacks. By taking into account every variable simultaneously, this model, which employed Long Short Term Memory Recurrent Neural Networks (LSTM-RNN) as its foundational model, was capable of capturing the implicit relationships between the variables. Additionally, there are several works that support anomaly detection even though they do not

directly align with it. One kind of model called FenceGAN modifies the GAN loss so that the instances it generates stay inside the bounds of the actual data distribution. Therefore, it stops the production of abnormal data.

4.2 Intrusion Detection with Distributed Denial of Service (DDoS)

A denial-of-service (DDoS) attack occurs when a host's connection to its network is interrupted by sending an excessive number of requests to the targeted computer. This overloads the system, rendering it temporarily or permanently inaccessible to its authorized users. These days, it poses a serious risk to the integrity and security of computer networks. Many machine learning (ML) based network intrusion detection systems (NIDS) have been created in recent years in an attempt to thwart this attack. One of the most frequent flaws in these methods is the creation of manipulated input data that tricks classification and prediction algorithms. Several scholars have proposed adversarial training as a way around this. In order to create adversarial DDoS instances for training data to identify both SYN and HTTP flood attacks, Abdelaty's GADoT system used a GAN. This training model differs from other similar approaches in that it is evaluated without the victim model's knowledge, resulting in an F1 score of above 98% and FNR decreases below 1.8%.

When a DDoS attack is adversarial, GAN is also employed in its detection. Due to the low performance of DL based detection systems in the event of adversarial attacks. In order to detect UDP flood assaults in Software Defined Networks (SDNs), there is a system in which they compared the output of CNN, LSTM, and MLP neural networks with different datasets, using GAN to optimize the model employed in the system. An additional SDGAN model addresses adversarial DDoS attack issues as well. It has two symmetric discriminators that can detect adversarial DDoS traffic at the same time, and it was trained using CycleGAN adversarial DDoS data. With a True Positive Rate (TPR) of 87.2%, it surpassed the other ML based models that it was assessed against, demonstrating its capacity for protection.

4.3 Phishing

Phishing is a type of cybercrime wherein malevolent actors pose as reputable companies and send targeted emails or texts containing sensitive information, such as banking and credit card credentials. While machine learning algorithms show great promise in stopping phishing assaults, their effectiveness is limited because training data is a major factor in determining the efficiency of ML algorithms. Since adversarial approaches can supplement existing datasets, they have been utilized extensively to alleviate this constraint. From phishing websites Adversarial Auto encoder

(AAE) could produce samples that can be employed to train their model in order to increase the detection accuracy.

Unbalanced data classification is a problem for machine learning algorithms, as most phishing detection techniques fail to recognize the unbalanced character of phishing email datasets. In order to affect categorization, LeakGAN created new artificial instances in order to equilibrate the training procedure. These artificial cases were included in the first unbalanced training set, which was then given for sequence classification to the BERT model, leading to a 99.6% increase in the F1 score.

4.4 Adversarial Input (Image) Generation

Evasion-based attacks on AI systems are generated via GAN approaches; some of these techniques are briefly explained in this section. Adversarial attacks can also be produced by modifying these methods. With GAN, a wide variety of images have been produced. For instance, a number of generators might produce separate images before synthesizing the full image of Hanock's suggested composite model. Furthermore, the state of the art outcomes were attained by synthesizing the front side face photo through the side face photographs throughout the face generation process in TPGAN. In order to fine-tune it to obey a simple truncation, BigGAN later changed it by performing orthogonal regularization. In comparison to the previous best model, this produced a superior Frechet Inception Distance (FID) of 9.6 and IS (inception score) of 166.3.

Table 1 illustrates how the FineGAN model outperforms the CUB 128×128 model when applied to the Stanford Dogs dataset, with a lower FID score of 11.25 as well as higher IS score of 52.53. Additionally, the CUB 128×128 model exhibiting better performance in association with InfoGAN model (i.e. IS 47.32 FID 25.66) than it does with the datasets for the Dogs (i.e. IS 43.16 FID 29.34) and Stanford Cars (i.e. IS 28.62 FID 17.63). The FID of 9.5 for the "WGAN-GP + TT Update Rule" model using "LSUN Bedroom 64×64 " is lower than that of the dataset CIFAR-10 (i.e. FID 24.8). Moreover CIFAR-10 functions better in association with the SS-GAN model (i.e. FID 15.65). Generative Adversarial Networks (GANs) are used by Natural GAN (NGAN) to reduce the distance between the inner representations of heterogeneous adversarial assault samples.

CycleGAN is used to convert images, such as changing a sobbing face into a cheerful one or a horse into a zebra. There is a classification score of 59.5 reported using the object transfiguration dataset. Then, an expansion of CycleGAN called StarGAN is suggested, wherein this is used to train one category to another. With a classification score of 78.1%, we can conclude that, out of all the models in Table 2, instaGAN, and an instance aware GAN, performs the best. When it comes to unsupervised image-to-image translation tasks, DTN has the highest classification accuracy of 84.4% when utilizing the SVNH to MNIST dataset, followed by ADDA with 76.0% accuracy using the same dataset.

Table 1 Benchmark analysis using different GAN models on different datasets for image generation

Dataset	Model	Metric name	Metric value
CUB 128×128	FineGAN	FID	11.25
		IS	52.53
Stanford dogs	FineGAN	FID	25.66
		IS	46.92
CUB 128×128	InfoGAN	FID	13.2
		IS	47.32
Stanford cars	InfoGAN	FID	17.63
		IS	28.62
Stanford dogs	InfoGAN	FID	29.34
		IS	43.16
CIFAR-10	WGAN-GP + TT update rule	FID	24.8
LSUN bedroom 64×64	WGAN-GP + TT update rule	FID	9.5
CIFAR-10	Improved GAN	IS	6.86
CelebA-HQ 128×128	SS-GAN (sBN)	FID	24.36
CIFAR-10	SS-GAN (sBN)	FID	15.65
ImageNet 128×128	SS-GAN (sBN)	FID	43.87
LSUN bedroom 256×256	SS-GAN (sBN)	FID	13.3
CAT 256×256	RaSGAN	FID	32.11
CIFAR-10	RSGAN-GP	FID	25.6

Table 2 The task of BENCHMARK analysis and transcription

Translation type	Dataset	Model	Metric name	Metric value
Unsupervised image-to-image translation	SVNH-to-MNIST	DTN	Classification accuracy	84.40%
Image-to-image translation	Object transfiguration (sheep-to-giraffe)	InstaGAN	Classification score	78.1
Image-to-image translation	Object transfiguration (sheep-to-giraffe)	CycleGAN	Classification score	59.4
Unsupervised image-to-image translation	SVNH-to-MNIST	ADDA	Classification accuracy	76.0%
Image-to-image			PSNR	10.769
Translation			SSIM	0.1757

Table 3 Benchmark analysis for superior resolution and reconstruction work

Dataset	Model	Metric name	Metric value
BSD100—4x upscaling	SRGAN + residual-in-residual dense block	PSNR	27.85
		SSIM	0.7455
FFHQ 256 × 256 4x upscaling	ESRGAN	FID	166.36
		MS-SSIM	0.747
		PSNR	15.43
		SSIM	0.267
Manga 109-4x upscaling	Bicubic	PSNR	24.89
		SSIM	0.7866
Manga 109-4x upscaling	SRGAN + residual-in-residual dense block	PSNR	31.66
		SSIM	0.9196
PIRM-test	ESRGAN	NIQE	2.55
Set 14-4x upscaling	SRGAN + residual-in-residual dense block	PSNR	24.89
		SSIM	0.7917
Urban 100-4x upscaling	SRGAN + residual-in-residual dense block	PSNR	27.03
		SSIM	0.8153
Urban 100-4x upscaling	Bicubic	PSNR	23.14
		SSIM	0.6577

GANs are often employed to increase image resolution and generate previously unheard of levels of quality in images. Karras proposed a new training process in which new layers are gradually added from a low resolution to build the discriminator and generator, increasing the model's speed and stability. Subsequently, SRGAN gained an adversarial loss component to improve its performance. Table 3 displays the SRGAN performance utilizing the residual-in-residual dense block on various datasets. It works well with the Manga 109-4x upscaling dataset because its SSIM (0.9196) and PSNR (31.66) are both the highest.

After then, the performance of urban 100-4x upscaling and BSD100-4x upscaling differs little, with SSIM 0.7455 and 0.8153 and PSNR 27.85 and 27.03, respectively. Finally, the Set 14-4x upscaling dataset has a higher SSIM (0.7917) than the BSD100-4x upscaling alone, but a lower PSNR (24.89) than the preceding ones. Bicubic outperforms the other two models, ESRGAN and Bicubic, with a higher PSNR. Different GANs have been created with the specific goal of image style in mind [32].

4.5 Deepfake Video Generation

Deepfake multimedia, which can elude biometric authentication systems, can be produced using GAN. The GAN methods used to create Deepfake videos will be

covered in this section. GANs are quite useful for simulating and comprehending videos. Venric demonstrated a model that generated 64×64 video at a maximum frame rate of one second in 32 frames per second, outperforming simple baselines. Additionally, this model has the ability to identify behaviors with less oversight. A distinct generative model called TGAN was created in order to exploit this and learn the semantic representation of videos without labels. Generators come in two forms [33]. A temporal generator is one of them; it takes an input and utilizes it to create a set of latent variables as the output. Each of the variables represents a single frame of an image in a video. An additional one is a picture generator that uses a set of such latent variables to generate video. Table 4 demonstrates that, for both combinations “UCF-101 16 frames, 64×64 , unconditional” and “UCF-101 16 frames, Unconditional, Single GPU,” TGAN with singular value clipping (TGAN-SVC) yields a higher inception score of 11.85 than TGAN alone (9.18).

Video prediction, or foretelling the next frames in a video sequence, is one of the most important uses of GANs. Mathieu applies GAN for the first time in this challenge. In this process, the generator may forecast the final frame of the video by using the frame sequences that came before it. For the same objective, Sandra developed another model, FutureGAN, which did not require any additional constraints or conditions particular to the dataset. It achieved such competitive outcomes in video prediction, matching the state-of-the-art across a variety of datasets. A different model, VPGAN, is likewise able to create fictitious films of any object moving in a specific direction [34]. It is suggested for stochastic video prediction. By using the UCF101 dataset, FREGAN provides both a high refresh rate and a high frame rate, forecasting future video frames by analyzing a sequence of past frames. This model provides a peak signal-to-noise ratio (PSNR) of 34.94. Additionally, it displayed a 0.95 SSIM (Structural Similarity Index).

Table 4 Analysis of benchmarks for diverse video-related GAN uses

Task	Dataset	Model	Metric name	Metric value
Video generation	UCF-101 16 frames. 64×64 , unconditional	TGAN-SVC	Inception score	11.85
Video generation	UCF-101 16 frames, unconditional, single GPU	TGAN-SVC	Inception score	11.85
Video frame prediction	UCF101	FREGAN	PSNR	34.94
			SSIM	0.95
Monocular 3D human pose estimation	Human3.6M	VIBE	Average MPJPE (mm)	65.6
3D human pose estimation	3DPW	VIBE	PA. MPJPE	55.9
			MPJPE	93.5
			MPVPE	113.4
			FLOPs (G)	4.17

The creation of precise natural motion sequences is greatly aided by GANs. In order to distinguish between human motion and motions produced by networks of temporal pose and form regression, VIBE (Video Inference for Body Pose and form Estimation) was developed. The VIBE model had been used in a number of experiments. Table 4 displays the outcomes of two of these methods: 3D Human Pose Estimation using 3DPW dataset and Monocular 3D Human Pose Estimation using Human3.6M dataset.

5 Conclusion

In order to present a comparative analysis of Generative Adversarial Networks, we have examined and reviewed them along with their different varieties in this article. To give you an idea of their developments in numerous disciplines, we have also included a wide range of their applications. We have also demonstrated how GANs have a great potential for the use in applications pertaining to cyber security. It is evident from looking at their applications that different kinds of GAN models can be applied to comparable jobs. In order to determine which model is best for a given task, it is possible to do the same work using many models later on. We have discussed in this study how various GAN approaches may provide new cybersecurity challenges. For instance, GAN can be used to create adversarial input to weaken AI systems, create Deepfake photos and videos by getting past authentication systems, and build effective DDoS assaults, phishing emails, and other types of attacks. From the standpoint of cyber security, developing a suitable defense against these novel threats would also necessitate a thorough comprehension of the various GAN models' operational mechanisms and the ways in which they produce these vulnerabilities. We have provided a quick GAN analysis in this study to help cyber security researchers investigate and comprehend the latest difficulties.

References

1. Zenati, H., Romain, M., Foo, C.-S., Lecouat, B., Chandrasekhar, V.: Adversarially learned anomaly detection. In: 2018 IEEE International Conference on Data Mining (ICDM), pp. 727–736 (2018)
2. Ye, Z., Lyu, F., Li, L., Fu, Q., Ren, J., Hu, F.: SR-GAN: semantic rectifying generative adversarial network for zero-shot learning. In: 2019 IEEE International Conference on Multimedia and Expo (ICME), pp. 85–90 (2019)
3. Shirazi, H., Muramudalige, S.R., Ray, I., Jayasumana, A.P.: Improved phishing detection algorithms using adversarial autoencoder synthesized data. In: 2020 IEEE 45th Conference on Local Computer Networks (LCN), pp. 24–32 (2020)
4. Shieh, C.-S., Nguyen, T.-T., Lin, W.-W., Lai, W.K., Horng, M.-F., Miu, D.: Detection of adversarial DDoS attacks using symmetric defense generative adversarial networks. *Electronics* **11**(13) (2022)

5. Qachfar, F.Z., Verma, R.M., Mukherjee, A.: Leveraging synthetic data and PU learning for phishing email detection. In: *Proceedings of the Twelfth ACM Conference on Data and Application Security and Privacy, CODASPY'22*, pp. 29–40. Association for Computing Machinery, New York, NY (2022)
6. Nugraha, B., Kulkarni, N., Gopikrishnan, A.: Detecting adversarial DDoS attacks in software-defined networking using deep learning techniques and adversarial training. In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 448–454 (2021)
7. Ngo, P.C., Winarto, A.A., Kou, C.K.L., Park, S., Akram, F., Lee, H.K.: FenceGAN: towards better anomaly detection. In: *2019 IEEE 31st International Conference on Tools with Artificial Intelligence (ICTAI)*, pp. 141–148 (2019)
8. Ledig, C., Theis, L., Huszár, F., Caballero, J., Cunningham, A., Acosta, A., Aitken, A., Tejani, A., Totz, J., Wang, Z., Shi, W.: Photo-realistic single image super-resolution using a generative adversarial network. In: *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 105–114 (2017)
9. Kocabas, M., Athanasiou, N., Black, M.J.: Vibe: video inference for human body pose and shape estimation. In: *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 5253–5263 (2020)
10. Abdelaty, M., Scott-Hayward, S., Doriguzzi-Corin, R., Siracusa, D.: GADoT: GAN-based adversarial training for robust DDoS attack detection. In: *2021 IEEE Conference on Communications and Network Security (CNS)*, pp. 119–127 (2021)
11. Cherian, A.K., Poovammal, E., Rathi, Y.: Improving image resolution on surveillance images using SRGAN. In: Suma, V., Chen, J.I.-Z., Baig, Z., Wang, H. (eds.) *Inventive Systems and Control*, pp. 61–76. Springer Singapore, Singapore (2021)
12. Hinton, G., Deng, L., Yu, D., Dahl, G.E., Mohamed, A.-R., Jaitly, N., Senior, A., Vanhoucke, V., Nguyen, P., Sainath, T.N., Kingsbury, B.: Deep neural networks for acoustic modeling in speech recognition: the shared views of four research groups. *IEEE Signal Process. Mag.* **29**(6), 82–97 (2012)
13. Hu, Z., Wang, J.T.L.: Generative adversarial networks for video prediction with action control. In: El Fallah Seghrouchni, A., Same, D. (eds.) *Artificial Intelligence. IJCAI 2019 International Workshops*, pp. 87–105. Springer International Publishing, Cham (2020)
14. Asghar, M.R., Hu, Q., Zeadally, S.: Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Comput. Netw.* **165**, article no. 106946 (2019)
15. Upadhyay, D., Sampalli, S.: SCADA (supervisory control and data acquisition) systems: vulnerability assessment and security recommendations. *Comput. Secur.* **89**, article no. 101666 (2020)
16. Xu, Y., Yang, Y., Li, T., Ju, J., Wang, Q.: Review on cyber vulnerabilities of communication protocols in industrial control systems. In: *IEEE Conference on Energy Internet and Energy System Integration (EI2)*, pp. 1–6. IEEE, Beijing, China (2017)
17. Carvalho, L.K., Wu, Y.C., Kwong, R., Lafortune, S.: Detection and mitigation of classes of attacks in supervisory control systems. *Automatica* **97**, 121–133 (2018)
18. Jakovljevic, Z., Lesi, V., Pajic, M.: Attacks on distributed sequential control in manufacturing automation. *IEEE Trans. Ind. Inf.* **17**(2), 775–786 (2021)
19. Elnour, M., Meskin, N., Khan, K., Jain, R.: A dual-isolation-forests based attack detection framework for industrial control systems. *IEEE Access* **8**, 36639–36651 (2020)
20. Al-Abassi, A., Karimipour, H., Dehghantanha, A., Parizi, R.M.: An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access* **8**, 83965–83973 (2020)
21. Gauthama Raman, M.R., Somu, N., Mathur, A.: A multilayer perceptron model for anomaly detection in water treatment plants. *Int. J. Crit. Infrastruct. Prot.* **31**, article no. 100393 (2020)
22. Kravchik, M., Shabtai, A.: Detecting cyber attacks in industrial control systems using convolutional neural networks. In: *Proceedings of CPS SPC 18 Conference*, Toronto, Canada, Oct 2018, pp. 72–83
23. Gupta, S., Arshi, O., Aggarwal, A.: Wireless hacking. In: *Perspectives on Ethical Hacking and Penetration Testing*, pp. 382–412. IGI Global (2023)

24. Shaikh, M.S., Ali, S.I., Deshmukh, A.R., Chandankhede, P.H., Titarmare, A.S., Nagrale, N.K.: AI business boost approach for small business and shopkeepers: advanced approach for business. In: Ponnusamy, S., Assaf, M., Antari, J., Singh, S., Kalyanaraman, S. (eds.) *Digital Twin Technology and AI Implementations in Future-Focused Businesses*, pp. 27–48. IGI Global (2024). <https://doi.org/10.4018/979-8-3693-1818-8.ch003>
25. Ali, S.I., Kale, G.P., Shaikh, M.S., Ponnusamy, S., Chouhan, P.S.: AI applications and digital twin technology have the ability to completely transform the future. In: Ponnusamy, S., Assaf, M., Antari, J., Singh, S., Kalyanaraman, S. (eds.) *Harnessing AI and Digital Twin Technologies in Businesses*, pp. 26–39. IGI Global (2024). <https://doi.org/10.4018/979-8-3693-3234-4.ch003>
26. Shaikh, M.S., Chandrawat, U.B., Choudhary, S.M., Ali, S.I., Ponnusamy, S., Khan, R.A., Sheikh, A.G.: Harnessing logistic industries and warehouses with autonomous carebot for security and protection: a smart protection approach. In: Ponnusamy, S., Assaf, M., Antari, J., Singh, S., Kalyanaraman, S. (eds.) *Harnessing AI and Digital Twin Technologies in Businesses*, pp. 239–257. IGI Global (2024). <https://doi.org/10.4018/979-8-3693-3234-4.ch017>
27. Arshi, O., Chaudhary, A.: Fortifying the internet of things: a comprehensive security review. *EAI Endors. Trans. Internet Things* **9**(4), e1 (2023)
28. Shaikh, M.S., Ponnusamy, S., Ali, S.I., Wanjari, M., Mungale, S.G., Ali, A., Baig, I.: AI-based advanced surveillance approach for women’s safety. In: Ponnusamy, S., Bora, V., Daigavane, P., Wazalwar, S. (eds.) *Wearable Devices, Surveillance Systems, and AI for Women’s Wellbeing*, pp. 13–25. IGI Global (2024). <https://doi.org/10.4018/979-8-3693-3406-5.ch002>
29. Mungale, S.G., Mungale, N.G., Shaikh, M.S., Mungale, S.G., Wazalwar, S.S., Wanjari, M.M., Jichkar, R.A.: Safeguard wrist: empowering women’s safety. In: Ponnusamy, S., Bora, V., Daigavane, P., Wazalwar, S. (eds.) *Wearable Devices, Surveillance Systems, and AI for Women’s Wellbeing*, pp. 192–205. IGI Global (2024). <https://doi.org/10.4018/979-8-3693-3406-5.ch012>
30. Arshi, O., Gupta, G., Aggarwal, A.: IoT forensics. In: *Advanced Techniques and Applications of Cybersecurity and Forensics*, pp. 57–81. Chapman and Hall/CRC (2024)
31. Kitey, H., Chandankhede, P., Jajulwar, K., Shaikh, M.S., Fatinge, P.M.: Solar power generation technique and its challenges—a comprehensive review. *Grenze Int. J. Eng. Technol.* Grenze ID: 01.GIJET.10.1.122. Grenze Scientific Society (2024)
32. Chopkar, P., Wanjari, M., Jumle, P., Chandankhede, P., Mungale, S., Shaikh, M.S.: A comprehensive review on cotton leaf disease detection using machine learning method. *Grenze Int. J. Eng. Technol.* Grenze ID: 01.GIJET.10.2.537. Grenze Scientific Society (2024)
33. Arshi, O., Chaudhary, A.: Intelligence (AGI). In: *Artificial General Intelligence (AGI) Security: Smart Applications and Sustainable Technologies*, p. 1 (1990)
34. Sheikh, M.S., et al.: Harnessing logistic industries using autonomous carebot for smart surveillance, protection and security. In: Al-Turjman, F. (eds.) *The Smart IoT Blueprint: Engineering a Connected Future. AIOSS 2024. Advances in Science, Technology & Innovation*. Springer, Cham (2024). https://doi.org/10.1007/978-3-031-63103-0_20

Future Emerging Challenges and Innovations in Next Gen-Cybersecurity and Information Systems Security



Umna Iftikhar, Huma Rashid, and Hafiz Muhammad Attaullah

Abstract Within the dynamic realm of cybersecurity, this research investigates the critical need to safeguard private information and vital infrastructure from a growing variety of cyberattacks. In the extensive usage of IoT devices that has made these threats, in which it includes sophisticated phishing attacks and the pervasive ransomware, worse. The conversation highlights how crucial it is to improve conventional security measures while the utilizing cutting-edge technology like artificial intelligence (AI) for real-time threat identification and reaction. To setup and successfully manage the complexity of digital transformation, it also promotes proactive tactics like strong risk mitigation frameworks and the ongoing monitoring. The dynamics facilitate a cross the sector and worldwide collaboration to exchange intelligence about threats and the use of strict security architectures, including zero-trust models and DevSecOps. In order to fortify international defenses, anticipate new threats, and prepare for a robust digital future, the study intends to cultivate these alliances and implement cutting-edge methods.

Keywords Cybersecurity challenges · Next-generation defense strategies · AI in threat detection · Proactive risk management · Digital transformation resilience

1 Introduction

Modern societies now rely heavily on cybersecurity to protect everything from sensitivities the personal information to vital infrastructures. As of now the dependence on digital technologies grows, so it does the complexity of cyber threats. These can now

U. Iftikhar (✉)

Faculty of Engineering Science and Technology, Iqra University, Karachi, Pakistan

e-mail: yamnaiftikhar@gmail.com

H. Rashid · H. M. Attaullah

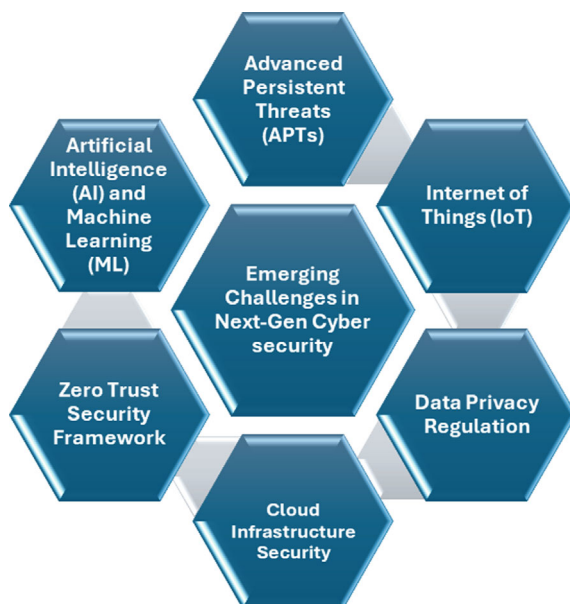
Faculty of Computing, Mohammad Ali Jinnah University, Karachi, Pakistan

take many forms, from intricate phishing schemes to ransomware attacks. Cybercriminals now have more points of entry into networks than ever before, thanks to the Internet of Things (IoT) widespread adoption of Internet-connected gadgets, which has increased the attack surface. Strategies for cybersecurity in the future must change to fully address these issues, future cybersecurity strategies must change. In order to identify the irregularities and react to the threats instantly, it is also necessary to use cutting-edge technology like artificial intelligence in addition to strengthening conventional defenses [1]. International and cross-sector collaboration is now essential for firms to keep ahead of cyber threats. The sharing of intelligence on threats, and the best practices enables a better coordinated defense against international cyberattacks. Enterprises, government, and cybersecurity expert must collaboratively develop and implement policies that encourage cybersecurity resilience while upholding the people's rights to privacies and data protections [2]. We can manage the complexity of contemporary cybersecurity and guarantees the safe digital future for everybody by adopting these principles and responsibly utilizing cutting-edge technologies. Moreover, the advents of DevSecOps techniques and cloud-native securities architectures has completely now changed however enterprises handle security in dynamics, agile developments environment [3]. DevSecOps ensures seamless integration of security issues into the software development lifecycle, from conception to deployment, and beyond. This strategy uses automatic testing for security, ongoing surveillance, and remediation to improve application resilience while facilitating a quick reaction to new threats [4]. At the same time, identity-centric security models and zero-trust architecture have completely changed the way people think about network security by focusing on strict access controls and ongoing authentication. Zero-trust necessitates ongoing identity and device verification for any device attempting to access resources, as it anticipates that threats can come from within as well as outside the network boundary. This proactivist approach reduces the attack surfaces and, restricts lateral movement, and the fortifies security measures against complex cyber threats in the event of a breach. The Communication and cooperation across industries and geographic boundaries are becoming more and more important as firms navigate the constantly changing cyber threat landscape [5].

2 Emerging Challenges in Next-Gen Cyber Security

But since technologies and advancement so quickly, these new threats are appearing in the jeopardize so the integrity of our information system [6]. The spread of Internet of Things (IoT) devices, with greatly expands the attack surface for cybercriminals, is one of the main causes for concern. Further, it is increasing the prevalence of cyberattacks utilizing the artificial intelligence (AI) and the machine learning (ML) that has complicated the threat detection and response processes. In addition of new vulnerabilities have emerged due to the Bring Your Own Device (BYOD) movement and the growing dependence on cloud-based services [7]. Figure 1 describes the environment that next-generation cybersecurity must negotiate: complex dangers,

Fig. 1 Sophisticated dangers, such as AI-driven assaults and Advanced Persistent Threats, must be avoided by next-generation cybersecurity. Robust, adaptive security solutions are becoming more and more necessary as IoT devices proliferate and create increasingly complex digital ecosystems



such as sophisticated persistent threats and assaults powered by AI. It becomes more and more important to have strong, and flexible security measures for IoT devices proliferate and complicate digital ecosystems. The Information systems security has specialists who needs to stay ahead for the curve and for create cutting-edge solutions that has make use of AI, ML, and other cutting-edge technologies such as counter these threats. It is entails to putting strong the threat intelligence and capabilities into practice, improving incident response plans, and encouraging a cybersecurity awareness culture among the users [8]. By the recognized and resolving the new issues, further we can ensure the securities and the confidentiality of our computer networks and guard against the disastrous effects of cyberattacks.

2.1 Increasing Complexity of Cyber Attacks

Advanced Persistent Threats (APTs) are specifically designed and intelligent attacks that are made to get through traditional security measures. APTs are extremely rare types of cyberattacks that are typically opportunistic and indiscriminate. They organize and carry out their assaults with the express intent of targeting particular people or teams [9]. Variety of strategies, including spear phishing, phishing, and social engineering, to obtain first access to a network. Once inside, they covertly traverse the network by escalating privileges and using sophisticated tools and strategies such as spyware, vulnerabilities, and lateral movement. With descriptions of their key characteristics, attack phases, potential outcomes, and recommended defense

tactics. Table 1 provides an in-depth review of Advanced Persistent Threats (APTs) [10, 11].

APTs are particularly harmful because of their ability to remain undetected for months or even years at a time. Traditional security tools like firewalls and intrusion detection systems are usually ineffective against APTs since they are designed to evade detection [12]. To counteract Advanced Persistent Threats (APTs), organizations need to adopt a proactive, intelligence-driven cybersecurity strategy. Being vigilant and quick to react to fresh dangers is necessary for this. It also involves using improved threat recognition and incident handling skills to detect and address APTs. Enterprises should use robust security measures, such as segmentation of the network, multi-factor authentication, and encryption, to further decrease the attack surface and halt lateral movement.

The proliferation of Internet of Things (IoT) devices creates a large target pool that malicious actors can exploit, increasing the intricate nature of cyberattacks. IoT devices, which can be anything from smart home appliances to industrial control systems, usually have no basic security safeguards, making them vulnerable to misuse. The sheer size of IoT devices, combined with their lack of standardization and inconsistent security procedures, creates an ideal mix of vulnerability. To address this issue, organizations need to handle IoT security holistically [13].

To mitigate the effects of IoT-related attacks, this strategy should involve putting in place robust security mechanisms, conducting regular vulnerability assessments, and developing incident response plans. This multifaceted approach helps safeguard against threats and enhances the overall security of IoT environments [14].

Table 2 provides a summary of the characteristics, attack aspects, and safety measures related to AI-driven assaults, Internet of Things weaknesses, and persistent threats. Adding IoT devices into networks that currently exist could also introduce new security flaws because those devices may or may not have been designed with

Table 1 Offers a thorough overview of Advanced Persistent Threats (APTs) by describing their salient features, the phases of an attack, the possible consequences, and the suggested defensive strategies

Category	Aspect	Description
Stages of an attack	Initial compromise	Use spear phishing, phishing, which or exploiting vulnerabilities to get first access
	Establish foothold	Utilize backdoors or malware to keep access to the network
	Lateral movement	Navigate laterally via the network, gaining access to sensitive information and raising privileges
	Command and control	Create channels of communication (C2) with the system that has been compromised
	Data exfiltration	Utilize avoidance strategies such as encryption to steal confidential information
	Post-exploitation	To stay hidden, use cutting-edge tools and strategies to keep access

Table 2 Analyzing the common traits, attack characteristics, and precautions of Advanced Persistent Threats, AI-powered attacks, and IoT vulnerabilities

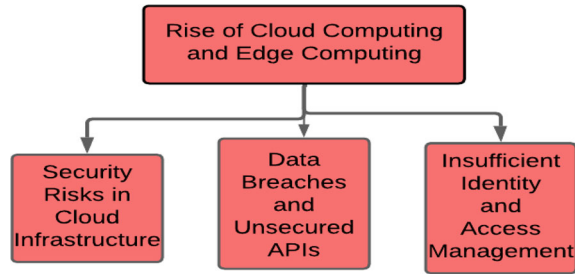
Category	Common traits	Attack characteristics	Precautions
APTs	Use advanced techniques to evade detection	Sophisticated	Intelligence-driven approach
	Target specific organizations or individuals	Targeted	Proactive security controls
	Persistence	Involves social engineering	Network segmentation
AI-powered attacks	Utilize advanced technology	Adaptive and learning-based	Adaptive and learning-based
	Can target specific entities	Automated decision making	Continuous monitoring
	Can be persistent	Scalable attacks	Implementing AI ethics and guidelines
IoT vulnerabilities	Exploit weaknesses in system	Device exploitation	Regular firmware updates
	Can target a wide range of devices	Network breaches	Strong encryption
	Difficult to detect	Data interception and manipulation	Device authentication

security in mind. For instance, a smart thermostat can serve as a gateway for hackers to access the entire network even though it may not be as safe as a regular laptop. As a result, enterprises must adopt a zero-trust architecture in which any device, including IoT devices are monitored and subject to stringent access controls since they are viewed as possible threats.

2.2 Rise of Cloud Computing and Edge Computing

The manner that businesses handle data processing, storage, and administration has changed dramatically as a result of the increasing adoption of cloud computing. Using cloud-based infrastructure instead of conventional on premise infrastructure offers better cost-effectiveness, scalability, and flexibility [15]. But this change also presents fresh cybersecurity difficulties. Cybercriminals find the cloud to be a tempting target because to its larger attack surface caused by the greater volume of data stored there. Advanced cybersecurity tools including cloud workforce protection platforms (CWPPs), cloud security gateways, and security brokers for cloud access (CASBs) are crucial for reducing these threats.

Fig. 2 Organizations may assure an uninterrupted utilization of clouds and edge computing technology while safeguarding their data and apps from new cyber threats by taking a comprehensive approach to cybersecurity



Cloud-based applications and information are protected and kept intact by these solutions, which offer real-time monitoring, detection of risks, and response to incidents capabilities. Another ground-breaking innovation is edge computing, which modifies data processing and analysis by moving data computing near to its source [16]. Real-time processing capabilities are improved and latency is decreased as a result. New security issues are raised as well, though. Strong security features, such as access control, authentication, and encryption, are provided by these solutions to safeguard edge-based apps and data [17]. It is essential to integrate cloud and edge computing technologies within current information systems security frameworks as firms embrace them. This include putting robust management of access and identity systems into place, keeping an eye on things constantly, and following cybersecurity best practices when it comes to encryption, safe data storage choices, and access management (IAM) systems [18]. Businesses must also develop incident response plans and conduct regular security audits in order to identify vulnerabilities and reduce potential hazards. Figure 2 by adopting a comprehensive cybersecurity strategy, organizations can ensure the continuous use of cloud and edge computing technologies while protecting their data and apps from emerging cyber threats.

2.3 *Security Risks in Cloud Infrastructure*

The likelihood of cyberattacks and data breaches increases as more businesses move their data and apps to the cloud. To reduce these risks, advanced cybersecurity techniques including continuous monitoring, intelligent threat detection, and incident response are crucial [19]. Nevertheless, security issues with cloud infrastructure persist despite these precautions, such as illegal access, data loss, and Denial of Service (DoS) assaults [20].

- **Data Breaches and Unsecured APIs**

Sensitive data hosted in a public cloud without proper protection or access controls is a major risk for data breaches. Attackers may also be able to access cloud-based data and systems without authorization through insecure APIs (Application Programming Interfaces). To stop such attacks, security experts emphasize the significance

of strong security measures like encryption, multi-factor authentication, and safe coding techniques [21]. To find vulnerabilities and fix them earlier than they can be exploited, regular security inspections and penetration tests are also essential.

- **Insufficient Identity and Access Management**

Inadequate Identity and Access Management is a significant security issue associated with cloud infrastructure (IAM). IAM policies that are not properly established might provide unauthorized people access to private information and systems, which can result in security incidents and data breaches. By providing automated access and identity management, real-time monitoring, and analytics, cloud-based identity and access management systems, among other advanced cybersecurity solutions, can reduce this risk [22]. These solutions guarantee that data and resources hosted in the cloud can only be accessed by authorized users [23].

- **Edge Computing's Increased Attack Surface**

Data analysis and management have been revolutionized by the use of edge computing, that processes data close to its source [24]. This decentralized strategy does, however, also widen the attack surface. Cybercriminals have more possible points of entry when there are numerous devices more nodes at the edge. Attackers now have greater avenues for nefarious activity, including ransomware, DoS, and data breach attempts, thanks to this enlarged attack surface. Effective security controls at the edge are essential for next-generation cybersecurity strategies to mitigate these dangers. This entails putting in place safe authentication and access controls, protecting data in transit as well as at rest, and installing sophisticated detection and response to threats systems. For edge devices, regular updates and fixes are also necessary to stop known vulnerabilities from being exploited. It takes incident response skills and real-time monitoring to promptly recognize and handle security threats [25]. Businesses should implement a thorough cybersecurity plan that addresses edge computing security, utilizing AI and machine learning to identify and address anomalies at the edge, and implementing Zero Trust architectures. By adopting a proactive and flexible approach, firms may lower their risk of attacks from hackers and secure their critical data and systems [26].

- **Expanding IoT Attack Surface**

Cybercriminals have an increased attack surface due to the growing amount of Internet of Things (IoT) devices. The infrastructures, networks, and devices within a company that have vulnerabilities that an attacker could exploit are collectively referred to as the attack surface [27]. Hackers have an exponentially greater number of possible access points into networks as additional IoT devices become internet-connected. IoT devices are simple targets since many of them have old software, weak passwords, or unpatched vulnerabilities. To find and fix vulnerabilities earlier than they can be exploited, this entails putting advanced threat identification, response to incidents, and penetration testing into practice.

- **Security Risks in Cloud Infrastructure**

The likelihood of cyberattacks and data breaches increases as more businesses move their data and apps to the cloud. One of the main issues is that cloud-based resources are less visible and controlled, which makes it more difficult to identify and address security risks. To reduce these risks, advanced cybersecurity techniques including continuous monitoring, intelligent threat detection, and incident response are crucial. Nevertheless, security issues with cloud infrastructure persist despite these precautions, such as illegal access, data loss, and Denial of Service (DoS) assaults [28].

- **Data Breaches and Unsecured APIs**

Data breaches are a significant risk when sensitive information is stored in the cloud without adequate encryption or access controls. Unsecured APIs (Application Programming Interfaces) can also serve as entry points for attackers, allowing unauthorized access to cloud-based data and systems [29]. Security experts stress the importance of robust security measures like multi-factor authentication, encryption, and secure coding practices to prevent such breaches. Regular security audits and penetration testing are also crucial to identify and address vulnerabilities before they can be exploited.

- **Insufficient Identity and Access Management**

Insufficient Identity and Access Management (IAM) poses a significant security concern in cloud infrastructure. Inadequately set IAM policies can enable unauthorized individuals to get access to critical data and systems, resulting in data breaches and other security problems. Cloud-based IAM systems are advanced cybersecurity solutions that can reduce this risk by providing real-time monitoring, analytics, and automated identity and access management capabilities. These solutions guarantee that specific authorize user can obtain access to cloud-based resources and data.

- **Edge Computing's Increased Attack Surface**

Data management and analysis have changed dramatically as a result of edge computing, which processes data closer to its source. This decentralized strategy does, however, also widen the attack surface. Cybercriminals have more possible points of entry when there are more devices and nodes at the edge. Attackers now have greater avenues for nefarious activity, including ransomware, DoS, and data breach attempts, thanks to this enlarged attack surface. Robust security controls at the edge are essential for next-generation cybersecurity strategies to mitigate these dangers. This entails putting in place safe authentication and access controls, encrypting data in transit and at rest, and installing sophisticated threat detection and response systems. For edge devices, regular updates and fixes are also necessary to stop known vulnerabilities from being exploited. It need incident response skills and real-time monitoring to promptly recognize and handle security threats. Businesses should implement a thorough cybersecurity plan that addresses edge computing security, utilizing AI and machine learning to identify and address anomalies at the edge,

and implementing Zero Trust architectures. Organizations may lessen the risk of cyberattacks and safeguard their sensitive data and systems by adopting a proactive and flexible strategy.

- **Expanding IoT Attack Surface**

Cybercriminals have an increased attack surface due to the increasing number of Internet of Things (IoT) devices. The systems, networks, and devices within a company that have vulnerabilities that an attacker could exploit are collectively referred to as the attack surface. The number of potential entry points for hackers increases exponentially with the number of IoT devices that are connected to the internet. IoT devices are simple targets since many of them have old software, weak passwords, or unpatched vulnerabilities. Furthermore, a lot of IoT devices are open to abuse since they lack integrated security measures. Organizations must implement next-generation cybersecurity strategies that take into account the particular dangers provided by IoT devices in order to solve these issues. To find and fix vulnerabilities before they can be exploited, this entails putting advanced detection of threat, response of incident, and penetration testing into practice. Organizations can strengthen their defenses against the damaging effects of cyberattacks by taking this action.

3 Emerging Challenges in Information Systems Security

With the advent of Next-Gen Cybersecurity, the field of security for information systems is changing quickly. Organizations face novel and intricate issues due to the rapid improvements in technology, growing dependence on internet infrastructure, and an increase in cyber attacks. The widespread use of Internet of Things (IoT) devices is a major cause for concern since it increases the attack surface and makes people more susceptible to cyberattacks. Additionally, new security concerns including data breaches, illegal access, and AI-driven attacks are brought about by the increasing use of cloud computing, artificial intelligence, and machine learning. Proactive security measures and fast reaction skills are essential given the sophistication of cyber threats, which include ransomware, phishing assaults, and Advanced Persistent Threats (APTs). Utilizing modern technologies such blockchain, quantum computing, and autonomous security systems, organizations must take a proactive and flexible approach to cybersecurity in order to fortify their defenses, identify threats instantly, and react quickly to new ones. They may defend their digital assets and information systems against the constantly changing threat landscape by doing this.

3.1 Data Privacy and Protection

The exponential development of data gathering and collecting in the modern digital age makes protecting and safeguarding information a crucial problem. Data breaches, unauthorized use, and misuse risks have increased as an organization's reliance on information technologies to safeguard, analyze, and transport sensitive data grows. The protection of personal data, intellectual property, and proprietary corporate information must be given top priority in next-generation cybersecurity measures. The environment surrounding data privacy is becoming increasingly complex due to the growth of analytics for big data, AI, and IoT. The attack surface grows as more gadgets are connected to the internet, which makes it simpler for hackers to take advantage of weaknesses (Fig. 3).

Furthermore, there are more opportunities of data leakage and illegal access due to the increased usage of social media, mobile devices, and cloud services. Security of information systems must use strong data protection techniques, such encrypting it access controls, and detection of anomalies, to meet these difficulties and guarantee the availability, confidentiality, and integrity of sensitive data. It is essential to take an active and multi-layered strategy to safeguard and secure data, which includes investing in sophisticated detection and response to threats capabilities,

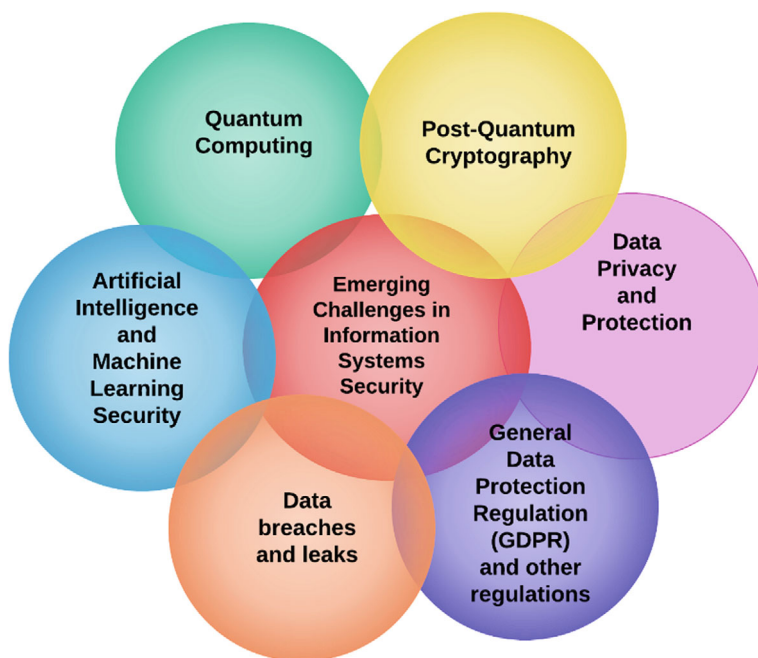


Fig. 3 The growing complexity of cyberattacks highlights the significance of taking proactive security measures and having the ability to respond quickly

establishing strong data governance policies, and conducting frequent risk assessments. To preserve confidence with their stakeholders and consumers, businesses must also give top priority to accountability, transparency, and compliance with laws like the CCPA and GDPR. This will help them to effectively reduce the risks related to data breaches.

3.2 General Data Protection Regulation (GDPR) and Other Regulations

It is more important than ever to preserve sensitive information in an increasingly digital society. The General Data Protection Regulation (GDPR), a historic EU law that went into effect in 2018, establishes a new benchmark for privacy and data protection by granting consumers control over their personal data and guaranteeing that businesses manage it with the highest care. GDPR enforces stringent guidelines for the gathering, storing, and processing of data, and it carries heavy penalties for noncompliance. Regulations like GDPR pose a lot of difficulties for Next-Gen Cybersecurity and Information Security. To stop data breaches and guarantee compliance, businesses need to invest in strong data protection measures including the use of encryption, restricted access, and incident response strategies. Big data, cloud computing, and the Internet of Things have created new vulnerabilities that need for proactive data protection measures. By doing this, businesses may safeguard their brand, avert fines from authorities, and cultivate consumer trust. The future development of cybersecurity will be shaped by laws like GDPR as the nature of threats changes. Organizations can maintain the reliability of their informational systems and stay ahead of any emerging dangers by giving security and confidentiality of data top priority.

3.3 Data Breaches and Leaks

Data is essential to enterprises in the modern digital era. Security breaches and leaks are becoming more common as our reliance on technology grows. When unauthorized parties use hacking, phishing, malware assaults, or insider threats to obtain sensitive information—such as bank records, personal data, or proprietary company information—this is known as a data breach. An unfortunate data breach can result in monetary losses, harm to one's reputation, and legal ramifications. Protecting sensitive data is becoming increasingly difficult due to the rise of next-generation cybersecurity threats, such as nation-state attacks, advanced persistent hazards (APTs), and zero-day exploits. Furthermore, as IoT devices, cloud-based services, and social networking platforms proliferate, the attack surface increases and attackers can more easily exploit vulnerabilities. To reduce the effect of breaches, organizations

must take a proactive approach to cybersecurity and invest in cutting-edge threat identification systems, encryption technology, and incident response procedures.

3.4 Artificial Intelligence and Machine Learning Security

The increasing use of machine learning (ML) and artificial intelligence (AI) makes it critical to secure these technologies. AI and ML systems must be shielded from possible attacks in order to prevent them from becoming weaknesses, according to next-generation cybersecurity standards. This is especially important for information systems security, since cyber threats are detected and addressed by AI-powered tools. On the other hand, hacked AI and ML algorithms might continue attacks or offer fictitious security guarantees, putting whole networks in jeopardy. Because AI and ML systems are susceptible to a variety of threats, including data ingestion, model inversion, and adversarial examples, securing these systems is difficult. Furthermore, the use of machine learning and artificial intelligence in cybersecurity can open up new attack avenues, such as the usage of AI-powered tools as attack vectors. Robust security measures are needed to mitigate these dangers. These include safe data management procedures, strict testing and validation procedures, and ongoing AI and ML system monitoring and updating. Setting AI and ML security as a top priority guarantees that these potent technologies promote cybersecurity rather than weaken it. Investigators, developers, and security experts must work together to create and execute efficient defenses that keep up with the quickly changing AI and ML world. By doing this, we can fully utilize the advantages of AI and ML while maintaining the integrity of information systems, resulting in a safer digital world (Table 3).

3.5 Quantum Computing and Post-quantum Cryptography

A revolutionary development in the area of next-generation cybersecurity is quantum computing. Quantum computers, which work using quantum bits, or qubits, as opposed to ordinary computers, which use bits, are capable of processing information at exponentially faster rates. A quantum computer, for example, could theoretically assess every combination simultaneously when attempting to break a password, whereas a traditional computer would test each conceivable combination one at a time. This incredible processing capacity seriously jeopardizes current encryption methods, emphasizing the need for innovative security solutions to fend off possible quantum threats. As a result, it is imperative that businesses make investments in encryption that is resistant to quantum attacks and continue to be on the lookout for new ones.

Post-Quantum cryptography is crucial for information systems security defense against these potential threats. Imagine a situation in which a sensitive database is compromised by a quantum computer; in the absence of post-quantum cryptography

Table 3 Table classifies different types of data breaches and offers illustrative examples to show the various kinds of risks related to cybersecurity that confront firms in preserving sensitive information

Classification of data breaches	Description	Examples
Ransomware attacks	Malware that encrypts data and demands ransom payment for decryption keys	WannaCry, NotPetya
Phishing attacks	Deceptive emails or messages to trick users into revealing sensitive information or credentials	Fake login pages, CEO fraud
Insider threat	Authorized users who misuse access privileges to steal or expose sensitive data	Employee data theft, negligent data handling
Cloud misconfigurations	Incorrectly configured cloud services or APIs that expose data to unauthorized access	Publicly accessible storage buckets, misconfigured databases
IoT security issues	Vulnerabilities in Internet of Things devices allowing unauthorized access or data interception	Compromised smart home devices, IoT botnets
Supply chain attacks	Cyber attacks targeting vulnerabilities in third-party software or services used by an organization	SolarWinds supply chain attack, software supply chain hacks

protections, the consequences would be disastrous. Organizations can maintain data security even in the face of advanced quantum threats by implementing post-quantum cryptography. It will take a lot of time and money to make the switch to post-quantum encryption, so being proactive is essential.

Numerous strategies, such as multivariate, code-based, and lattice-based encryption, are being investigated in the field of post-quantum cryptography research and development. Table 4 lists the new issues in information technology security, with an emphasis on the effects of quantum computing on confidentiality of information, regulatory compliance, and security issues with AI and machine learning. It describes each category's salient features, related difficulties, and defensive measures. As Next-Gen Cybersecurity develops further, Post-Quantum Cryptography will play a critical role in protecting private data and reducing the risks associated with quantum computing.

Table 4 The emerging challenges in information systems security, focusing on data privacy and protection, regulatory compliance, AI and machine learning security, and quantum computing impacts

Category	Characteristics	Challenges	Protection strategies
Data privacy and protection	Ensuring confidentiality, integrity, and availability of data	Data breaches	Encryption
	Protecting sensitive information	Data leakage	Regular audits and monitoring
General Data Protection Regulation (GDPR) and other regulations	Legal framework for data protection	Compliance requirements, penalties for non-compliance	Data protection policies
	Establishes guidelines for data handling and privacy	Complex regulatory landscape	Regular compliance checks
Artificial intelligence and machine learning security	Secure development and deployment of AI/ML models	Model manipulation	Secure model training, robust testing and validation
	Protecting against adversarial attacks	Data poisoning, algorithmic bias	Monitoring and anomaly detection
Quantum computing and post-quantum cryptography	Potential to break traditional cryptographic algorithms	Vulnerability of current encryption methods	Research and development of post-quantum cryptography
	Development of quantum resistant algorithms	Need for new cryptographic standards	Transition planning, risk assessments

It highlights key characteristics, associated challenges, and protection strategies for each category

4 Innovations in Next Gen-Cybersecurity

Figure 4 illustrates the implementation of Next Gen Cybersecurity, which involves the use of sophisticated technology to identify, address, and automate the management of threats, hence improving the effectiveness and efficiency of security measures. Artificial intelligence (AI) and machine learning (ML) can be utilized for automated many cybersecurity processes, thereby allowing human security investigators to dedicate their attention to more intricate and valuable jobs. AI-driven systems have the capability to examine network traffic, detect any risks, and autonomously implement measures to prevent or limit their impact, without the need for human involvement. This not only enhances the speed and efficacy of cybersecurity responses but also lessens the workload on human security staff.

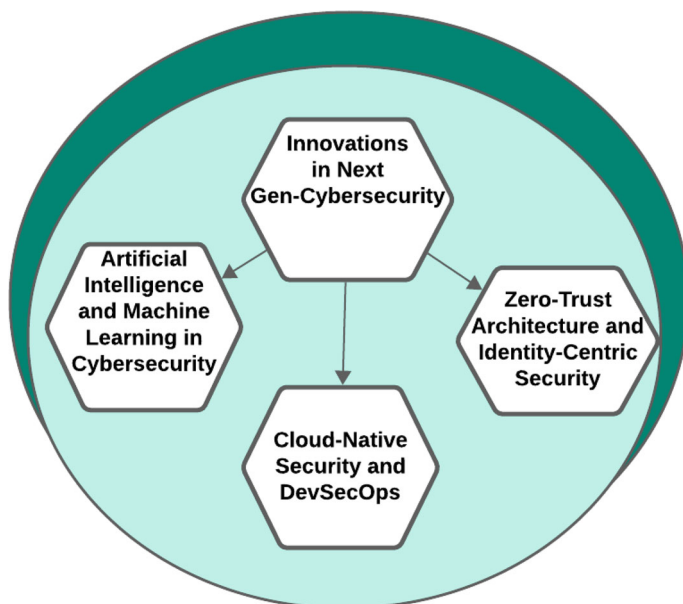


Fig. 4 Next-Gen Cybersecurity: using cutting-edge technology to automatically identify, respond to, and manage threats in order to improve security efficacy and efficiency

4.1 Artificial Intelligence and Machine Learning in Cybersecurity

Conventional security solutions frequently depend on rule-based approaches, which can be ineffective and sluggish in addressing contemporary, advanced cyber threats. Security teams may identify and rank high-risk threats using AI-powered threat detection, and routine chores can be automated to free up personnel for more important projects.

Machine Learning (ML)-based incident response and automate are essential components of Next-Gen Cybersecurity, facilitating prompt and efficient reactions to security issues. Conventional incident response approaches frequently rely on manual procedures, which can be time-consuming, susceptible to mistakes, and demanding of resources. On the other hand, incident response that is based on machine learning use algorithms to examine event data, detect recurring trends, and carry out reaction activities automatically. This strategy enables businesses to promptly address events, resulting in a decrease in both the average time it takes to identify an incident (MTTD) and the average time it takes to respond to an incident (MTTR). ML-based incident response allows security professionals to focus on high-priority occurrences, while automation handles the majority of the workload. This enables the allocation of resources to more important activities.

Furthermore, automation and ML-based incident response are crucial for lessening the effects of security mishaps. Machine learning algorithms are able to determine the underlying cause of an incident, forecast the probability of similar incidents in the future, and automate response tasks like recovery, eradication, and containment by examining incident data. This feature aids companies in reducing the possibility of system intrusions, data breaches, and reputational harm. Furthermore, incident response procedures can be optimized by ML-based automation and incident response, which lowers expenses and improves overall security posture.

4.2 Cloud-Native Security and DevSecOps

Scalability, agility, and flexibility are the cornerstones of cloud-native security architectures, which enable them to quickly adjust to shifting threat landscapes and business requirements. They frequently integrate cutting-edge security technology, including artificial intelligence, machine learning, and robotics, to promptly identify and address problems as they occur. Cloud-Native Security Architectures allow companies to create secure software more quickly and effectively by incorporating security into every stage of the application's development lifecycle.

Cloud-Native Security Architectures play a vital role in safeguarding sensitive data and applications on the cloud. Organizations can guarantee the privacy, availability, and integrity of their cloud-based assets by putting strong security policies and governance frameworks in place. In addition to adhering to legal and regulatory obligations, this entails safeguarding against cyber threats, illegal access, and data breaches.

In conventional development practices, the establishment and configuration of infrastructure were carried out manually, making them susceptible to human mistakes and security weaknesses. Infrastructure as Code (IaC) is a method where you specify your infrastructure by writing code, similar to how you would write code for an application. This technique facilitates version control, automated testing, and continuous improvement, so ensuring uniformity and safety throughout your infrastructure. Infrastructure as Code (IaC) solutions such as Terraform, AWS CloudFormation, and Azure Resource Manager aid in the management of infrastructure configuration, hence minimizing the likelihood of misconfigurations and breaches of security.

Next-Generation Cybersecurity relies on Infrastructure as Code (IaC) to guarantee the security and reliability of cloud-native applications. By establishing infrastructure as codes, you can automate security assessments and ensure compliance, thereby minimizing the likelihood of human mistakes and accelerating the deployment process. By utilizing Infrastructure as Code (IaC), it is possible to incorporate security measures and monitoring directly into the infrastructure. This allows for immediate identification and response to any threats.

4.3 Zero-Trust Architecture and Identity-Centric Security

Given the current digital environment, conventional security strategies that rely on boundaries are inadequate in safeguarding organizations against progressively advanced cyber attacks. Zero-Trust Architecture is a cutting-edge method that operates under the assumption that every one of networks and systems have been infiltrated. As a result, no user or device, regardless of their affiliation with the business, is automatically considered trustworthy. Access to resources is allowed based on a philosophy of “never trust, always verify.” This means that users and devices must constantly identify and authorize themselves in order to access specific resources. This approach ensures that even if a breach happens, the potential for attack is minimal.

Zero-Trust Architecture is based on the principle of micro-segmentation, which involves dividing the network into smaller, isolated zones. Each zone has its own access controls and security regulations. This strategy allows companies to restrict the lateral mobility of attackers within the network, so stopping them from moving around freely in the event of a breach. Organizations can greatly mitigate the probability of data breaches, accelerate incident response, and improve overall security posture by deploying Zero-Trust Architecture.

Identity-Centric Security models prioritize the protection of identities by implementing strong authentication, permission, and accounting (AAA) procedures, along with robust analytics or machine learning-based identification of threats. This methodology empowers businesses to promptly identify and counter identity-based risks, thereby mitigating the likelihood of credentials theft, phishing, and other forms of identity-related assaults. By prioritizing identity-centric security, organizations can improve their overall security posture, reduce the attack surface, and protect their most valuable assets—their identities. In the context of Next-Gen Cybersecurity and Information Systems Security, Identity-Centric Security is critical, as it enables organizations to stay ahead of evolving threats, such as AI-powered attacks, and protect their digital transformation initiatives. Table 5 summarizes innovations in next-generation cybersecurity, focusing on AI and machine learning, cloud-native security and DevSecOps, and zero-trust architecture and identity-centric security. It highlights key characteristics, associated challenges, and protection strategies for each category. By integrating Identity-Centric Security with Zero-Trust Architecture, organizations can create a robust security framework that is capable of detecting and responding to advanced threats in real-time, ensuring the confidentiality, integrity, and availability of their digital assets.

Table 5 Summarizes innovations in next-generation cybersecurity, focusing on AI and machine learning, cloud-native security and DevSecOps, and zero-trust architecture and identity-centric security

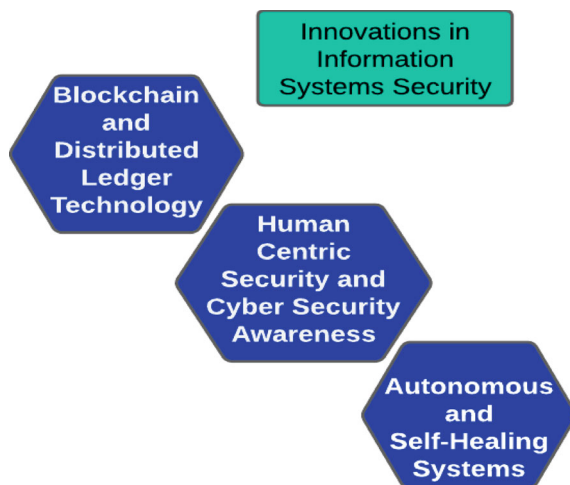
Category	Characteristics	Challenges	Protection strategies
Artificial intelligence and machine learning in cybersecurity	Automated threat detection	Model accuracy Data quality issues	Continuous model training Robust data preprocessing
	Behavioral analysis Anomaly detection	Adversarial attacks	Continuous model training Robust data preprocessing
Cloud-native security and DevSecOps	Integrated security throughout the development lifecycle	Rapid deployment cycles Complex environments	Automated security testing Continuous integration/continuous deployment (CI/CD) pipelines
	Automated security testing and compliance	Ensuring consistent security	Security as code
Zero-trust architecture and identity-centric security	No implicit trust Continuous verification of identity and access	Implementation complexity Scalability	Strong authentication mechanisms Least privilege access controls
	Micro-segmentation	User experience	Micro-segmentation policies

It highlights key characteristics, associated challenges, and protection strategies for each category

5 Innovations in Information Systems Security

Artificial Intelligence-powered Security Systems are revolutionizing the way we approach cybersecurity. By leveraging machine learning algorithms and natural language processing, AI-powered systems can detect and respond to threats in real-time, reducing the risk of human error. These systems can analyze vast amounts of data to identify patterns and anomalies, enabling them to predict and prevent attacks before they occur. In Fig. 5, cutting-edge security systems are transforming cybersecurity with advanced machine learning and natural processing of language ability. These systems have the capability to promptly identify and react to potential dangers, examine data to forecast and avert attacks, and streamline incident response to improve effectiveness and allow human resources to concentrate on crucial responsibilities. In addition, AI-driven systems have the capability to automate incident response, thereby allowing human security analysts to allocate their attention towards more intricate and valuable assignments.

Fig. 5 Advanced security systems are revolutionizing cybersecurity through the use of cutting-edge machine learning and processing of natural languages technologies. These systems have the capability to identify and react to potential dangers immediately, examine data to anticipate and avert attacks, and streamline incident response to improve efficiency and allow humans to concentrate on essential activities



5.1 *Blockchain and Distributed Ledger Technology*

Blockchain technology is an innovative concept that has fundamentally changed our perception of data security. A blockchain is essentially a distributed, electronic record-keeping system that logs transactions over a chain of computers. Essentially, a blockchain operates by utilizing a decentralized network of peers to authenticate and maintain the ledger in real-time, rather than depending on one centralized organization for data verification and storage. The decentralized nature of this approach renders it exceedingly difficult for any singular body to manipulate or modify the data, so guaranteeing that the information saved on the blockchain remains impervious to tampering and safe. An important benefit of the blockchain system is its capacity to offer comprehensive encryption and authentication, guaranteeing that only authorized individuals can access and perceive confidential data. This feature makes it a perfect choice for safeguarding confidential information in sectors such as banking, healthcare, and administration, where unauthorized access to data can result in severe repercussions. Utilizing blockchain technology, businesses can establish a safe and reliable environment for cooperation and data exchange, helping them to keep ahead of new cyber threats and shield confidential data from prying eyes. Figure 6 illustrates the architecture of a blockchain, which consists of decentralized ledger systems. These systems store data across a network of computers and provide transparency and security using encryption methods and consensus procedures. The revolutionary design of this technology removes the requirement for intermediates in transactions, hence enhancing trust and efficiency across multiple industries.

Distributed Ledger Technology (DLT) is a more inclusive name that incorporates blockchain technology, along with other decentralized ledger systems. Distributed Ledger Technology (DLT) allows numerous participants to record and validate transactions on a common ledger, eliminating the requirement for a central governing

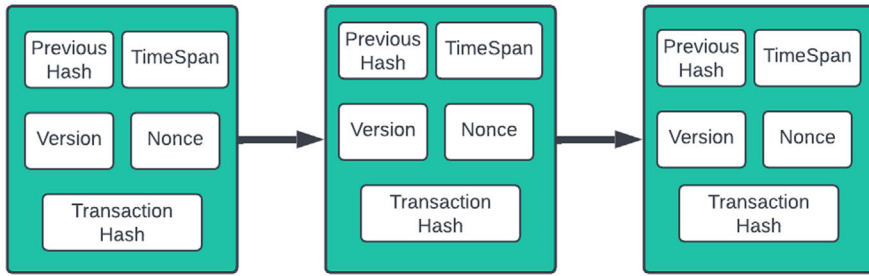


Fig. 6 Shows how the basis of decentralized systems is made up of blockchain components including immutable ledgers, cryptographic hash functions, and smart contracts

body. This decentralized architecture facilitates expedited, highly secure, and exceptionally efficient data sharing, rendering it an appealing solution for a diverse array of sectors and applications. Within the realm of Information Systems Security, Distributed Ledger Technology (DLT) provides a resilient and effective method for safeguarding confidential information against illegal entry and digital risks.

• Transaction Hash Mechanism

Every system's initial task is to confirm the sender's identity in order to ensure that the transaction between sender and a receiver is being requested by the sender and no one else. For instance, when Bob transfers Alice \$10, a request for this transaction is made. The third-party verifier is intermediary needs to confirm that Bob actually sent this communication [30]. The maximum amount of transactions that can be contained in a block varies according to the block size and size of every transaction. Blockchain cannot ensure transaction privacy since all transaction values and balances for each public key are available to the public. Blocks have block headers, which include block version, Merkle tree root hashes, timestamps, and the N bits target limit of a valid block hash, nonces, and previous block hashes. Contains the transaction number and transactions in the block body.

As was already mentioned, the primary phenomenon that gave origin to the name "Blockchain" is the collection of blocks that are connected in chain order. Many transactions are included in each block and are verified.

- **Previous Hash:** The field can be thought as a connection to parents hash, or the link between a block and the one before it in the chain. A hash function will be used to generate a value from all the data in the previous block, which will then be used to populate the Prev Hash field in the next block. This value is obtained using a 256-bit hash function in Bitcoin.
- **Timestamp:** When the block was discovered [31].
- **Nonce:** In PoW, this field is used to demonstrate the costs that a node has incurred to obtain the privilege to add his block to the chain.
- **Version:** The node that is submitting the block for the chain has specified the protocol version in this field.

- **Transactional Hash:** The hash value of each block is a valid transactions is included in this field, sometimes referred to as the Merkle root.

DLT offers the advantage of presenting a cohesive and comprehensive perspective on data across many entities and systems. This lowers the possibility of data breaches and cyberattacks by enabling enterprises to monitor and validate the flow of data in real-time [30]. Furthermore, Distributed Ledger Technology (DLT) facilitates the secure and efficient exchange of data among various entities, hence minimizing the requirement for middlemen and expediting decision-making processes. Through the use of Distributed Ledger Technology (DLT), enterprises may establish a secure and reliable platform for sharing and collaborating on data. This allows them to proactively address growing cyber threats and safeguard their confidential data from unwanted intrusion.

- **Components of Blockchain**

When considering Distributed Ledger Technology (DLT) approaches, it is important to recognize that while these systems provide notable benefits like as decentralization, dependability, permanence, and consensus, they also pose issues that can affect scalability. These obstacles encompass problems related to the rate at which transactions may be processed, the amount of storage needed, and the additional processing burden. These constraints can become more severe in applications that operate on a large scale [32]. DLT solutions may not fully meet all criteria or objectives in practical applications due to inherent difficulties. This frequently requires a compromise between the advantages of decentralization and the capabilities of the system to handle a large scale. Decentralization guarantees that no singular authority has complete control over the entire system, hence fostering transparency and diminishing the likelihood of manipulation or fraud. Nevertheless, this decentralization might result in performance bottlenecks, particularly when managing a substantial number of transactions concurrently. Figure 7 shows how the basis of decentralized systems is made up of blockchain components including immutable ledgers, cryptographic hash functions, and smart contracts. They provide secure, transparent, and streamlined operations across diverse applications like as cryptocurrency and decentralized finance (DeFi) [33]. To tackle these compromises, firms must meticulously assess their objectives according to their individual use cases and operational requirements. For example, applications that are essential to the mission and demand high data processing speed and minimal delay may find traditional centralized systems more appropriate in the immediate future. However, in cases where ensuring the accuracy and security of data, the ability to track and verify actions, and the capacity to withstand failures in a single component are of utmost importance, organizations may prefer to use Distributed Ledger Technology (DLT) solutions, even if they may face scalability difficulties [34].

Furthermore, Table 6 presents an examination of consensus processes in blockchain, which showcases several methods for verifying transactions and ensuring the integrity of the network. Proof of Work and Proof of Stake are two alternative methods used in blockchain technology to achieve decentralization, security, and

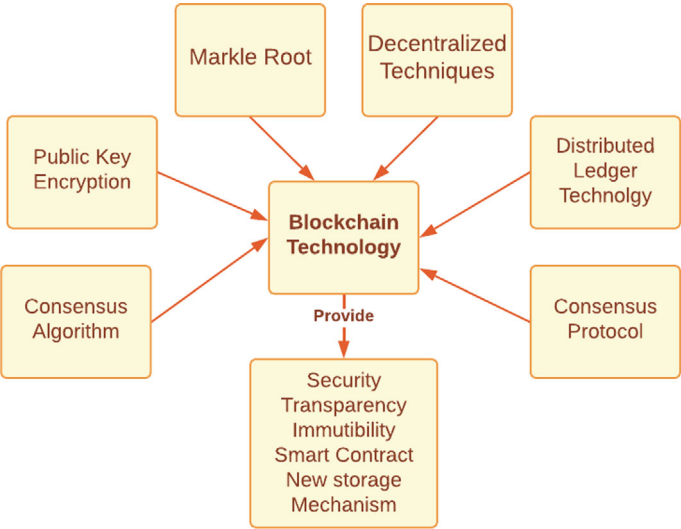


Fig. 7 Decentralized systems are built upon fundamental elements of blockchain, including hash functions for cryptography, immutable ledgers, and smart contracts. They guarantee the secure, translucent and efficient functioning of diverse applications such as cryptocurrency and decentralized financial services (DeFi)

scalability [34]. While Proof of Work relies on energy-intensive computations, Proof of Stake selects participants based on the amount of stake they have. These methods respond to the varying goals and priorities of different blockchain systems.

Table 6 A comparison of consensus mechanisms in blockchain illustrates varying approaches to validating transactions and maintaining network integrity

S. No.	Proof of Work (POW)	Proof of Stake (POS)	Proof of Burn (POB)
1.	Miners who have completed more work upon investing more power are more likely to mine the new block	Miners are chosen through an election process for the upcoming block to be mined	To mine a new block using a virtual asset, PoB purchases some cryptocurrencies (wealth)
2.	Used public key encryption algorithm	Using RSA algorithm	Using RSA algorithm
3.	Used in financial sectors that deal with industry	Used in financial sectors that deal with industry	Used in financial sectors that deal with industry
4.	Inefficient use of power	Efficient use of power	Efficient use of power
5.	Using Bitcoin Script	Using GO Lang	Using GO Lang

From Proof of Work’s energy-intensive computations to Proof of Stake’s stake-based selection, each method balances decentralization, security, and scalability differently, catering to diverse blockchain needs and priorities

Research and development efforts to improve scalability while maintaining security and decentralization are part of the continuous evolution of DLT technology. Efforts are being made to investigate and implement improvements like splitting, layer-2 solutions, and improved consensus methods in order to reduce these trade-offs and enhance the overall performance of distributed ledger technology (DLT) systems.

Types of Vulnerabilities

Blockchain vulnerabilities such as Sybil attacks, 51% attacks, and double spend attacks pose significant risks to decentralized networks and cryptocurrencies. Sybil attacks exploit multiple false identities to manipulate consensus, undermining trust. 51% attacks allow control of a majority of computing power to reverse transactions, violating blockchain's security principles. Double spend attacks exploit transaction confirmation delays to spend the same funds twice, compromising transaction integrity. Addressing these vulnerabilities requires robust security measures and vigilant monitoring to maintain blockchain's integrity and trustworthiness in decentralized applications [35]. Sybil attack in 2002, Brian Zill of Microsoft Research proposed naming an assault after the subject of the book Sybil. Initial Sybil attack methods were presented by Douceur. By constructing a large number of false identities, one adversarial peer can launch a Sybil assault to undermine the system's confidence and redundant technique. Karlof and Wagner found in 2003 that a possible danger to wireless was posed by the Sybil attack distributed sensor network is one example. As of late, many researchers have demonstrated the Sybil attack's enormity. Danger to P2P network architecture. After discovering that Sybil attacks can also damage Bitcoin systems, Bissias et al. created a hybrid approach called Xim to thwart this attack. The Sybil attack could potentially affect Bitcoin mining. According to research by Eyal et al. BitFury Group concluded that Sybil attacks are likely to be successful in public blockchains that use Proof-of-Stake (PoS) and Proof-of-Work (PoW).

51% Attack

One of the most well-known blockchain attacks is the 51%-attack, which assumes that a small number of miners hold more than 50% of the network's computing power. The attackers could stop fresh attacks by stopping transactions from receiving confirmations between businesses and customers [36]. Assailants can be faster than honest miners to finish evidence of work. Their transactions will therefore be linked to the most extensive chain. the more significant the mining hash rate and control, the more quickly blockchain attacks occur. Transactions can be turned around using the 51%-attack and repeatedly spend the same money when the attackers handle more than 50% of the network's hash rate for mining. Satoshi Nakamoto devised the structure. Bitcoin and determined the likelihood of an attack on various computing resources under the hands of the attackers [37].

Double Spend Attack

When someone tries to spend the same amount of money twice on the blockchain, it is known as a double-spending assault [32]. In an effort to undo the transaction he has done, an attacker might first try to produce a legitimate transaction for inclusion in a block then, after some time has passed, creating a fake conflicting transaction and pushing it into a newly forked fraudulent block [38]. The attacker should next strive to grow the network's false branch he generated until it is confirmed and acknowledged as the legitimate branch that contains the fraud claim.

5.2 Autonomous and Self-healing Systems

Autonomous systems are capable of identifying potential vulnerabilities and taking proactive measures to prevent attacks, thereby reducing the risk of breaches and minimizing downtime [39]. Self-healing systems, on the other hand, can automatically repair and restore damaged or compromised systems, ensuring business continuity and minimizing the impact of an attack. By leveraging these cutting edge technologies, organizations can stay one step ahead of cybercriminals and ensure the integrity of their information systems. Autonomous and self-healing systems are game-changer they enable organizations to respond to threats at machine speed, rather than relying on manual processes that can take hours or even days [40].

5.3 Human-Centric Security and Cybersecurity Awareness

Human-Centric Security is essential in today's digital environment to guard against sophisticated threats like ransomware assaults, social engineering, and phishing scams. Organizations can mitigate the risk of cyberattacks by prioritizing the human factor, hence minimizing the potential for hackers to exploit vulnerabilities. In addition, Human-Centric Security allows firms to respond more efficiently to incidents, reducing downtime and mitigating reputational harm. Human-Centric Security will become more and more crucial in Next-Gen Cybersecurity plans as cyber threats continue to change [41]. An essential element of human-centric security is cybersecurity awareness, which empowers people to recognize and react to possible risks. This entails instructing people about the potential dangers of the internet, advocating for secure computing habits, and fostering responsible conduct in the online sphere. Programs for raising awareness about cybersecurity issues can be customized to target certain businesses, associations, or user groups. They can also include workshops, training materials, and awareness campaigns. Organizations may mitigate the likelihood of cyber assaults, safeguard critical data, and ensure uninterrupted business operations by actively promoting Cybersecurity Awareness. A summary of recent developments in security of information systems is provided in Table 7,

which emphasizes distributed ledger and blockchain technology, self-healing and autonomous systems, human-centric security, and cybersecurity awareness. The text provides an overview of the main features, difficulties, and methods of safeguarding for each category [42]. The significance of Cybersecurity Awareness has increased significantly in recent times. In light of the growing complexity of cyber dangers, it is imperative for individuals to possess the necessary knowledge and expertise to promptly recognize and address these threats. By prioritizing Cybersecurity Awareness, organizations can stay ahead of emerging threats, protect their digital assets, and maintain a competitive edge in today’s fast-paced business environment.

Next Gen and Blockchain Integration Architecture

Integrating next-generation technologies with blockchain involves a multi-layered architecture designed to leverage the strengths of both blockchain (for security, transparency, and decentralization) and modern technologies (for scalability, speed, and user interface) [43]. Below is an architecture framework that can serve as a guideline for integrating blockchain with next-gen technologies such as Artificial Intelligence (AI), Internet of Things (IoT), and cloud computing. The integration of IoT sensors with cloud services and blockchain technology creates a robust ecosystem for data processing, analysis, storage, and verification. These services use advanced algorithms and machine learning models to turn raw data into actionable insights. For instance, in an industrial setup, real-time data from IoT sensors on machinery can be analyzed to predict maintenance needs, thereby preventing downtime. In healthcare, patient data from wearable devices can be monitored continuously to alert medical professionals about potential health risks. The scalability of cloud services ensures

Table 7 Summarizes innovations in information systems security, focusing on blockchain and distributed ledger technology, autonomous and self-healing systems, and human-centric security and cybersecurity awareness

Category	Characteristics	Challenges	Protection strategies
Blockchain and distributed ledger technology	Decentralized and tamper evident record keeping	Scalability issues, integration with existing systems	Layered security protocols, consensus mechanism
	Enhanced transparency and trust	Regulatory compliance	Regular security audits
Autonomous and self-healing systems	Automated detection and response	Complexity in implementation	Continuous monitoring, fail-safe
	Self-repair and system resilience	Risk of incorrect autonomous actions	Regular updates and testing
Human-centric security and cybersecurity awareness	Focus on user behavior and training	Human error, resistance to training programs	Regular training and awareness programs
	Increased awareness	Ensuring engagement and retention	Simulated phishing exercises

It highlights key characteristics, associated challenges, and protection strategies for each category

that they can handle vast amounts of data generated by the multitude of IoT sensors deployed [44]. Once the data has been processed and insights have been derived, the processed information can be securely recorded onto a blockchain. Blockchain technology offers an immutable ledger that ensures data integrity and transparency. Each piece of processed data is encrypted and added to a block; once a block is completed, it is added to the chain in a timestamped and securely indexed manner. The decentralized nature of blockchain means that no single entity has control over the entire data set, and each transaction or data record is verified and agreed upon by the majority of nodes in the network [45]. Figure 8 securely recording data on a blockchain has several benefits, particularly in terms of data integrity and transparency. For instance, in supply chain management, the transparency provided by a blockchain enables all stakeholders to trace the origin and journey of products, ensuring accountability and reducing fraud. In healthcare, blockchain can ensure that patient records are accurate and have not been tampered with, thereby enhancing trust in the medical data used for diagnoses and treatments [46]. Additionally, since blockchain records are immutable, they provide an auditable trail that can be used for regulatory compliance and dispute resolution [47].

The combination of IoT, cloud computing, and blockchain technologies results in a robust framework for efficient and safe real-time data collecting, processing, analysis, and storage [48]. Through the utilization of Internet of Things (IoT) sensors and devices, a significant volume of data may be continuously collected from many origins, offering valuable insights into operational activities [49]. Cloud computing

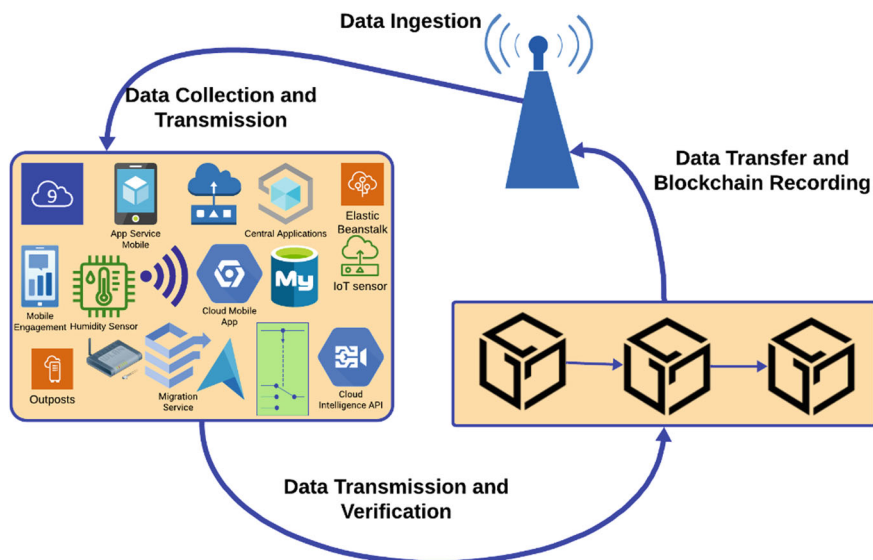


Fig. 8 The figure illustrates the wireless transmission of data from IoT sensors to cloud services for the purpose of processing and analysis. Subsequently, the data is securely documented on a blockchain, guaranteeing the integrity and transparency of the data

enables firms to quickly analyze and process data, allowing them to gain actionable insights and predictive analytics. This helps maximize efficiencies and make educated decisions [50].

6 Conclusion

Real-time data gathering, processing, analysis, and safe storage are made possible by the robust ecosystem created by the integration of blockchain technology, cloud services, and IoT sensors. This partnership has the potential to significantly improve operational effectiveness, predictive capacity, accuracy of data, and transparency in a number of industries, including smart cities, healthcare, agriculture, and manufacturing. In the healthcare industry, Internet of Things (IoT) devices have the capability to continuously monitor vital signs of patients. Simultaneously, cloud services can securely archive and analyze this information in order to forecast any health problems. Additionally, blockchain technology can guarantee that patient data is unchangeable and protected from unauthorized access. Similarly, within the field of agriculture, Internet of Things (IoT) sensors may be utilized to monitor the overall health of the soil. Cloud platforms can then analyze the collected data on crops in order to maximize the harvests. Additionally, blockchain technology can be employed to verify the supply chain, thereby assuring transparency throughout the entire process from the farm to the table. Smart cities can utilize these technologies to effectively manage resources, boost public safety, and improve citizen services. Similarly, industrial settings can anticipate machinery malfunctions and improve production efficiencies. Nevertheless, this merging of technologies brings very notable cybersecurity obstacles. The growing proliferation of IoT devices enlarges the potential targets for cyber attacks, necessitating stringent measures to protect these devices from security breaches. With the increasing importance of cloud services in information storage and processing, it is crucial to guarantee their ability to scale and withstand cyberattacks in order to avoid data breaches and interruptions in service. Blockchain technology, while offering intrinsic security benefits, necessitates strong mechanisms to protect integrity of data and privacy, particularly as it expands in size. Advancements in future cybersecurity are crucial to tackle these concerns. These advancements encompass sophisticated encryption techniques that safeguard data during transmission and while stored, distributed authentication protocols that authenticate user identities without relying on a single point of vulnerability, and threat detection systems powered by artificial intelligence that can acquire knowledge and adjust to emerging cyber threats. In addition, organizations must adjust their security methods to adequately protect sensitive information and maintain compliance with updated data protection regulations set by governments and regulatory authorities. By implementing these sophisticated security protocols, the industry may construct a robust and impervious infrastructure, therefore promoting a reliable environment for the upcoming era of interrelated technologies and guaranteeing the complete realization of their transformative advantages. Subsequent research in this field ought to

concentrate on improving the amalgamation and compatibility of blockchain technology, cloud services, and IoT sensors in order to construct ecosystems that are even more robust and safe. Research and development endeavors can focus on establishing standardized frameworks to guarantee smooth communication and data interchange among different IoT gadgets and cloud platforms.

Furthermore, investigating the possibility of edge computing to enhance cloud capabilities may provide substantial advantages, especially in the realm of instantaneous data processing and minimizing delay. Within the domain of cybersecurity, it is imperative that future efforts focus on enhancing encryption methods to protect data over its full lifecycle. It is essential to design cryptographic methods that are resistant to quantum computing in order to proactively address the vulnerabilities it presents. In addition, enhancing artificial intelligence and machine learning algorithms for the purpose of identifying and stopping potential dangers can offer more advanced and flexible security solutions. In relation to blockchain technology, it is imperative to prioritize endeavors aimed at enhancing scalability solutions and refining consensus processes to guarantee the continued efficiency and effectiveness of blockchain applications as they expand. Exploring permissioned blockchain systems may offer a compromise between security and performance, hence enhancing the technology's suitability for diverse company requirements. Establishing thorough policies and regulations that handle the growing cybersecurity issues related to these technologies would require close cooperation between academic institutions, business, and regulatory agencies. Ultimately, it is crucial to consistently focus on promoting public awareness and education on the advantages and potential drawbacks linked to these sophisticated technology. Encouraging a mindset of security awareness can enable users to actively participate in safeguarding their personal data and enhance the overall strength of interconnected systems. This comprehensive strategy will facilitate sustainable innovation and the appropriate implementation of IoT, cloud, and blockchain technologies, thereby advancing their beneficial influence in diverse industries.

References

1. Husain, M.S., Faisal, M., Sadia, H., Ahmad, T., Shukla, S. (eds.): *Advances in Cyberology and the Advent of the Next-Gen Information Revolution*. IGI Global (2023)
2. Idougli, L., Tkatek, S., Elfayq, K., Guezzaz, A.: Next-gen security in IIoT: integrating intrusion detection systems with machine learning for industry 4.0 resilience. *Int. J. Electr. Comput. Eng.* (2088-8708) **14**(3) (2024)
3. Jha, A.V., Teri, R., Verma, S., Tarafder, S., Bhowmik, W., Mishra, S.K., Appasani, B., Srinivasulu, A., Philibert, N.: From theory to practice: understanding DevOps culture and mindset. *Cogent Eng.* **10**(1), 2251758 (2023)
4. Wiedemann, A., Wiesche, M., Gewalt, H., Krcmar, H.: Integrating development and operations teams: a control approach for DevOps. *Inf. Organ.* **33**(3), 100474 (2023)
5. Evren, R., Milson, S.: *The Cyber Threat Landscape: Understanding and Mitigating Risks*. Technical report. EasyChair (2024)

6. Ibrahim, A.: Guardians of the Virtual Gates: Unleashing AI for Next-Gen Threat Detection in Cybersecurity (2022)
7. Mangla, C., Rani, S., Qureshi, N.M.F., Singh, A.: Mitigating 5G security challenges for next-gen industry using quantum computing. *J. King Saud Univ. Comput. Inf. Sci.* **35**(6), 101334 (2023)
8. Dash, J., Barekar, S.S., Borhade, R.R., Ikhar, S., Afaq, A., Bendale, S.P.: Next-Gen security: leveraging advanced technologies for social medical public healthcare resilience. *South East. Eur. J. Public Health* 35–51 (2024)
9. Ahmetoglu, H., Das R.: A comprehensive review on detection of cyber-attacks: data sets, methods, challenges, and future research directions. *Internet Things* **20**, 100615 (2022)
10. Guembe, B., Azeta, A., Misra, S., Osamor, V.C., Fernandez-Sanz, L., Pospelova, V.: The emerging threat of AI-driven cyber attacks: a review. *Appl. Artif. Intell.* **36**(1), 2037254 (2022)
11. Lehto, M.: Cyber-attacks against critical infrastructure. In: *Cyber Security: Critical Infrastructure Protection*, pp. 3–42. Springer International Publishing, Cham (2022)
12. Alhayani, B., Abbas, S.T., Khutar, D.Z., Mohammed, H.J.: Best ways computation intelligent of face cyber attacks. *Mater. Today Proc.* 26–31 (2021)
13. Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A., Akin, E.: A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics* **12**(6), 1333 (2023)
14. Duo, W., Zhou, M.C., Abusorrah, A.: A survey of cyber attacks on cyber physical systems: recent advances and challenges. *IEEE/CAA J. Autom. Sin.* **9**(5), 784–800 (2022)
15. Gulyas, O., Kiss, G.: Impact of cyber-attacks on the financial institutions. *Procedia Comput. Sci.* **219**, 84–90 (2023)
16. Cao, K., Hu, S., Shi, Y., Colombo, A.W., Karnouskos, S., Li, X.: A survey on edge and edge-cloud computing assisted cyber-physical systems. *IEEE Trans. Ind. Inf.* **17**(11), 7806–7819 (2021)
17. Abdulqadir, H.R., Zeebaree, S.R.M., Shukur, H.M., Sadeeq, M.M., Salim, B.W., Salih, A.A., Kak, S.F.: A study of moving from cloud computing to fog computing. *Qubahan Acad. J.* **1**(2), 60–70 (2021)
18. Mansouri, Y., Ali Babar, M.: A review of edge computing: features and resource virtualization. *J. Parallel Distrib. Comput.* **150**, 155–183 (2021)
19. Alghofaili, Y., Albattah, A., Alrajeh, N., Rassam, M.A., Al-Rimy, B.A.S.: Secure cloud infrastructure: a survey on issues, current solutions, and open challenges. *Appl. Sci.* **11**(19), 9005 (2021)
20. Kunduru, A.R.: Security concerns and solutions for enterprise cloud computing applications. *Asian J. Res. Comput. Sci.* **15**(4), 24–33 (2023)
21. Torkura, K.A., Sukmana, M.I.H., Cheng, F., Meinel, C.: Continuous auditing and threat detection in multi-cloud infrastructure. *Comput. Secur.* **102**, 102124 (2021)
22. Olabanji, S.O., Olaniyi, O.O., Adigwe, C.S., Okunleye, O.J., Oladoyinbo, T.O.: AI for identity and access management (IAM) in the cloud: exploring the potential of artificial intelligence to improve user authentication, authorization, and access control within cloud-based systems. In: *Authorization, and Access Control Within Cloud-Based Systems*, 25 Jan 2024
23. 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)
24. Boopathi, M., Gupta, S., Mohammed Zabeeulla, A.N., Gupta, R., Vekriya, V., Pandey, A.K.: Optimization algorithms in security and privacy-preserving data disturbance for collaborative edge computing social IoT deep learning architectures. *Soft Comput.* (2023). <https://doi.org/10.1007/s00500-023-08396-2>
25. Khan, A., Ahmad, A., Ahmed, M., Sessa, J., Anisetti, M.: Authorization schemes for internet of things: requirements, weaknesses, future challenges and trends. *Complex Intell. Syst.* **8** (5), 3919–3941 (2022)
26. Tournier, A.J., De Montjoye, Y.-A.: Expanding the attack surface: robust profiling attacks threaten the privacy of sparse behavioral data. *Sci. Adv.* **8**(33), eabl6464 (2022)

27. Ashley, T., Gouriseti, S.N.G., Brown, N., Bonebrake, C.: Aggregate attack surface management for network discovery of operational technology. *Comput. Secur.* **123**, 102939 (2022)
28. Gupta, B.B., Chaudhary, P., Chang, X., Nedjah, N.: Smart defense against distributed denial of service attack in IoT networks using supervised learning classifiers. *Comput. Electr. Eng.* **98**, 107726 (2022)
29. Mazhar, N., Salleh, R., Zeeshan, M., Muzaffar Hameed, M.: Role of device identification and manufacturer usage description in IoT security: a survey. *IEEE Access* **9**, 41757–41786 (2021)
30. Nabi, F., Zhou, X., Iftikhar, U., Attaullah, H.M.: A case study of cyber subversion attack based design flaw in service oriented component application logic. *J. Cyber Secur. Technol.* **8**(3), 204–228 (2024)
31. Pommier, C.: How the private and public key pair works (2017)
32. Zhang, S., Lee, J.-H.: Double-spending with a Sybil attack in the bitcoin decentralized network. *IEEE Trans. Ind. Inf.* **15**(10), 5715–5722 (2019)
33. Yadav, A.K., Singh, K.: Comparative analysis of consensus algorithms of blockchain technology. In: *Ambient Communications and Computer Systems*, pp. 205–218. Springer, Singapore (2020)
34. Bissias, G., Ozisik, A.P., Levine, B.N., Liberatore, M.: Sybil-resistant mixing for bitcoin. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*, pp. 149–158. ACM (2014). Proof of stake versus proof of work white paper
35. Douceur, J.R.: The Sybil attack. In: *International Workshop on Peer-to-Peer Systems*, pp. 251–260. Springer (2002)
36. Ye, C., Li, G., Cai, H., Gu, Y., Fukuda, A.: Analysis of security in blockchain: case study in 51%-attack detecting. In: *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*, pp. 15–24. IEEE (2018)
37. Pop, C., Cioara, T., Anghel, I., Antal, M., Salomie, I.: Blockchain based decentralized applications: technology review and development guidelines. *arXiv preprint [arXiv:2003.07131](https://arxiv.org/abs/2003.07131)* (2020)
38. Iftikhar, U., Anwer, M., Butt, R., Ahmed, G.: Towards 5G, 6G and 7G sustainable and potential applications using blockchain: comparative analysis and prospective challenges. In: *2023 4th International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*, pp. 1–7. IEEE (2023)
39. Tan, Y.J., Susanto, G.J., Ali, H.P.A., Tee, B.C.K.: Progress and roadmap for intelligent self-healing materials in autonomous robotics. *Adv. Mater.* **33**(19), 2002800 (2021)
40. Hafaiedh, I.B., Slimane, M.B.: A distributed formal-based model for self-healing behaviors in autonomous systems: from failure detection to self-recovery. *J. Supercomput.* **78**(17), 18725–18753 (2022)
41. Grobler, M., Gaire, R., Nepal, S.: User, usage and usability: redefining human centric cyber security. *Front. Big Data* **4**, 583723 (2021)
42. Deibert, R.J.: Toward a human-centric approach to cybersecurity. *Ethics Int. Aff.* **32**(4), 411–424 (2018)
43. Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A.: Integration of blockchain and cloud of things: architecture, applications and challenges. *IEEE Commun. Surv. Tutor.* **22**(4), 2521–2549 (2020)
44. Medhane, D.V., Sangaiah, A.K., Shamim Hossain, M., Muhammad, G., Wang, J.: Blockchain-enabled distributed security framework for next-generation IoT: an edge cloud and software-defined network-integrated approach. *IEEE Internet Things J.* **7**(7), 6143–6149 (2020)
45. Yang, W., Aghasian, E., Garg, S., Herbert, D., Disiuta, L., Kang, B.: A survey on blockchain-based internet service architecture: requirements, challenges, trends, and future. *IEEE Access* **7**, 75845–75872 (2019)
46. Tseng, L., Wong, L., Otoum, S., Aloqaily, M., Othman, J.B.: Blockchain for managing heterogeneous internet of things: a perspective architecture. *IEEE Netw.* **34**(1), 16–23 (2020)
47. Fernandez-Carames, T.M., Fraga-Lamas, P.: A review on the application of blockchain to the next generation of cybersecure industry 4.0 smart factories. *IEEE Access* **7**, 45201–45218 (2019)

48. Rane, S.B., Narvel, Y.A.M.: Re-designing the business organization using disruptive innovations based on blockchain-IoT integrated architecture for improving agility in future Industry 4.0. Benchmark. Int. J. **28**(5), 1883–1908 (2021)
49. Appasani, B., Mishra, S.K., Jha, A.V., Mishra, S.K., Enescu, F.M., Sorlei, I.S., Bîrleanu, F.G., Takorabet, N., Thounthong, P., Bizon, N.: Blockchain-enabled smart grid applications: architecture, challenges, and solutions. Sustainability **14**(14), 8801 (2022)
50. Murthy, Ch.V.N.U.B., Lawanya Shri, M., Kadry, S., Lim, S.: Blockchain based cloud computing: architecture and research challenges. IEEE Access **8**, 205190–205205 (2020)