CYBERSECURITY IN HEALTHCARE APPLICATIONS

Edited by S Poonkuntran,
Rajesh Kumar Dhanaraj,
S AanjanKumar
and Malathy Sathyamoorthy

A **Chapman & Hall** Book

CRC Press
Taylor & Francis Group

Cybersecurity in Healthcare Applications

The book explores the critical challenge of securing sensitive medical data in the face of rising cyber threats. It examines how artificial intelligence can be leveraged to detect and mitigate cyber threats in healthcare environments. It integrates advanced technologies such as AI security applications, blockchain techniques, cryptanalysis, and 5G security to strengthen the protection of healthcare systems. By offering insights into the latest vulnerability assessment technologies and effective protection strategies, this book serves as an essential resource for professionals and researchers dedicated to enhancing cyber security in the healthcare industry.

Cybersecurity in Healthcare Applications

Edited by
S. Poonkuntran, Rajesh Kumar Dhanaraj,
S. Aanjankumar, and Malathy Sathyamoothy

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

A CHAPMAN & HALL BOOK

First edition published 2025
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

ISBN: 9781032708195 (hbk)
ISBN: 9781032711362 (pbk)
ISBN: 9781032711379 (ebk)

DOI: 10.1201/9781032711379

Typeset in Times
by Newgen Publishing UK

Contents

Preface

The book explores the critical challenge of securing sensitive medical data in the face of rising cyber threats and proposes a solution to the challenge of securing healthcare systems in the digital age. The traditional security system for health records has evolved into a more intelligent system that incorporates technical improvements and cybersecurity modules. The solution involves the integration of advanced technologies such as AI security applications, blockchain techniques, cryptanalysis, and 5G security. AI can help to identify and prevent cyber threats in real-time by analyzing large volumes of data and detecting anomalies. This book also discusses utilization of ransomware security functions, which can provide enhanced security and privacy features for healthcare systems. By offering insights into the latest vulnerability assessment technologies and effective protection strategies, this book serves as an essential resource for professionals and researchers dedicated to enhancing cyber security in the healthcare industry.

About the Editors

S. Poonkuntran earned a BE degree in Information Technology from Bharathidasan University, Tiruchirappalli, India; and MTech and PhD degrees in Computer and Information Technology from Manonmaniam Sundaranar University, Tirunelveli, India. He is presently with VIT Bhopal University, Madhya Pradesh, India as Professor and Dean for the School of Computing Science and Engineering. He has more than a decade of experience in teaching and research and successfully executed three funded research grant projects from the Indian Space Research Organization, Defense Research Development Organization, and Ministry of New and Renewable Energy, Government of India, to the tune of 1.10 Crores. He received two seminar grants from Anna University, Chennai, and the All-India Council for Technical Education-Indian Society for Technical Education to the tune of 4 Lacs. He has published more than 90 technical publications, authored 8 books and 2 chapters and 5 patents. He is the recipient of Cognizant Best Faculty Award 2017–18 and served as a State Level Student Coordinator for Region VII, CSI, India in 2016–17. He is a lifetime member of IACSIT, Singapore, CSI, India, and ISTE, India. His research areas of interests include information security, computer vision, artificial intelligence, and machine learning.

Rajesh Kumar Dhanaraj is a distinguished Professor at Symbiosis International (Deemed University) in Pune, India. Before joining Symbiosis International University, he served as a Professor at the School of Computing Science & Engineering at Galgotias University in Greater Noida, India. His academic and research achievements have earned him a place among the top 2 per cent of scientists globally, a recognition bestowed upon him by Elsevier and Stanford University. He earned his B.E. degree in Computer Science and Engineering from Anna University Chennai, India, in 2007. Subsequently, he obtained his M.Tech degree from Anna University Coimbatore, India, in 2010. His relentless pursuit of knowledge culminated in a Ph.D in Computer Science from Anna University, Chennai, India, in 2017. He has authored and edited over 50 books on various cutting-edge technologies and holds 22 patents.

Furthermore, he has contributed over 115 articles and papers to esteemed refereed journals and international conferences, in addition to providing chapters for several influential books. Dr. Dhanaraj has shared his insights with the academic community by delivering numerous tech talks on disruptive technologies. He has forged meaningful partnerships with esteemed professors from top QS-ranked universities around the world, fostering a global network of academic excellence. His research interests encompass Machine Learning, Cyber-Physical Systems, and Wireless Sensor Networks. Dr. Dhanaraj's expertise in these areas has led to numerous research talks on Applied AI and Cyber Physical Systems at various esteemed institutions. Dr. Dhanaraj has earned the distinction of being a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE). He is also a member of the Computer Science Teacher Association (CSTA) and the International Association of Engineers (IAENG). Dr. Dhanaraj's commitment to academic excellence extends to his role as an Associate Editor and Guest Editor for renowned journals, including Elsevier's *Computers and Electrical Engineering*, *Human-centric Computing and Information Sciences*, Emerald's *International Journal of Pervasive Computing and Communications*, and Hindawi's *Mobile Information Systems*.

His expertise has earned him a position as an Expert Advisory Panel Member of Texas Instruments Inc., USA.

S. Aanjankumar holds a doctorate in botnet security and an M.E. in software engineering from Anna University. He has academic experience spanning 10 years and has worked at various levels up to Associate Professor, UG-HoD. He has 17 publications in peer-reviewed international and national journals with high impact factors and 11 publications in various international conferences held in India and abroad. He has authored a book titled *Graph Theory and Applications* under the Anna University syllabus, and the *Botnet Evolution* book under the VSRD publication has been adopted by Amity University for web security reference. He is also a reviewer for SCI journals, and he has 3 SCI journal publications with an impact factor above 3, 12 Scopus-indexed publications, 2 book chapters, 1 Indian patent and 1 UK Design Patent that he has authored and published. His main areas of research include software engineering, cyber forensics, network security, and human-computer interaction.

Malathy Sathyamoorthy is an Assistant Professor in the department of Information Technology, KPR institute of Engineering and Technology, Coimbatore, Tamil Nadu, India. She earned her M.E. degree in Computer Science and Engineering from Anna University, India in 2012. She completed a Ph.D degree in Information and Communication Engineering from Anna University, Chennai, India, in 2023. She is a life member of the Indian Society for Technical Education (ISTE) and International Association of Engineers (IAENG). She published more than 25 Research Papers in various high-quality SCI impact factor journals cum Scopus/ESCI indexed Journals, 22 Papers in international conferences indexed with Springer and IEEE Xplore, 2 patents, 1 book and 4 book chapters in various SCOPUS, WEB OF SCIENCE Indexed Books with Springer, CRC Press and Elsevier. Wireless Sensor Networks, Networking, Security and Machine Learning are her research interests. She is a reviewer in Springer – Wireless Networks and an editorial board member in many international conferences.

Contributors

A Sirajudeen
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

S Alwyn Rajiv
Kamaraj College of Engineering and Technology, Virudhunagar

M J Abinash
Department of Information Technology & PG (CS), AKCAS, Krishnankoil, Srivilliputhur, India

T Anitha
Department of Computer Science and Engineering, Sathyabama Institute of Science and Technology, Chennai, India

A V Santhosh Babu
Professor, Department of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Tiruchengode, Namakkal, Tamil Nadu, India

Mansi Bakhshi
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh

A P Chaithanya
PhD Scholar, Department of Pharmaceutics, Bharath Institute of Higher Education and Research, Chennai, Tamilnadu, India

R Nancy Deborah
Velammal College of Engineering and Technology, Madurai

S Devaraju
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh

Rajesh Kumar Dhanaraj
Professor, Symbiosis International (Deemed University), Pune, India

D Elavarasi
Department of Computer Science and Engineering, Mount Zion College of Engineering and Technology, Pudukkottai, India.

Thenmozhi Ganesan
Department of Computer Applications, Alagappa University, Karaikudi

S Gayathri
Assistant Professor, Department of Information Technology, Kamaraj College of Engineering and Technology, Virudhunagar, India

V Gayathri
Assistant Professor, Department of Information Technology, Kamaraj College of Engineering and Technology, Virudhunagar, India

G Indumathi
Department of ECE, Mepco Schlenk Engineering College, Sivakasi-626005, Tamil Nadu, India

Joseph James
Assistant Professor, Department of Computational Intelligence, Faculty of Engineering & Technology, SRM Institute of Science and Technology, Chennai, India

Jawahar S
Department of Computer Science and Applications, Christ Academy Institute for Advanced Studies, Bangalore 560 083, Karnataka

G Prabu Kanna
School of Computing Science and Engineering, VIT Bhopal
University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

V Karthikeyan
Department of ECE, Mepco Schlenk Engineering College, Sivakasi, Tamilnadu, India

R Kavitha
Department of Information Technology, Velammal College of Engineering and Technology Madurai, India

Vinesh Kumar
School of Computing Science and Engineering, VIT Bhopal
University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

E Lloyds
Government Sivagangai Medical College, Sivagangai

Anoop Arun M
Associate Professor, Dept. Of Computer Science & Engineering, Vivekananda College of Engineering & Technology, Puttur, Karnataka, India

P Mahalakshmi
Assistant Professor, Department of Information Technology, Kamaraj College of Engineering and Technology, Virudhunagar, India

K B Manikandan
Assistant Professor, Vignan's Foundation for Science, Technology and Research University, Guntur, AP

M Manimaran
School of Computing Science and Engineering, VIT Bhopal
University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

Jay Prakash Maurya
School of Computing Science and Engineering, VIT Bhopal
University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

Monoj Kumar Muchahari
Institute of Engineering and Management, Department of Computer Application & Science, Kolkata, West Bengal, India

P Karthikeyan
Professor, Department of Electronics and Communication Engineering, Velammal College of Engineering and Technology, Viraganoor, Madurai, Tamilnadu, India

Senthilnathan Palaniappan
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore 632014, India

M R Thiyagu Priyadharsan
School of Electrical & Electronics Engineering (SEEE), VIT Bhopal University, Sehore, Madhya Pradesh, India

R Saranya Priyadharshini
Assistant Professor, Department of Information Technology, Kamaraj College of Engineering and Technology, Virudhunagar, India

Aslina Banu R
Department of Computer Science and Engineering, Sri Raaja Raajan college of Engineering and Technology,Tamilnadu, India

R Priya
Assistant Professor, Department of CSE, Pollachi Institute of Engineering and Technology, Poosaripatti, Tamilnadu, India

V Arun Raj
Department of ECE, Mepco Schlenk Engineering College, Sivakasi-626005, Tamil Nadu, India

K Thirumalai Raja
Professor, Department of Civil Engineering, SNS College of Technology, Coimbatore, India

S Aanjankumar
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

V S Meenakshi
PG and Research Department of Computer Science, Chikkanna Government Arts College, Tiruppur, Tamil Nadu, India

S Poonkuntran
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

Somasundaram A
Department of Computer Science and Applications, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India

B Sakthivel
Associate professor, Department of Electronics and communication Engg, Pandian Saraswati Yadav College of Engineering, Sivagangai, Tamil Nadu, India

G Sambasivam
School of Computing and Data Science, Xiamen University Malaysia, Malaysia

S Saravanan
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

Malathy Sathyamoorthy
Associate Professor, Department of Information Technology, KPR Institute of Engineering and Technology, India

G Sivakarthi
Velammal College of Engineering and Technology, Madurai

M Soundarya
Velammal College of Engineering and Technology, Madurai

D Sridhar
School of Computing Assistant Professor, Dr. Vishwanath Karad MIT World Peace University, Pune, Maharashtra

S Sureshkumar
Assistant professor, Department of CSE, p. a. college of engineering and technology, Pollachi, Tamilnadu, India

M Thenmozhi
Department of Artificial Intelligence and Data Science, Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu, India

Samriddhi Tripathi
School of Computing Science and Engineering, VIT Bhopal University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh 466114, India

Palanisamy Vellaiyan
Department of Computer Applications, Alagappa University, Karaikudi

Ilayaraja Venkatachalam
School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India

Asha Vidyadharan
School of Computing Science and Engineering, VIT Bhopal
University, Bhopal-Indore Highway, Kothrikalan, Sehore, Madhya Pradesh, India

A Vinora
Velammal College of Engineering and Technology, Madurai

Y Palin Visu
Department of ECE, St. Mother Theresa Engineering College, Vagaikulam, Tamilnadu, India

1 An Introduction to the Challenges and Issues Identified in Digital Health and Wellness Cybersecurity

M. J. Abinash, G. Prabu Kanna, S. Aanjankumar, G. Sambasivam, and P. Karthikeyan

1.1 INTRODUCTION

More than ever, cybersecurity is necessary for scientific organizations. Healthcare technologies have the ability to improve, save, and lengthen survival. Technologies that measure fitness and distribute medication, hold digital fitness records, and allow telemedicine—which permits doctors to provide care remotely, even internationally—are amongst them. More and more patients use their personal mobile apps, which may additionally now be integrated with telehealth and telemedicine to structure the scientific Internet of Things (IoT) for collaborative sickness administration and care coordination. Health departments, communal and senior care institutions, diagnostic providers, lookup and educational organizations, healthcare consultancies, and fundamental healthcare practices are among a limited range of the spaces where ransomware assaults, identity theft, and facts theft can happen.[1] The connectivity of healthcare devices is changing with them. Even though many have been unbiased in the past, they are now a part of the clinical system. Ten to fifteen related devices are currently positioned beside each mattress in US hospitals. Advanced authentication structures in addition to employee training, an imperative afterthought that some companies would neglect at the risk of making headlines in the cybersecurity area.[2] One sector of the healthcare enterprise is mainly susceptible to cyberattacks, and thieves often take advantage of this to open a vulnerability in the Security chain of the organization. Health businesses keep a significant network in which big volumes of data are continuously shared since they matter on a vast range of suppliers and backyard services.[3] Ransomware and Wannacry attacks have currently had and continue to have an impact on the healthcare sector, almost disrupting the lives of health centre sufferers who are self-treating. Apart from the data technology vulnerabilities current in infrastructures, social engineering is a novel kind of cyberattack that

DOI: 10.1201/9781032711379-1

specifically pursues human weaknesses.[4] Technological trends can be hastily utilized to enhance accuracy in the healthcare sector. Cyberattacks are typical and pose a danger to patients, including health information (PHI) and non-public information. Such assaults have the potential to compromise patient security through impeding and upsetting hospitals' traditional business. When buying assets, the European Union Agency for Cybersecurity suggests considering cybersecurity from the outset. It has additionally sparked and prompted healthcare infrastructures to enforce similarly useful cybersecurity practices.[5] The cybercrime threat increases with the degree of electronically built-in healthcare. There are two kinds of theft: exterior theft and interior theft. Hackers from the backyard of the healthcare enterprise compromise scientific and patient structures to steal and gather data, typically with monetary gain in mind. They would possibly use the personal facts of patients to publish fraudulent insurance claims. When hackers demand a ransom from healthcare organizations in order to get more effective personal information systems, this is another example of external theft. Advanced malware and phishing methods have the ability to install detrimental software or attain login credentials on a device, probably contaminating the whole system. The reality that a hostile cyber presence can be introduced into a network with just one reputedly legit hyperlink is one of the hardest components of dealing with malware. Staff participants must be educated to spot cooperative phishing attempts.[6,7] We are still learning how to make cyberspace impenetrable, though. The virtual environment formed via networked PC systems that influence many elements of our lives is now referred to as "cyberspace," yet protecting it is a challenging task. In addition to the truth that more and more devices are being linked to the Internet, more manufacturers are also making them, which raises the possibility of failure as nicely as the scale and variety of the structures that make up cyberspace. In addition, there are big variations in cybersecurity. While defenders have to be on the lookout for each detail and be organized for everything at any time, attackers have a greater range of possibilities. Therefore, negligence is not always the reason for profitable attacks. Sometimes safety controls are in existence, but they are no longer employed appropriately, such as when they come in the way of consumer requests. Owing to these challenges, reactive security—which acknowledges that we are unable to quit each and every threat—is gaining popularity.[8] Of course, privacy breaches existed earlier than the generation of computerized fitness records. But modern networked facts allow for extra viable ports of entry; faraway access, which makes statistics theft undetected; and getting right of entry to to a whole extra health record, which makes it a more profitable goal for doable attacks. In the past, a paper report or a snatched laptop may have put a lot of patients at risk of an information leak, but given that this records is now digital and reachable throughout a number of networks, a privacy breach can potentially affect millions of people.[9] The healthcare zone must prioritize statistics security of gathering patients' personal fitness information records. However, the primary cause of the industry's challenges is the sheer number of entrance and access points, which prevent a single company from developing an effective information security solution. Securing the process of getting admission to commercial enterprise apps and data based on profile is essential in the healthcare industry.[10] The principal objective of this chapter is to look into attainable functions of cybersecurity in the healthcare sector; the key cybersecurity characteristics and technology for the

healthcare sector, are seen at the more than a few roles cybersecurity performs in the sector; and a listing of the enormous number of applications for cybersecurity in the healthcare sector, threats and redress associated to network, data, and software program security.

1.2 CYBERSECURITY FEATURES AND TECHNOLOGIES FOR THE HEALTHCARE INDUSTRY

Cyberthreats that are new and developing and that probably endanger or affect personal safety are constantly being addressed by healthcare IT security. C-suite executives and senior management in hospitals are urged to viewing cybersecurity as a completely technical problem that their IT departments can resolve. Rather, cybersecurity needs to be included in the hospital's established enterprise, governance, hazard management, and operations continuity frameworks as a top strategic priority for both company danger and patient safety.

The numerous cybersecurity factors and methods are examined in the context of healthcare in Figure 1.1. Data loss prevention, vulnerability scan trials, looking out for methods of penetration, digitalization of the forensic industry, anti-theft units and programs, etc. are some of these features and tools. The fundamental objective of these cybersecurity assistances is to supply extra profitable and efficient offerings to more underserved businesses, such as the healthcare sector.[11,12] Overall, cybersecurity is a vital element of clinical gadgets and healthcare. Due to the increasing usage of technology in healthcare, it is imperative to make certain that the structures are impenetrable from any practicable cyber threats. Cybersecurity additionally helps to forestall unauthorized access to clinical products and ensure that they are in perfect operational order. Additionally, it safeguards touchy economic data, non-public medical data, and non-public affected person information. Moreover, cybersecurity guards healthcare amenities against ransomware and malware assaults that compromise

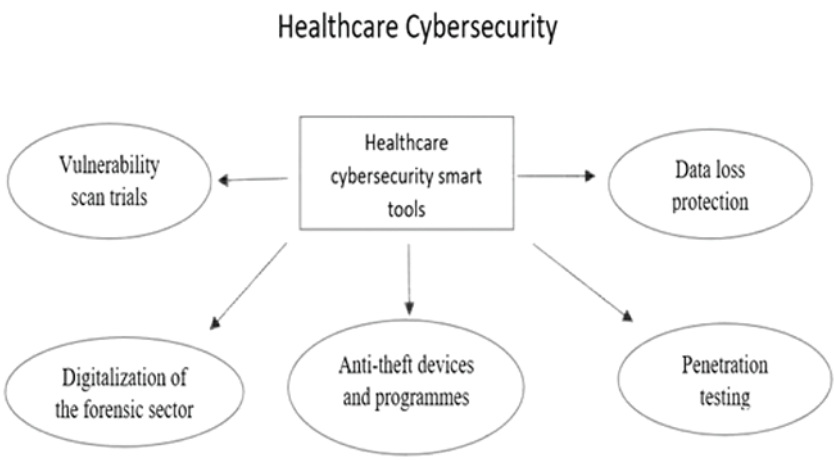

FIGURE 1.1 Healthcare Cybersecurity.

affected healthcare devices' malfunctions and leads to information leaks. In the end, it contributes to affected person safety and health by retaining the precision and dependability of scientific devices and systems.

Cybersecurity acts as a guard in opposing unauthorized use, access, and disclosure of patient data, scientific records, and assets. The wide variety of digital gateways that could be used for cybercrime is growing as technological know-how advances. The Internet of Things (IoT), big data, and cloud computing have opened up new possibilities for affected person fitness monitoring. In actuality, one of the IoT gadget use cases that is increasing the fastest is the healthcare sector. As more healthcare businesses are pressured to enter into contracts with outside companies for certain components of their service delivery, a wide variety of security risks end up appearing. Along with hiring special sanitary service vendors and outside caterers, they may also designate a point of contact for affecting person assistance. With each new company comes an accelerated threat of a compromise involving protected fitness information. Like most other industries, the healthcare sector uses interconnected networks to optimize efficacy and utilize data. However, increased connection additionally makes hacks more likely.[13,14]

Given the healthcare industry's growing reliance on drugs and cell devices and its expanding technological complexity, groups ought to think about imposing encryption and other protection measures. Network protection can also generally be supported by antivirus software, however these packages need to be up to date on an everyday basis. Antivirus software needs to be updated often to make certain that healthcare companies are blanketed from the latest threats, given the changing nature of cyber risk management strategies.[15] The fitness information management sector employs professionals in healthcare cybersecurity. The security, privacy, and accuracy of affected person information are accountable to fitness information management. As larger institutions move toward digital health records and systems, experts will be wanted to handle this data and make it invulnerable. Backups are a vital issue of each safety response and recovery plan. Backups are tricky because they might propagate touchy data, including scientific records, over other networks, increasing additional uncertainties and dangers. Patient information, which the regulation recognized as the Health Insurance Portability and Accountability Act now and again designates as including fitness information, is amongst the utmost sensitive information that is presently reachable and is frequently the goal of adversarial attacks. In most healthcare facilities, organizing a bodily connection to the clinic network is pretty easy.[16] The enterprise has grown to be extra built-in through the use of telemedicine, e-health, the net of scientific things, digital fitness records, and synthetic brain technologies. As automation and interoperability have improved with technology, the probability of cyber failures has increased. When operational technologies (OTs) are linked with the Internet of Things, greater standardization challenges are created. IoT and OTs have been previously managed independently through standardization procedures. As such, the amalgamation of countless product classes gave rise to supplementary cybersecurity concerns. As a result, in order to tackle and overcome the new difficulties introduced with the aid of the hastily changing digital world, new sorts of governance are required. In the healthcare sector, employee error and unauthorized disclosure are the principal reasons in statistics of privacy breaches.

It is no longer surprising that the majority of scientific staff participants do not prioritize laptop safety in an already overloaded environment. When it comes to essential cybersecurity, the healthcare area falls behind other sectors. Examples include manufacturing and finance, which often build their infrastructure with record-keeping fortification. The reward that cybercriminals may receive for engaging in this type of activity is unknown.[17]

1.3 ATTACKS ON CYBERSECURITY

Attacks including denial of service, probing, malware, zero-day, phishing, sinkhole, consumer root, adversarial, poisoning, evasive, integrity violation, and causal attacks can all have an influence on the cybersecurity system. Most studies have used deep studying algorithms to discover these dangers. Below is a listing of some of the assaults that we looked at for this survey. We analysed a number of studies that addressed the identification of cybersecurity attacks using the deep mastering idea. The nature and dreams of the assailants are also covered.

1.3.1 Attackers of Many Types

Three kinds of knowledge are at the attacker's disposal. In a black box attack, the attacker is uninformed about and lacks understanding of the deep learning model. In the gray container model, the attackers have a widespread understanding of the model and are aware of the specifics of certain of its components. In simple terms, this is the worst-case scenario, where the attacker is aware of the white box model but is unaware of the potential background effects after targeting an organization. Below are safeguarding methods for user data and organization data.

1.3.2 Adversaries' Goals

This classification illustrates the variations in the enemies' goals. When a focused attack by means of an adversary motives a neural network to classify data incorrectly, this is recognized as an integrity violation. When an adversary attacks the system's obtainability and makes it unobtainable for a defined duration of time, this is recognized as an availability breach. When a rival tries to get personal information that constitutes a privacy violation, two major techniques are used by the attacker to execute the assault: a focused attack and a random attack. During the targeted assault, the adversary focuses on a particular area of the coaching sample in an attempt to get a fallacious result. By focusing on any area of the education sample, the random assault attempts to incorrectly identify the output result.

1.4 TYPES OF CYBERSECURITY ATTACKS

Denial-of-Service attack (DoS): The technique includes flooding the goal recipient with traffic, stopping them from the usage of the applicable PC in order to use the service. The major objective of this attack is to deactivate or freeze the service, both permanently or temporarily,[18] to disrupt services, overburden networks with data,

and restrict licensed customers from accessing their personal networks in order to launch denial-of-service attacks. A denial-of-service (DoS) attack pursues crushing a system's assets to the extent that it is unable to react to official requests for service. An allotted denial-of-service attack is similar in that it seeks to exhaust the sources of a system. A DoS assault is initiated via a variety of malware-infected host machines that are managed by the attacker.[19] A denial-of-service (DoS) attack sends an excessive amount of unauthorized requests to the target website. All of the responses drain the site's assets because each request has to be answered. This frequently results in the internet site shutting down indefinitely and stops it from imparting the standard services to users as defined in Figure 1.2.

Malware attack:
There are many different types of cyberattacks like this one. Malicious software viruses, along with worms, spyware, ransomware, adware, and trojans, are referred to as "malware". The trojan contamination poses as an proper piece of software. Ransomware blocks get right of entry to the network's vital components, whilst adware steals all of your non-public records as well as your knowledge. Adware is software that shows banner commercials and other types of advertising and marketing on a user's screen.[20]

Man in the middle (MITM):
Cybersecurity vulnerabilities recognized as "man-in-the-middle" (MITM) attacks let an attacker listen in on information that is exchanged between two people, networks, or devices. It affects the integrity of the data. Miscommunication between the events arises when an intruder discreetly eavesdrops on a dialogue between two parties, modifies the records in the middle, and then sends it to the other counterpart. Thus, these methods enable remote MITM attacks. Trojan malware is commonly employed to sidestep antivirus software's detection.[21]

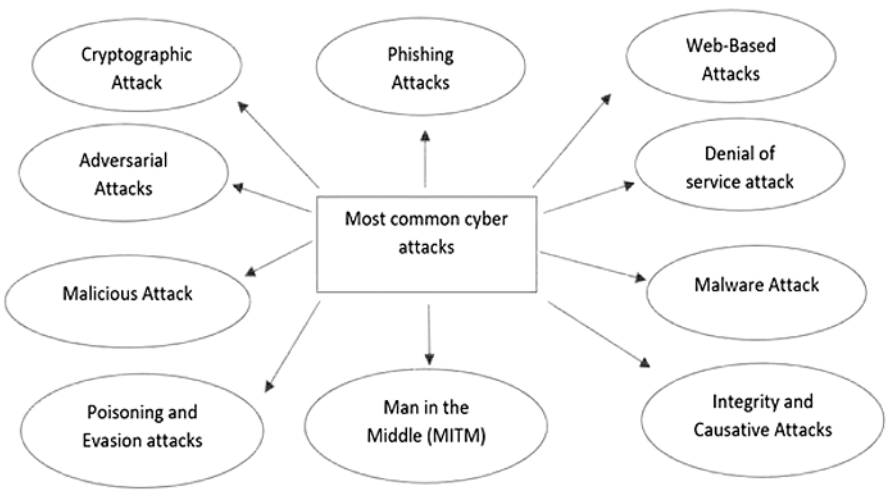

FIGURE 1.2 Most common cyberattacks.

Malicious attack:
If malware such phishing or unsolicited mail emails, or an exterior disk, is used to hack or exchange records without the user's consent. Without the user's awareness, malicious software ruins the machine. Trojan horses, spyware, ransomware, rootkits, and viruses are examples of malicious software. A malware assault requires the program to be hooked up on the target device. To do this, the consumer desires to take action. Therefore, in addition to the usage of firewalls that can discover malware, customers must be informed about the types of software program to avoid, the types of hyperlinks they should double-check before opening, and the emails and attachments they should no longer deal with.[22]

Remote to nearby attack:
The attackers use the network connections to their gain and attack the gadget by taking advantage of the vulnerabilities, regularly referred to as bugs, in the system. The attackers make use of their pre-existing accounts to reap unauthorized right of entry to the system throughout the local attack. While far flung assaults are less complicated to neutralize, local assaults are harder to detect. Intruders transmit packets amongst the gadgets and the network is the medium to process distant local attacks. It exploits the flaws in a machine.[23]

Phishing:
Phishing is the act of tricking individuals or groups into disclosing records or performing an unfavorable PC operation. Phishing is the practice of sending fraudulent emails to deceive recipients into disclosing private information or to urge the download of unsafe malware. According to the 2020 phishing report by way of the European Network and Information Security Agency (ENISA), agencies misplaced over 26 billion USD as a result of electronic mail compromise attacks. Malware was once blanketed in 42.8% of all Microsoft Office report attachments that have been downloaded. Phishing scams extended by 667% in a single month.[23]

Adversarial attacks:
One wonders if deep mastering is suitable for privacy-related functions in light of adversarial attacks, a method that considers the text, image, and graph protection of the Deep Neural Network model. For the bank often uses the customer's photo to verify whether or not they are an authorized user when inquiring for identification. When a financial institution offers savings to someone who isn't always authorized, it suffers massive losses. Deep neural networks want protection tactics because of this. An adversary using a deep neural community can hack a system with the aid of injecting bogus inputs and making the mannequin classify things wrongly. In adversarial attacks, which are frequently white-box attacks, perturbations similar to the training input are inserted by the attackers. Often, the defences against white field attacks are not very effective.[24] They additionally appeared at the troubles these methods created and developed a sketch to fend off this assault utilizing protective distillation and the targeted gradient sign method. P-tampering is an attack that occurs when a mastering technique is blended with a horrendous malevolent noise. Here, the education data, which has a probability of

p, is manipulated through the attacker. He can solely select hostile examples with actual labels, though.[25]

Web-based attacks:
Recently, there has been an enlargement in the use of internet services, which has led to an expansion in web-based attacks. These assaults are appealing to hackers due to the fact that they furnish them the hazard to make the most of more than a few device flaws, malicious URLs, scripts, and even download dangerous files. Even with the ongoing updates and enhancements to browser security measures, hackers are nevertheless in a position to find new vulnerabilities. Attacks by the net affect the accessibility of websites and APIs and have the power to jeopardize facts, confidentiality, and integrity. Form jacking, the use of browser extensions, as well as downloading malicious applications through on-line converters are the most established sorts of web-based assaults.[26]

Cryptographic attack:
Cryptographic assaults are a tactic involving using hackers to target cryptographic solutions, like encryption keys, ciphertext, etc. These assaults intend to both extract the plaintext from the ciphertext and decrypt the encrypted data. Hackers may additionally strive to stay away from the protection of a cryptographic system by using finding flaws in encryption algorithms, cryptographic protocols, key administration techniques, or cryptography methodologies. Encrypting sensitive records helps to stop unauthorized use. Decoding the encrypted statistics is the aim of the cryptographic assault, though. Messages are encrypted using binary coding, but in the present day, it is pretty easy to decrypt them and utilize them for monetary gain.[27]

Poisoning and evasion attacks:
Attacks with poisoning take place in the deep gaining knowledge of the training stage. To reduce the forecast accuracy of the deep learning algorithm, the attacker introduces the virus into learning samples. The extrapolation technique of deep learning is the goal of most evasion attacks. Here, the attacker manipulates the neural community to furnish false input, which leads to a false categorization result. In each case the attacker is in control of the input data. The Particle Swarm Optimization (PSO) method was once applied to combat the attacks with the aid of focusing on the education segment in the situation of poison attacks and the interference phase in the case of evasive assaults. The accuracy of the classification fell when malware samples had been added, going from 95% to 33% for poisoning attacks and from 93% to 33% for different attacks.

Integrity attacks:
Altering or tainting the facts saved on the machine is the important objective of integrity attacks. The attacker usually encrypts necessary records belonging to the association covertly and demands a hefty ransom to decrypt it, a best attack for switching records integrity. By partly inserting malware into the chosen aspects and hopping between other computers, the attacker can infiltrate a system that is not experiencing any problems.

Causative attacks:
The major goal of the causal attack is to cause the decision-making algorithm to generate an inaccurate neural network classification. This illustrates how causal assaults can be launched in opposition to most estimation algorithms, an invulnerable parameter estimation technique that can distinguish between assaults and the neural network model. An overview of the cybersecurity attacks that were carried out is given in Table 1.1.

1.4.1 Fundamental Ideas and Frameworks in Cybersecurity

In order to show how chance management strategies may be utilized to address security-related problems, it starts with frequent dangers to records and systems. For instance, well-intentioned safety precautions might also have negative aspect effects, such as providing hackers with admission to personal data. Practical security solutions may also be challenging to graph due to the fact that asymmetries and externalities are the root reason of many safety challenges.[31]

TABLE 1.1
The applications of cybersecurity in healthcare

S.No	Applications	Descriptions
1.	Healthcare information security	Cybersecurity can identify, assess, then react toward cyberattacks more rapidly than human intervention. It increases facts technology safety and productivity for organizations with restrained time, money, or human resources. It would possibly notably affect how records are processed throughout apps. Robotics quickly scans huge volumes of data for irregularities or uses cybersecurity to alert users to viable risks. With time, machines examine from ever-larger information sets and improve their capability to discover anomalies. The patient's fitness comes first in healthcare, and this depends more and more on clinical methods and technology.
2.	Medical equipment security	It is essential to make medical equipment invulnerable, encrypt facts on every feasible occasion, and conduct vulnerability assessments on the software program that's mounted on these devices. Threats to cybersecurity are ever-growing. Software manufacturers frequently launch updates for their merchandise due to the fact that no machine is flawless. The transition to telecommuting has worsened the problem of healthcare agencies being among the most common aims of cyberattacks. As the scientific system commercial enterprise develops, implanted units are depending extra and more on software to store lives. After the software is made available, hackers will try to cause an application trouble by attacking it with whatever compromised versions of the protocol that they are able to identify.

(*continued*)

TABLE 1.1 (Continued)
The applications of cybersecurity in healthcare

S.No	Applications	Descriptions
3	Securing and safeguarding patient databank	Training in cybersecurity must be furnished to all personnel participants who are accountable for protecting affected person data. To enhance cybersecurity in healthcare, tools like antivirus software, backups, information recovery, prevention of records loss, e-mail gateways, event response systems, firewalls, intrusion detection systems, policies, cell machine administration, security cognizance, patch super vision, web gateways, and further basic security precautions are employed. Criminals can also be fascinated by compassionate patient statistics due to their achievable excessive monetary worth. Since extra-medical specialists and non-clinical workforce are now supplying affected person care offerings online, they are more vulnerable to cyberattacks. The majority of the compliance structures in the vicinity today for safeguarding scientific data and statistics are reactive in nature, reprimanding healthcare corporations following data breaches.
4	Securing stakeholders' access to healthcare	Constant verbal exchanges with staff members and different important stakeholders, making use of strong authentication measures to tightly close means of admission to software systems and data, as properly as *aides mémoire* of safety behaviours are in addition indispensable approaches in the prevention of a protection disaster. Cybercriminals may also be able to take advantage of any vulnerable point in the supply chain to gain right of entry to a target. Within a healthcare ecosystem, sturdy enterprise ties can jeopardize the ecosystem as a whole. Many proprietary purposes and technologies are typically used in healthcare institutions, and these ought to be integrated into an IT protection architecture. In the state-of-the-art world, strengthening healthcare cybersecurity has grown to be crucial considering that hackers continuously target organizations. A good sized evaluation of cyberthreats and attainable risks to a healthcare business enterprise was supplied in the preceding discussion.
5	Enhancing healthcare outcomes	By facilitating easier entry to and effectiveness in affected person care, cybersecurity enhances healthcare consequences. The development of digital applied sciences as well as the growing interconnectivity of a variety of healthcare structures have led to the emergence of cybersecurity vulnerabilities in the healthcare industry. The protection of healthcare structures provides substantial problems for cybersecurity. These structures include digital fitness records, scientific devices, software, and gear utilized in the administration and provision of healthcare. When overworked teams of workers,

TABLE 1.1 (Continued)
The applications of cybersecurity in healthcare

S.No	Applications	Descriptions
		individuals, and IT groups' hostilities hold up with changing demands, fundamental cybersecurity rules can without problems be neglected, endangering affected person fitness and clinical data. Customers are becoming extra mindful of security flaws consisting of phishing attempts, damaged portals, and old-fashioned browser usage, therefore healthcare data handling third party vendor corporations that go through from community breaches hazard hastily losing the trust of their patients. The healthcare area has historically been seen as an appropriate target for cybercriminals. They are experimenting with more advanced methods of breaking healthcare cybersecurity regulations, such as valuing patient data and having a low threshold for outages that can impair affected person care.
6	Preventing attacks	The goal of healthcare cybersecurity is to thwart intrusions with the aid of defending patient information on systems from unauthorized admittance, use, and disclosure. The safety plus uprightness of quintessential patient data may want to jeopardize patients' lives in the course of a hack. Cyberattacks can be many distinct things, which include ransomware or identity theft. The size of the facility determines how serious an attack is. Cybercriminals' advances will quickly make it feasible for them to interfere with the technologies that healthcare groups presently use. Hospital IT teams need to create and put into effect cutting-edge, integrated security applied sciences if they wish to prosper. Thankfully, automation has benefits for both thieves and the healthcare sector. Healthcare protection professionals will be capable of remaining in advance of the wave of malware threats centred solely at their agency as safety automation advances.
7	Providing assistance to security teams	In many different ways, this technology helps avoid protection breaches in the healthcare industry. Service carriers can first consider their community infrastructure, discover any manageable protection holes, and even assist protection teams in making positive legal guidelines like the Healthcare Identifiers Act are followed. Establishing a strong safety system requires extra than just hiring a progressive IT specialist. To maintain data security, it involves finding susceptible infrastructure links and conducting popular audits. Controlling information to gain right of entry to points and security structures requires a proactive approach as well. There is an international cyberattack pandemic that has destroyed organizations and left customers severely injured. The healthcare quarter has been a particularly tough hit, with a deluge of cyberattacks.

1.4.2 Information Security and Systems Security

Information safety threats. Information security has three protecting objectives: availability, integrity, and secrecy. Protect exclusive facts to avoid unauthorized access. Integrity: the ability to give up or discover unauthorized statistics modification. Availability: defend in opposition to unauthorized erasure or interference. These protecting objectives cover data at rest, which is facts stored on a computer or paper, as properly as records in transit, which is information sent over a network. The terms "unauthorised" things to do are used in the definitions, indicating that there is agreement on which actors are allowed get admission to the data.[28] Three key dreams of content protection are availability, integrity, and confidentiality. We can also be concerned about the identities of the other actors in addition to the content. For instance, we would like to comprehend whether or not an email message's sender has been fraudulently represented. The motive of protection: Authenticity discourages actor impersonation and normally functions by providing a means for others to affirm a declare of identification. An associated and even greater wonderful protective purpose is nonrepudiation, which precludes actors from negating that they carried out a unique behaviour, such as delivering a message. Genuineness and non-repudiation are prerequisites for maintaining actors' accountability.

Information security, however, is simply one facet of device security. There are positive systems that have zero interesting facts. Nevertheless, we count numbers of their functionality, or on a procedure that runs according to plan. For systems, availability and integrity are two common safety goals. One intention of intellectual property protection can be to hold the secrecy of a precise method. In the topic of systems security, cyber-physical systems—that is, systems that have an impact on the real world—such as industrial robots, traffic lights, autopilots, and control structures for chemical or energy plant operations—are of particular interest. Since some of these structures are fundamental infrastructures, their failures ought to have a substantial have an effect on society.

1.4.3 Data Security and Network Security Threats

Data transfer and storage are critical to many computing operations. When data is saved on a system, adversaries can alter it with each "data in transit" and "data at rest". Conversely, information can be gathered extra-surreptitiously in the course of transmission by means of listening in on the communication. Eavesdropping is possible in many disbursed structures with more than one aspect that speak over public networks. Any verbal exchange that takes place between the sender and the recipient can be viewed by way of attackers in manipulating intermediary systems, including routers or Wi-Fi get admission to points. Wireless communications can doubtless be intercepted via an attacker if they are near to the parties involved in the conversation. Eavesdroppers are acknowledged as passive attackers considering they do not now impede communications. Encrypted conversation requires the sender and the recipient to establish a cryptographic key. Usually, this key is simply an adequate number of random bits. The sender and the recipient share a single key when making use of symmetric cryptography. The key must be exchanged "out of band", that is, over a channel uncontrolled by way of the parties'

viewed attackers. The technique through which the sender feeds a message and the key into an encryption mechanism yields the encrypted communication, or ciphertext. The recipient decrypts the ciphertext through giving the identical key to the decryption function. An eavesdropper would have the greatest advantage in guessing the key. Remember that encryption frequently only encrypts the message's content; the names of the sender and recipient are disclosed in clear text. Routers need these addresses in order to forward messages to the right people. Because they can still confirm who is talking with whom, when, and how often, eavesdroppers are capable to analyse the network traffic and based on the traffic flow it will perform assaults. It is possible to sidestep visitors' evaluation efforts by means of the usage of a number of encryption layers and sending messages across extra nodes to obfuscate their path.

One of the most necessary elements of sophisticated attacks is goal comprehension. Because networked devices may also be customized to the victim's environment, they furnish a plethora of facts that can be used to launch assaults that have a greater risk of success. Attackers gain from this due to the fact the Internet is designed to be an open network. Network operator records are publicly handy to enable communication between machine directors globally in the resolution of a problem.

1.5 MULTIPLE ASPECTS OF CYBERSECURITY IN THE FIELD OF HEALTHCARE

In the medical industry, cybersecurity performs several tremendous roles. More than a few uses and advancements of cybersecurity in the healthcare area are explained in depth in Figure 1.3 The major duties that are highlighted are records protection,

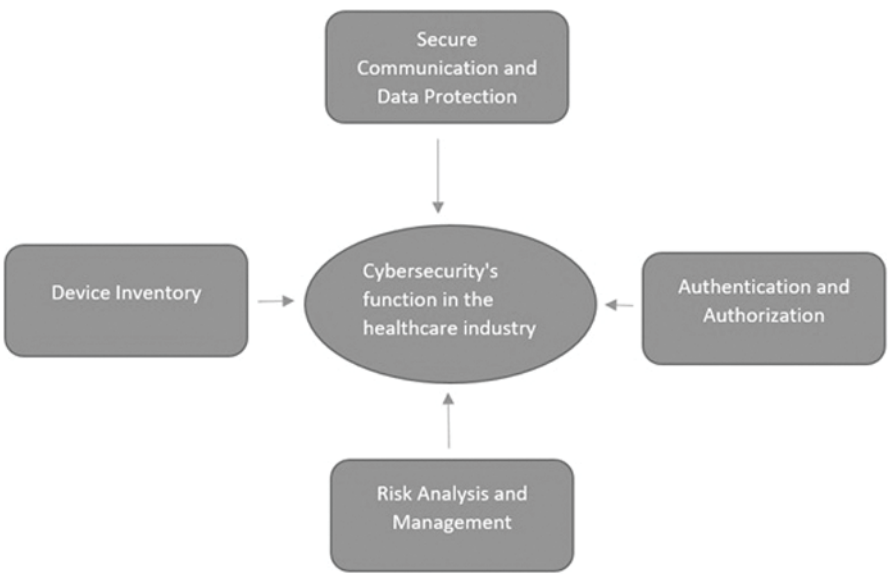

FIGURE 1.3 Functions and developments of cybersecurity in the healthcare industry.

a number of equipment and services that decorate healthcare operations, managing dangers in familiar situations and their evaluation, safety training, complete protection of patient facts and history, etc. Their contributions and successes are extremely important, especially in the healthcare sector.[29] Patient information includes each individually identifiable piece of information and scientific information. Patients' and physicians' reputations can suffer from an information breach. Cyberattacks are much less probable when IT structures that handle and preserve medical information are extra-securely configured. Laws set up security requirements to protect scientific statistics and impose protections for affected persons, facts, and healthcare organisations. The elaborate net of devices, apps, technology, and regulatory compliance makes cybersecurity in healthcare a challenging endeavour requiring specialized knowledge. The use of cybersecurity in healthcare will grow in importance as greater applied sciences are employed in the field.

Cybercriminals are drawn to healthcare corporations due to the fact that they comprise fairly treasured information. Modern technology has been used increasingly through the healthcare enterprise in latest decades. Examples of this technological know-how encompass greater medical equipment, cloud-based healthcare facts storage, software for keeping patient profiles, and other tools. Healthcare professionals' duties have been made simpler by using these technological know-how advancements, which have additionally led to a paperless environment. Nevertheless, there is now a higher chance of information breaches and cyberattacks.[30, 31] Given the interconnectedness of IT, IoT, and IoMT devices, augmented reality, robotics, and other technologies, it is obvious that the majority of healthcare organizations' cutting-edge perimeter-based security approaches will no longer be advantageous in thwarting sophisticated assaults. Healthcare firms need to move away from a perimeter-based safety paradigm whilst preserving their funding in the fundamentals in order to continue to be in advance of these developments. It is acceptable that all healthcare amenities repair mistakes as soon as they can. Usage of computational methods to defend its customers because unpatched vulnerabilities in the virus make it dangerous. Every time the contamination reactivates, it ought to be stopped. Software patches, on the other hand, are solely useful if IT options use mounted fixes to keep present programs present-day as they are developed. Complicated IT systems have to take into account how to manage an attack's aftermath in addition to retaining up-to-date software programs and gorgeous gadget and community safety settings. Because of this, full data backups that include all saved facts and software programs ought to be an essential characteristic of all managed IT systems. Organizations can submit their records and get returned to business more rapidly if they have a reproduction of it. In addition to outdated and susceptible software, employees can serve as a backdoor for malicious apps to infect all working tools and networks. Many healthcare facilities donate equipment to carers and different non-staff individuals. This increases the threat of system theft or loss. In this way, thieves can obtain lost or stolen goods. In this instance, restricting the device's usability is quintessential to forestall a records breach. Additionally, a range of alternatives are accessible, which include far off wiping and locking, GPS function tracking, and more. Wireless networks can be used to get admission to the server's affected

person data. If records are not safeguarded, cybercriminals can effortlessly get them. Therefore, describing the device that will communicate with the server in order to retrieve the data is essential. It helps ensure compliance by way of assisting in the detection and blocking of leaks and by means of imparting trustworthy facts protection.[32] Most humans suppose that the hardest element for scientific establishments to do is cut costs. But safeguarding affected person information is more important and challenging than reducing costs. Everyone knows that most profitable cyberattacks make use of generic vulnerabilities. Simple adjustments can also tackle these shortcomings. Unfortunately, the majority of people overlook installing the most present-day security updates on their devices, leaving holes that hackers can take advantage of. Systems for cybersecurity and healthcare preserve indispensable patient data. Hackers may also learn from this information. Cyberattacks on healthcare networks may additionally cause ambulances to be diverted, appointments and strategies to be cancelled, and in excessive cases, even fatalities. Healthcare organisations' cybersecurity group of workers will find it simpler to hold the security of their structures with the help of the preceding guidance. Healthcare facilities such as hospitals, clinics, and doctors' places of work need to deliver splendid care while maintaining the protection of their sufferers and employees.[33] For the program to feature besides errors, regular updates are also required. The majority of antivirus programs alert users when there are updates available, and some even have computerized updates. Vital health data needs to be blanketed from unanticipated occasions like fires, natural catastrophes, etc. Having a healing design and growing backups of the small print are crucial components of this process. Maintaining backups is indispensable for protecting facts and for quickly and exactly restoring them when needed. Because it requires little technical know-how and no hardware investment, cloud computing is a popular backup option. This function can be used by healthcare corporations to prevent users from carrying out specific tasks, like printing, sending data to an exterior tough drive, collaborating in illegal e-mail exchanges, and importing information on the Internet. Additionally, records usage administration can be mixed with records discovery and categorization to ensure that touchy fabric is identified and not exploited.[34]

1.6 APPLICATIONS OF CYBERSECURITY IN HEALTHCARE

Because healthcare businesses take care of massive quantities of records that hackers view as having exquisite financial and intelligence value, they are specifically inclined to receive assaults. Critical and secret data may include, however are not restrained to, financial data, social protection numbers, the patient's exclusive fitness history and information, and records applicable to research and innovation. Hospitals rent a state-of-the-art cyber-network of units to meet their requirements and manage large volumes of tools and data. Large companies most probably have a good sized network connected to servers that hold quintessential information. MRI tools usually have a couple of workstations linked to them so that operators can alter MRI images. These devices could be used as viable factors of entry through hackers attempting to get entry to the network's information-storage systems. Sensitive data might, of

course, be partly decrypted or disclosed. Clinicians utilize pseudonymization as a method to explain medical diagnoses or therapies to patients. Doctors additionally use anonymization when it comes to information that is a section of records or a diagram to improve a certain service. Strong protection measures must be in place at healthcare companies to reduce the possibility of e-mail account compromise breaches and other occurrences associated to cyber safety risks.[35,36] Computer systems in the healthcare enterprise are a prime target for extortion attempts for the reason that they assist companies in supplying awesome patient offerings and keep touchy data. Phishing is a popular cyberattack technique in which a hacker targets a reliable enterprise or man or woman in an effort to acquire their favour. E-mails have long been conceived of as a possible entry point because of their phone files and phoney Internet links. E-mail breaches are specifically concerning because personnel in the healthcare sector frequently send touchy data through e-mail. As a result, safety theories and strategies related to e-health are comparable to those applied via producers of integral linked systems.[37] The principal contrast is that scientific devices control fitness data, which is extremely lucrative to hackers. Strict legal guidelines apply to private scientific records. These restrictions enforce additional security protocols to make certain the privacy of affected person data. If there is a protection breach, healthcare agencies have to pay hefty expenses. The health enterprise ought to be aware of this perilous circumstance and organized to take all requisite security measures, inclusive of allocating sufficient monetary and technological resources, to safeguard its health apps and records banks. Data in the health area is sensitive given that most documents have the potential to be quite burdensome if hacked. Cybercriminals in many instances target healthcare organizations, hoping to exploit gaps in protection approaches to gain entry to touchy data. Healthcare personnel should be able to gain entry to and make use of the available technologies. The end-user is one potentially inclined hyperlink in an otherwise robust cybersecurity system. Phishing and spoofing attempts may be directed towards employees. The perfect method is to use real-world hacking and phishing scenarios. Employees want to be informed about how to file questionable activities. It is essential to furnish training to employees concerning the suitable use of technology whilst upholding network security.[38] Employees should know precisely the place they stand in the company's protection system. The healthcare sector can gain from the use of digital forensics, multiple-factor authentication, anti-theft devices, catastrophe recovery and continuity plans, community fragmentation, identity testing, information interchange, and hazard scanning. Among industries with the highest ranges of law and oversight worldwide is the healthcare sector. Laws, regulations, and insurance policies impose strict restrictions and duties on healthcare payers and providers. Cyber healthcare threats have additionally long been a serious difficulty due to a wide variety of variables.

1.7 INTEGRATION OF MACHINE LEARNING AND CYBERSECURITY

The main benefit of combining machine learning and cybersecurity is the ability to use artificial intelligence to identify, analyse, and control cyberattacks, as briefly explained in the section below.

1.7.1 Machine Learning in Cybersecurity

Cyberspace structures are vulnerable to a wide variety of attacks, which include replay, man-in-the-middle, impersonation, password guessing, unauthorized information updates, malware injection, flooding, denial of carrier and disbursed denial of service (DDoS), among many others. As a result, in order to discover and end these assaults, we require reliable safety procedures. With the pre-processed information that is provided, the laptop mastering fashions (machine studying ML algorithms) can learn about exclusive cyberattacks that appear online. The computing device mastering algorithms are in a position to discover any indication of infiltration, or cyberattack, in real-time, or on-line mode. Figure 1.4 shows the "machine learning in cyber security" scenario. These Internet-connected gadgets, which include laptops, computer computers, smartphones, and Internet of Things (IoT) devices, can be utilized for a range of on-line functions, including social protection numbers, on-line banking transactions, and on-line admission to healthcare data. Hackers are continuously looking for weaknesses in these sorts of systems, and they launch their attacks as soon as they discover any. Depending on the circumstance, countless ML techniques, such as supervised learning, unsupervised learning, reinforcement learning, and deep learning, can be utilized for the detection and mitigation of cyberattacks. Which approach (supervised learning, unsupervised learning, reinforcement learning, or deep learning) precisely suits the structures relies upon their verbal exchange surroundings and accessible resources. Cloud servers are a splendid alternative for gaining knowledge of (training) and predicting (testing) cyberattacks due to their high processing and storage capacities.

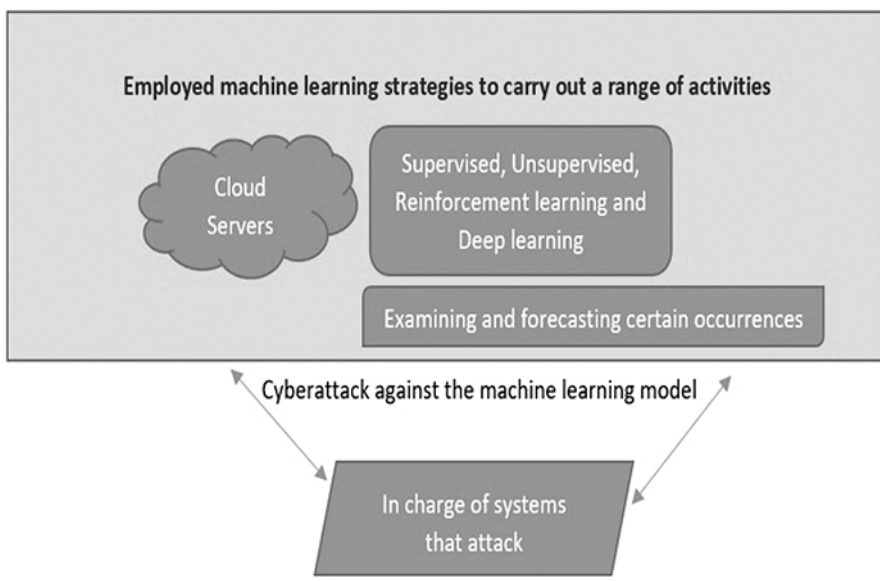

FIGURE 1.4 Cybersecurity scenario for machine learning.

1.7.2 Cybersecurity in Machine Learning

The situation of "cyber protection in laptop learning", or desktop studying (ML) security, is shown in Figure 1.4. Machine studying fashions are used to analyse and forecast a broad range of events. The effectiveness of computers gaining knowledge of models, however, might also be impacted by using specific attacks, such as runtime interruption, membership inference, dataset poisoning, mannequin poisoning, and privacy breach attacks.[39] These assaults can also lead to ML fashions wrongly anticipating related phenomena. A "dataset poisoning attack" occurs when a hacker modifies values in the dataset to introduce adversarial samples, which cause the computing device learning model to make inaccurate predictions. The objective of the "model poisoning attack" is for the attacker to regulate the parameters and disrupt the interior workings of the models in order to similarly pollute them. In an effort to depict sensitive data, the attacker in a "privacy breach attack" tries to accumulate quintessential mannequin information. The membership inference assault is one form of privacy infringement. Furthermore, an attacker conducting a "runtime disruption attack" subverts the laptop studying workflow and impacts the accuracy of the prediction outcomes by means of focusing on the model's execution process. Therefore, unique cyber safety structures (including hashing algorithms, encryption techniques, as properly as signature generation and verification procedures) are wanted to defend in opposition to these assaults. When these cyber protection measures are put into practice, the ML fashions and associated datasets turn out to be secure, and we get the expected outcomes and predictions.

1.7.3 Positive Impact of Combining Cybersecurity with Machine Learning

Cybersecurity and computing devices cooperate to work interdependently and can enrich each other's effectiveness. What follows are some of the advantages of their becoming a member of securing information by functioning as cybersecurity forces.

ML models' full proof security: As used to be formerly said, ML models are prone to a wide variety of threats. The likelihood of these attacks could potentially affect the ML model's functionality, accuracy, and forecasts. On the other hand, these undesirable events can be prevented by way of the use of particular cyber protection measures. The use of cyber safety measures secures the ML models' performance and overall performance by processing datasets, permitting us to attain correct predictions and outcomes.[40]

Enhanced efficacy of cyber security methods: The software of laptop mastering algorithms for intrusion detection systems enhances their effectiveness, ensuing in improved precision and detection rates with a reduced cost of false positives. ML techniques, such as deep learning algorithms, reinforcement learning, unsupervised learning, and supervised learning, can be utilized based totally on the related systems and communication environment.

Effective detection of zero-day attacks: Cybersecurity strategies that use computer learning models to discover intrusions appear to be particularly profitable in figuring out zero-day attacks, additionally regarded as unknown malware attacks. They take place as a result of using certain deployed computing device studying

models to help with the detection. The way that computers gain knowledge to operates is by means of gathering and evaluating specific features; If a program's aspects coincide with those of a malicious program, then that program is deemed malicious. This detection process can be handled automatically by the ML model Therefore, mingling cyber protection and machine studying can correctly discover zero-day attacks.

Minimal need for human intervention: The majority of duties in desktops gaining knowledge of (ML) systems are completed through the used ML models. When cyber safety and computing device learning are combined, the majority of the jobs that these systems are used for are performed either entirely or almost entirely by humans.

Speedy scanning and moderation: For the reason that ML-based intrusion finding structures use unique ML algorithms, they are highly efficient at figuring out the presence of threats. Because of this, integrating computing devices gaining knowledge of cyber safety systems enables rapid intrusion detection and speedy response in the tournament that an incursion is detected.

The determination of a gorgeous desktop mastering algorithm is all that needs to be done.

1.7.4 Comparative Analysis

We have compared several methods under the headings of "machine learning in cyber security" and "cyber security in machine learning" in this part. The information is provided below.

1.7.4.1 Machine Learning's Performance Comparison in Cyber Security Protocols

Types of attack	Accuracy	Method used
Poisoning attack	91.80%	Isolation of poisoned point[41]
Poisoning attack	93.10%	Generative adversarial Networks[42]
Privacy attack	98.62%	Privacy preserving method[43]
Privacy attack	97.00%	Additive homomorphic encryption[44]
Accessing attack	98.6%	Combining fine tuning and pruning defence[45]
Accessing attack	99.97%	Activation cluster based scheme[46]

1.8 CONCLUSION AND FUTURE RESEARCH

Maintaining data change and storage privacy is crucial. Several protection measures have been proposed to guard the privacy of the information. However, these techniques are now not high quality in the case of a zero-day assault or a format flaw. Improvement is therefore required on the grounds that skilled hackers and cyberattacks are leveraging greater advanced technological know-how to get round device security. Consequently, it is necessary to implement new safety procedures with increased performance and safety structures that are resistant to zero-day vulnerabilities.

Compatibility of diverse tools and mechanisms: The "uniting of cyber safety and ML" makes use of a variety of equipment and mechanisms, including hashing techniques, laptop learning algorithms (clustering, classification, CNNs), encryption algorithms, signature creation and verification algorithms, and so forth. These mechanisms and equipment signify specific types of protection procedures. They also require specific hardware types and configurations. In these situations, there can also be compatibility issues with these mechanisms and tools.

Performance and overloading: As previously said, we combine ML with cybersecurity via a vary of methods. In order to run these quite numerous algorithms, we want a few extra resources. If not, the assignments may not be executed accurately. Combining and using a number of techniques may additionally thereby overload the system, which could further limit its functionality. As a result, we ought to exercise caution whilst deciding on our algorithms and try hard to create fresh, resource-efficient computing device studying or protection algorithms.

Increasing the accuracy of the system: Machine learning models depend on unique datasets to function; mistakes in these datasets or in the model's setups ought to cause problems. For example, the device may predict something wrong or the precision that has been performed may no longer be perfect. Researchers should therefore work to discover solutions to these problems; new strategies can be created to discover mistakes in datasets or improve system accuracy.

Cybercrime has an impact on a number of areas, including finance, manufacturing, IT, legal, and education. Due to its reliance on the persistent transmission of massive volumes of essential data, the healthcare sector is among the most coveted. Cyberattacks and data breaches have been happening at an alarmingly erratic pace. As cyber rules advance, healthcare facilities need to manage more than just patients' medical conditions. They prioritize health information security because they are also in charge of data preservation. Cybersecurity in the healthcare industry refers to securing electronic assets and data against unauthorized use, access, or disclosure. The majority of healthcare organizations continue to devote a tiny portion of their IT budget to cybersecurity despite the rise in cyberattacks. These assaults have an impact on how patients are handled in medical facilities. These breaches can affect patients not only because private information is exposed and potentially misused, but also because tampering with data may result in a delayed or inaccurate diagnosis. The finest performance of medical device security should be adhered to in order to ensure that cybersecurity safeguards function comprehensively. Use inventory data to ensure that all devices in the estate have been recognized. Despite the healthcare industry's considerable investment in cybersecurity, dissatisfied personnel may opt to intentionally disclose patient information out of animosity or to capitalize on the underground market for protected health records. This technology will have a large impact on healthcare in future generations.

REFERENCES

[1] J. Tully, J. Selzer, J.P. Phillips, P. O'Connor, & C. Dameff. (2020). Healthcare challenges in the era of cybersecurity. *Health Security*, 18(3), 228–231.

[2] M. Arvindhan, D. Rajeshkumar, A.L. Pal, A review of challenges and opportunities in machine learning for healthcare, in: *Exploratory Data Analytics for Healthcare*, (2021), pp. 67–84. Taylor & Francis

[3] C. Abraham, D. Chatterjee, R.R. Sims, Muddling through cybersecurity: insights from the US healthcare industry, *Bus. Horiz*. 62 (4) (2019) 539–548.

[4] S. Nifakos, K. Chandramouli, C.K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, S. Bonacina, Influence of human factors on cyber security within Healthcare Organizations: a systematic review, *Sensors* 1 (2021) 5119. https://doi.org/10.3390/s21155119.

[5] D. Markopoulou, V. Papakonstantinou, The regulatory framework for the protection of critical infrastructures against cyberthreats: identifying shortcomings and addressing future challenges: the case of the health sector in particular, *Comput. Law Secur. Rev*. 41 (2021) 105502.

[6] S.T. Argaw, J.R. Troncoso-Pastoriza, D. Lacey, M.V. Florin, F. Calcavecchia, D. Anderson, A. Flahault, Cybersecurity of hospitals: discussing the challenges and working towards mitigating the risks, *BMC Med. Inform. Decis. Mak*. 20 (1) (2020) 1–10.

[7] S.J. Choi, M.E. Johnson, The relationship between cybersecurity ratings and the risk of hospital data breaches, *J. Am. Med. Inform. Assoc*. 28 (10) (2021) 2085–2092.

[8] C.S. Chan, Complexity the worst enemy of security, 2012. www.schneier.com/news/archives/2012/12/complexity_the_worst.html. Last access 7 July 2019.

[9] L. Coventry, D. Branley, Cybersecurity in healthcare: a narrative review of trends, threats, and ways forward, *Maturitas* 113 (2018) 48–52.

[10] A. Turransky, M.H. Amini, Artificial intelligence and cybersecurity: tale of healthcare applications, *Cyberphys. Smart Cities Infrastruct.: Optim. Oper. Intell. Decis. Mak*. (2022) 1–11.

[11] S. Nifakos, K. Chandramouli, C.K. Nikolaou, P. Papachristou, S. Koch, E. Panaousis, S. Bonacina, Influence of human factors on cyber security within healthcare organisations: a systematic review, *Sensors* 21 (15) (2021) 5119.

[12] P. Radanliev, D. De Roure, Advancing the cybersecurity of the healthcare system with self-optimising and self-adaptative artificial intelligence (part 2), *Health Technol. (Berl.)* 12(5) (2022) 923–929.

[13] D. Branley-Bell, L. Coventry, E. Sillence, Promoting cybersecurity culture change in healthcare, in: *The 14th PErvasive Technologies Related to Assistive Environments Conference*, 2021, pp. 544–549.

[14] T. Andre, Cybersecurity an enterprise risk issue, *Healthc. Financ. Manage*. 71 (2) (2017) 40–46.

[15] S. Murphy, Is cybersecurity possible in healthcare, *Natl. Cybersecur. Inst. J*. 1 (3) (2015) 49–63.

[16] K.L. Offner, E. Sitnikova, K. Joiner, C.R. MacIntyre, Towards understanding cybersecurity capability in Australian healthcare organisations: a systematic review of recent trends, threats and mitigation, *Intell. Natl. Secur*. 35 (4) (2020) 556–585.

[17] J. Al-Muhtadi, B. Shahzad, K. Saleem, W. Jameel, M.A. Orgun, Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment, *Health Informat. J*. 25 (2) (2019) 315–329.

[18] A.A. Diro, N. Chilamkurti, Distributed attack detection scheme using deep learning approach for Internet of Things, *Future Gener. Comput. Syst*. 82 (2018) 761–768.

[19] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: *2ND IEEE PERCOM Workshop on Security Privacy and Trust in the Internet of Things*, 2017.

[20] V. Mnih, A.P. Badia, M. Mirza, A. Graves, T. Lillicrap, T. Harley, D. Silver, K. Kavukcuoglu, Asynchronous methods for deep reinforcement learning, in: International Conference on Machine Learning, 2016, pp. 1928–1937.

[21] P. Ratta, A. Kaur, S. Sharma, M. Shabaz, G. Dhiman, Application of blockchain and internet of things in healthcare and medical sector: applications, challenges, and future perspectives, *Hindawi J. Food Qual*. 1 (2021) Article ID 7608296.

[22] V.S. Naresh, S.S. Pericherla, P.S.R. Murty, S. Reddy, Internet of things in healthcare: architecture, applications, challenges, and solutions, *Comput. Syst. Sci. Eng*. 6 (2020) 411–421. © 2020 Tech Science Press.

[23] J. Wang, W. Chen, L.Wang, Y. Ren, R. Simon Sherratt, Blockchain-based data storage mechanism for industrial internet of things, *Intelligent Automation and Soft Computing* 26 5 (2020) 1157–1172.

[24] H. Xu, Y. Ma, H. Liu, D. Deb, H. Liu, J. Tang, A. Jain, Adversarial attacks and defenses in images, graphs and text: A review, 2019, *arXiv preprint* arXiv:1909.08072.

[25] Z. Katzir, Y. Elovici, Gradients cannot be tamed: Behind the impossible paradox of blocking targeted adversarial attacks, *IEEE Trans. Neural Netw. Learn. Syst*. 32 (1) (2020) 128–138.

[26] L. Fernandes, Data security and privacy in times of pandemic, in: Proceedings of the Digital Privacy and Security Conference, 2021.

[27] W. Jiang, H. Li, S. Liu, X. Luo, R. Lu, Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles, *IEEE Trans. Veh. Technol*. 69 (4) (2020) 4439–4449.

[28] J.P. Anderson, Information security in a multi-user computer environment. *Adv. Comput*. 12 (1972) 1–36.

[29] M.S. Jalali, J.P. Kaiser, Cybersecurity in hospitals: a systematic, organizational perspective, *J. Med. Internet Res*. 20 (5) (2018) e10059.

[30] A.R. Ravi, R.R. Nair, Cybersecurity threats and solutions in the current e-healthcare environment: a situational analysis, *Med.-Legal Update* 19 (2) (2019) 141–144.

[31] S. Mierzwa, S. RamaRao, J.A. Yun, B.G. Jeong, Proposal for the development and addition of a cybersecurity assessment section into technology involving global public health, *Int. J. Cybersecur. Intell. Cybercrime* 3 (2) (2020) 48–61.

[32] A. Namburu, D. Sumathi, R. Raut, R.H. Jhaveri, R.K. Dhanaraj, N. Subbulakshmi, B. Balusamy, FPGA-based deep learning models for analysing corona using chest X-ray images, *Mob. Inf. Syst*. 2022 (2022), 1–14.

[33] D. Giansanti, Cybersecurity and the digital-health: the challenge of this millennium, *Healthcare* 9 (2021) 62.

[34] D.K. Alferidah, N.Z. Jhanjhi, Cybersecurity impact over big data and IoT growth, in: 2020 International Conference on Computational Intelligence (ICCI), IEEE, 2020, pp. 103–108.

[35] C.N. Vanitha, S. Malathy, A multi-syndrome pathology for breast cancer through intelligent learning, in: IOP Conference Series: Materials Science and Engineering (Vol. 1055, No. 1). IOP Publishing, 2021, February, pp. 012073.

[36] D. Rajesh Kumar, K. Rajkumar, K. Lalitha, V. Dhanakoti, Bigdata in the management of diabetes mellitus treatment, in: Chakraborty, C., Banerjee, A., Kolekar, M., Garg, L., Chakraborty, B. (eds) Internet of Things for Healthcare Technologies. Studies in Big Data, vol 73. Springer, Singapore, 2021.

[37] D. Lee, S.N. Yoon, Application of artificial intelligence-based technologies in the healthcare industry: opportunities and challenges, *Int. J. Environ. Res. Public Health* 18 (1) (2021) 271.

[38] S. Ghafur, E. Grass, N.R. Jennings, A. Darzi, The challenges of cybersecurity in health care: the UK National Health Service as a case study, *Lancet Digital Health* 1 (1) (2019) e10–e12.

[39] Y. Sun, A.K. Bashir, U. Tariq, F. Xiao, Effective malware detection scheme based on classified behavior graph in IIoT, *Ad Hoc Netw*. 120 (2021) 102558.

[40] J. Yang, Z. Bian, J. Liu, B. Jiang, W. Lu, X. Gao, H. Song, Noreference quality assessment for screen content images using visual edge model and AdaBoosting neural network, *IEEE Trans. Image Process*. 30 (2021) 6801–6814.

[41] N. Peri, N. Gupta, W.R. Huang, L. Fowl, C. Zhu, S. Feizi, T. Goldstein, J.P. Dickerson, Strong baseline defenses against clean-label poisoning attacks, in: ECCV Workshop, 2020, pp. 55–70.

[42] J. Chen, X. Zhang, R. Zhang, C. Wang, L. Liu, De-pois: an attackagnostic defense against data poisoning attacks, 2021, CoRR, arXiv:2105.03592.

[43] P. Mohassel, Z.Y. Secureml, A system for scalable privacy preserving machine learning, in: IEEE Symposium on Security and Privacy, S&P, San Jose, USA, 2017, pp. 19–38, http://dx.doi.org/10.1109/SP.2017.12.

[44] L.T. Phong, Y. Aono, T. Hayashi, L. Wang, S. Moriai, Privacy preserving deep learning via additively homomorphic encryption, *IEEE Trans. Inf. Forensics Secur*. 13 (2018) 1333–1345, http://dx.doi.org/10.1109/TIFS.2017.2787987.

[45] K. Liu, B. Dolan-Gavitt, S. Garg, Fine-pruning: defending against backdooring attacks on deep neural networks, 2018, *CoRR*, arXiv: 1805.12185.

[46] B. Chen, W. Carvalho, N. Baracaldo, H. Ludwig, B. Edwards, T. Lee, I. Molloy, B. Srivastava, Detecting backdoor attacks on deep neural networks by activation clustering, in: SafeAI@AAAI, Honolulu, USA, 2019.

2 Blockchain Frameworks for Healthcare Data Storage and Exchange

R. Nancy Deborah, S. Alwyn Rajiv, A. Vinora, M. Soundarya, and G. Sivakarthi

2.1 INTRODUCTION

A cyber-physical scheme is a group of closely combined communication systems and equipment that provide a variety of security concerns in various manufacturing applications, comprising healthcare. Safety and confidentiality of patient records continue to be top issues since healthcare records are delicate and valuable, and it is primarily under attack online. Furthermore, from an industrial standpoint, the cyber-physical system is essential to remote data interchange via sensor nodes in dispersed areas. Because of its decentralized, immutable, and transparency features, blockchain technology presents a promising answer to the majority of securities-related problems in the healthcare sector.[1]

To enhance Healthcare 4.0, Kumar, M. et al. (2023) have proposed a system that makes use of the BigchainDB, Tendermint, IPFS, MongoDB, and AES encryption methods. A secure and dependable data exchange architecture modeled after blockchain technology is suggested. Additionally, a secure healthcare architecture powered by blockchain is shown for managing and accessing patient and physician records. A patient-centric approach is being taken in the creation of a blockchain-oriented Electronic Healthcare Record (EHR) interchange system. This implies that the owner retains complete ownership over their data, with blockchain technology providing security and privacy. According to our testing findings, the suggested design can withstand more security threats and recover data even in the event that two or three nodes fail. The proposed paradigm places the patient first; without user authorization, not even system administrators can access data. In order to enhance security and privacy, this gives the patient control over their data.[2]

According to Haleem, A. et al. (2021), blockchain technologies can reliably detect serious errors, even potentially harmful ones, in the therapeutic area. It can thereby improve the effectiveness, safety, and clearness of medical information interchange throughout the healthcare organization. Medical services can improve the analysis of medical evidence and obtain new understandings with the usage of this skill. They have researched the many advantages of blockchain technology for healthcare. A diagrammatic overview of blockchain technology's multiple features, enablers, and unified work-flow procedure to support global healthcare is presented. Finally, they presented and debated eighteen notable blockchain uses in the medical field. Since

 DOI: 10.1201/9781032711379-2

blockchain technology is essential to controlling deception in clinical tribunals, it has the potential to increase data efficiency for the healthcare business. In the healthcare sector, it can help ease concerns about data manipulation and allows for a different data storage configuration at the utmost level of safekeeping. It provides liability, adaptability, connectivity, and validation for data access. For a number of motives, health histories need to be kept secure and sound. Blockchain helps with the decentralized safety of medical data and averts certain risks.

The following sections talks about the need for blockchain in healthcare and provide an extensive view of how different blockchain frameworks are used in healthcare data storage and exchange.

2.2 NEED FOR BLOCKCHAIN IN HEALTHCARE

Patient data, such as name, personal information, and a description of their ailment, is extremely vulnerable and frequently infringed in the modern era of smart homes and smart cities. Digital records of these details are kept in an Electronic Health Record (EHR) network. Future medical research aimed at improving patient care and clinical practice performance may find value in the EHR. Patients and their caregivers cannot access this data, but hackers can easily obtain and use it without the third party's permission. This creates an imbalance between data security and accessibility. The solution to this problem is blockchain technology. Transactions are decentralized through blockchain, which is also an immutable ledger. The three main attributes of blockchain are decentralization, transparency, and security. These basic features ensure a high level of system security, prevent data abuse, and limit access by authorized personnel.

A blockchain-based security system that combines decentralization and encryption to protect EHRs and allows patients, caregivers, physicians, and insurers to have a secure way to access their clinical data has been proposed at in his work Taloba, A. I. et al. (2021). Moreover, the recommended approach strikes a balance between availability and data security. The study shows how the recommended system makes it easier for physicians, patients, caregivers, and outside agencies to efficiently store and retrieve patient medical records from electronic health records (EHRs).[3]

In most healthcare amenities, paper-based medical records have been replaced by electronic health records, or EHRs. However, there are issues with the integrity, security, and usability of currently available EHR systems. Connectivity and users' ability to control personal data are major problems in the healthcare business. Blockchain technology has evolved into a powerful tool for providing secure, immutable, and user control over stored records, but the potential benefits of EHR systems remain unknown

Researchers Reegu, F. A. et al. (2023) developed an interactive blockchain-based EHR system that meets the necessities of several national and international EHR standards including HL7 (Health Level 7) and HIPAA. In an effort to close this knowledge gap. The study method used to examine the state of the EHR field, especially the implementation of blockchain-based HER. The article examines several global and national EHR standards, describing associated challenges performance in current blockchain-based EHR systems. It then outlines the requirements of the standards for collaboration

Without the need for widespread storage, the proposed system could provide health care providers with a secure means of exchanging health information. Additionally, it can provide features such as security, immutability, and user control over archived records. This work contributes to our understanding on how blockchain technology can be used in EHR design and leads to interoperable, blockchain-based EHR systems that can meet the requirements specified in many national and international EHR standards in addressing that our research patient confidentiality, confidentiality, can enable the efficient exchange and storage of electronic health information while preserving record integrity will have a significant impact on the healthcare profession.

2.3 BLOCKCHAIN FRAMEWORKS

The creation and implementation of blockchain-based totally applications are made possible with the aid of blockchain frameworks are defined in Figure 2.1, which might be vital gear. The structure and practices required for setting up, jogging, and protection of decentralized networks are furnished via those frameworks. Blockchain frameworks are important for preserving patient facts's integrity, privateness, and interoperability within the context of healthcare records sharing and garage.

The possibility of the use of device mastering thoughts together with blockchain system administration to systematize duties in the healthcare setup has been investigated by way of Gul, M. J. J. et al. (2020). Their examine uses reinforcement studying to automate multi agent blockchain methods. According to our research, agents are capable of being taught to carry out the tasks specified in the blockchain

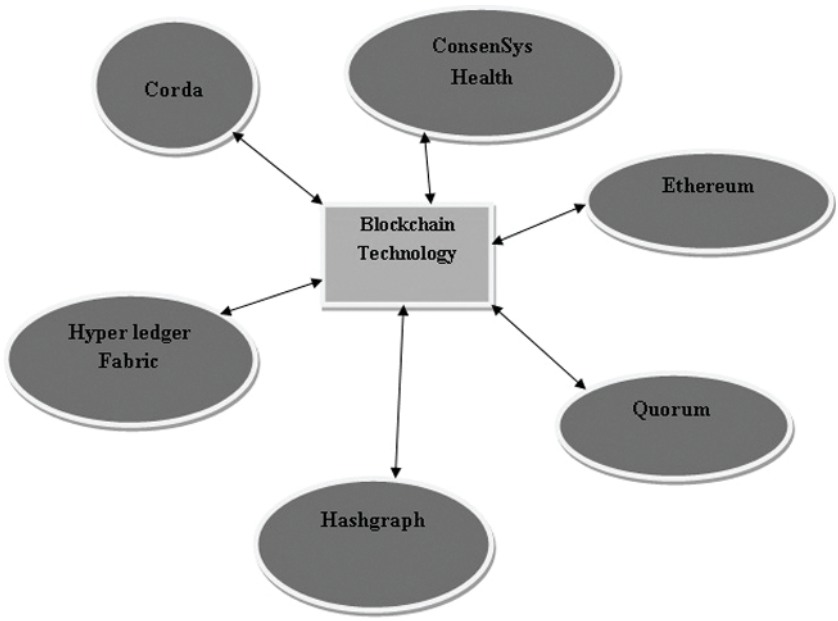

FIGURE 2.1 Blockchain in healthcare.

management system for the healthcare system. Additionally, it implies that machine learning principles make data access and storage efficient.[4]

The main goal of the study proposed by Agarwal, A. et al. (2023) is to securely store and maintain patient records in a cloud database. In the data-intensive field of healthcare, a great deal of data is produced, shared, stored, and accessed on a daily basis. The healthcare data that is stored on the cloud is protected by the Blockchain innovation. The distributed computing and clinical data-containing blockchain will link various healthcare providers. It enables healthcare providers to access patient details more securely from any location. It protects the information from hackers. Before being transferred to the cloud, the data is encoded. Before downloading the data, the healthcare provider must decode it. The information can be easily retrieved by the client and server and is ultimately accessed by utilizing cryptography during the encryption stage. The privacy and safekeeping of healthcare-related data in the cloud has been tested in this suggested study using the Java platform and medical records.

Hyperledger Fabric, an open-source project sponsored by the Linux Foundation, is one well-known blockchain framework. With its modular architecture, Hyperledger Fabric is specifically designed for use in enterprise systems, enabling businesses to automate their blockchain network works. Make access one of the power providers, essential for healthcare systems that must manage sensitive patient data. Smart contracts are supported by Hyperledger Fabric, allowing for pre-defined business logic on the blockchain.

Another famous blockchain platform widely known for its clever settlement features is Ethereum. Developers are capable of broaden and install decentralized applications (DApps) on Ethereum way to the decentralized platform. Ethereum has been explored for use in the healthcare industry for functions including medicinal drug dispensing and affected person consent management. Ethereum 2.0, a evidence-of-concept consensus platform, aims to increase scalability and strength efficiency.

The blockchain platform Corda was built with businesses and their specific needs in mind. It prioritizes anonymity and does not need a global blockchain network for direct transactions between parties. Corda has been conceived in the healthcare industry to coordinate credentials of healthcare providers, speed up workflow processes and enable secure data sharing among stakeholders

JPMorgan Chase created Quorum, a performance-focused version of Ethereum. It is a preferred option for consortium-based healthcare networks because it can be used with private permissioned blockchain networks. Healthcare organizations have seen Quorum used to monitor drug dispensing and guarantee the accuracy of clinical trial data.[5]

A directed acyclic graph (DAG) is used through a hash graph distributed ledger system to achieve consensus. It promises to deliver high-speed and secure services. Hashgraphs had been explored for use in the healthcare enterprise for obligations including managing patient consent, appropriately changing facts, and assuring the integrity of clinical records

The healthcare-specific blockchain era is called ConsenSys Health. It offers a number of blockchain-based totally healthcare statistics management systems and gear. Services which include affected person consent management, data transaction assurance, and healthcare records security are handled via ConsenSys Health.

The implementation of a healthcare blockchain infrastructure calls for careful attention of several factors. Because health records are governed via strict privacy and security regulations, compliance is vital. Another assignment is the combination of present fitness care structures; To facilitate an easy transition, blockchain structures should be able to speak easily with traditional structures.

Healthcare privateness is important, and blockchain systems must include robust safeguards to defend the privateness of patient facts. Permissive blockchains, which could best be accessed by using legal customers, are in particular useful in medical conditions. In addition, these structures have to facilitate the encryption and safety of sensitive records the use of cryptographic strategies.

Stakeholder collaboration is vital for successful use of blockchain in the scientific area. Creating a network or group of payers, technology professionals, regulators, and healthcare providers can help create a coordinated blockchain implementation strategy. Through collaboration, it will be possible to address issues unique to the healthcare industry and assure that the benefits of blockchain—such as increased transparency and data integrity—are shared by manufacturers things in all living things will feel.

In summary, blockchain infrastructures are essential for building and implementing blockchain-based healthcare solutions. Each plan meets Helt requirements.[6]

2.4 BLOCKCHAIN FRAMEWORKS FOR HEALTHCARE DATA STORAGE AND EXCHANGE

The healthcare industry has become increasingly interested in blockchain technology with its promise to improve data security, connectivity, and transparency. Blockchain systems can be used in the exchange and storage of healthcare information to ensure patient privacy and data integrity. The following blockchain systems have been explored for medical applications.

The Hyperledger Fabric:
The Linux Foundation hosts Hyperledger Fabric, an open source blockchain platform. It offers a modular design that enables customizable subscription services, smart contract execution, and consensus techniques. Healthcare organizations have used Hyperledger Fabric to manage electronic health records (EHRs), guaranteeing data integrity and facilitating secure data exchange between providers

Ethereum transactions:
Ethereum is a decentralized platform that allows the formation and implementation of smart contracts. To improve efficiency and effectiveness, it is moving from a proof-of-work approach to a proof-of-work model (Ethereum 2.0). Many healthcare applications have been identified including medication management, patient consent processing, and secure data communication using Ethereum

Corda:
The open-source blockchain platform for transactions is called Korda. It prioritizes privacy and dispenses with the need for an international blockchain network that enables

direct communication between the parties. Healthcare services include gathering credentials for healthcare providers, streamlining workflows, and guaranteeing secure data transfers between stakeholders, all of which have been ensured for Corda.[7]

Quorum:
JPMorgan Chase created Quorum, a performance-focused version of Ethereum. It is suitable for association-based healthcare transactions because it is fabricated on a permissioned private blockchain network. The use of quorum in healthcare settings, such as monitoring drug administration and validating clinical trial data, has been explored.

Hashgraph:
A directed acyclic graph (DAG) is used by the hashgraph distributed ledger system to reach consensus. It makes the promise to offer high throughput transactions that are quick and safe. Healthcare use cases including managing patient permission, safe data sharing, and maintaining the accuracy of medical records have all been given consideration for hashgraph.

ConsenSys Health:
A blockchain system created especially for the healthcare industry is called ConsenSys Health. It provides a set of programs and instruments for blockchain-based healthcare data management. Applications including patient consent management, data interoperability assurance, and healthcare data security have all been handled by ConsenSys Health.

Chakraborty, S. et al. (2019) have described that Blockchain Network adheres to the idea of complete anonymity and privacy when identifying the users involved in a transaction. Research on blockchain technology has shown that there are a number of different ways to organize the traditional system's access control. Blockchain technology has demonstrated exceptional dependability in a number of industries recently, including banking, healthcare, smart homes, information storage management, and security. Their work pertains to the field of Smart Healthcare, which has become increasingly prosperous in terms of providing patients with efficient medical care while protecting patient privacy and providing medical professionals with up-to-date, reliable data in real time.

It is critical to take privacy concerns, regulatory compliance, and compatibility with current systems into account when deploying blockchain in the healthcare business. Furthermore, the establishment of a successful blockchain network in the healthcare sector depends on stakeholder participation.[8]

2.5 HYPERLEDGER FABRIC FOR HEALTHCARE DATA STORAGE AND EXCHANGE

The Linux Foundation-hosted open-source blockchain technology Hyperledger Fabric is becoming more and more popular in the healthcare industry owing to its ability to offer safe and clear data transmission and storage. Its permissioned blockchain technology and modular design make it especially well-suited for handling private

medical data. Figure 2.2 shows how the hyperledger fabric framework has been implemented in healthcare.

Sheeraz, M. M. et al. (2023) have stated that organizational trust, security, and privacy are necessary for the sharing and preservation of medical data. While various research groups, hospitals, or lone scientists publish their findings, there are occasions when they also need to share the data. An obvious and safe framework for changing scientific facts is essential in this example. They have recommended a blockchain-primarily based mechanism for several entities to percentage medical facts. The agencies don't need to believe each other because the machine guarantees protection, privacy, transparency, and accept as true with more security models. Because the machine requirement is permissioned, a non-public blockchain, also called a permissioned blockchain, is used. The blockchain infrastructure has been hooked up using Hyperledger material due to its modular and adaptable nature.

Let's look into using Hyperledger Fabric to the interchange and storing of healthcare facts.

Permissioned Blockchain: Hyperledger Fabric is a permissioned blockchain, because its users are established folks that are known to each other. Permissioned blockchains provide a regulated environment for regulating getting admission to sensitive affected person information in the healthcare industry, where records protection and privacy are critical. This guarantees that the community can most easily be utilized by legal entities.

Privacy and Confidentiality: A personal statistics accumulating feature constructed into Hyperledger Fabric allows parties to proportion specific facts handiest with every different health record. This feature is vital for handling patient information within the healthcare industry because it allows sensitive data to be confined to individuals who are without delay concerned with the affected person's care. Thus, secrecy and privacy are preserved with out affecting the blockchain's overall transparency.

Smart contracts: Hyperledger Fabric smart contracts allow pre-defined enterprise good judgment to be executed at the blockchain. Smart contracts have the potential to automate and consolidate transactions inside the healthcare industry, consisting

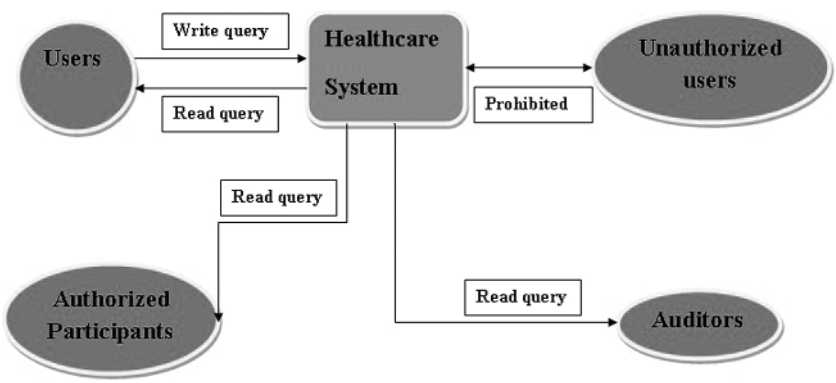

FIGURE 2.2 Architecture of Hyperledger Fabric.

of meeting for consensus or compliance with rules. This automation guarantees that techniques are regular and reduces the risk of human mistakes.

Data intake: By making an allowance for better illustration of modern-day healthcare, Hyperledger Fabric encourages numerical productivity. This is especially essential within the healthcare industry where many facilities often use disparate digital fitness document (EHR) systems. Hyperledger Fabric's interoperability with modern-day structures allows for especially seamless adoption of totally blockchain-based answers without interrupting set up enterprise tactics.[9]

Consensus Mechanism: Pluggable consent algorithms are introduced into the use of Hyperledger Fabric, permitting firms to select the consensus mechanism that suits their genuine use case This flexibility is crucial in the healthcare enterprise due to the fact in every different situation you can invoke special stages of consent. Organizations might also moreover balance performance and protection in accordance with their very own goals thanks to the modular consensus method.

Immutable Auditing: A tamper-resistant audit path is ensured with the useful resource of the unchangeable nature of facts on a blockchain. This characteristic is essential to the healthcare industry for tracking adjustments to affected person facts, retaining records integrity, and adhering to felony and regulatory requirements. Transparency and accountability during the healthcare surroundings can be advanced by immutable auditing.

Management of the Supply Chain: Hyperledger Fabric has packages beyond statistics interchange and storage, including pharmaceutical delivery chain management. It makes it feasible to observe drug manufacture, distribution, and authentication transparently. In the healthcare industry, this use case is crucial for stopping problems like fake medicines and maintaining supply chain integrity.

Consortium and Multi-Organization Networks: In the healthcare industry, several companies often working together to offer affected person care. Hyperledger Fabric helps the development of consortium networks wherein several entities can participate. By facilitating the easy sharing of healthcare records among legal individuals, this collaborative method promotes a patient-centric and holistic technique to healthcare delivery.

Finally, Hyperledger Fabric addresses the specific difficulties confronted by using the healthcare quarter to provide a stable platform for the sharing and storage of records. Healthcare data is touchy and controlled, and its permissioned blockchain technique, privacy protections, interoperability support, and bendy consensus methods make it an ideal design. Hyperledger Fabric stands out as a possible foundation for developing secure, obvious, and interoperable structures which could significantly enhance healthcare management as the industry investigates blockchain alternatives.[10]

2.6 ETHEREUM FOR HEALTHCARE DATA STORAGE AND EXCHANGE

The healthcare industry is interested in Ethereum because of its potential to renovate data interchange and storage. Ethereum is a decentralized platform that is well-known for its smart contract capability. Figure 2.3 shows the different layers of Ethereum framework that have been implemented in healthcare

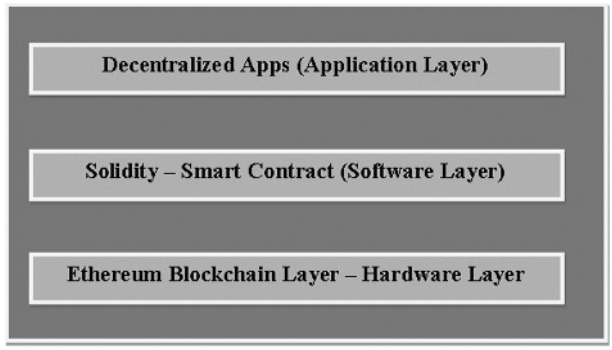

FIGURE 2.3 Architecture of Ethereum.

According to Ukanah, O. et al. (2020), healthcare data can be created, duplicated, and altered more quickly than in the past. The engine that powers more effective treatment is data. Unfortunately, the shortage of interoperability in the existing healthcare organization leads to inconsistent workflow tools, separated and fragmented data, and slow communications. Apart from possessing crucial attributes such as immutability, decentralization, and transparency, blockchain technology has the potential to tackle pressing issues in the healthcare segment, such as insufficient histories at the point of care and difficult access to patients' private health data. In order to create an effective and profitable healthcare system, software applications and technical platforms must be able to safely and quickly communicate, exchange data and practice that are in the records of health societies and app sellers. This is known as interoperability. They have talked about storing electronic medical records in their work using smart contracts. Ethereum's blockchain network is used in the implementation of addressing issues with centralized platforms. The implementation was successful in lowering storage costs by storing huge files off-chain (IPFS), and the results were encouraging.

This chapter explores the use of Ethereum in healthcare to manage patient data in a transparent and safe manner:

Smart Contracts: The chief benefit of Ethereum is its ability to implement smart contracts, which are self-executing agreements with terms clearly defined in the code. Smart contracts can automate a number of healthcare-related tasks, which include dealing with patient consent, processing insurance claims, and making sure of regulatory compliance. Healthcare tactics are run extra efficaciously because of this automation, which also lowers the possibility of mistakes.

According to Marry, P. et al. (2023) the usage of e-healthcare has improved social and fitness consequences and decreased clinical errors. However, a main impediment to the improvement of e-healthcare is the safety troubles related to patient statistics storage in IT frameworks. Blockchain generation has surfaced as a feasible treatment for this hassle and has the capacity to absolutely renovate the healthcare region. This framework establishes the foundation for a blockchain-based strategy that includes clever contracts, context-primarily-based getting

admission to control, a public ledger, and a private ledger to securely manage patient statistics. Interoperability, and reliably getting right of entry to patient facts are all guaranteed by using the encouraged structure. Furthermore, the counseled totally blockchain-based framework gives a dependable and effective way of dealing with complex clinical procedures. The file delves into the capability uses of blockchain generation inside the clinical domain, encompassing stable and private health facts sharing for medical research. The authors propose making use of smart contracts to keep scientific information in a unique, readable, compatible, and audible way.[11]

Security and Decentralization: Because Ethereum is a decentralized community of nodes, it's far from possible for one celebration to control the complete machine. Due to the removal of single points of failure and reduced danger of unwanted getting admission, this decentralization improves safety. Given the crucial significance of data security inside the healthcare enterprise, Ethereum's decentralized architecture gives a strong basis for the defense of patient facts.

Interoperability: Ethereum may be seamlessly incorporated with other healthcare systems because of its interoperability with current requirements and protocols. In the healthcare zone, where numerous agencies may additionally appoint varied digital fitness file (EHR) structures, interoperability is important. Because of its flexibility, Ethereum is able to act as a hyperlink between specific systems, encouraging verbal exchange and less complicated teamwork.

Patient-centric records usage: Ethereum offers sufferers additional possession over facts related to their health. Patients can control their health information and select to share it with healthcare vendors whilst keeping privacy at the same time, enabling getting right of entry to to crucial information, through decentralized identifiers (DIDs) and suitable credentials. This patient-centric method fits properly with an increasing trend that empowers people to pay for their healthcare.

Tokenization and incentives: Due to the tokenization performance of Ethereum, it is feasible to create tokens that encompass specific healthcare properties or possibly affected person records themselves. This creates opportunities for promoting engagement in healthcare networks and facts alternately through incentives. Patients would receive incentives for donating their information to researchers, which would assist in building larger, extra beneficial databases.

Supply Chain Management: Pharmaceutical delivery chains inside the medical enterprise can be managed by the usage of Ethereum's impermeable, transparent ledger. Ensuring the authenticity and reliability of pharmaceuticals addresses problems along with counterfeit medications and improves typical affected person safety.

Switching to Ethereum 2.0: Ethereum is in the process of a sizable update known as Ethereum 2.0, which involves shifting from a consensus manner based on evidence of work to at least one based totally on evidence of stake. The goals of this modification are to improve safety, power performance, and scalability. Large-scale healthcare programs could gain more from an Ethereum network; this is more scalable on the grounds that it can take care of extra transactions in the healthcare industry.

Research Collaboration: Due to Ethereum's decentralized structure, networks for securing information and sharing findings amongst teachers from diverse universities

may be installed. This can encourage more collaboration at the same time as protecting statistics' safety and confidentiality, which can speed up clinical research.[12]

To sum up, Ethereum offers a flexible framework for replacing and storing clinical facts. Because of its decentralization, interoperability, and clever contract abilties, it is far better prepared to address the particular problems faced by the healthcare area. Ethereum's capability effect on healthcare records control is predicted to grow because it develops similarly, specifically with the discharge of Ethereum 2.0, establishing new avenues for innovation and cooperation in the healthcare sphere.

2.7 CORDA FOR HEALTHCARE DATA STORAGE AND EXCHANGE

R3 developed Corda, a blockchain platform with structures that make it particularly beneficial for changing and storing medical information. Corda is supposed to be used in commercial enterprise settings. Corda's emphasis on interoperability, security, and privacy fits in well with the demands of the healthcare region. Figure 2.4 indicates how the Corda framework has been implemented in healthcare

Mohanty, D. (2019) has described how a preliminary coin imparting (ICO) the usage of public Blockchain Ethereum can be used to attract funding from the marketplace and how Corda can be used as a private permissioned ledger for dealings among members. The healthcare region has made use of this.

An analysis of Corda's capacity uses in healthcare is provided below:

Privacy and Permissioning: Corda is a permissioned blockchain, which means that the wealthiest people who've been granted entry to can get entry to and utilize the network. In the healthcare enterprise, shielding sensitive affected person information is important. With Corda, healthcare providers may transmit data selectively and safely without revealing unnecessary information because of its fine-grained access controls.

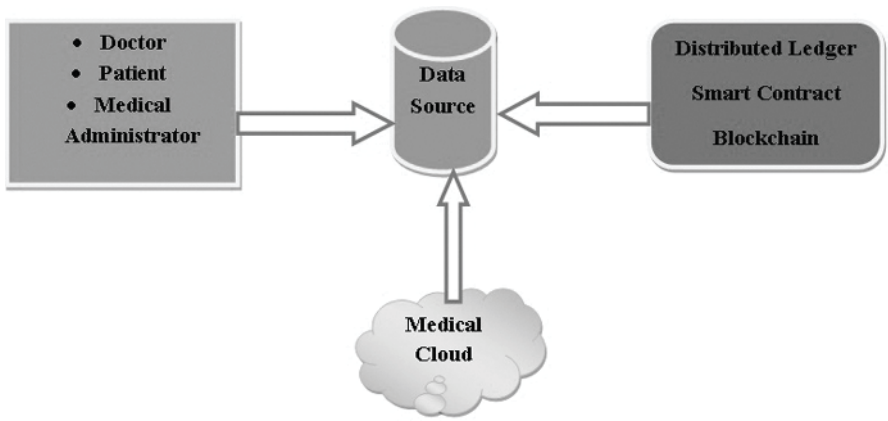

FIGURE 2.4 Architecture of Corda.

Sharing of Data Between Parties: Because of the peer-to-peer nature of Corda's architecture, parties can conduct direct transactions without requiring a worldwide broadcast. This feature facilitates safe data exchange between pertinent parties in the healthcare industry, including payers, patients, and healthcare providers. By making it easier to create private and secure channels for data transmission, Corda makes sure that only authorized parties are privy to sensitive information.[13]

Logic in Business and Artificial Intelligence: Corda facilitates the use of "CorDapps," or smart contracts. These smart contracts allow complex business logic to be executed on the blockchain. Healthcare processes such as processing claims, managing patient consent, and conducting compliance checks could all be automated with the use of smart contracts. Because of this automation, healthcare activities run more smoothly and with a decreased possibility of error.

Integration and Interoperability: The easy integration of Corda with current enterprise systems is part of its architecture. In the healthcare sector, Corda's compatibility with numerous electronic health record (EHR) systems and legacy infrastructure is advantageous. This removes the need to totally redesign present systems and facilitates the transition to blockchain-based solutions.

Credential Administration: In the healthcare industry, Corda can be used to manage and validate credentials. Verifying the credentials of healthcare practitioners is one way to do this, as is making sure that only approved individuals can contact particular patient data or take part in particular transactions. Maintaining the integrity and reliability of healthcare networks depends on credential management.

Safe Communication of Patient Data: Corda is a good fit for patient data exchange because of its emphasis on private and secure transactions. With smart contracts, patients can give certain healthcare providers or researchers access to their data, giving them more control over it. This patient-centered strategy fits nicely with the rapidly changing healthcare trends that place a strong emphasis on data ownership and individual empowerment.[14]

Adherence to Regulations: Smart contracts can now immediately incorporate legal and regulatory requirements thanks to Corda. This is a useful function in the healthcare enterprise, wherein following legal guidelines like HIPAA is essential. Healthcare companies can make certain that their operations follow industry-unique rules by way of automating compliance exams with clever contracts.

Association Networks: Corda makes it less complicated to build consortium networks, which permits several corporations to work together on a commonplace blockchain infrastructure. In the healthcare industry, this will entail collaboration among insurers, regulatory groups, and healthcare carriers. Consortium networks shield the confidentiality and security of touchy scientific information at the same time as facilitating statistics sharing and teamwork.

In end, Corda meets the specific desires of the healthcare zone to provide a strong platform for the sharing and storing of information. It is an appealing choice for developing safe and effective healthcare blockchain answers because of its emphasis on privacy, permissioning, smart contracts, and interoperability. With its capabilities, Corda offers itself as a promising platform for revolutionizing the management and sharing of healthcare facts, in particular because the industry continues to investigate new technologies.[15]

2.8 QUORUM FOR HEALTHCARE DATA STORAGE AND EXCHANGE

PMorgan Chase's employer-centered blockchain generation, Quorum, affords abilities that make it appropriate to be used in healthcare data alternatives and garage applications. Quorum is nicely suitable to the safety and privateness needs of the healthcare region due to its scalability, privacy capabilities, and potential to build permissioned blockchain networks. Here we take a look at how Quorum may be used within the medical field:

Permissioning and Privacy: Quorum is made to facilitate personal transactions wherein the simplest authorized users can view touchy statistics. Because patient privacy is of supreme significance in the healthcare sector, Quorum's privacy features facilitate the safe and private sharing and storage of data. Networks with permissions make sure that only reliable organizations can access the pertinent medical data.

Deals That Are Secret: To preserve the privacy of transaction details, Quorum uses secret transactions. This functionality is essential for safeguarding private patient data in the healthcare industry. It guarantees the confidentiality of information such as medical diagnoses, treatments, and personal identifiers, offering a safe storage environment for healthcare data.

Smart Contracts: Smart contracts, which enable the implementation of self-executing contracts with predetermined rules, are supported by Quorum. Smart contracts have the potential to automate a number of healthcare-related tasks, including managing patient consent, processing insurance claims, and performing compliance checks. Smart contract automation improves operational effectiveness and lowers error risk.

Business-Level Scalability: Because Quorum was created with scalability in mind, enterprise-level applications can benefit from its use. Scalability is crucial in the healthcare industry because it allows various healthcare organizations, such as hospitals and research institutions, to meet their different needs for data transmission and storage, given the massive amounts of data generated on a daily basis.[16]

Chain of Supply Traceability: Healthcare supply chain management is a good fit for Quorum's traceable and transparent ledger. It makes it viable to screen pharmaceutical gadgets from the point of production to the factor of distribution, making certain of their integrity and validity. This is vital to improving patient safety and eliminating faux medicines.

Adherence to Regulations: With Quorum, agencies can include regulatory specs into clever contracts to assure that statistics management and transactions follow region-precise laws. Agreement with laws like the Health Insurance Portability and Accountability Act (HIPAA) is crucial for the healthcare industry, and Quorum's capabilities assist groups achieve those necessities.

Cooperation: The interoperability abilities of Quorum facilitate integration with corporate systems that are currently in location, inclusive of digital health file (EHR) structures. This guarantees a seamless shift to blockchain-primarily based answers without interfering with cutting-edge workflows inside the healthcare zone. The effective incorporation of new technology into the cutting-edge healthcare infrastructure depends on interoperability.

Association Networks: Quorum makes it less complicated to establish consortium networks, which permits numerous organizations to participate in a not unusual blockchain infrastructure. Consortium networks facilitate secure fact-sharing and collaboration while defensive patient privacy inside the healthcare industry, with cooperation among insurers, healthcare companies, and other stakeholders is regular.

In conclusion, Quorum addresses the particular problems confronted via the healthcare sector to offer a solid platform for the sharing and protection of facts. For healthcare agencies wishing to apply blockchain generation, its privacy capabilities, scalability, clever contract talents, and emphasis on employer-grade answers make it an appealing choice. Because of its traits, Quorum is positioned as a platform that can improve the security, transparency, and effectiveness of healthcare information control because the enterprise looks for brand new and innovative ways to manage patient records.[17]

2.9 HASHGRAPH FOR HEALTHCARE DATA STORAGE AND EXCHANGE

Hashgraph is an allotted ledger technology (DLT) with unique properties that make it really worth considering for the sharing and storage of healthcare records. It uses a directed acyclic graph (DAG) for consensus. The speedy throughput, protection, and consensus fairness that hashgraph guarantees might be positive in several medical programs. What follows is an investigation on the capabilities that make use of of Hashgraph inside the scientific subject:

High Scalability and Throughput: The excessive throughput of a hashgraph network is attributed to its potential to address a massive number of transactions in a certain amount of time. High throughput is crucial for handling the volume of information interchange and warehouse inside the healthcare industry, as massive volumes of records are produced on an everyday basis. The DAG-primarily based architecture of Hashgraph would possibly provide the scalability required for medical packages.

Unchangeable and Tamper-Resistant Record: The consensus algorithm utilized by Hashgraph seeks to provide an unchangeable and impenetrable transaction report. This function is vital to the healthcare industry to safeguard patient confidentiality and guarantee the safety and authenticity of medical facts. Compliance with regulatory standards and audit trails may also rely heavily at the ledger's immutability.

Quick Consensus: The asynchronous Byzantine Fault Tolerance (aBFT) consensus mechanism on Hashgraph allows for quick and powerful consensus on transaction orders. The brief consensus system of Hashgraph can facilitate actual-time records interchange in the healthcare industry, where prompt access to accurate patient facts is critical for assisting brief choice-making in scientific situations.[18]

Safety and Equitable Treatment: Hashgraph asserts that its consensus method offers an increased diploma of security. Since the consensus mechanism utilized by Hashgraph is honest, every player has an equal chance to affect the transaction order. Building trust among community individuals may be facilitated via these components, specially within the healthcare enterprise wherein data safety and equitably getting right of entry to are crucial.

Transactions which might be traceable and obvious: Healthcare packages can gain from Hashgraph's transparent and traceable nature, which ensures that every event causing concern has get right of entry to transaction history. Tracking the raft of medication via the pharmaceutical delivery chain, confirming the legitimacy of prescribed drugs, and enhancing affected person safety are all made feasible by way of this transparency.

Decentralization: As with fashionable blockchain networks, hashgraph seeks to achieve decentralization in consensus without requiring electrical-in depth mining. For healthcare companies looking to use blockchain era in an extra ecologically responsible way, this is probably useful. Additionally, decentralization complements the network's usual resilience and security.

Control and Ownership of Patient Data: Patients will also have an impact over their health facts by way of the use of patient-centric models, which may be applied with Hashgraph. Patients can manage who has access to their information through the use of obvious and secure clever contracts that allow gaining admission to healthcare experts, researchers, and different companies in accordance with pre-hooked-up hints. This is consistent with changing healthcare tendencies that place an excessive price on affected person facts possession.

Networks for Collaborative Research: The skills of Hashgraph can make it simpler to establish cooperative studies networks in the clinical field. Data may be competently shared between researchers at exclusive universities, advancing clinical studies. Consideration of collaborators is fostered with the aid of the ledger's tamper-resistant nature, which ensures the accuracy of research data.

Although Hashgraph has several exciting capabilities, it's critical to remember that its recognition inside the healthcare sector will rely upon the particular desires of the packages as well as the general nation of the enterprise. Furthermore, before deploying Hashgraph for the storing and interchange of healthcare information, elements including regulatory compliance, interoperability with modern-day structures, and the maturity of the technology have to be carefully taken into consideration. In the healthcare industry, like with any new technology, a hit solution development and implementation rely closely on stakeholder engagement.[19]

2.10 CONSENSYS FOR HEALTHCARE DATA STORAGE AND EXCHANGE

Blockchain technology company ConsenSys offers a range of tools and solutions; its flagship product, ConsenSys Health, was developed specifically with healthcare applications in mind. ConsenSys Health provides blockchain-based solutions for organizing and securing medical information. This is an analysis of the way ConsenSys, and specifically ConsenSys Health, can simplify the exchange and archiving of health information:

Security and Privacy: ConsenSys Health places a premium on security and privacy when handling patient data. The usage of blockchain tools based on cryptography ensures that confidential patient data is stored in a hack-proof and secure environment. ConsenSys Health's solutions are intended to comply with HIPAA and other regulations when it secures patient information.

Decentralized Identity Administration: By focusing on decentralized identity solutions, ConsenSys Health gives people greater control over their health information. Patients can protect privacy and enable access to sensitive data by selectively sharing their health information with verified credentials and decentralized identities (DIDs). This is consistent with the concept of self-universality in medicine.

Integration and Interoperability: Solutions provided by ConsenSys Health are designed to work with existing healthcare infrastructure. By means of the increasing practice of multiple electronic health record systems and other legacy systems, performance is essential for healthcare data processing. The products offered by ConsenSys Health are designed to integrate blockchain technology with traditional for consumption role.[20]

Intelligent Contracts for Mechanized Procedures: ConsenSys Health makes use of clever contracts to automate a number of medical tactics. In addition to coping with affected person consent, smart contracts can automate the processing of claims and streamline administrative methods. Smart settlement automation improves productivity and lowers the opportunity for errors in healthcare operations.

Collaboration and Data Sharing: Healthcare stakeholders may apportion information in an obvious and safe way thanks to ConsenSys Health solutions. When facts need to be shared among several stakeholders, together with sufferers, insurers, and healthcare companies, this cooperative approach may be very beneficial. The establishment of consortium networks for safe statistics sharing is made less complicated by ConsenSys Health.

Authentication and Adherence: Healthcare vendors' certification requirements are met through ConsenSys Health. Retaining the credibility of healthcare networks calls for making sure that touchy affected person information is readily available to legal specialists. Healthcare practitioners' credentials can be managed and validated on the blockchain with the assist of ConsenSys Health's answers.

Handling Consent from Patients: One important aspect of exchanging healthcare data is managing affected person permission. ConsenSys Health offers solutions for placing blockchain-primarily based clever contracts controlling patient consent into practice. This ensures that getting entry to facts is ruled through programmable, obvious regulations, giving sufferers extra control over who can get admission to their health facts.

Research and Clinical Trials: Clinical trial and healthcare research control may be finished with ConsenSys Health. Clinical trial information can be made more open and safer by using blockchain, which additionally guarantees traceability and lowers the possibility of fraud. Data-driven healthcare decisions and extra dependable studies' outcomes may additionally result from this.

To sum up, ConsenSys Health affords an extensive range of gadgets and alternatives for the interchange and storing of scientific information. Its emphasis on interoperability, privacy, safety, and clever agreement automation complements the sensitive and complex nature of healthcare records. ConsenSys Health's products offer a platform that tries to enhance openness, safety, and efficiency in coping with healthcare records as the sector investigates blockchain alternatives in addition. But, for generation to be correctly used within the healthcare enterprise, like with some other projects, stakeholders need to paintings collectively and deliver careful thought to regulatory compliance.[21]

REFERENCES

1 Agarwal, A., Joshi, R., Arora, H., & Kaushik, R. (2023). Privacy and security of healthcare data in cloud based on the blockchain technology. *2023 7th International Conference on Computing Methodologies and Communication (ICCMC)*. doi:10.1109/iccmc56507.2023.10083822

2 Block Convey. (2023, October 9). Leveraging blockchain framework to ensure the security of electrical medical records. Retrieved 4 December 2023, from www.blockconvey.com/post/leveraging-blockchain-framework-to-ensure-the-security-of-electrical-medical-records.

3 Chakraborty, S., Aich, S., & Kim, H.-C. (2019). A secure healthcare system design framework using blockchain technology. *2019 21st International Conference on Advanced Communication Technology (ICACT)*. doi:10.23919/icact.2019.8701983

4 Elangovan, D., Long, C. S., Bakrin, F. S., Tan, C. S., Goh, K. W., Yeoh, S. F., … Ming, L. C. (2022). The use of blockchain technology in the health care sector: Systematic review. *JMIR Medical Informatics*, 10(1), e17278. doi:10.2196/17278

5 Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K., & Siddique, A. H. (2023). Blockchain application in healthcare systems: A review. *Systems*, 11(1), 38. doi:10.3390/systems11010038

6 Gul, M. J. J., Paul, A., Rho, S., & Kim, M. (2020). Blockchain based healthcare system with Artificial Intelligence. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. doi:10.1109/csci51800.2020.00138

7 Haleem, A., Javaid, M., Singh, R. P., Suman, R., & Rab, S. (2021). Blockchain technology applications in healthcare: An overview. *International Journal of Intelligent Networks*, 2, 130–139. doi:10.1016/j.ijin.2021.09.005

8 Han, Y., Zhang, Y., & Vermund, S. H. (2022). Blockchain technology for electronic health records. *International Journal of Environmental Research and Public Health*, 19(23), 15577. doi:10.3390/ijerph192315577

9 Hölbl, M., Kompara, M., Kamišalić, A., & NemecZlatolas, L. (2018). A systematic review of the use of blockchain in healthcare. *Symmetry*, 10(10), 470. doi:10.3390/sym10100470

10 Khujamatov, K., Reypnazarov, E., Akhmedov, N., & Khasanov, D. (2020). Blockchain for 5G Healthcare architecture. *2020 International Conference on Information Science and Communications Technologies (ICISCT)*. doi:10.1109/icisct50599.2020.9351398

11 Kumar, M., Raj, H., Chaurasia, N., & Gill, S. S. (2023). Blockchain inspired secure and reliable data exchange architecture for cyber-physical healthcare system 4.0. *Internet of Things and Cyber-Physical Systems*, 3, 309–322. doi:10.1016/j.iotcps.2023.05.006

12 Marry, P., Yenumula, K., Katakam, A., Bollepally, A., & Athaluri, A. (2023, June 14). Blockchain based Smart Healthcare System. *2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS)*. doi:10.1109/icscss57650.2023.10169704

13 Mohanty, D. (2019). Healthcare—Corda and Ethereum Hybrid Use Case. In *R3 Corda for Architects and Developers* (pp. 153–174). doi:10.1007/978-1-4842-4529-3_7

14 Noon, A. K., Aziz, O., Zahra, I., & Anwar, M. (2021, November 9). Implementation of Blockchain in Healthcare: A Systematic Review. *2021 International Conference on Innovative Computing (ICIC)*. doi:10.1109/icic53490.2021.9691510

15 Panwar, A., Bhatnagar, V., Khari, M., Salehi, A. W., & Gupta, G. (2022). A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. *Computational Intelligence and Neuroscience*, 2022, 3045107. doi:10.1155/2022/3045107

16 Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., … Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system. *Sustainability*, 15(8), 6337. doi:10.3390/su15086337

17 Saeed, H., Malik, H., Bashir, U., Ahmad, A., Riaz, S., Ilyas, M., … Khan, M. I. A. (2022). Blockchain technology in healthcare: A systematic review. *PloS One*, 17(4), e0266462. doi:10.1371/journal.pone.0266462

18 Sheeraz, M. M., Mozumder, M. A. I., Khan, M. O., Abid, M. U., Joo, M.-I., & Kim, H.-C. (2023, February 19). Blockchain system for trustless healthcare data sharing with hyperledger fabric in action. *2023 25th International Conference on Advanced Communication Technology (ICACT)*. doi:10.23919/icact56868.2023.10079423

19 Sun, Z., Han, D., Li, D., Wang, X., Chang, C.-C., & Wu, Z. (2022). A blockchain-based secure storage scheme for medical information. *EURASIP Journal on Wireless Communications and Networking*, 2022(1). doi:10.1186/s13638-022-02122-6

20 Taloba, A. I., Rayan, A., Elhadad, A., Abozeid, A., Shahin, O. R., & El-Aziz, R. M. A. (2021). A framework for secure healthcare data management using blockchain technology. *International Journal of Advanced Computer Science and Applications: IJACSA*, 12(12). doi:10.14569/ijacsa.2021.0121280

21 Ukanah, O., & Obimbo, C. (2020). Blockchain Application in Healthcare. *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*. doi:10.1109/csci51800.2020.00218

3 Leveraging Blockchain Frameworks for Enhanced Healthcare Data Storage and Exchange

Asha Vidyadharan, S. Devaraju, M.R. Thiyagu Priyadharsan, S. Poonkuntran, and D. Elavarasi

3.1 INTRODUCTION

The healthcare sector possesses a wealth of information about patient histories, diagnostic findings, treatment strategies and other critical details that could revolutionize the delivery of healthcare. With appropriate use, this enormous data source can lead to significant gains in patient outcomes, personalized treatment, and predictive analytics. However, there are difficulties due to sensitivity and volume for data processing. Existing methods are nowadays mostly perceived as too antiquated to change the increasing cybersecurity threats and digital landscape. There are breaches due to the susceptibility and segmented architecture, which frequently generate inconsistent information about the inefficiencies, lack of trust and patient care between stakeholders.

The result in patient data provides the consequences of financial loss due to compromising the information, like legal ramifications and reputation harm. Due to the interconnection of the world through networks, there are probably significant data breaches happening in the healthcare industry which cannot afford to persist unaware. Without sacrificing accessibility or transparency, managing healthcare information must be completely remodified at the security level in a prioritized manner.

Blockchain affords a new methodology for data management which helps to prioritize transparency and security. The distributed architecture helps prohibit data storage in an unsafe location, keep unchangeable data and guarantee time-stamped input. This architecture improves the oversight and security of medical data by adopting a more productive environment and transparency, therefore data can transfer between any platforms without fear. Healthcare is more active today with the help of blockchain technology. The medical data are created for strong security forces, data-driven insights and patient empowerment. An individual with the necessary credentials and internet connectivity can access necessary health data from anywhere, potentially lowering the cost of information exchange. Additionally, blockchain's immutability

 DOI: 10.1201/9781032711379-3

and cryptographic designs ensure an accurate record of events, making it difficult for malicious third parties to alter the data within the record[1]. The healthcare industry could potentially conserve around $100–$150 billion annually by 2025 through blockchain adoption, by diminishing expenses linked to data security incidents, tech overheads, management expenses, backend operations, staff overheads, and by curtailing deceptive actions and fake items[2].

Blockchain has the capability to accommodate various networks, like public (open source), private (restricted to authorized members), or hybrid (a combination of both). Blockchain can probably employ diverse consensus algorithms, namely proof-of-work (requiring nodes to solve a mathematical puzzle), proof-of-stake (requiring nodes to stake some value), or proof-of-authority (requiring nodes to possess a known reputation or identity)[3].

E. Vashishtha and H. Kapoor[1] predict a significant growth in the healthcare blockchain market, reaching USD 14.25 billion by 2032, driven by the urgent need to resolve frequent data breaches. They propose the blockchain for sheltered health data management, combating pharmaceutical counterfeiting described in Figure 3.1 and implementing strategic measures in healthcare operations. Major players like IBM, Athenahealth and Allscripts are noted for embracing blockchain, with the Synaptic Health Alliance facilitating data interchange in healthcare. Public healthcare data management networks are identified as major revenue contributors, with an expected growth in private networks for enhanced privacy and security. Biopharmaceuticals, medical devices and hospitals lead in blockchain adoption, with Europe dominating the market and North America showing growing interest.

Articles[2–4] discusses the probability of Health IT reducing diagnostic errors, tailoring care through precision medicine, and how the pandemic led to a transformation in data usage within healthcare. It[2] mentions the obstacles of siloed and unclean data to utilizing data analytics and AI. It also highlights the probability of blockchain in guaranteeing the sheltered transfer and verifying health data amidst the growing usage of digital health tools. By leveraging blockchain's immutability and integrity verification, healthcare entities could enhance data security, conform with supervisory ethics like HIPAA, and foster trust among users and stakeholders. The capability of blockchain to enable secure and openly accessible data exchange plays a critical part in advancing healthcare management for interoperability[5].

The article from Health IT Answers[6,7] outlines five major challenges in healthcare data security for 2022:

- Ransomware: Continual threats with a high success rate due to the value of healthcare data.
- Mobile Applications: When medical apps are used more frequently, security risks arise, particularly when user security procedures aren't up to par.
- Lack of Interoperability: Communication barriers between different digital systems risk data exposure.
- IoT Vulnerabilities: Security incidents from unmanaged IoT devices due to insufficient built-in security measures.
- Limited Resources: Lack of necessary staff, funding, or expertise to tackle cybersecurity threats effectively.

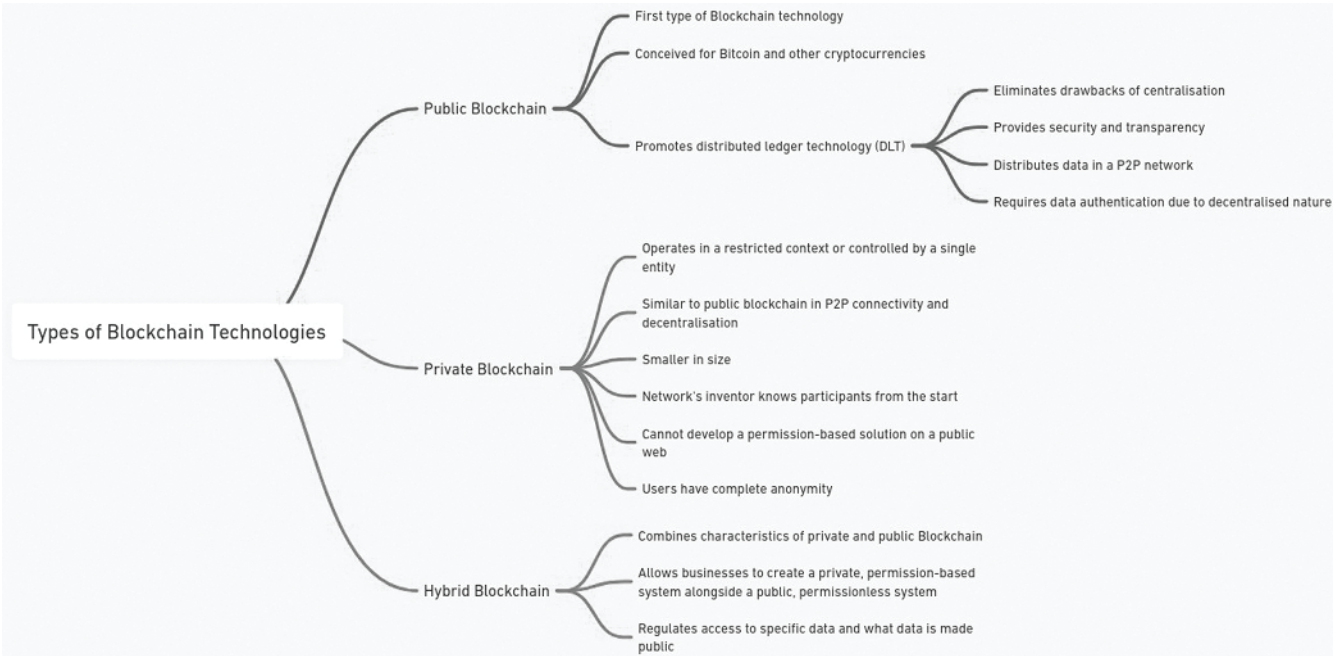

FIGURE 3.1 Various kinds of blockchain technologies.

A blockchain-based method safely outsourcing health information in a cloud environment was proposed by Benil and Jasper[13]. tackled the problem of data deduplication, which is essential for effective data storage and management. All events relating to the outsourcing of Electronic Health Records are recorded on public blockchain in order to preserve authenticity and data security. Conforming to K. Paranjape et al.[9] blockchain technology is used to decentralize the structure of data repository which facilitates the quick access to patient information for hospitals, doctors and pharmacists in enhancing the security of data organization in medical services. In[10], S. Malathy et al. proposed using blockchain in healthcare in the following steps:

1. Data Management: Data Management in Blockchain technology makes electronic health records more accurate and it is possible to provide the healthcare information retrieval process more easily, e.g. drug administration prescriptions.
2. Security: Blockchain expands data security and provides the patients' information more accurately and securely, which is dependable for a patient-centric method of treatment.
3. Blockchain Type Selection: A degree of trust depends on the requirement for a third party being reliable to take the right decision. Worst and Gervais' decision model provides the blockchain technology for the medical information whether the protection of the data is in a private, public permissioned, or public permissionless way.
4. Resolving Trust concerns: Blockchain is decentralized for easy processing and it can be resolved for trust the medical data infrastructure.

3.2 KEY BLOCKCHAIN PRINCIPLES

The following sections describe the functions of the blockchain, a separate structure for data security inside a specific network or organization.

3.2.1 Decentralization Architecture

Blockchain functions on a decentralized framework, compared to traditional centralized systems, where one entity controls the data. Through decentralization, data is dispersed throughout a network of computers, each of which serves as a node. The hazards of data modification and illegal access are greatly decreased by this approach.

3.2.2 Immutability

A transaction is very hard to change or remove once it is registered on the blockchain. This feature ensures data dependability; it is necessary in healthcare to maintain accurate and unaltered patient information are described in Figure 3.2.

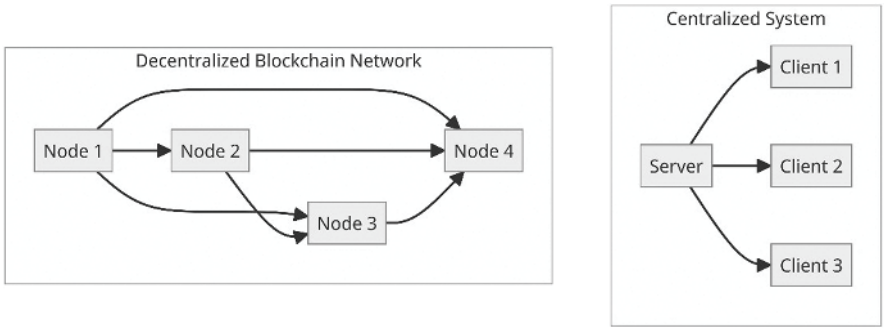

FIGURE 3.2 Network diagram illustrating Centralized System vs. Decentralized Blockchain.

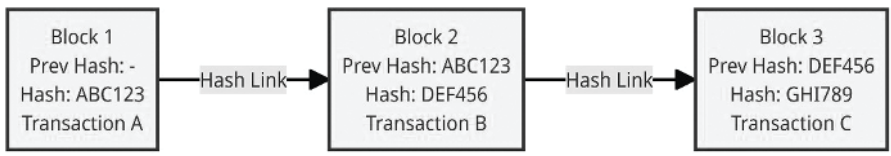

FIGURE 3.3 Representation of blockchain structure.

3.2.3 Transparency

Blockchain offers a certain amount of transparency by enabling all network members to examine the same data while maintaining confidentiality and privacy. Transparency in healthcare data management promotes accountability and compliance by ensuring the traceability and authenticity of data exchanges are described in Figure 3.3.

3.2.4 Cryptographic Hashing

A key component of blockchain technology is cryptographic hashing, which involves converting data into a character string with a constant length called a hash value. Data integrity is protected by this technique.

3.2.5 Consensus Mechanisms

Protocols that add a transaction to the block and deem it valid are known as consensus methods. A few consensus techniques have advantages and disadvantages of their own.

3.2.6 Smart Contracts

Smart agreements function independently and have limitations incorporated right into the code. They function autonomously and do tasks without the need for a middleman when predefined conditions are satisfied. By streamlining procedures like billing,

claim management and data sharing protocols, these digital agreements have the potential to increase productivity and lower operational costs in the healthcare sector.

3.3 CURRENT CHALLENGES IN HEALTHCARE DATA MANAGEMENT

It is significant to understand the contests that the healthcare industry faces when managing patient data before delving into the realm of blockchain technology. Due to its reliance on paper-based records and centralized data repositories, the traditional healthcare system faces particular difficulties.

Data management is still essential in today's changing healthcare environment for ensuring effective and patient-focused care. However, as the following highlights, the industry faces certain challenges that prevent proper data management.

3.3.1 Data Breaches

The state of data breaches in the medical field is alarming. According to recent figures, throughout the previous three years, data breaches have affected almost 93% of medical facilities. Only in the first quarter of 2023, 145 notifications of data breaches were received by the US Office of Civil Rights. The implications of these breaches are enormous; according to one source, HCA Healthcare experienced a catastrophic data breach that compromised the details of more than 11 million people. As of now, the data for 2023 show that 395 events have affected the records of around 60 million people. There is a 75.6% chance that at least 5 million records will be compromised in 2023. It is estimated that healthcare providers lost $6.45 million as a result of data breaches, with $429 lost on average for each compromised record. There is a substantial financial effect as well[11,12].

3.3.2 Interoperability Issues

For efficient data transfer and improved patient care, interoperability is crucial in healthcare data management. Even with the emphasis on interoperability, Electronic Health Record (EHR) systems have distinctive design essentials which prevent them from networking with further systems. It will lead to errors or interruptions that compromise the sensitive data. Electronic patient data requires a verification process before being applied to the process. Whenever the information is shared, it leads to mistakes or inconsistencies of severe significance. Robust validation and verification actions are required to make sure the recipient accepts the accurate information at the right interval.

3.3.3 Lack of Transparency

The active communication and usage of health information might be more stimulating while the healthcare information is handled with a lack of transparency. To enhance the healthcare domain, it is very important to eliminate obstacles in information exchange with better transparency. To improve the transparency, continuous efforts are still substantial such as limiting information flow and integrity of the information.

3.3.4 Data Integrity and Accuracy

Due to human error, uneven data input, data silos and processing will contribute unfinished and erroneous healthcare data to the medical domain, which will challenge the medical information to obtain possible patient care.

3.3.5 Scalability

Whenever the healthcare information upswings, information handling should be scalable in order to meet upward demand while conserving security and performance. To handle this kind of issue in the medical domain systematically, it should prioritize interoperability, increase transparency and strengthen cybersecurity in the supervision of healthcare information. Blockchain technology offers a possible resolution to these issues by offering transparent, decentralized and completely secure and efficient management of medical information[8,13].

3.4 BLOCKCHAIN IN HEALTHCARE DATA STORAGE

Blockchain technology offered the immutability, decentralization and transparency for practical resolution of the current concerns in healthcare information storage. These issues will be handled using blockchain in different ways[14].

1. Security and Privacy
Cryptographic hashing is used to apply the blockchain technology to ensure data validity and confidentiality. This security and privacy are a strong option for safeguarding sensitive medical information against unauthorized access and data breaches.

2. Interoperability
Blockchain increases healthcare information management by influencing a communal platform for transparent information exchange among several events safely.

3. Data Provenance and Transparency
Blockchain technology will permit observable and confirmable data transactions which ensures the origin of information and stimulate transparency in the medical domain.

4. Breaking Down Data Silos
Breaking down the barriers associated with traditional medical information and ensuring that it easier to store and exchange information through the blockchain domain.

Distributed archive can be steadily combined into healthcare information storage and management results due to its adaptability in addressing numerous industry challenges. Blockchain helps to store the healthcare information in different sources and is explained below[15,16]:

5. Effective Document Storage and Management
Blockchain allows storage of large volumes of medical information and simple-to-track information records over time, and speedily recovers information when required. For instance, DocFlow, a blockchain-based document management tool, can be employed for digital health records (EHR) access protection, insurance management, and clinical research data encryption.

6. Data Security
The healthcare industry has witnessed numerous data breaches, with 692 reported in the 2021–2022 period alone. Blockchain, especially private blockchains, provides robust data security by allowing only authorized users to access sensitive data. For example, Patientory is a mobile application that uses a private blockchain network, PTOYMatrix, to securely retain healthcare documents and grant users' entire control of health data.

7. Medical Research
Blockchain can function as a universal database for medical research, enabling researchers worldwide to access vast volumes of advanced information crucial for enhancing patient treatment. Companies like Nebula Genomics are leveraging blockchain to build substantial genetic databases and incentivize users to safely share their encrypted genetic data for further analysis.

8. Counterfeit Prevention
Blockchain technology helps in combating counterfeit medical products by ensuring authenticity of medical equipment and drugs. Applications namely BlockPharma have the capability to integrate with pharmaceutical companies' information systems for the storage of drug details and QR codes on the blockchain, providing users with the means to authenticate the legitimacy of their purchased medicines.

9. Insurance Process Enhancement
Blockchain's smart contracts have the capability to streamline insurance management by automatically processing insurance requests according to pre-established rules. This results in faster, more transparent insurance settlements with reduced costs. For instance, Etherisc is a distributed insurance protocol which allows different industries, including healthcare, to create insurance solutions, cutting down inefficiencies like high processing fees and lengthy settlement procedures.

10. Preservation and Exchange of Patient Information
Blockchain networks are applied in the medical sphere to store and transfer information securely. They can also play a decisive role in identifying significant errors, including potentially harmful ones, within the medical domain, and contribute significantly to combating fraud in clinical trials, ultimately leading to improved healthcare outcomes.

3.4.1 Use Case: MedRec – Empowering Patients Through Blockchain

MedRec is a groundbreaking solution developed to solve the concerns of managing medical records to ensure information interoperability in the healthcare sector. By employing technology based on blockchain principles, MedRec establishes a decentralized and immutable framework, offering transparency in the management of EHR. It streamlines access data from a patient-centric perspective and simplifies the exchange of information among various healthcare stakeholders[10,17].

- MedRec completely decentralizes access rights through an Ethereum blockchain, empowering patients with control over the distribution of their records.
- It operates like the World Wide Web, where patients and providers operate nodes that authorize others to retrieve data.
- There are no centralized data repositories established by MedRec. Rather, its modular system architecture works with the local systems that providers already have in place.
- Exchange of information for protecting and maintaining network data through the system offers patients data that are aggregated, de-identified as mining incentives.
- MedRec uses an Ethereum Proof-of-Authority blockchain with Smart Contracts to support its permission and data access management.
- It is useful for internal management of records by hospital networks consisting of many independent providers and scales to multiple, large-scale networks.

Figure 3.4 showcases the interaction between patients, providers, and the MedRec system, emphasizing the function of Ethereum blockchain, smart contracts, and proof

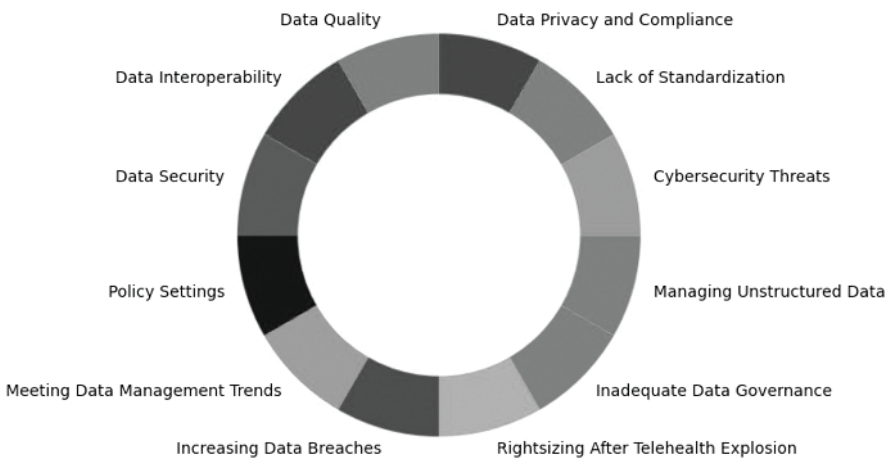

FIGURE 3.4 Challenges in healthcare data management.

of work mechanism. It also highlights the internal record management by independent providers and their scalability to large networks[18,19].

3.5 BLOCKCHAIN FOR HEALTHCARE DATA EXCHANGE

The following sections describe the functions of the blockchain in data exchange, a separate structure for data exchange inside a specific network or organization.

3.5.1 Data: The Modern Pulse of Healthcare

Data has emerged as the vital component of today healthcare era. Ranging from digital health records to medical imagery and investigative findings, the depth and intricacy of healthcare data are expanding at an unprecedented rate. Stakeholders are expecting good decisions, research and enhancement of patient outcomes to share information in efficient and secured way described in Figure 3.5. Blockchain technology helps us to exchange information among different stockholders safely[9,20].

3.5.2 Challenges of Data Exchange

Exchanging of healthcare information will affect interoperability, privacy and decentralized systems in a traditional way. It is very difficult for healthcare groups to alterinformation. It increases the probability of errors, delays and inefficiencies. The blockchain domain provides a probable resolution for these kinds of concerns and improved healthcare information is accomplished.

3.5.3 Facilitating Secure and Transparent Data Exchange

Blockchain helps to decentralize and enable cryptographic security to develop a robust framework in a secure and transparent exposition of healthcare information. The transparency f blockchain ensures data integrity to record transactions on an absolute ledger, transactions that are noticeable and confirmable. Additionally, the decentralized method decreases the hazards allied to unauthorized access and failure in central points.

1. Security
Security is enabled to consensus processes in cryptographic hashes using blockchain technology, which ensures integrity and confidentiality during transactions.

2. Transparency
Blockchain technology inspires confidence and accountability of data exchanges in the healthcare domain between various stakeholders due to its transparency.

3. Efficiency
Efficiency is important while transferring data in real time; the blockchain helps to increase real-time information access, deals with minor administrative costs and systematizes repetitive tasks to modernize healthcare information exchange.

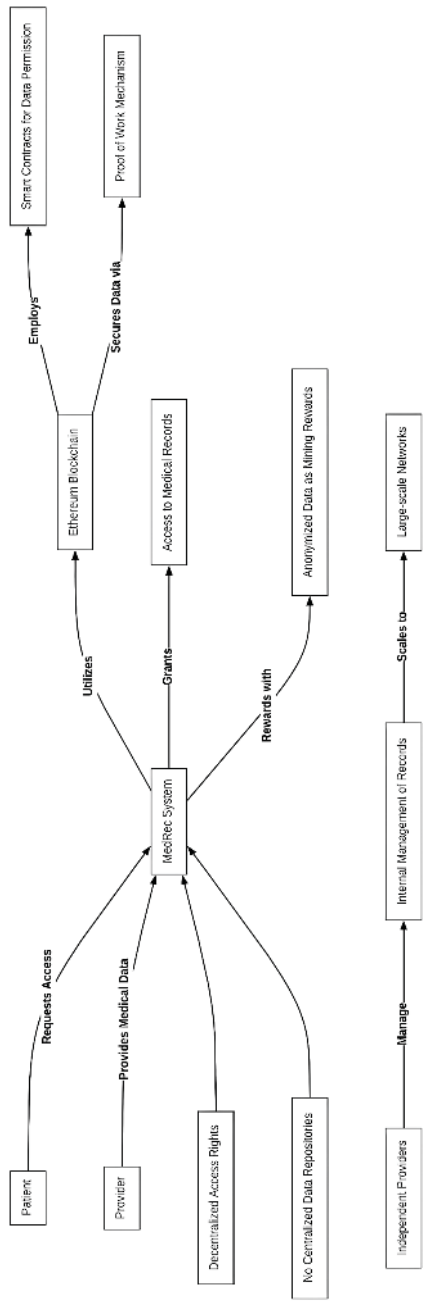

FIGURE 3.5 MedRec Blockchain Workflow.

3.5.4 Smart Contracts in Healthcare Data Exchange

Computerization of healthcare information exchange progressions could be proficient for smart contracts, which are obviously embedded necessities. This embedded mechanism helps to decrease error risk and provide high efficiency.

1. Automating Consent Management
Health information is maintained to streamline the agreement management process, grant the smart contracts or retract access more effortlessly.[14]

2. Streamlining Billing and Processing of Claims
Smart contracts help to decrease administrative costs and speed up the settlement process by introducing an automation process for claims and invoices.

3. Enhancing Provider-Patient Interactions
Smart contracts help healthcare and patient information providers to interconnect effortlessly by automating the process for reminders, follow-up and appointments schedule.

4. Clinical or Medical Trials and Research Collaboration
Blockchain technology simplifies safe association with scientists and easy to perform clinical research. It confirms data traceability and validity to lessen the risk of data manipulation and fraud.

3.6 POPULAR BLOCKCHAIN FRAMEWORKS IN HEALTHCARE

Selecting a right framework of blockchain is very critical due to affect the effectiveness and usability in final results directly[21,22].

1. Ethereum
Ethereum serves as a decentralized platform which enables the development of other decentralized applications (DApps). Ethereum is used to create transparent and immutable patient records in the healthcare sector which ensures integrity and security. Smart contracts shorten and systematize a portion of healthcare progressions, which increase productivity and decrease the administrative burden: Keeping patient consent for data exchange, verifying the authenticity of drugs and promising the accuracy of clinical information.

2. Hyperledger Fabric
Hyperledger Fabric is a mechanism which provides a platform with multiple applications with approval in the blockchain technology. Data security is particularly valuable for many applications related to the healthcare sector. Hyperledger Fabric, in contrast to public blockchain, enables the formation of private channels and restrictive admission to delicate patient information when it is approved. In the healthcare sector, handling the pharmaceutical supply chain facilitates the efficient and security of patient information among healthcare sectors.

3. Multichain
Blockchain networks with private permission can be established using Multichain as well-defined architecture. The healthcare domain need to find better results for simplicity in setup and alteration. Multichain provides more security and privacy to track medical information safely only for authenticated persons. There are two examples of application setups supporting the accuracy of health information repositories and monitoring the basis of medical apparatus.

3.6.1 Comparative Analysis

Blockchain architecture helps to identify the healthcare applications for providing factors for better scalability, security and integration. Though for certain scalability issues, the Ethereum proposals give robust foundation for smart contracts. Hyperledger Fabric delivers privacy and dynamic permissioned control for sensitive medical information. Multichain suggest the hurried and user-friendly setup for tiny healthcare facilities.

3.6.2 Existing Healthcare Systems Integration

Blockchain frameworks integrate the existing and current healthcare information systems for considering interoperability and standards. The blockchain results should be able to altercate information and establish connections with existing EHR systems in order to function efficiently.

3.6.3 Security and Privacy

Security and privacy are essential in healthcare. Blockchain frameworks provide various mechanisms to secure data and ensure privacy. Encryption, consensus mechanisms, and further security protocols play an essential role in protecting patient data and confirming that it is only accessible to authorized parties. Table 3.1 defines Comparative analysis of how different blockchain frameworks addresses security and privacy concerns specific to healthcare data.

3.6.4 Security Protocols and Best Practices

Implementing additional security protocols and maximum scrutiny is critical to safeguarding healthcare data.

1. *Regular Audits and Updates:* All blockchain frameworks should be regularly audited for vulnerabilities, and timely updates should have been applied to address any identified security issues.
2. *Access Control:* Proper access control mechanisms should be in place to confirm that only approved individuals can access sensitive patient data.
3. *Data Anonymization:* In cases where patient data needs to be shared for research or other purposes, data anonymization techniques should have been employed to protect patient privacy.

TABLE 3.1
Comparative analysis of how different blockchain frameworks addresses security and privacy concerns specific to healthcare data

Feature/Concern	Ethereum	Hyperledger Fabric	Multichain
Encryption	Uses advanced cryptographic techniques for data encryption. Smart contracts can incorporate encryption algorithms.	Provides granular control, supporting data encryption both at respite and in transit. Supports HSMs for secure key management.	Supports encryption of data at respite and during transmission.
Consensus Mechanisms	Utilizes Proof of Work and transitioning to Proof of Stake. Ensures data integrity is energy-intensive.	Pluggable consensus mechanism allowing flexibility to prioritize data integrity while considering efficiency.	Less energy-intensive consensus model, suitable for efficiency but may offer lower security compared to PoW/PoS.
Access Control	Provides mechanisms for creating private transactions and confidential contracts.	Channels for private transactions. Fine-grained access control.	Allows for the creation of 'streams' for restricted data access.
Data Anonymization	Possible through smart contracts, but requires careful implementation.	Can be implemented within chaincode (smart contracts in Hyperledger Fabric).	Can implement some data part handling logic.
Security of Smart Contracts	Critical to confirm the security of smart contracts as vulnerabilities could lead to data breaches.	Chaincode security is essential, and proper auditing and testing practices are required.	Not applicable as Multichain does not rely on smart contracts in the same way.
Secure Key Management	Essential for managing encryption keys, especially data encryption context.	Supports Hardware Security Modules (HSMs) for secure key management.	Requires robust key management practices to ensure data security.

4. *Security of Smart Contracts:* For frameworks like Ethereum, ensuring the smart contracts security is crucial, as vulnerabilities could be exploited to access or alter sensitive data.
5. *Secure Key Management:* To prevent unauthorized access to encrypted data, appropriate key management procedures should be followed.

By addressing these privacy and security concerns, blockchain frameworks can provide a private and secure means of exchanging and storing healthcare data. By doing

this, it will be ensured that patient data is secure and accessible to authorized individuals only.

3.7 SCALABILITY AND PERFORMANCE

Healthcare blockchain technology has to be scalable in order to handle growing patient data volumes and the growing need for real-time data access. Blockchain frameworks are always being optimized and innovated to report these scaling issues and enhance performance.

3.7.1 Scalability Challenges in Healthcare

1. *Volume of Data:* Patient records, medical images, test results, and other information are all included in healthcare data. For blockchain networks, the vast amount of data is a major difficulty because every transaction and data input needs network-wide consensus, which might cause congestion and delayed transactions.
2. *Real-time Access:* Access to patient information should be regularly available in real time in the healthcare domain. Blockchain networks have latency issues especially for Proof of Work consensus techniques, which will disturb the speedy retrieval of patient information.
3. *Size and Complexity of the Network:* Blockchain technology has scalability risks in size and complexity which additional healthcare providers and organizations can implement directly.

3.7.2 Techniques and Innovations for Improved Performance

1. *Sharding:* Sharding will help to divide the blockchain network into minor parts for controllable chunks, or shards, which is accomplished with autonomously observing transactions and smart contracts. Sharding is used to increase the capacity and network speed.
2. *Data Pruning:* It will help to remove the unnecessary data from the blockchain for the purpose of advancing performance and creating space for fresh data.
3. *Off-chain Transactions:* This network will be handling a high capacity of transactions and processing additional transactions off-chain and position on the network.
4. *Parallel Processing:* This will help the blockchain to rapidly increase the performance significantly and it will allow the processing of parallel smart contracts and transactions.
5. *Layer 2 Solutions:* Blockchain-based technologies intended to resolve the issues of scalability and performance.
6. *Caching:* Caching techniques will help to retrieve data much faster to store regularly demanded information.
7. *Optimized Consensus Mechanisms:* This mechanism will help to employ more efficient consensus methods like PoS or DPoS, transaction speed and scalability could be improved.

8. *Managing Medical Records:* Blockchain technology excludes the necessity for multiple systems and complex information handovers by permitting the secure delivery and storage of EHRs.
9. *Safeguarding Pharmaceutical Supply Chain Integrity:* Blockchain permits whole transparency and traceability during pharmaceutical supply chain. Blockchain increases patient safety by decreasing drug abuse and acquires rid of counselling by ensuring a medication from point of production to delivery.
10. *Telehealth and Distant Medical Services:* Trust and security are more important in online medical services, which are increased by the blockchain domain. So as to guarantee precise diagnoses and apt treatment sanctions, patients could safely transfer medical information with telehealth providers.

3.8 SUMMARY: LEVERAGING BLOCKCHAIN IN MANAGING HEALTHCARE DATA

Blockchain leads different benefits matched with existing healthcare information supervision methods. Comparative learning displays how blockchain-based medical results will change the healthcare domain. Table 3.2 defines A comparative learning displays what way blockchain-based medical results will change healthcare domain**.** To summarize, the blockchain domain in healthcare resolutions increases interoperability, efficiency, security, transparency and confidence in numerous areas of the healthcare ecosystem. Eventually, it will expand patient care and results by transforming data management in the medical domain.

3.9 CONCLUSION

The innovative approaches for switching and preserving data are helping in recent healthcare scenarios with applying the blockchain technology. It challenges the significant concerns for facing the healthcare sector, such as data security, patient control, interoperability and integrity. Encryption methods and decentralized storage are in-built security structures of blockchain technology that guard the stable medical records. Data integrity is confirmed by the immutability of the blockchain archive which is used to avoid unlawful variations and strengthen confidence amongst all stakeholders intricate in the healthcare domain. Blockchain also helps to enhance interoperability which protects the information and to transfer the information among different healthcare organizations and systems easily. Due to amplified transparency and confidentiality protection, patients are using the blockchain domain to have control over health information.

However, a few challenges are adopted in this technology which increase the speed and trust about the technology for better understanding. This blockchain technology advances and passes beyond up-to-date challenges; blockchain-based clarifications will significantly increase the efficiency of medical information for exchange and storage. It is significant to safeguard the advantages and compensate for the shortcomings, and the medical sector is effectively furnished to grip this shift in thinking.

TABLE 3.2
Comparative analysis of traditional healthcare data management and blockchain-enabled healthcare solutions

Aspect	Traditional Healthcare	Blockchain in Healthcare
Data Protection and Confidentiality	• Vulnerable to hacks and breaches. • Single points of failure are associated with centralized databases.	• Secure and immutable records ensuring data remains unaltered without network consensus. • Enhanced data security and privacy.
Data Fragmentation	• Fragmented data across different healthcare providers. • Challenging to access a comprehensive medical history.	• Enhanced interoperability allowing seamless access and updates to patient records by different healthcare providers.
Interoperability	• Frequently, systems are unable to connect with another one, resulting in inefficiencies and potential medical errors.	• Enhanced interoperability, minimizing the potential for medical errors. • Seamless communication between different systems.
Trust and Transparency	• Patients must trust healthcare providers to handle their data securely.	• Transparent, auditable ledger improving trust and transparency. • Patients control who has access to their data.
Billing and Insurance	• Complex billing processes prone to errors and fraud.	• Streamlined billing and insurance processes reducing administrative costs and fraud.
Drug Traceability	• Counterfeit drugs and inadequate supply chain traceability.	• Improved pharmaceutical supply chain tracking to guarantee drug authenticity.
Clinical Trials and Research	• Challenges in managing patient consent and securely storing research data.	• Streamlined process for conducting clinical trials, securely managing patient consent, and securely storing research data.
Telemedicine and Remote Patient Monitoring	• Potential security concerns with sharing patient data.	• Using integrated blockchain technology, securing real-time patient data sharing is possible with healthcare providers.

In conclusion, the healthcare sector is taking immense steps towards effective, secure, and confidential leveraging of blockchain frameworks to exchange and store information. This will primarily change the method for medical information which will manage trust and transparency in systems. In future, the blockchain technology will help the medical domain in all the aspects in various diseases with relevant patients' information to secure, protect, keep confidential and store.

REFERENCES

1. E. Vashishtha, H. Kapoor, Implementation of blockchain technology across international healthcare markets, *FMDB Transactions on Sustainable Technoprise Letters*, 1(1) (2023) 1–12. www.researchgate.net/publication/371249890_Implementation_of_Blockchain_Technology_Across_International_Healthcare_Markets
2. Blockchain in Healthcare: An Executive's Guide for 2023. Digitalauthority.me. [Online]. Available: www.digitalauthority.me/resources/blockchain-in-healthcare. [Accessed: 05-Oct.-2023]
3. E. Chukwu, L. Garg, A systematic review of Blockchain in healthcare: frameworks, prototypes, and implementations, *IEEE Access*, 8 (2020, January 28) 21196–21214.
4. HealthTech Magazine. Overcoming obstacles to data sharing in healthcare. [Online], 2023, January. Available: https://healthtechmagazine.net/article/2023/01/overcoming-obstacles-data-sharing-healthcare
5. V. Dhillon, D. Metcalf, M. Hooper, Blockchain in healthcare, in: *Blockchain- enabled applications*, Apress, Berkeley, CA, 2021, pp. 201–220.
6. Health IT Answers. 5 Biggest challenges of health care data security in 2022, 2022. www.healthitanswers.net/5-biggest-challenges-of-health-care-data-security-in-2022
7. C. Poongodi, K. Lalitha, R.K. Dhanaraj, The role of blockchains for medical electronics security, in: *Essential enterprise blockchain concepts and applications*. Auerbach Publications, 2021, pp. 231–262.
8. A. Singh, R. K. Dhanaraj, M. A. Ali, B. Balusamy, V. Sharma, Blockchain technology in biometric database system, in: *2022 3rd International Conference on Computation, Automation and Knowledge Management (ICCAKM)*. IEEE, 2022, November, pp. 1–6.
9. K. Paranjape, M. Parker, D. Houlding, J. Car, Implementation considerations for Blockchain in healthcare institutions, *Blockchain in Healthcare Today*, 2 (2019, July 9) 10–30953.
10. S. Malathy, K. Sangeetha, C.N. Vanitha, R.K. Dhanaraj, Integrated architecture for IoTSG: internet of things (IoT) and smart grid (SG), in: *Smart grids and internet of things: an energy perspective*. Wiley Online Library, 2023, pp. 127–155.
11. A. Ekblaw, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data, in: *Proceedings of IEEE Open & Big Data Conference*, vol. 13, 2016, August 13, pp. 13.
12. D.V. Dimitrov, Blockchain applications for healthcare data management, *Healthcare Informatics Research*, 25(1) (2019 January) 51.
13. T. Benil, J. Jasper, Blockchain based secure medical data outsourcing with data deduplication in cloud environment, *Computer Communication*, 209 (2023 September) 1–13. [Online]. https://doi.org/10.1016/j.comcom.2023.06.013
14. M. Hölbl, M. Kompara, A. Kamišalić, L. Nemec Zlatolas, A systematic review of the use of blockchain in healthcare, *Symmetry*, 10 (2018) 470. https://doi.org/10.3390/sym10100470
15. R. Gupta, S. Tanwar, S. Tyagi, N. Kumar, M.S. Obaidat, B. Sadoun, Habits: blockchain-based telesurgery framework for healthcare 4.0, in: *2019 International Conference on Computer, Information and Telecommunication Systems (CITS)*. IEEE, 2019, August 28, pp. 1–5.
16. G. Srivastava, R.M. Parizi, A. Dehghantanha, The future of blockchain technology in healthcare internet of things security, in: Blockchain Cybersecurity, Trust and Privacy, Springer, 2020, pp. 161–184.

17. G. Rathee, A. Sharma, H. Saini, R. Kumar, R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, *Multimedia Tools and Applications*, 75 (2019 June 3) 1–23.
18. B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, *IEEE Access*, 8 (2020, May 12) 90478–90494.
19. E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.Y. Song, A.K. Bashir, A.A. Abd El-Latif, DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems, *IEEE Access*, 8 (2020, June 2) 111223–111238.
20. R. Kumar, N. Marchang, R,.Tripathi, Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and Blockchain, in: *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)*. IEEE, 2020, January 7, pp. 1–5.
21. D. Chhabra,M. Kang, V. Lemieux, Blockchain, AI, and Data Protection in Healthcare: A Comparative Analysis of Two Blockchain Data Marketplaces in Relation to Fair Data Processing and the 'Data Double-Spending'Problem, in: *Blockchain and Artificial Intelligence-Based Solution to Enhance the Privacy in Digital Identity and IoT*. CRC Press, 2024, pp. 125–154.
22. G. Tripathi, M.A. Ahad, S. Paiva, S2HS-A Blockchain-based approach for smart healthcare system, in: Healthcare, vol. 8. Elsevier, 2020, March 1, p. 100391. No. 1.

4 FOG Computing and Blockchain-Supported Identity Management for IoMT

An Advancement in Personalized Healthcare

Jay Prakash Maurya, Vinesh Kumar, S. Aanjankumar, Malathy Sathyamoorthy, and Aslina Banu R

4.1 INTRODUCTION

IoT technology is revolutionizing the medical industry by providing individualized care through devices that track patients' medical histories, identifying and treating ailments in real time, and providing real-time health tracking. IoT-based medical technology is enabling more individualized healthcare and improved patient outcomes. Through the network of medical equipment, we can monitor important signs, identify diseases, and provide tailored treatments.[1] These networks' connected devices focus various applications i.e telemedicine, patient monitoring, medical imaging, and preventative medical care. They enable secure, reliable, and accurate data analysis, saving operating costs, improving patient outcomes, and increasing treatment quality.[2] This is particularly beneficial for elderly patients with chronic illnesses who cannot visit a doctor's office.[3] IoT-based devices share healthcare diagnosis data, enhancing patient care efficiency.[4] This technology is expected to continue evolving in the future to improve patient outcomes and overall healthcare. Below are some IoMT examples available in the market as some devices. Apart from the ones given below, lot of other devices are available to support personal devices.

1. Smartphones and smart watches
2. Smart pill boxes
3. Smart scales
4. Smart blood pressure machine
5. Smart oxygen inhalers
6. Smart thermometers

DOI: 10.1201/9781032711379-4

4.1.1 Personalized Healthcare

Personalized healthcare is a recent innovation that aims to tailor treatments and care to each patient's individual needs. This can include advice on medications, exercises, or specially prepared meals. The benefits of personalized care include patients feeling more in control of their health, gaining a better understanding of their bodies, and potentially being less expensive than conventional care. This approach reduces the amount of medical care needed, ultimately improving overall health outcomes. Healthcare stakeholders (patients, healthcare professionals, etc.) can access information and provide preventative or control measures (prescription) as per individual patient needs.[5] Apart from flexibility and control over individual health, more factors are participating in popularity, given below

1. Offering comprehensive, personalized experience through prioritizing medical treatment and focusing on susceptibility.
2. Generation and utilization of electronic sources of data like healthcare records, and genomic data used in personalized advice.
3. Patients' individual needs and preferences through analysis of generated data. The cost reduction by reducing the total number of tests or treatments.
4. A personalized healthcare system must be supported by controlled cryptographic policies where an individual's identity is important.
5. Education and skill development using technology and a simulation system such as virtual reality, augmented reality, and artificial intelligence applied in small devices and interface platforms.

4.1.2 Recent Development

IoMT is a growing field of application in areas like healthcare that uses wireless technologies to ensure medical apparatus communication. Wireless technology advancement deals in Wi-Fi, Bluetooth, and RFID technology are a field of concern. Active participation of IoMT is seen in robotic-assisted systems, surgical tools production, patient diagnosis and monitoring, and virtual reality-based training systems.[6] IoMT managed through cloud application can be tuned in available healthcare settings, remote monitoring, diagnostics, and telemedicine. It improves patient outcomes by collecting and analyzing data from linked medical devices.[7] It reduces costs and improves efficiency by automating processes and reducing administrative tasks. Applications include drug delivery systems, wearable medical devices, and home health monitoring systems.[2]

4.1.3 Identity Management and Ecosystem

An important component of IoMT for securing a customized healthcare environment is identity management. It includes user identification, access control, and provisioning as a key concept associated with identity management. Procedures, regulations, and technological advancements within any healthcare system may securely manage

and confirm digital identities. In a secure system supported by cryptographic rules, confirmed identities and predefined responsibilities give people, gadgets, or other entities proper access to resources, data, and services. To avoid unwanted access and breaches, and to boost the efficiency of connected IoMT devices, the ecosystem helps the modern personalized healthcare environment to manage IoMT devices and protect sensitive data, also fulfilling regulatory requirements, and ensuring effective user access.[8]

IAM (Identity Access Management) is a single term that is named for involving and tracking behaviors or actions in each asset and environment. Key components related to IAM are given below. Figure 4.1 shows the supported key services that IAM can provide and also a mandatory research domain for a number of application areas like healthcare.

- Authentication and authorization: Forces for implementation of proper access rights, due to scalable and available solutions.
- RBAC (Role Based Access Control): to secure from internal attack.
- Single Sign-on: Back-end application and service authentication by third party centralized system.
- Federation of services: Service support from internal network to cloud services.

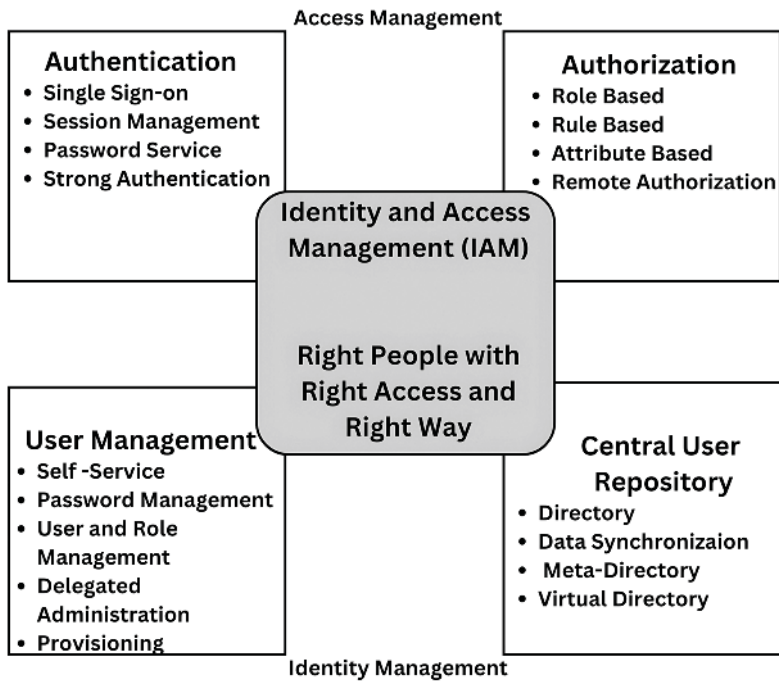

FIGURE 4.1 Describes the key components of an IAM strategy.

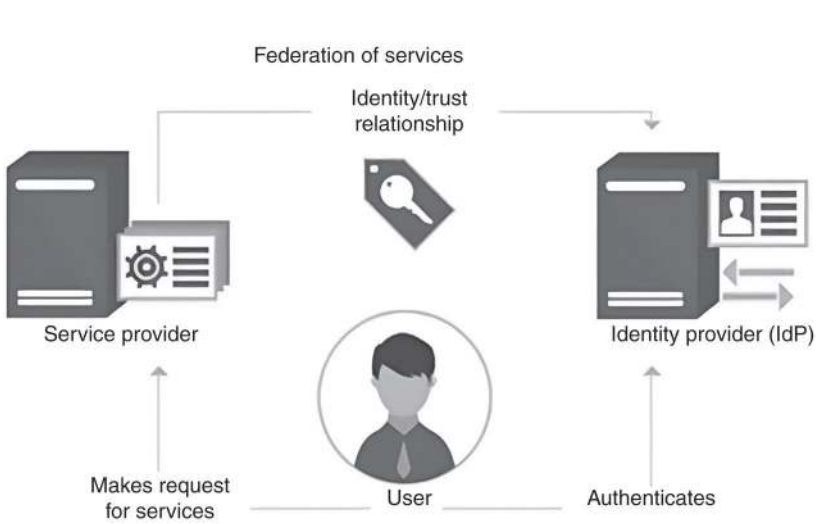

FIGURE 4.2 IAM ecosystem.

Figure 4.2 shows the critical role of each entity to ensure appropriate services' access, authentication, and authorization of users, devices, and entities across various digital platforms and systems.[9] Key components of the Identity Management Ecosystem include:

- Identity Providers (IdPs): Organizations or services responsible for authenticating users and issuing digital identities. Examples include active directory, social media platforms, and identity as a service (IDaaS) provider.
- User / User Repository: A centralized storage system where user identity data is maintained, including attributes, credentials, and access permissions. Common repositories include LDAP directories and databases.
- Authentication Mechanisms: Techniques and methods used to verify user identities, such as username/password, biometrics, two-factor authentication (2FA), and single sign-on (SSO).
- Federation Services: Technologies and standards (e.g., SAML, OAuth, OpenID Connect) that enable cross-domain or cross-organization authentication and authorization.
- Identity and Access Management (IAM) Solutions: Comprehensive platforms or suites that provide identity lifecycle management, access governance, and other identity-related features. Rules/policies to govern cryptographic tokens (e.g., JWT, OAuth tokens) for the exchange of identity and managing identities.
- Authentication and Authorization APIs: Interfaces that allow applications and services to integrate with identity management systems for user authentication and access control.

4.2 ARTICLES REVIEWED

1. **Kamarajugadda et al.** suggested, a proposed technique (BBO-SVM) for diagnosing and predicting heart diseases. The BBO method is used to adjust SVM parameters, and the model has performed well, indicating that results accurately forecast heart disease.[10]
2. **Tai et al.** completed a study using Deep Neural Networks (DNNs) and Extended Reality (XR) to propose IoMT for COVID-19 diagnosis. It uses a specialized prediction algorithm based on ACGAN to enhance human ergonomic performance. The authors visualize navigational cues through a Haptic-AR system, potentially guiding and offering a novel method for treating COVID-19 using deep learning for IoMT prediction and remote surgical plan cues.[11]
3. **Selvaraj, S. et al**. highlight the potential of the IoT in providing emergency services and monitoring patients remotely, particularly those with cardiac conditions. The study examines various research projects related to IoT-based healthcare systems, focusing on an ECG monitoring system using machine learning to identify signs of illness. However, the main drawbacks include high power consumption, resource scarcity, and security issues.[12]
4. **Aljabr et al.** suggest using an end-to-end IoMT architecture to manage pandemic circumstances. This architecture improves real-time medical care, encourages interaction between users and the IoMT system, and reduces morbidity and financial burden by reducing follow-up visits. It accelerates response time in medical emergencies, aiding citizens, medical (Government / Private) professionals for pandemic situations effectively, delivering essential supplies, and creating social distancing.[6]
5. **Ghubaish et al.** This paper discusses the importance of IoMT-based systems for remote patient monitoring. It presents advanced data security techniques during data collection, transmission, and storage. The authors analyze potential attacks on IoMT systems and recommend a security architecture that combines various measures to meet security requirements and prevent most attacks.[13]
6. According to **Villegas-Ch et al.**, devices within the IoMT network must be preregistered and an identifier mechanism must be set to verify and authenticate. IoT devices must be preregistered with an identity verifier before they can use an infrastructure authentication mechanism. A lot of challenges to issuing and managing identity for individual devices and working with heterogeneous types of infrastructure.[14]
7. According to **Yaacoub et al.**, IAM must manage standard user, admin, authorization process, access control, and privileged access.[15]

The extension of work in reference work for IAM was progressed by different researchers for referencing and connecting Blockchain and FOG-based identity management proposed work. The related work of IAM field is discussed in Section 4.5.

4.3 CHALLENGES

IoMT as a technology needs interconnection between medical equipment for data gathering, sending to another equipment node.[12] After collection of data on a centralized node in minimal latency time, defined monitoring and diagnosis process help to suggest treatments. This process can be made possible by IoMT and may have the potential to revolutionize healthcare, but there are also several issues:

1. Energy optimization
2. Cost optimization
3. Accuracy of transferred data
4. Data transformation
5. Data load balancing and overload handling
6. Legal and ethical
7. Infrastructure reliability
8. Regulation and compliance
9. Privacy and security

To address these issues, an ecosystem for the IoMT that is secure, interoperable, and patient-centric needs to be developed in partnership between stakeholders, regulatory bodies (government and medical facility managers), technical and medical facilitators.[13] Important challenges that are the focus of this chapter are highlighted in Figure 4.3. Fog computing can be used to address and resolve the significant problems listed above.[3,14]

Table 4.1 shows the referenced challenges and respective technology solutions, to be addressed to respective IoMT. It is shown in Table 4.1 that experimental work was done on chosen number of issues identified in article review as applications of fog computing.[16]

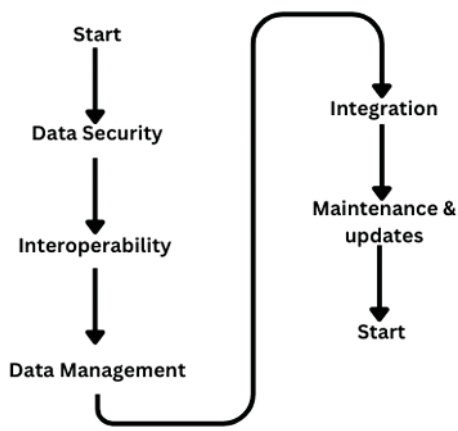

FIGURE 4.3 IOMT Framework challenges/issues.

TABLE 4.1
Technological solution respective to issues

Issue	Solution area
9	Blockchain
	Encryption
	Access Control
	Identity Management
4	Protocols development
	EC
8	EC
3	Data Validation Through Edge Computing
	Calibration
7	FC
	Failsafe Mechanisms
1	Offloading and Edge Processing
6	Consent Management
	Data Control
5	Edge Processing
	Cloud Bursting
2	FC
	Reusable Edge Resources

4.4 IAM FOR IOMT DEVICES

IAM management for IoMT may be possible through the different possible techniques of cryptography. Implementation of secure policy always defines a way to provide identity and access management rules and must be judged based on the risk management of a healthcare framework. Different types of methods were already suggested by researchers for IAM and supported IAM. Some of the major techniques are discussed below from a technical perspective and technical relevance perspective.[17]

4.4.1 Privileged Access Management (PAM)

The IoMT admin users are granted special privileges through privileged access management (PAM) to access all IoMT devices and sensors. Passwords for IoMT admin users are different from those for IoMT devices. Administrators are unable to recall each of these passwords. Single Sign-on for Personalised Access Management is possible through a single unique identifier for accessing and securing multiple services.

4.4.2 Authentication (Identity Based)

Heterogeneous devices in IoMT issue important security concerns for IoT components like standards, protocols, and identification. Among these, the identity of a device is an important factor for security mechanisms like encryption, signatures, and authentication. Multi-factor authentication and mutual authentication mechanisms are popular in this field.

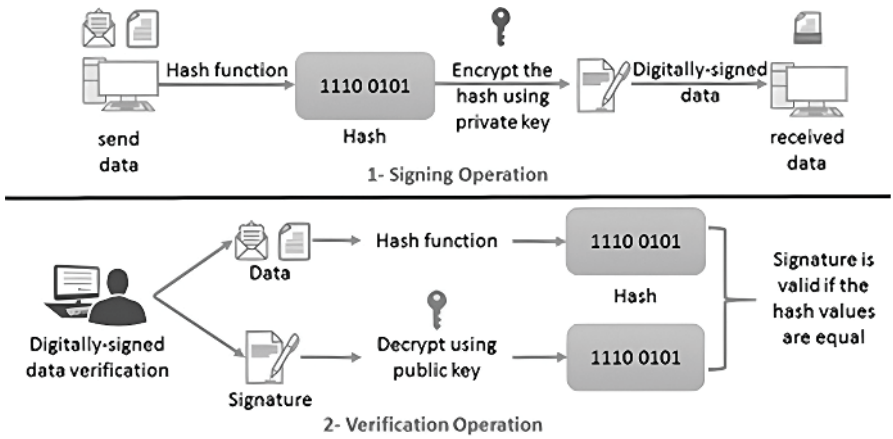

FIGURE 4.4 Digital signature processing.

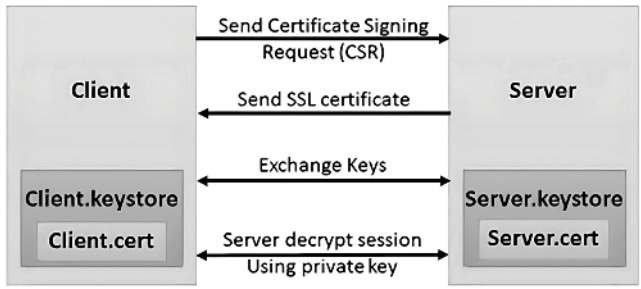

FIGURE 4.5 SSL operation.

4.4.3 Digital Signature

A digital signature enables the IoT system administrator to authenticate and verify IoT devices using his or her own private key (Figure 4.4). The processing of the signature and verification processes from the source to the destination is depicted in Figure 4.5. During the signature process, the data is encrypted with a private key using a hash function. The data is decrypted during the verification process using the public key and the hash algorithm. The signature is legitimate if the results of the hash function and data decryption are identical; if not, the signature is invalid (Abdullah et al., 2019[18]). Validated applications and services using signature, X.509 Certificate help with digital identification between certificate authority and customer.

4.4.4 Raw Public Key

The Internet Engineering Task Force provides a mechanism to communicate client and server security published under RFC7250 for public key infrastructure. RPK defined by

IETF supports a chain of certificates for transport layer security (TLS) and Datagram Transport Layer security. The RPK method is supported by AES-128-CCM and AES-128-CBC on IOT device communication handling. Nodes in the IOMT public network use RPK public key value for checking installed certificates on clients.[19]

4.5 PROPOSED MODEL AND ARCHITECTURE

The IoMT-based system needs improvement in security, privacy, and efficiency. The proposed model suggested two techniques, fog computing and blockchain, to improve IOMT application with decentralized resources over a centralized cloud server. Fog computing helps in improving bandwidth utilization and real-time data processing applications, whereas blockchain issues privacy and secure communication over connected IoMT nodes using the decentralized methods and application of the IoMT framework.[20] This chapter proposes a framework, for which an architectural diagram is given in Figure 4.6.

A fog node between the IoMT device layer and cloud storage layer offers reduced latency, low energy consumption, heterogeneity, and interoperability. Its flexible and scalable structure allows for easy app addition without disrupting the entire healthcare system. This arrangement enhances patient mobility and provides a secure distributed architecture, guarding patient data privacy. The proposed framework and experiment work on sensing mechanism, fog layer, data transportation, BC, and cloud layer to reduce computational power, quick response, secure authentication, authorization, and secure anonymity. The suggested framework will address the latency issue and eliminate time lag, while the BC layer will address any potential security risks.[21]

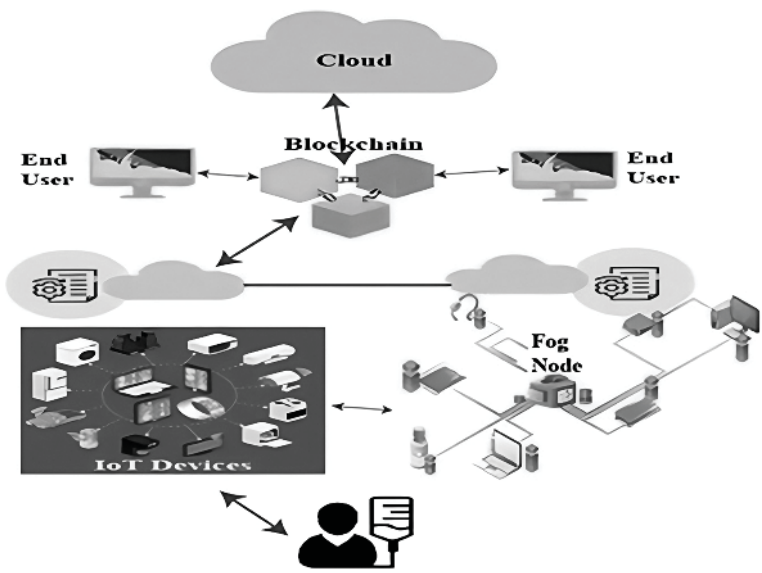

FIGURE 4.6 Proposed IOMT framework.

4.5.1 Physical Unclonable Function (PUF Key) and Blockchain

IoMT device identity and communication using the decentralized blockchain method start using the PUF key. All IoMT devices have IC made up of transistors and have slightly different physical properties. This variation is due to the measurable differences in electronic properties like voltage threshold and gain factor. This pattern of the IC cannot be cloned or copied, like a unique identifier, which is a minute variation into a binary data of 0's and 1's. This is called a silicon fingerprint for any IoMT device and can be turned into a cryptographic key and reversible tool. There are two major types of implementations of PUF in devices SRAM PUF and butterfly PUF. Most of the PUF implementations uses two processes: Error detection and privacy amplification.[11]

A PUF key generation implementation program has been added in part of the experiment and shows a clear idea about key generation using a software concept but it is actually implemented on hardware. Most of the work in methodology is to give an identity for an IoMT node in the IoMT healthcare system using PUF. The second step is to combine this PUF key with MAC address as a block to connect and allow authorization between parties. The authentication server needs PUF information to authenticate the IoMT device and block transmission (Figure 4.7). In this decentralized system, block validation is done by an authentication server, and PUF core support matches all PUFs in different blocks in need of communication for a transaction. The transaction is only possible when matches are the rom PUK (Personal Unblocking Key) code. A block of information is added in each transaction and in nonreadable format. For each access and transmission, it is important to verify PUF and dedicated MAC.

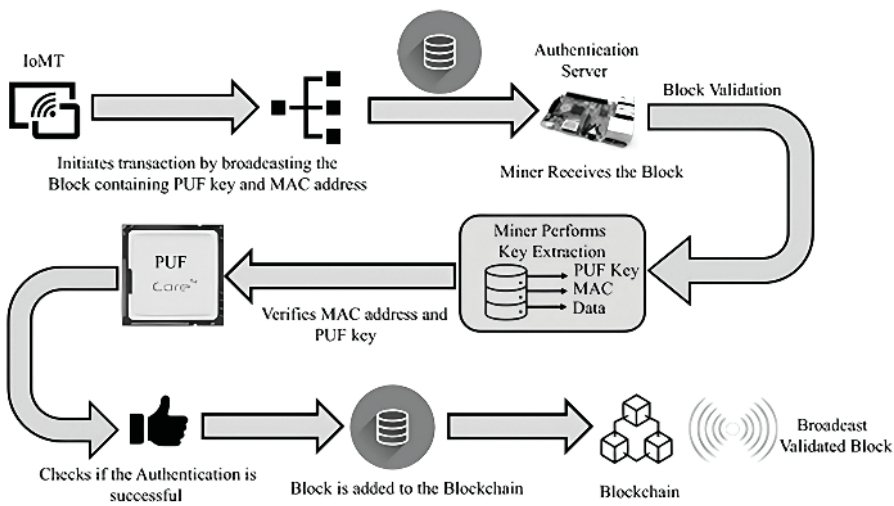

FIGURE 4.7 PUF and block creation process.

TABLE 4.2
Node initialization parameter

S. No	Experimental Parameter	Parameter Initial Value
1	Unique Identifier for a node	1, 2, 3, ...
2	Position of node on Simulation Framework (X,Y Co-ordinate)	(10, 15)
3	Collected / simulated Heart Rate in bpm	75
4	Collected / Simulated blood pressure in mmhg	120/80
5	Temperature of node in ^{o}F	98.6
6	Data transmission Latency Time from one node to another (mili second)	40
7	Transfer rate capacity (MB/s)	0.3
8	Node Energy level in (%)	100

Steps:

1. Start a defining a model, IoMT device node using Block information having PUF and MAC address of the device.
2. Data sensing through sensors. Infrastructure establishment through fog computing, and a blockchain methods.
3. Data collection and process on fog node.
4. Apply encryption and hashing on processed data.
5. Start a blockchain transaction.
6. Initiate a blockchain's validation process.
7. Updating device status based on the validation.

4.5.2 Experimentation

Forty-five simple IoMT sensor nodes were initialized with the listed parameter values (Table 4.2) to begin and taken for network simulation of the proposed suggested model. The first experiment involved initializing each of the 45 nodes as a straightforward IOT node, can be seen as equivalent to an IoMT (no FC or the use of the Blockchain) node to secure data.[22] This implementation of nodes was depicted in Figure 4.8.

4.5.3 Simulation Set up of Nodes

#Identity management and access using PUF (physical Unclonable Function)

```
#include "ns3/core-module.h"
#include "ns3/network-module.h"
#include "ns3/internet-module.h"
```

FIGURE 4.8 Node initial set-up for simulation.

```
#include “ns3/point-to-point-module.h”
#include “ns3/applications-module.h”

using namespace ns3;

NS_LOG_COMPONENT_DEFINE (“PUFIdentityManagement”);

class PUFIdentity {
public:
    uint64_t pufResponse;

    PUFIdentity() {
        pufResponse = GeneratePUFResponse();
    }

    bool Authenticate(uint64_t challenge) {
        return pufResponse == challenge;
    }

private:
    uint64_t GeneratePUFResponse() {
        return 0xabcdef0123456789;
    }
};

void AuthenticateNode(Ptr<Node> node, uint64_t challenge) {
    Ptr<PUFIdentity> identity = node->GetObject<PUFIdentity>();
    if (identity->Authenticate(challenge)) {
        NS_LOG_INFO(“Node “ << node->GetId() << “ authenticated
    successfully.”);
    } else {
        NS_LOG_INFO(“Node “ << node->GetId() << “ authentication failed.”);
    }
}

int main (int argc, char *argv[])
{
    // Enable logging
    LogComponentEnable(“PUFIdentityManagement”, LOG_LEVEL_INFO);

    // Create nodes
    NodeContainer nodes;
    nodes.Create(2);

    // Install PUFIdentity on nodes
    for (NodeContainer::Iterator it = nodes.Begin(); it != nodes.End(); ++it) {
        Ptr<Node> node = *it;
        node-<AggregateObject(CreateObject<PUFIdentity>());
    }
    // Send challenge to node 1 and authenticate with node 2
```

```
    uint64_t challenge = 0x123456789abcdef0; // Example challenge
    Simulator::Schedule(Seconds(1),    &AuthenticateNode,    nodes.Get(1),
challenge);

    Simulator::Run ();
    Simulator::Destroy ();

    return 0;
}
```

Node initialization using FC and Blockchain

```
#include “ns3/core-module.h”
#include “ns3/network-module.h”
#include “ns3/internet-module.h”
#include “ns3/point-to-point-module.h”
#include “ns3/applications-module.h”
#include “ns3/ipv4-global-routing-helper.h”
#include “ns3/mobility-module.h”

using namespace ns3;

NS_LOG_COMPONENT_DEFINE (“IoMTBlockchain”);

class IoMTDevice {
public:
    IoMTDevice(uint32_t id, Ptr<Node> node) : m_id(id), m_node(node) { }

    uint32_t GetId() const { return m_id; }
    Ptr<Node> GetNode() const { return m_node; }

private:
    uint32_t m_id;
    Ptr<Node> m_node;
};

class FogNode {
    public:
        FogNode(uint32_t id, Ptr<Node> node) : m_id(id), m_node(node) { }

        uint32_t GetId() const { return m_id; }
        Ptr<Node> GetNode() const { return m_node; }

    private:
        uint32_t m_id;
        Ptr<Node> m_node;
};

int main (int argc, char *argv[])
{
```

```
// Enable logging
LogComponentEnable("IoMTBlockchain", LOG_LEVEL_INFO);

// Create nodes
NodeContainer iotMTDevices, fogNodes;
iotDevices.Create(20); //  IoMT devices
fogNodes.Create(5);   // 3 fog nodes

// Set up mobility for IoMT devices
MobilityHelper mobility;
mobility.SetMobilityModel ("ns3::ConstantPositionMobilityModel");
mobility.Install (iotDevices);

// Set up internet stack
InternetStackHelper stack;
stack.Install (iotDevices);
stack.Install (fogNodes);

// Assign IP addresses to IoMT devices and fog nodes
Ipv4AddressHelper address;
address.SetBase ("10.4.4.0", "254.754.755.0");
address.Assign (iotDevices);

address.SetBase ("10.2.1.0", "254.754.755.0");
address.Assign (fogNodes);

// Set up point-to-point links between fog nodes
PointToPointHelper p2p;
p2p.SetDeviceAttribute ("DataRate", StringValue ("5Mbps"));
p2p.SetChannelAttribute ("Delay", StringValue ("2ms"));

NetDeviceContainer devices;
for (uint32_t i = 0; i < fogNodes.GetN() - 1; ++i) {
    devices = p2p.Install (fogNodes.Get(i), fogNodes.Get(i + 1));
}

// Install blockchain nodes on fog nodes
for (uint32_t i = 0; i < fogNodes.GetN(); ++i) {
    Ptr<Node> node = fogNodes.Get(i);
    NS_LOG_INFO("Installing blockchain node on Fog Node " << i);
    // Install blockchain node code here
}

// Initialize IoMT devices and connect to fog nodes
for (uint32_t i = 0; i < iotDevices.GetN(); ++i) {
    Ptr<Node> iotNode = iotDevices.Get(i);
    Ptr<IoMTDevice> iotDevice = CreateObject<IoMTDevice>(i, iotNode);
    // Initialize IoMT device code here
    // Connect IoMT device to a fog node
```

```
        uint32_t fogNodeId = i % fogNodes.GetN(); // Assign IoMT devices
    to fog nodes in round-robin manner
        Ptr<Node> fogNode = fogNodes.Get(fogNodeId);
        NS_LOG_INFO("Connecting IoMT Device " << i << " to Fog Node "
    << fogNodeId);
        // Connect IoMT device to fog node using communication protocol
    }

    Simulator::Run ();
    Simulator::Destroy ();

    return 0;
}
```

4.6 RESULTS

Our proposed model works to reduce IoMT device time for communication, distribution, and congestion. Table 4.3 shows the simulation outcomes on distributed 45-node (established) compared with conventional FC nodes. The performance of the usual metrics and parameters improved. The outcome of the customized node implementing blockchain on health information is displayed in Table 4.4. Data was securely transferred to 20 healthcare equipment nodes, where it was verified.

Overall comparisons using common metrics are shown in Table 4.3, along with percentage improvements. In the aforementioned Table 4.3, simulation results of IoMT variations as proposed in Section 4.5. The impact of blockchain functions is also shown in Table 4.3. Each fog computing cluster consisted of 5 nodes that were connected by a hub with an improved data transfer. It was observed from experiment

TABLE 4.3
Improvement in results using FC

Metric / Parameter	Traditional IoT	Implementation using FC	Improvement (%)
Bandwidth Usage (MB/s)	12	4	80%
Server Load	Yes	Minimized by 60%.	-------
Data Privacy (Data Exposure Risk)	Yes	No	-------
Data Processing Time (s)	5	2	60%
Security Rating	Moderate	High	-------
Battery Life Extension	------	Improved by 40%.	--------
Latency (milliseconds)	250	50	80%
Network Dependency (%)	91%	31%	66.70%
Real-Time Decision (%)	42%	92%	125%
Redundancy and Resilience (%)	Very Limited	Improved	-------
Scalability	Very Limited	Distributed	--------

TABLE 4.4
Security using blockchain and its validity

[1]	[2]	[3]	[4]	[5]	[5]	[6]	Blockchain Validity
1	(11, 16)	76	118/76	98.6°F	39	0.4	Valid
2	(7, 21)	79	120/80	98.8°F	44	0.5	Valid
3	(12, 9)	67	126/82	98.4°F	37	0.35	Valid
4	(7, 11)	89	122/78	99.2°F	41	0.45	Valid
5	(15, 19)	76	118/76	98.5°F	42	0.4	Valid
6	(24, 7)	90	120/79	99.4°F	47	0.5	Valid
7	(4, 18)	63	124/81	98.2°F	40	0.4	Valid
8	(11, 21)	75	130/85	98.9°F	43	0.45	Valid
9	(26, 11)	87	114/75	98.7°F	45	0.4	Valid
10	(7, 9)	79	130/85	98.3°F	38	0.35	Valid
11	(17, 17)	90	122/78	99.0°F	46	0.45	Valid
12	(21, 4)	72	120/79	98.6°F	41	0.4	Valid
13	(2, 15)	91	124/81	99.5°F	49	0.5	Valid
14	(12, 20)	64	126/82	98.4°F	42	0.4	Valid
15	(24, 9)	78	130/85	98.8°F	44	0.45	Valid
16	(5, 11)	86	114/75	98.6°F	43	0.4	Valid
17	(16, 19)	72	122/78	98.4°F	38	0.36	Valid
18	(26, 7)	91	119/77	99.1°F	47	0.45	Valid
19	(8, 18)	73	126/82	98.9°F	41	0.4	Valid
20	(18, 5)	82	120/79	99.3°F	46	0.5	Valid

that selecting a node as a fog node may increase the data risk. Therefore, research in this area is interested in identifying nodes as FOG nodes.

4.7 CONCLUSION AND FUTURE WORK

IoT have a known application domain in today era i.e. IoMT to help out medical files. This reference work is subjected to the emerging technologies to transform IoT applications in healthcare and transition into more personalization using modern communication standards. An experimental framework using simulation of layered architecture on nodes and initialization of node using optimal parameter is given in Table 4.5. This table compares the work of traditional and fog computing and blockchain-based computation for securing communication. The blockchain fog computing-based proposed model for healthcare systems shows improvements and provides an energy-efficient, low latency, and scalable system as per the demands of today's era. Massive data sharing, security, privacy of data, and analysis of the network are again a challenge. This work also focuses on physical unclonable functions based on the identity generation of IoMT node and fog-enabled data transmission from the node. Data generated by IoMT devices can be more secure, authentic, and legitimate with decentralization.[23] It also describes the majority of these problems that a BC can fix. In future work, a research direction can be planned to cover security

TABLE 4.5
Comparison of IOMT with and without FC, an advancement using blockchain

Metric / Parameter	Traditional IoMT	Implementation of FC	Improvement (%)
Bandwidth Usage (MB/s)	13	3	77%
Cost Efficiency (%)	-----	Raised by 40%.	-----
Data Accuracy (%)	85%	92%	8.20%
Data Exposure Risk	Raised	Reduced	-----
Processing Latency Time (s)	8	3	62.50%
Security Rating	Moderate	Raised	-----
Energy Efficiency (%)	------	Raised by 30%.	-----
Interoperability	Limited	Protocols(standard)	-----
Data Transfer Latency (milliseconds)	300	50	83%
Real-Time Analytics (%)	Limited	Improved	-----
Regulatory Compliance (%)	Compliance challenges	Improved	-----

and privacy improvement in the fog computing domain. In future, node security will be the biggest agenda for any IoT application that must guarantee secure communication over public channel. Moreover, efficient use of available channels through new scheduling algorithms designs to help low latency, energy consumption, and other related issue in subsequent field.

REFERENCES

1. Prasanth, A., Lakshmi, D., Dhanaraj, R.K., Balusamy, B., & Sherimon, P.C. (Eds.). Cognitive Computing for Internet of Medical Things. CRC Press, 2022.
2. Dwivedi, R., Mehrotra, D., & Chandra, S. Potential of Internet of Medical Things (IoMT) applications in building a smart healthcare system: A systematic review. *J. Oral Biol. Craniofacial Res*. 2021, 12, 302–318.
3. Alam, S., Shuaib, M., Ahmad, S., Jayakody, D.N.K., Muthanna, A., Bharany, S., & Elgendy, I.A. Ghubaish -based solutions supporting reliable healthcare for fog computing and Internet of Medical Things (IoMT) integration. *Sustainability* 2022, 14(22), 15312. https://doi.org/10.3390/su142215312
4. Bikash, P., Bhattacharyya, S., & Pal, K. IoT-based applications in healthcare devices. *Journal of Healthcare Engineering*, 2021, 2021(1), 6632599. https://doi.org/10.1155/2021/6632599
5. Awaisi, K.S., Hussain, S., Ahmed, M., Khan, A.A., & Ahmed, G. Leveraging IoT and fog computing in healthcare systems. *IEEE Internet Things Mag*. 2020, 3, 52–56.
6. Aljabr, A. A., & Kumar, K. Design and implementation of Internet of Medical Things (IoMT) using artificial intelligent for mobile-healthcare. *Meas. Sens*. 2022, December, 24, 100499. https://doi.org/10.1016/j.measen.2022.100499
7. Meola, A. (n.d.). IoT Healthcare in 2023: Companies, medical devices, and use cases. Insider Intelligence. www.insiderintelligence.com/insights/iot-healthcare/

8. Da Xu, L., Lu, Y., & Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J*. 2021, 8, 10452–10473.
9. Explore 3 IoT trends in healthcare for 2021 | TechTarget. (n.d.). IoT Agenda. www.techtarget.com/iotagenda/feature/Explore-3-IoT-trends-in-healthcare
10. Kamarajugadda, K.K., Movva, P., Raju, M.N., Kant, S.A., & Thatavarti, S. IoMT with Cloud-Based Disease Diagnosis Healthcare Framework for Heart Disease Prediction Using Simulated Annealing with SVM. SpringerLink, 2021, February 2. https://doi.org/10.1007/978-3-030-52624-5_8
11. Tai, Y., Gao, B., Li, Q., Yu, Z., Zhu, C., & Chang, V. Trustworthy and intelligent COVID-19 diagnostic IoMT through XR and deep-learning-based clinic data access. *PubMed Central (PMC)*. 2021, February 1. https://doi.org/10.1109/JIOT.2021.3055804
12. Selvaraj, S., & Sundaravaradhan, S. Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Appl. Sci*. 2019, December 30, 2(1). https://doi.org/10.1007/s42452-019-1925-y
13. Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. Recent advances in the Internet-of-Medical-Things (IoMT) systems security. *IEEE Internet Things J*. 2021, June 1, 8(11), 8707–8718. https://doi.org/10.1109/jiot.2020.3045653.
14. Villegas-Ch, W., García-Ortiz, J., & Urbina-Camacho, I. Framework for a secure and sustainable internet of medical things, requirements, design challenges, and future trends. *MDPI*. 2023, May 30. https://doi.org/10.3390/app13116634
15. Yaacoub, J.P.A., Noura, M., Noura, H.N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst*. 2020, 105, 581–606.
16. Alsuhibany, S. A., Abdel-Khalek, S., Algarni, A., Fayomi, A., Gupta, D., Kumar, V., & Mansour, R. F. Ensemble of deep learning based clinical decision support system for chronic kidney disease diagnosis in medical internet of things environment. *Computational Intelligence and Neuroscience*, 2021, *2021*(1), 4931450. https://doi.org/10.1155/2021/4931450
17. Khan, I.A., Moustafa, N., Razzak, I., Tanveer, M., Pi, D., Pan, Y., & Ali, B.S. XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks. *Future Gener. Comput. Syst*. 2022, 127, 181–193.
18. Abdullah L, Quintero J. Sealed computation: a mechanism to support privacy-aware trustworthy cloud service. Information & Computer Security. 2019 Oct 23;27(5):601–20.
19. Rajesh, E., Basheer, S., Dhanaraj, R.K., Yadav, S., Kadry, S., Khan, M.A., ... & Cha, J.H. Machine learning for online automatic prediction of common disease attributes using never-ending image learner. *Diagnostics* 2022, 13(1), 95.
20. Singh, S.K., Rathore, S., & Park, J.H. BlockIoTIntelligence: A blockchain-enabled intelligent IoT architecture with artificial intelligence. *Future Gener. Comput. Syst*. 2020, 110, 721–743.
21. Srivastava, J., Routray, S., Ahmad, S., & Waris, M.M. Internet of medical things (IoMT)-based smart healthcare system: Trends and progress. *Comput. Intell. Neurosci*. 2022, 2022, 7218113.
22. Aslam, T., Maqbool, A., Akhtar, M., Mirza, A., Khan, M.A., Khan, W.Z., & Alam, S. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. *Comput. Mater. Contin.* 2021, 70, 1089–1108.
23. Dwivedi, A., Srivastava, G., Dhar, S., & Singh, R. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors* 2019, 19, 326.

5 Artificial Intelligence and Security Management in Digital Healthcare Using Fifth Generation Communications

A. Vinora, E. Lloyds, R. Nancy Deborah, G. Sivakarthi, and M. Soundarya

5.1 INTRODUCTION

A variety of Internet applications are used in the healthcare industry to offer customers, providers, and insurance companies instant access to information. Apps for electronic medical records (EMR), telemedicine services, internet pharmacies, and patient and health insurance websites are examples. In addition to healthcare-specific internet apps, clinics and hospitals confront cyber security risks connected to web-based email services, cloud storage services, dentists' computer-aided design (CAD) systems, hospital inventory management systems, and other relevant variables. Security enhancements and new technologies were made available to protect 5G-based intelligent healthcare networks (Abdul Ahad et al., 2023)[1].

When it comes to attacks on online healthcare apps, a web server is frequently the most susceptible piece of infrastructure for an organization. Vulnerabilities in a web application, web server, or related infrastructure can be exploited by an attacker using programs, data, or instructions. Administrators of healthcare online applications must adopt security measures such as online application firewalls (WAF), strong authentication, encryption, and vulnerability evaluation[2].

Reaping the benefits of 5G networks in healthcare environments requires careful consideration of network security and data privacy. Sophisticated IoT platform that runs on the cloud that can be customized for a healthcare data collection and monitoring system. The goal of the platform is to enhance remote patient monitoring and develop healthcare services. Data may be gathered from several sources, combined with a flexible semantic web, stored in the cloud for further analysis, and presented in an understandable way by the system. When creating a healthcare monitoring system that oversees Electronic Medical Records (EMRs), privacy concerns must be given top priority. The suggested solution makes use of common IoT features while efficiently protecting privacy (S. S. Vellela et al., 2023). Because adversaries may introduce new weaknesses, 5G technology may broaden the attack surface. Security experts are well

 DOI: 10.1201/9781032711379-5

aware of how 5G-based advancements in data exchange and storage, as well as the growing usage of IoT devices, will eventually increase the risk to data security. The increased usage of virtualization and the cloud, as well as the complexity of medical identity theft, intrusions of health privacy, and medical data management will result in a bigger, more diversified cyber-attack surface. The introduction of untrustworthy components into a 5G network increases the risk of a danger to 5G data's availability, confidentiality, and integrity as well as the potential for hostile or subpar hardware and software to infiltrate communications infrastructure.

5.1.1 5G

"5G" is considered as the most recent version of network mobility. Devices, machines, and people may all be connected via a new type of network called 5G. Thanks to 5G wireless technology, more users will experience greater peak internet speeds, enormous network capacity, improved availability, extremely low latency, more reliability, and a more constant user experience. Enhanced productivity and efficiency provide new user experiences and link new sectors (D. Manimegalai et al, 2023).

A digital signal is altered across many channels using orthogonal frequency-division multiplexing, or OFDM, to reduce interference. 5G makes use of OFDM concepts along with the 5G NR air interface. Sub-6 GHz and other greater bandwidth technologies are also utilized by 5G. The same mobile networking technology that powers 4G LTE also powers 5G OFDM. However, the next 5G NR air interface could improve OFDM much more by providing far greater scalability and flexibility. More people and objects may have 5G access as a result, serving a variety of use cases (B. Pradan et al., 2023)[3].

Aside from faster and more stable mobile broadband services than 4G LTE, 5G is expected to open up new service opportunities such as mission-critical communications and Internet of Things connectivity. A new self-contained TDD subframe design is a revolutionary 5G NR air interface design method (Ali M. Al Shahrani et al., 2022). 5G is often used for three types of linked services: enormous IoT, mission-critical communications, and improved mobile broadband. One of 5G's distinctive advantages is its ability to support forward compatibility while offering future services.

5.1.2 Improved Mobile Internet Access

In addition to enhancing our devices, 5G mobile technology might offer new immersive experiences like augmented reality and virtual reality described in Figure 5.1. It will also give reduced latency, quicker and more dependable data rates, and cheaper cost-per-bit (Lela Mirtskhulava et al., 2021).

5.1.3 Conversations that are Essential to the Mission

Thanks to its ultra-accessible, dependable, and latency-free connectivity, new services like remote control of cars, critical infrastructure, and medical procedures can be made possible by 5G which have the potential to drastically revolutionize industries[4].

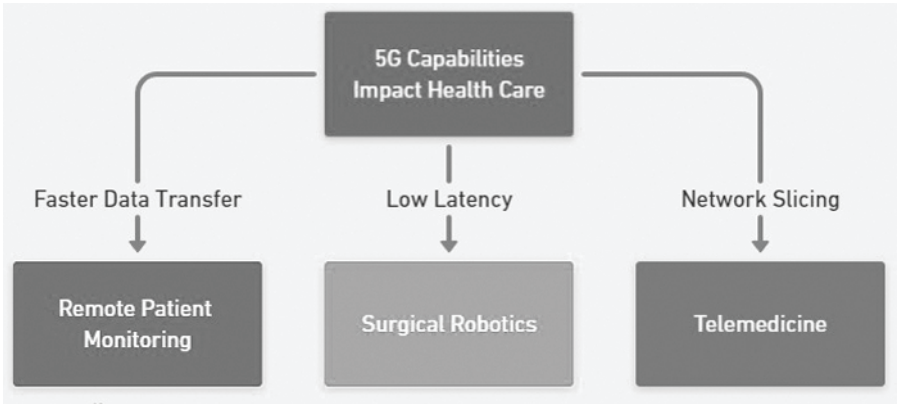

FIGURE 5.1 5G technology impact on healthcare.

5.1.4 Massive IoT

With 5G's capacity to reduce data rates, power consumption, and mobility, a vast array of embedded sensors in almost anything will be seamlessly connected, offering incredibly slim and affordable connection options. It is anticipated that the typical customer would use about 12 GB of data on their smartphone every month. The market for mobile apps has grown dramatically in many categories, such as food delivery, ride-sharing, movie streaming, and more.

The mobile ecosystem will reach new sectors thanks to 5G. Cutting-edge user experiences will be made possible by this, including instantaneous cloud access, local interactive content, new corporate apps, smooth Internet of Things capabilities, and limitless extreme reality (XR). 5G's fast data rates and dependable network will have a significant impact on businesses. Businesses will function more efficiently thanks to 5G's advantages, which will also provide faster access to more information for individuals. Certain organizations can fully utilize 5G capabilities, depending on the industry, especially those that require the high speed, low latency, and network capacity that 5G is expected to provide. For instance, industrial Ethernet may be run over 5G in smart factories, increasing output and operational accuracy[5].

5G might be especially efficient in sectors like virtual reality, entertainment, infrastructure, and automobile safety by providing higher data rates, reduced latency, and more communication between people and things. 5G might be used in smart cities in a number of ways to improve the quality of life for residents. There's more to 5G than just speed. By extending into new frequencies, 5G aims to provide even greater network capacity together with faster peak data rates. Not only may 5G provide much lower latency for faster replies but furthermore, a Gigabit LTE coverage base supports the upcoming 5G NR mobile network, offering widespread Gigabit-class access. With 5G, internet service could be completely transformed as wireless modems will be available in addition to the current wired ones. Compared to fiber, DSL, or cabled choices, 5G's coverage, performance, and deployment flexibility make it an attractive backhaul option now that Internet service providers (ISPs) may use its infrastructure to serve customers.

The full economic impact of 5G, according to our ground-breaking research of the 5G economy, is likely to be felt worldwide, helping a variety of industries and perhaps developing new markets for products and services. Compared to earlier network generations, this effect is significantly more pronounced. The automotive industry is among the sectors that are putting more and more pressure on traditional mobile networking companies to build the new 5G network. Many new and emerging applications will still require descriptions in the future. It is yet unclear what the "5G effect" might mean for the economy as a whole[6].

More than 60 countries have already deployed 5G. Customers are looking forward to the fast bandwidth and low latency. Nevertheless, 5G offers massive IoT, enhanced mobile broadband, and mission-critical applications that surpass these benefits. Although it is hard to say when everyone will have access to 5G, the technology is making a big splash in its first year of release. Three primary use cases for 5G's enhanced capabilities have been identified by the ITU-R (International Telecommunication Union's Radiocommunication Sector). These consist of Massive Machine Type Communications (mMTC), Ultra Reliable Low Latency Communications (URLLC), and Enhanced Mobile Broadband (eMBB). URLLC and mMTC won't be available in most places for a few years after eMBB is introduced in 2020. 5G is used for improved mobile broadband, or eMBB, and has faster connections, more capacity, and higher throughput than 4G LTE mobile broadband services. Cities and stadiums as well as music venues will benefit from 5G because of their higher traffic volumes.

It is possible to use the network for mission-critical applications that demand consistent and reliable data flow by utilizing "Ultra-Reliable Low-Latency Communications" (URLLC). To ensure that wireless communication networks meet their latency and reliability requirements, short-packet data transmission is used. To connect to a lot of devices, Massive Machine-Type Communications (mMTC) would be utilized. A portion of the 50 billion IoT devices will be connected via 5G technology. The majority of users will make use of the lower priced Wi-Fi. By giving emergency responders up-to-date information, drones operating over 4G or 5G networks will support disaster relief efforts. For a variety of services, the majority of cars will have a 4G or 5G cellular connection, because autonomous vehicles must be able to function in locations without a network connection. Most autonomous vehicles do, however, also use tele-operations to complete tasks, and 5G technology is very useful in these situations[7].

5.2 5G IN HEALTHCARE

In the healthcare sector, medical data management, 5G will enable remote surgery, remote monitoring, and real-time medical imaging. An emerging trend in the healthcare industry is IoT. Rather than consulting documents to obtain patient data, physicians can more efficiently obtain the patient's entire medical history by using the Internet. This expedites the process of prescribing medication and, as a result, enhances the standard of care provided to the patient (D. A. Gandhi et al., 2018). By applying these strategies, doctors will be able to eliminate guesswork, diagnose patients more rapidly and precisely, and get a deeper understanding of their patients'

circumstances. Digital innovations like Tele-health's continuous advancement, Fifth-generation wireless networks (5G), deep learning and machine learning, big data (BD) and supercomputing, blockchain technology, and other digital security tools have made it possible to create an integrated ecosystem that will open up new opportunities in the healthcare and other industries. The hospital-centric, specialty-focused healthcare paradigm is quickly giving way to a scattered, patient-centric one (Abdul Ahad et al., 2023). 5G networks have considerably reduced latency—less than 70 milliseconds—than the 4G network. Furthermore, because 5G uses higher-frequency millimeter waves than current networks, its data transfer speed is about 100 times faster than 4G's current 10 megabits per second[8].

The introduction of 5G has caused a shift in the healthcare sector, making it more data-driven and less of a system for treating patients. When it comes to healthcare, patient apps—especially those used outside of traditional medical facilities—offer 5G operators the most potential. Some of the few use examples include the rise in online consultations, remote surgery, health monitoring, telemedicine, and related applications. Doctors and family members will be able to ascertain if patients are receiving their prescribed therapy on time with the use of the Real Time Clock (RTC), sensors, and RFID tags that are connected to the Raspberry Pi. An SMS will be sent to the patient's corresponding doctors and family members if any odd behaviour is noticed (S. Lavanya et al., 2017). It is believed that 5G healthcare models would make healthcare more customer-focused and emphasize offering services and care to patients at affordable costs, putting consumers at the center of an ecosystem in which they are impacted directly by all stakeholders. In addition, it will cause a paradigm change in the way that people think about healthcare. Fifth-generation wireless networks (5G), an integrated ecosystem that will offer new opportunities in the healthcare and other industries has been made feasible by deep learning and machine learning, big data (BD) and supercomputing, blockchain technology, and other digital security technologies. Data mining methods, such as clustering, to data that is taken from global healthcare databases and put into a big data platform will analyze healthcare data efficiently (P. Dhaka et al., 2016). The main weaknesses in the healthcare system examined the benefits of integrating 5G, blockchain, and related technologies with the healthcare system, and assessed the capabilities and advantages of each (K. Khujamatov et al., 2020).

With the deployment of 5G, the healthcare industry will have access to real-time medical imaging, remote surgery, remote monitoring, and medical data management. Information accessed from the remote database should be highly secure and accessible only to those who are authorized. An Elliptical Curve Cryptography (ECC)-based Pervasive Mobile Healthcare system is proposed that integrates access control and authentication, to tackle these issues and enable users to access multimedia medical records securely and at any time. The categories of users who are permitted to use the program are made possible via authentication. Data encryption and decryption processes provide security (G. Sudha et al, 2013). Usage of technological advancements by physicians aid in diagnosing patients more quickly and accurately, remove guessing, and better visualize their patients' situations. Both patient applications and innovation will benefit from 5G. Therefore, the main focus of innovation will be on achieving goals that were previously unattainable due to data

restrictions. Due to their inherent agility, startups are aware of emerging trends in the market. They therefore stand for innovation speed. This is only feasible for startups, as larger businesses frequently have longer strategy planning cycles. Hence, it would take them two or three quarters to determine whether to proceed, compared to the five days it will take startups to develop a solution.

The global pandemic has brought to light the shortcomings in our current healthcare system. There has been a sharp rise in the number of Covid-19 patients in emergency rooms and critical care units across the country. Appointments for elective and other less urgent procedures are being canceled by prospective patients, which is costing other practice areas money or leaving other spaces empty[9].

Providing everyone with affordable, high-quality healthcare is the aim of the new ecosystem. By facilitating telemedicine, improving data interchange between patients, care givers, and insurers in the healthcare insurance market and allowing always-on device connection, 5G will raise the standard for connected healthcare. Furthermore, 5G concentrates on its potential to meet the demands for senior care, assisted living, smart hospitals, etc. in the healthcare industry (B. Dzogovic et al., 2020). More precise data on life and health insurance will result in lower premiums and enable a proactive, customized health insurance with an anticipatory approach that encourages customers to lead healthier lives. This is made possible by increased data availability.

5.3 MAKING THE MOST OF THE PHARMACEUTICAL SECTOR

A pharmaceutical company finds, makes, and distributes medications. Pharma companies are already using 5G to ship their goods worldwide to the healthcare sector. The pharmaceutical industry is heavily controlled. which is not surprising considering the high standards of quality and patient safety. This is one more factor that motivates industry standards and SOPs (Standard Operating Procedures). But the current pharmaceutical IT infrastructures—some of which are still in use today—cannot keep up with the needs of the modern pharmaceutical industry. With the help of 5G standardization, an international establishing networking infrastructure is necessary for better industrial internet and Internet of Things (IoT) services. It may be used as the foundation for the implementation of fully digitalized pharmaceutical solutions. Furthermore, it is projected that AI will become more important in R&D, particularly in the biological sciences, as it continues to advance. 5G will encourage tech and pharmaceutical businesses to improve their Research and Development[10].

5.3.1 Transform Product Distribution

Healthcare delivery has never been the only aspect of its dissemination. It is necessary to administer medicines to patients in a safe and efficient manner at the appropriate times. It's handled by the logistics experts. 5G, in conjunction with pharmaceutical products, may be tracked and authenticated as they are moved through the supply chain with the use of edge computing and blockchain technology. A 5G-powered blockchain-based supply network for the pharmaceutical business includes features like contracts, encrypted communication channels, and integrated security checks at every stage of the chain of custody.

5.4 ROLE OF GOVERNMENT/POLICY MAKERS

To reach its full potential, the 5G sector needs the government to provide secure services. Given that it is anticipated that sensors and other gadgets would be able to converse and decide for themselves without the assistance of a human, 5G security is essential. The government has to allow access to radio spectrum that is currently set aside for other purposes, like satellite systems and radar. Finding the factors that affect the healthcare sector's service quality and creating a model of service quality appropriate for India are essential priorities (G. N. Akhade et al., 2013). Generally speaking, governments will have to take over businesses and government agencies due to the disruption that 5G will cause. Artificial and augmented intelligence applications will be made possible by 5G; however, rules separating computer and human decision-making will be required, particularly in the healthcare industry. 5G might bring about a revolution in some healthcare services. For example, by remotely analyzing vital signals collected by body-worn equipment, it might be able to identify serious diseases at an early stage[11].

5.4.1 Energy Efficiency

The high speed and capacity of 5G allows for the almost immediate transmission of medical data, including prescriptions, test results, imaging, and other data. It can also facilitate excellent video interactions. The expansion of functionality happens concurrently with a decrease in the energy consumption of all linked devices due to 5G's reduced power needs. Multiple "base stations" are necessary because 5G requires higher frequencies for broadcasting, which exacerbates the problem of signal degradation are described in Figure 5.2.

5.4.2 Cyber Attacks and Data Security

The goal is to become digital. It makes it vulnerable to cyberattacks, where two things can occur: data security for all data comes first. The patient's private information and

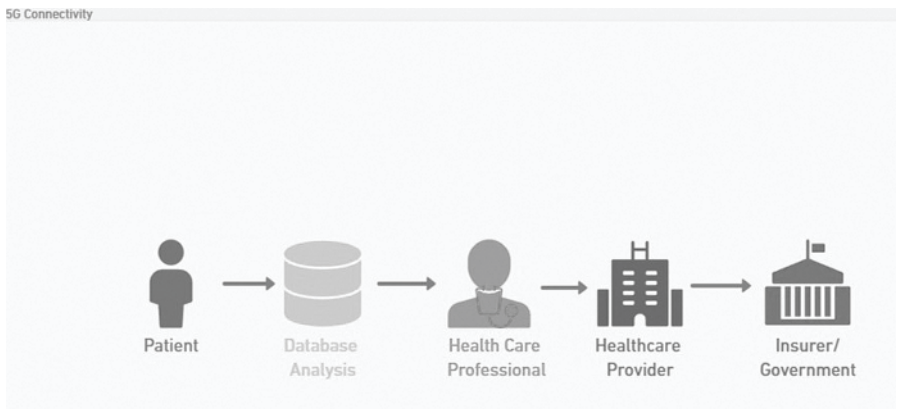

FIGURE 5.2 Process to acquire data and security to be framed by Government at the end.

privacy come in second and are far more crucial. Although there is no direct correlation between cyberattacks and 5G, there are many indirect ones because of the emergence of new solutions and the influx of individuals who were not previously in the healthcare system. They must thus understand healthcare regulations.

5.5 5G HEALTHCARE APPLICATIONS

Ten 5G applications in healthcare:

1. Patient monitoring from a distance
2. Linked ambulance
3. Virtual consultations
4. Video assists in the administration of prescriptions
5. AR/VR support for the visually impaired
6. Rehabilitation therapy and diversion
7. A remote specialist to assist with surgical teamwork
8. Instruction and training in AR/VR
9. High-throughput, real-time computer processing
10. Using video analytics to identify patterns in behavior[12]

5.5.1 5G-capable Remote Medical Services

1. Linked ambulance
The connected ambulances might assist emergency services in fulfilling ever-tougher goals and enhance patient outcomes in general. During the patient's transportation, through the use of wearables, sensors, streaming HD video, or body cameras, an ambulance that is connected to the hospital's A&E department may collect and transmit patient data. Patients are better known to hospital workers before they arrive. To improve efficiency across the emergency services, experts might occasionally be called upon to assist paramedics with certain operations or diagnostic evaluations without requiring them to visit the hospital.

Unlike other use cases, 5G technology is required for the implementation of linked ambulances. This is because:

- 5G may result in lower latency. Video and data must be transmitted instantly to the hospital and physicians since in an emergency, a moment's decision can have a big impact.
- 5G has a large bandwidth, live footage from emergency responder body cameras in the field may be streamed without compromising on quality or buffering.
- 5G's enhanced security and reliability

5.5.2 Virtual Consultations

For preliminary screening assessments, regular examinations (which don't include physical procedures), counseling or rehabilitation sessions, and a growing number of visual evaluations (like recognizing symptoms and conditions associated with

dermatology), two-way HD video is utilized to help patients and primary or secondary care providers communicate. Through remote scheduling, patients may visit medical specialists without having to travel, which lessens both the financial load and time commitment for the patient.
Compared to previous connection options, 5G promises to provide two-way virtual consultations at scale by providing the following benefits:

- Greater bandwidth compared to current cellular connectivity, which will enable the field to provide the required, reliable quality of service.
- Enhanced dependability and 5G security.

5.5.3 Patient Monitoring via Remote Access

It is believed that proactive and more efficient delivery of healthcare services, along with the treatment of chronic illnesses, can both benefit greatly from remote patient monitoring. Patients can gather and analyze patient characteristics using sensors, wearables, and e-health devices without having to visit primary care facilities or see medical professionals in person.

5G claims to offer the following benefits over previous connection alternatives: more mobility in comparison to in-home connectivity options like increased service security and dependability; and Wi-Fi. Large-scale remote patient monitoring will be made feasible by these advantages.

5.5.4 Medication Adherence with Video Assistance

In the healthcare business, patients' failure to follow prescribed regimens is a major difficulty, as evidenced by the fact that some elderly or mentally ill patients forget to take their medication on time. 5G can help address this problem by introducing video-enabled medication adherence, which puts qualified chemists and care givers in direct video connection with patients, guaranteeing that the right dosage and precipitation are taken at the appropriate time decribed in Figure 5.3.

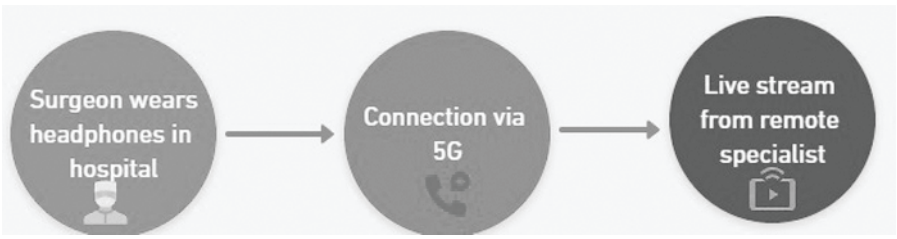

FIGURE 5.3 Methodology adopted in remote monitoring.

Video-enabled medicine adherence will be made possible at scale by 5G due to its:

- Greater bandwidth that allows real-time, high-quality video streaming
- SIM-based technology installation that is simpler than with other alternatives (e.g., Bluetooth/Wi-Fi)

5.5.5 5G is More Dependable and Secure than 4G

Futuristic communication technologies are helping blind people with augmented and virtual reality. Activities like crossing the street, reading a webpage, going inside a building, etc., that a person with normal vision might take for granted., can be challenging for someone with poor, impaired, or no vision. Those with visual impairments can use a pair of video streaming glasses or an AR/VR headset with 5G support to connect in the moment to a live adviser who can help them with certain daily tasks. A company by the name of Aira hopes to offer this sort of service to its customers. Because of the following, 5G will widely assist the blind and visually impaired with AR and VR:

- More bandwidth to enable the transmission of better-quality video to the guide.
- Low latency makes real-time data transmiision for improving quality of service. It is possible to transmit video to the guide, which is important in circumstances like crossing the street. Furthermore, jitter and lag in AR/VR headsets can cause motion sickness in users, therefore minimal latency is necessary for a positive user experience.

5.6 SECURITY PROBLEMS ENCOUNTERED IN 5G HEALTH APPLICATIONS

Threats are attempts to gain unauthorized access to data, resources, and services, as well as to cause data loss and damage to information systems.

5.6.1 Authentication

Since authentication makes it possible to verify user identities within the network, it is an essential part of the security of 5G-based smart healthcare networks. The smart healthcare network powered by 5G employs many techniques for data authentication. Its two components are authentication, primary and secondary. In both 5G and 4G networks, initial identification permits reciprocating confirmation between medical devices and networks. However, there are several problems with the primary authentication of 5G-based networks, such as knowledge control and inadequate support for the call of device authentication. To get above these obstacles, adaptable authentication methods and Authentication Protocol Privacy (5G-AKA) are employed. Technologies that are compatible with primary authentication include those outside of the Third Generation Partnership Project (3GPP).

5.6.2 Confidentiality

Confidentiality is one facet of security. Thanks to secrecy, the sender's information is only accessible to those who have authorization. The master base node (MeNB) produces and delivers the key needed by the secondary next-generation base node (SgNB) before each secure new radio (NR) transmission; the user likewise generates and transmits the same key. Radio resource control (RRC) can be achieved by signal exchange between user equipment (UE) and the secondary next-generation base node (SgNB). As a result, the keys both secure and ensure the validity of the user plane (UP) data and RRC conversations. 5G networks cannot be built, even if they incorporate integrity protection for UP data. The use of secrecy is supported by both UP and RRC.

Accessible Cloud resources are advantageous for the smart healthcare network powered by 5G, as they aid in the development of economic infrastructure. Nonetheless, security risks such as cyberattacks jeopardize the network's dependability. DDoS assaults impact network-slicing procedures because they demand logical and physical resources at the edge and cloud levels. Users of radio access facilities are unable to access cellular services due to jamming attempts. Attacks on 5G radio, control plane, and support system might bring down the smart health network.

5.6.3 Non-repudiation

The capacity to demonstrate the authenticity and legitimacy of a message or transaction and to keep the sender from withdrawing from the exchange is known as non-repudiation. User deniability cannot be prevented only by authentication. But in order to allow safe data transfer, discriminating between different users, or UEs, authentication is necessary to guarantee non-repudiation. Digital signatures can be used by 5G networks to guarantee non-repudiation. A unique code added to a communication by a digital signature can be used to confirm its authenticity and integrity. They employ cryptography to do this. As a result, the sender finds it difficult to withdraw from the connection.

5.6.4 Integrity

User plane integrity protection between Internet of Things (IoT) devices and next-generation node B (gNB) is one security feature of the 5G network. It works with the encryption that both gNB and IoT devices use. The implementation of resource-intensive functionality, such as integrity protection at high data rates, is constrained in IoT devices. A 5G-based smart healthcare network's architecture must include network integrity mechanisms. For example, 5G networks may utilize cryptographic methods such as the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA) to create a unique code that is appended to the data and may be utilized to verify the data's integrity. This ensures that the data was not altered during transmission.[13]

5.7 SECURITY MEASURES ADOPTED IN THE HEALTH SECTOR

This section will discuss a number of cutting-edge technologies used in smart healthcare through 5G. These technologies are divided into various groups. Thus, subcategories of 5G security for intelligent healthcare-related technological issues and state-of-the-art technologies are:

5.7.1 Blockchain in terms of 5G Security in Smart Healthcare

The term "blockchain" refers to novel and revolutionary technologies that allow for decentralized, secure identification and information administration and recording among many parties. It is seen as a watershed moment for smart healthcare networks powered by 5G. Blockchain is a distributed storage technique that operates on a peer-to-peer basis, maintaining chains of linked transaction blocks. Its dispersion, decentralization, and other characteristics improve the security of the smart healthcare network powered by 5G. A wide range of applications, including supply chain management, intelligent transportation, smart finance, and autonomous automobiles, are ideal for it because of its decentralized and distributed nature. Blockchain technology and 5G might greatly increase the financial benefit of data sharing. The ability of blockchain technology to provide 5G coverage has enabled the widespread deployment of IoT devices for smart healthcare by reducing latency and increasing speed and capacity. These devices may employ blockchain technologies' consensus arbitration, integrity, security, and decentralization as a support layer at the same time. The majority of IoT agreements and activities take place at the network layer, even if blockchain technology may provide security and secrecy. However, problems may be resolved on the chain.

Blockchain technology will almost certainly benefit from the deployment of 5G, which will accelerate block times, improve on-chain scalability, encourage node participation and decentralization, and allow the Internet of Things to offer intelligent healthcare. Multiple parties can securely send, receive, and view data thanks to the blockchain. The necessary data is shared by each member in a distributed ledger using blockchain technology. Thus, blockchain technology enhances 5G-based network security. Blockchain offers a safe alternative for data access in transportation applications, providing access to passenger record data for a number of systems that are essential to bus transportation stakeholders (patients in an ambulance, for example)[14].

Because it creates and transmits a legitimate SIP INVITE message to the destination component SIP, it is also related to the DoS attack. It may generate spoof IP addresses in three different ways: manually, randomly, or by choosing the spoof address from the subnet. It is possible to create IP addresses precisely or randomly, which are made up of numerous APs. The local service center (LSC) is in charge of overseeing the AP clusters. In the context of 5G, UE uses blockchain technology to offer dependable and secure access.

5.7.2 5G Security with Artificial Intelligence

AI is a key component of 5G-based network security as it makes it possible to run a system that can spot anomalies and forecast future events. 5G networks may be proactive and predictive in delivering reliable, effective services thanks to algorithms built on machine learning and deep learning. Artificial intelligence (AI)-based algorithms efficiently provide high-quality experiences (QoE), which helps to realize the various demands of 5G technology. By analyzing historical and contemporary patterns, artificial intelligence can be used to detect and identify a range of fraudulent activities, such as MITM attacks, radio jamming assaults, and other damaging deeds, in order to stop them from happening again[15].

5.8 CONCLUSION

5G could lessen the quantity of data that needs to be manually sorted by medical personnel and the number of sensors needed for data collection. However, healthcare data needs to be treated carefully since it is sensitive and security measures are a major concern. Combining edge computing with federated learning is one workable way to ensure the safety and privacy of ML models. This might include developing machine learning-based security solutions that preserve patient privacy while learning from data gathered from several edge devices.

Furthermore, employing explainable AI approaches could produce a security decision-making process that is more transparent and trustworthy. Smart healthcare systems enabled by 5G present significant security challenges and issues. To comprehend the security requirements of such systems, it is essential to diminish these concerns and hazards. Smart healthcare devices are not able to satisfy every security requirement of 5G-enabled smart healthcare because of their high cost, single point of failure, resource constraints, limited scalability, and standard security protocols. A new age in healthcare security and privacy has just been ushered in by several technologies, including blockchain and artificial intelligence. The main enabling technologies and architecture for 5G smart healthcare are presented in this chapter. The technological components of 5G smart healthcare security are availability, confidentiality, integrity, and non-repudiation. We also discussed a number of security issues and possible solutions that the 5G smart healthcare link brings. Lastly, young researchers are given access to open issues and prospective research areas.

REFERENCES

1. A. Ahad, Z. Ali, A. Mateen, M. Tahir, A. Hannan, N. M. Garcia, and I. M. Pires, “A Comprehensive review on 5G-based Smart Healthcare Network Security: Taxonomy, Issues, Solutions and Future research directions,” *Array*, vol. 18, 100290 pages, 2023. ISSN25900056, doi: 10.1016/j.array.2023.100290.
2. S. S. Vellela, V. L. Reddy, D. Roja, G. R. Rao, K. B. Sk and K. K. Kumar, “A Cloud-Based Smart IoT Platform for Personalized Healthcare Data Gathering

and Monitoring System," *2023 3rd Asian Conference on Innovation in Technology (ASIANCON), Ravet IN, India*, 2023, pp. 1–5, doi: 10.1109/ASIANCON58793.2023.10270407.

3. D. Manimegalai and M. Karthikeyan, "Exploring the Impact of 5G and the Promise of 6G: Transforming Healthcare Strategies and Technology," *2023 International Conference on Research Methodologies in Knowledge Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), Chennai, India,* 2023, pp. 1–8, doi: 10.1109/RMKMATE59243.2023.10368780.
4. B. Pradhan, S. Das, D. S. Roy, S. Routray, F. Benedetto and R. H. Jhaveri, "An AI-Assisted Smart Healthcare System Using 5G Communication," *IEEE Access*, vol. 11, 108339–108355 pages, 2023, doi: 10.1109/ACCESS.2023.3317174.
5. A. M. Al Shahrani, A. Rizwan, M. Sánchez-Chero, C. E. Rosas-Prado, E. B. Salazar, and N. A. Awad, "An Internet of Things (IoT)-Based Optimization to Enhance Security in Healthcare Applications," *Mathematical Problems in Engineering*, vol. 2022, Article ID 6802967, 11 pages, 2022, doi: 10.1155/2022/6802967.
6. L. Mirtskhulava, M. Iavich, M. Razmadze and N. Gulua, "Securing Medical Data in 5G and 6G via Multichain Blockchain Technology using Post-Quantum Signatures," *2021 IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo)*, Odesa, Ukraine, 2021, pp. 72–75, doi: 10.1109/UkrMiCo52950.2021.9716595.
7. K. Khujamatov, E. Reypnazarov, N. Akhmedov and D. Khasanov, "Blockchain for 5G Healthcare architecture," *2020 International Conference on Information Science and Communications Technologies (ICISCT)*, Tashkent, Uzbekistan, 2020, pp. 1–5, doi: 10.1109/ICISCT50599.2020.9351398.
8. B. Dzogovic, V. T. Do, B. Santos, N. Jacot, B. Feng and T. V. Do, "Secure Healthcare: 5G-enabled Network Slicing for Elderly Care," *2020 5th International Conference on Computer and Communication Systems (ICCCS)*, Shanghai, China, 2020, pp. 864–868, doi: 10.1109/ICCCS49078.2020.9118583.
9. M. F. Raji, J. Li, A. U. Haq, V. Ejianya, J. Khan, A. Khan, M. Khalil, A. Ali, G. A. Khan, M. Shahid, B. Ahamad, A. Yadav and I. Memon, "A New Approach for Enhancing the Services of the 5G Mobile Network and IOT-Related Communication Devices Using Wavelet-OFDM and Its Applications in Healthcare", *Scientific Programming*, vol. 2020, Article ID 3204695, 13 pages, 2020, doi: 10.1155/2020/3204695.
10. Q. Qiu, S. Liu, S. Xu, S. Yu, "Study on Security and Privacy in 5G-Enabled Applications", *Wireless Communications and Mobile Computing*, vol. 2020, Article ID 8856683, 15 pages, 2020, doi: 10.1155/2020/885668.
11. D. A. Gandhi and M. Ghosal, "Intelligent Healthcare Using IoT:A Extensive Survey," *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, 2018, pp. 800–802, doi: 10.1109/ICICCT.2018.8473026.
12. S. Lavanya, G. Lavanya and J. Divyabharathi, "Remote prescription and I-Home healthcare based on IoT," *2017 International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT)*, Coimbatore, India, 2017, pp. 1–3, doi: 10.1109/IGEHT.2017.8094069.
13. P. Dhaka and R. Johari, "HCAB: HealthCare analysis and data archival using big data tool," *2016 1st India International Conference on Information Processing (IICIP),* Delhi, India, 2016, pp. 1–6, doi: 10.1109/IICIP.2016.7975353.

14. G. N. Akhade, S. B. Jaju and R. R. Lakhe, "A Review on Healthcare Service Quality Dimensions," *2013 6th International Conference on Emerging Trends in Engineering and Technology*, Nagpur, India, 2013, pp. 126–127, doi: 10.1109/ICETET.2013.38.
15. G. Sudha and R. Ganesan, "Secure transmission medical data for pervasive healthcare system using android," *2013 International Conference on Communication and Signal Processing*, Melmaruvathur, India, 2013, pp. 433–436, doi: 10.1109/iccsp.2013.6577090.

6 Synergizing Cybersecurity and Neuro-imaging Biomarkers

Innovations in Deep Learning for Diagnosis and Progression Monitoring

M. Manimaran, D. Sridhar, K. B. Manikandan, S. Devaraju, and K. Thirumalai Raja

6.1 INTRODUCTION

In this computer era, cybersecurity plays a vital role for individuals, organizations, and governments globally. Many techniques were improved to exploit vulnerabilities in the digital era. For strengthening the biomedical field in the digital era, cybersecurity, deep learning and neuro-imaging biomarkers play a vital role in providing useful information to clear abnormalities in brain activity or communications systems. Magnetic resonance imaging (MRI) and Positron emission tomography (PET) will provide useful information on brain structure and functions in neuro-imaging biomarkers[1].

6.1.1 Prevalence and Impact

The World Health Organization (WHO) reported that an estimated 50 million people have dementia around the world with AD accounting for 65–75% of cases. Globally, Alzheimer's disease affects tens of millions of individuals, with incidence rates regularly increasing around age 35–45. Among older adults, it was the most common form of dementia and contributed considerably to incapacity and dependency. By 2050, the number of people with dementia is projected to triple, posing a massive burden on healthcare structures and society as a whole.

DOI: 10.1201/9781032711379-6

6.1.2 Challenges in Diagnosis and Monitoring

Accurate diagnosis of Alzheimer's disease at an early stage is in great demand. Current diagnostic strategies generally rely on clinical assessment, cognitive testing, and the exclusion of various capability motives for cognitive impairment. However, these strategies have limitations, particularly in distinguishing AD from different types of dementia and detecting sickness in its early stages, even when interventions may be more effective at that point.

The fundamental project in AD prognosis is the dearth of reliable biomarkers for detecting underlying pathological changes inside the mind. The current diagnostic requirements depend on scientific signs and symptoms, which can also be simple and emerge as evident in the later stages of the disease. Furthermore, tracking the disorder's development over the years is difficult because of the subjective nature of cognitive tests and the shortage of goal measures for monitoring changes in thought structure and features.

6.1.3 Role of Neuro-imaging Biomarkers and Deep Learning

Neuro-imaging is a promising method for enhancing AD analysis and monitoring. Neuro-imaging biomarkers provide valuable insights into sickness pathology and progression by visualizing the structural and practical changes within thoughts. Structural neuro-imaging techniques, such as computed tomography (CT) and magnetic resonance imaging (MRI), permit the visualization of brain atrophy and structural adjustments associated with AD. Functional neuro-imaging includes the findings of MRI (fMRI) and positron emission tomography (PET), which allows the assessment of metabolic and practical changes inside the brain.

6.2 NEURO-IMAGING BIOMARKERS IN ALZHEIMER'S DISEASE

Neuro-imaging techniques are a physiological change associated with Alzheimer's disease (AD) and their harmful effects on the cognitive spectrum. In this topic, several neuro-imaging biomarkers were used in AD research and scientific practice, which emphasized their importance in factual disease processing and various results.

6.2.1 Structural Neuro-imaging Techniques

One of the most important structural neuro-imaging techniques is a brain morphology which includes computed tomography (CT) and magnetic resonance imaging (MRI). MRI provides a high-resolution image which allows visualization of cognitive processes affected by AD. The areas found to undergo significant atrophy in AD were the hippocampus, entorhinal cortex, and cortex. In detecting cortical atrophy and ventricular growth, Computed Tomography (CT) scans were helpful and also a valuable estimation of the systemic modification of theories related to AD was provided[2] described in Figure 6.1 and Figure 6.2.

The hippocampal volume can be quantified using volumetric assessment strategies, including ROI assessment or voxel-based morphometry (VBM) techniques described in Figure 6.3.

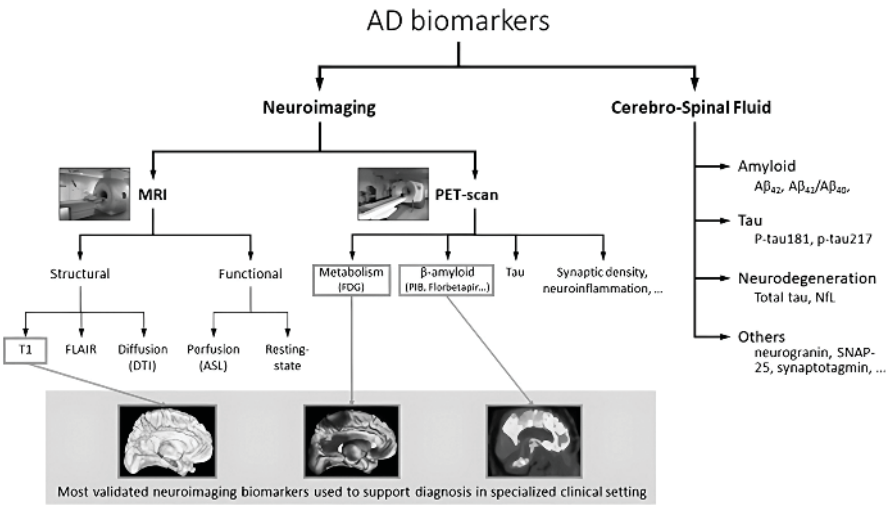

FIGURE 6.1 Neuro-Imaging Biomarkers in the diagnosis Framework.

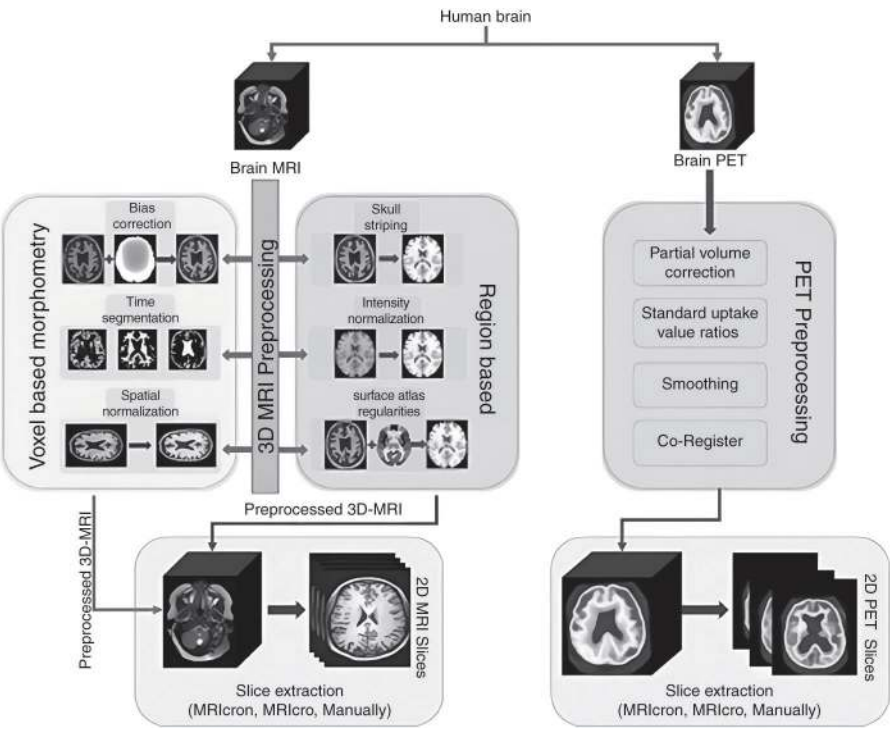

FIGURE 6.2 Neuro-imaging in Alzheimer's Disorder.

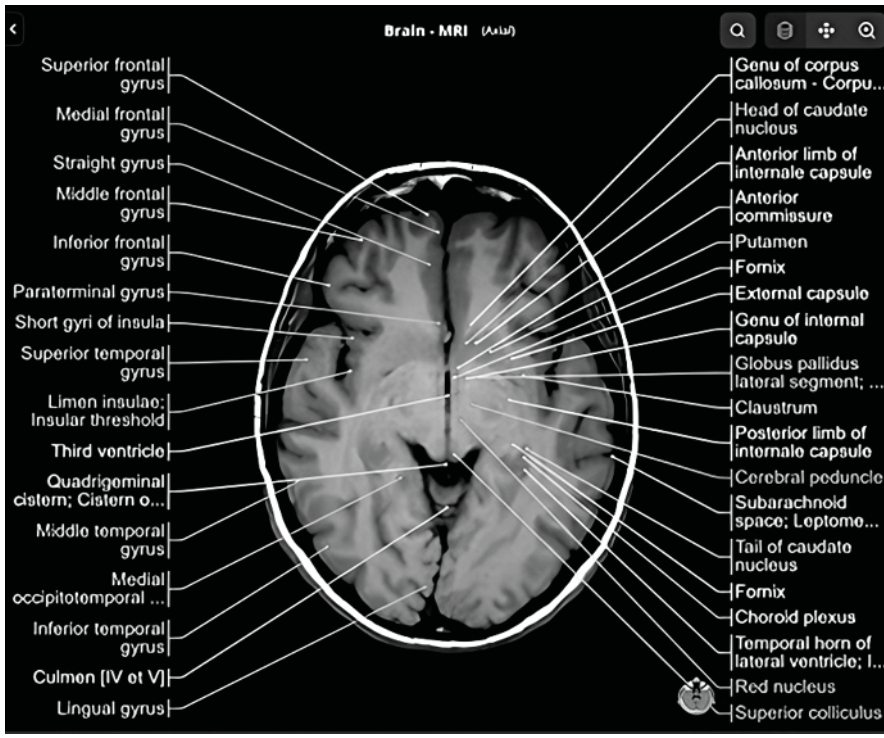

FIGURE 6.3 Example used of an MRI scan showing brain structures.

Calculating VBM is:

$$V = \sum_{i=1}^{n} T_{i\,x}\,\mathrm{A}i \tag{1}$$

- V = Total hippocampal volume
- Ai = Area of the ith hippocampal slice
- Ti = Thickness of the ith hippocampal slice

Although CT has a lower spatial detection than MRI, it remains a useful tool in medical settings for assessing mental anatomy and detecting structural abnormalities related to AD.

6.2.2 Functional Neuro-imaging Techniques

Functional neuro-imaging techniques, including magnetic resonance imaging (fMRI) and positron emission tomography (PET), offer insights into metabolic and practical alterations in the mind related to AD pathology.

PET imaging enables the visualization of metabolic techniques by detecting the uptake of radiolabelled tracers, including fluorodeoxyglucose (FDG), which measures glucose metabolism. In AD, PET research has continually proven hypometabolism in specific brain regions, including the posterior cingulate cortex, praecuneus, and temporoparietal regions, reflecting neuronal disorders and synaptic loss.

FMRI is used to degree adjustments in blood float and oxygen ranges in the brain, and gives statistics about neural activity and useful connectivity networks. Resting-state fMRI studies have revealed disruptions in useful connectivity networks in patients with AD, characterized by reduced connectivity inside the community that uses the default mode (DMN) and elevated connectivity in regions related to executive manipulation and interest.

Functional neuro-imaging techniques such as functional magnetic resonance imaging (fMRI) and positron emission tomography (PET) provide insights into metabolic and functional alterations within the mind associated with AD pathology.

PET imaging allows the visualization of metabolic processes inside the brain by detecting the uptake of radio labelled tracers, including fluorodeoxyglucose (FDG). Hypometabolism in unique mind regions, including the posterior cingulated cortex and temporoparietal areas described in Figure 6.4, is normally discovered in equation[3].

The components for calculating the local cerebral metabolic rate of glucose (rCMRglc) and the use of PET imaging were as follows:

$$rCMRglc = \frac{K_1 x \mathrm{C}}{K_2} \tag{2}$$

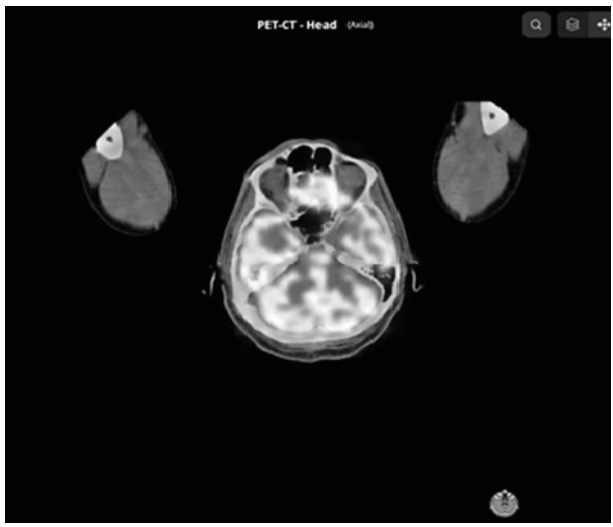

FIGURE 6.4 Example of a PET scan showing glucose metabolism.

Where:

- K_1 = Forward rate constant
- C = Concentration of FDG
- K_2 = Backward rate constant

fMRI provides information on cerebral activity by measuring variations in the blood float, oxygenation levels in the brain, and functional connectivity networks. Resting-country fMRI studies have found disruptions in functional connectivity networks in patients with AD, characterized by reduced connectivity inside the community that uses the default mode (DMN) and multiplied connectivity in areas related to executive control and attention.

6.2.3 Key Neuro-imaging Biomarkers

Several key neuro-imaging biomarkers are normally utilized in AD studies and clinical exercises to aid in the analysis and monitoring of ailment development. These biomarkers consist of measures of structural integrity (e.g., hippocampal quantity and cortical thickness), functional alterations (e.g., hypometabolism on PET and aberrant practical connectivity on fMRI), and the presence of amyloid and tau pathology (e.g., amyloid PET imaging and tau PET imaging).

Biomarkers applied in diagnosing and tracking Alzheimer's disease (AD) encompass various measures that capture structural integrity, practical alterations, and the presence of pathological hallmarks, such as amyloid and tau deposition. We delved into each category and provided comparisons where relevant.

fMRI provides information on cerebral activity by measuring variations in blood flow, oxygenation levels in the brain, and functional connectivity networks. Resting-state fMRI studies have revealed disruptions in functional connectivity networks in patients with AD, characterized by decreased connectivity within the network that uses the default mode (DMN) and increased connectivity in regions associated with executive control and attention.

6.2.3.1 Structural Biomarkers

- *Hippocampal Volume:* Structural MRI is generally used to evaluate hippocampal quantity, which is a key biomarker for AD pathology. Reduced hippocampal volume is indicative of neuro degeneration and associated with memory impairment in AD. Comparison: Studies frequently compare hippocampal quantity between patients with AD and healthy controls, in addition to across sickness degrees, to track progression.
- *Cortical Thickness:* MRI-based total measurements of cortical thickness provide insight into cortical atrophy, another hallmark of AD. Reductions in cortical thickness, mainly in areas vulnerable to AD pathology (e.g., entorhinal cortex and temporal lobes), are found in patients with AD compared to controls. Comparison: Cortical thickness measurements can be compared domestically or globally to examine sufferers with AD and wholesome human beings to assess changes introduced by infection.

6.2.3.2 Functional Biomarkers

- *Hypometabolism* on positron emission tomography (PET) imaging with a glucose analogy such as fluorodeoxyglucose (FDG) allows for the assessment of cerebral glucose metabolism. Hypometabolism in specific brain areas, mainly the temporoparietal and posterior cingulated cortices, is a characteristic feature of AD. Comparison: FDG-PET scans may be compared among AD patients with AD and controls to identify the metabolic abnormalities associated with the ailment.
- *Aberrant Functional Connectivity on fMRI:* Degree of blood oxygenation is measured spontaneously using functional magnetic resonance imaging (fMRI), which displays neurons and functional connectivity between brain areas. Alterations in functional connectivity, including disrupted default mode community (DMN) connectivity, have been found in AD. Comparison: Functional connectivity styles can be compared between patients with AD and controls to hit upon sickness-related alterations within the brain community.

6.2.3.3 Amyloid and Tau Pathology

- *Amyloid PET Imaging:* PET imaging with radiotracers targeting amyloid-beta plaques, consisting of florbetapir and PIB, allows for the *in vivo* detection of amyloid deposition in the brain. An extended amyloid burden is a characteristic feature of AD and is associated with disease severity.Comparison: Amyloid PET scans were compared between patients with AD and controls to evaluate the amyloid burden and resources in differential prognoses.
- *Tau PET Imaging:* Recent improvements in PET imaging have enabled visualization of tau pathology in the brain using radiotracers, including flortaucipir and RO948.Tau deposition, mainly in the form of neurofibrillary tangles, is correlated with cognitive decline and ailment progression in AD. Comparison: Tau PET scans were compared between patients with AD and controls to assess the tau pathology distribution and its relationship with scientific signs.

These neuro-imaging biomarkers provide valuable insights into the underlying pathological strategies of AD, enabling the early detection of neurodegeneration, tracking ailment development, and predicting cognitive decline and conversion to dementia[4].

6.3 DEEP LEARNING FUNDAMENTALS

Deep learning has revolutionized various fields, including medical image evaluation, by leveraging neural networks to mechanically extract complex patterns from records. Here, we introduce the essential concepts of gaining deep knowledge of neural networks, training methods, and optimization strategies and delve into how these ideas are implemented in neuro-imaging analysis of Alzheimer's disease (AD).

6.3.1 Introduction to Deep Learning

Deep study entails the education of neural networks to accumulate record representations. At its core, the neural community includes layers of interconnected neurons. Every neuron applies an activation function, executes a weighted sum of its inputs to the sum, and passes the final result to the subsequent layer. Deep getting-to-know improvement with multiple layers can capture complicated relationships in information.

6.3.2 Training Procedures and Optimization Techniques

Training a deep getting-to-know version entails optimizing the parameters to reduce a given loss function. This is normally achieved using gradient-primary-based optimization algorithms. For example, the parameters are up-to-date on the usage of stochastic gradient descent (SGD) inside the direction of the terrible gradient of the loss function with respect to each parameter. The method iteratively adjusts the version to obtain better predictions.

6.3.2.1 Convolutional Neural Networks for Neuro-imaging Analysis

Convolutional neural networks are widely used in neuro-imaging evaluation due to their capability to robotically understand hierarchical elements in photos. In the context of AD, CNNs can analyze MRI or PET scans to hit upon abnormalities that indicate the disease. The core operation in a CNN is convolution, which applies filters to the enter pix to extract capabilities[5].

The convolution operation is a key system in CNNs:

$$z[l] = W[l] * a[l-1] + b[l] \tag{3}$$

in which z[l] represents the output of the convolutional layer, W[l] denotes the clear out weights, a[l−1] denotes the input to the layer, b[l] is the unfairness term, and $*$ denotes the convolution operation.

6.3.2.2 Recurrent Neural Networks for Sequential Data Processing

RNNs are specialized in managing sequential information, which qualifies them for longitudinal neuro-imaging analysis. RNNs have comments connections that allow them to keep their internal kingdom, enabling them to file temporal relationships in sequential facts. In AD research, RNNs can analyze longitudinal MRI or fMRI scans to are expecting disease developmentdescribed in Figure 6.5.

A key method for RNNs is the hidden state update equation:

$$a < t >= g\left(Waaa < t-1 > + Waxx < t > + ba\right) \tag{4}$$

wherein $a < t >$ is the hidden state at time step t, Waa and Wa are weight matrices, $x < t >$ is the enter at time t, ba is the prejudice term, and g () is the activation characteristic.

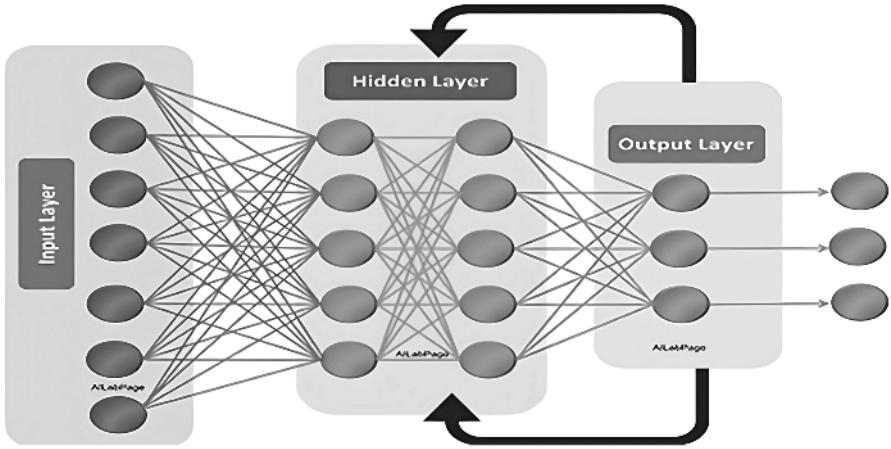

FIGURE 6.5 Convolutional Neural Networks (CNNs) for Neuro-imaging Analysis.

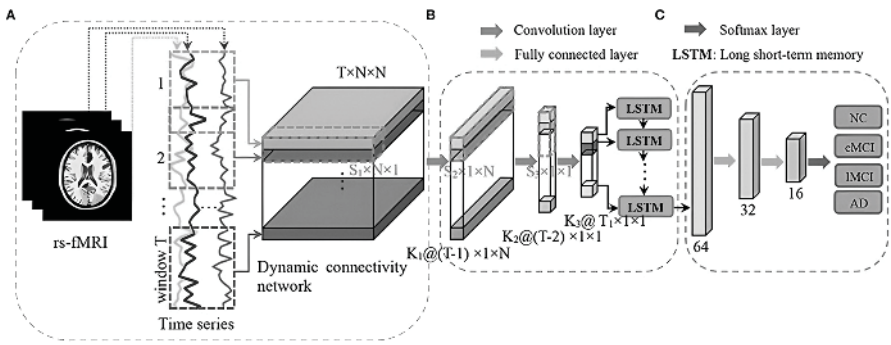

FIGURE 6.6 Recurrent Neural Networks (RNNs) for Sequential Data Processing.

6.3.2.3 Transfer Learning in Neuro-imaging Analysis

Transfer studying allows information to be transferred from one challenge to any other. In neuro-imaging evaluation for AD, CNN modelwith earlier education are adjusted on neuro-imaging datasets to improve performance described in Figure 6.6. This leverages the features learned through the previous schooling model on massive datasets, aiding responsibilities where labelled facts are scarce.

In sum, deep getting-to-know techniques, which include CNNs, RNNs, and transfer studying, are instrumental in reading neuro-imaging data for AD prognosis and progression monitoring. These strategies permit automated function extraction from pix and utilize formerly educated models to detect temporal correlations in sequential performance in records-restricted jobs.

6.4 INTEGRATION OF NEURO-IMAGING BIOMARKERS AND DEEP LEARNING IN CYBERSECURITY

Deep learning in cybersecurity was in recent years the result of the ability to revolutionize Alzheimer's disorder (AD) analysis by the use of neuro-imaging records described in Figure 6.7. This topic delves into recent studies and improvements in this field. It explores the challenges and opportunities related to learning deep mastering fashions by the usage of neuro-imaging biomarkers. It compares the effectiveness of deep learning techniques to the traditional system getting-t- know strategies[6].

6.4.1 Detecting Abnormal Brain Activity

In cybersecurity, detecting anomalous behaviour plays an important role in identifying potential threats and intrusions. Researchers aims to extend this theory to the realm of human cognition and behaviour by bringing in brain activity as an additional indicator of suspicious activity within digital systems by integrating Nneuro-imaging biomarkers and deep learning techniques are described in Figure 6.8. Detecting abnormal brain activity involves capturing deviations from established patterns of neural activity which may indicate malicious intended or unauthorized access. In real-time, the techniques of neuro-imaging such as functional magnetic resonance imaging (fMRI) and electroencephalography (EEG) offer non-invasive methods for monitoring brain activity. All techniques provide a valuable insight into cognitive processes, which include attention, memory, and decision making, which are integral to human-computer interaction. Researchers will develop robust classifiers capable of detecting deviations in cyber threat signals and these models are trained on labelled datasets including examples of normal and abnormal brain activity.

These are the several steps involved in detecting abnormal brain activity in cyber security:

1. *Data pre-processing and acquisition:* This was the first step where neuro-imaging data was collected using fMRI, EEG, or other imaging methods and pre-processed to removing noise and artifacts was processed.

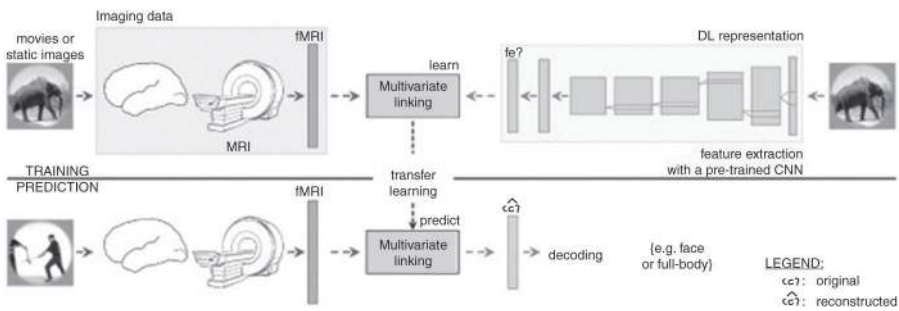

FIGURE 6.7 Transfer Learning in Neuro-imaging Analysis.

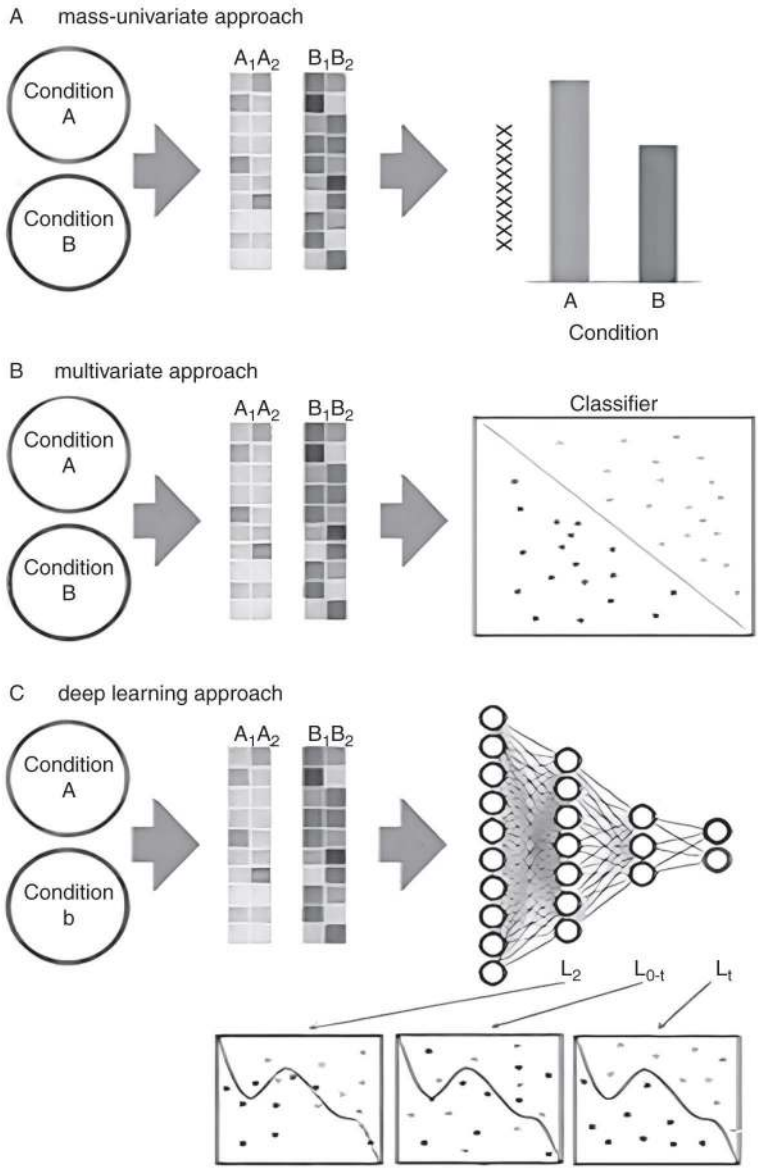

FIGURE 6.8 Deep Learning in Alzheimer's Disease Diagnosis.

2. *Features extraction:* Features were extracted from the neuro-imaging data using CNNs or RNNs, by capturing the spatial and temporal patterns of brain activity.
3. *Training the Model:* Deep learning models were trained on labelled datasets and also learned to distinguish between the normal and abnormal brain activity.

4. *Anomaly detecting:* A trained model was used to classify new states of brain activity as normal or abnormal based on trained patterns and features.
5. *Control and Response:* Detecting abnormal triggers to appropriate response actions, such as alerting system administrators, initiating security protocols, or adjusting access controls to prevent unauthorizing access.

By detecting abnormal brain activity, cybersecurity systems can enhance threat detection capabilities, identify potential attackers or identify compromised users based on deviations from normal cognitive functions. This proactive approach enables early intervention and mitigation of cyber threats, reducing the risk of data breaches, system compromises, and other security incidents.

6.4.2 Recent Studies and Advancements

Recent studies have shown the efficacy of deep getting-to-know models, particularly Convolutional Neural Networks, in AD diagnosis by the usage of Neuro-imaging records. CNNs were validated as being adept at robotically extracting meaningful features from various neuro-imaging modalities, along with MRI, PET, and fMRI scans.

The convolution operation inside the CNNs is represented via the subsequent method:

$$z[l] = W[l] * a[l-1] + b[l] \tag{5}$$

z[l]: The output of the modern layer l. It is obtained by means of acting a convolution operation at the input characteristic map a[l−1] with learnable weights W[l], followed via including a bias time period b[l].

W[l]: Learnable weights (parameters) related to the convolutional operation in layer l. These weights have been adjusted at some point of education to maximize the performance of the network.

∗: To compute the output feature map z[l], the convolution system consists of sliding a clear out (certain by learnable weights W[l]) across the input characteristic map a [l−1].

A[l−1]: Feature map enter from layer l−1. It represents the output of the previous layer after applying the activation features.

B[l]: Bias time period associated with convolutional operation in layer l. It is brought to the weighted sum of the inputs to introduce a shift or translation in the output feature map.

This permits the extraction of intricate patterns from imaging facts, facilitating the correct classification of AD sufferers and wholesome controls. Methodological strategies in these studies ranged from analyzing single-modality imaging records to integrating multimodal facts for progressed diagnostic accuracy. Transfer learning has also played a pivotal function in permitting the transfer of know-how from pretrained fashions to AD diagnosis tasks. Furthermore, interest mechanisms and recurrent neural networks (RNNs) have been employed to record temporal and spatial

dependencies in neuro-imaging records, thereby improving the performance of deep getting-to-know models.

6.4.3 Challenges and Opportunities

Despite these promising outcomes, learning deep getting-t- know fashions for AD diagnosis using neuro-imaging biomarkers provides numerous challenges. Data scarcity remains a sizeable hurdle, with the restricted availability of large, categorized datasets, mainly within the context of AD research. Additionally, neuro-imaging information exhibits variability attributable to variations in imaging protocols, scanner sorts, and affected person demographics, posing demanding situations for model generalization are described in Figure 6.9. Moreover, the interpretability of gaining deep knowledge of models is a problem as they frequently offer correct predictions without presenting insights into the underlying biological mechanisms of AD.

However, these demanding situations gift possibilities for further research and innovation. Techniques for augmenting facts, which include rotating photos, flipping, and scaling, can be hired to enhance the scale of the training datasets and enhance model robustness. Domain variation strategies offer another road for addressing dataset variability by way of transferring the information learned from one domain to every other. Additionally, efforts to beautify the interpretability of deep getting-to-know fashions, which includes interest techniques and layer-smart relevance propagation, are underway with more transparency in version predictions.

6.4.4 Comparison with Traditional Machine Learning Methodology

Comparing the effectiveness of deep getting-to-know strategies to traditional gadgets for gaining knowledge of techniques, each is famous for its strength and boundaries. While traditional techniques and home-made features taken from neuro-imaging facts are the inspiration of models inclusive of Random Forests and Support Vector

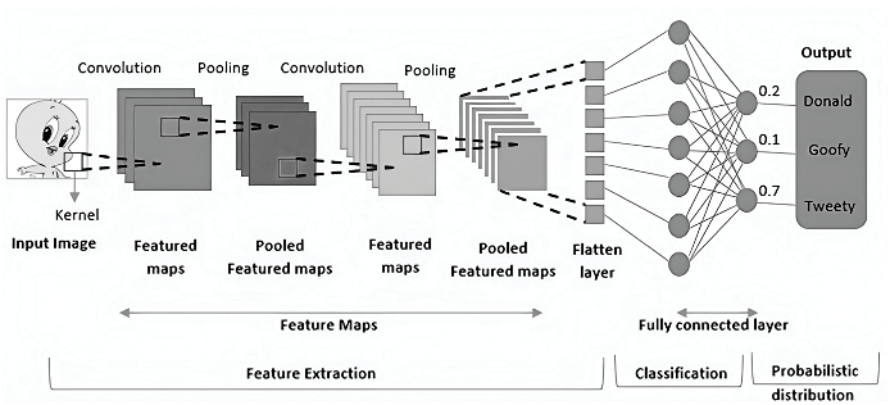

FIGURE 6.9 Illustration of a Convolutional Neural Networks design that uses neuro-imaging data to diagnose Alzheimer's Disease.

TABLE 6.1
Summary of challenges and opportunities in deep learning-based Alzheimer's Disease diagnosis

Challenges	Opportunities
Data shortage	Data augmentation techniques
Variability in Neuro-imaging statistics	Domain version techniques
Lack of interpretability	Enhancing version transparency

Machines (SVMs), gaining deep knowledge of fashions is able to mechanically expand hierarchical representations of information, potentially diffused capabilities indicative of AD pathology. However, deep studying models require a massive quantity of categorized facts for learning and may suffer from overfitting when applied to datasets with limited samples. Moreover, deep studying fashions are often opaque and lack interpretability as compared to conventional techniques are defined in Table 6.1. Summary of challenges and opportunities in deep learning-based Alzheimer's Disease diagnosis.

6.5 DEEP LEARNING FOR AN ALZHEIMER'S DISEASE PROGRESSION MONITORING

Deep mastering methodologies have demonstrated promise in the longitudinal analysis of Neuro-imaging records for tracking the development of Alzheimer's ailment (AD). This phase explores the utility of deep studying in monitoring disorder progression, the development of predictive fashions leveraging imaging biomarkers, and the importance of incorporating scientific and demographic variables to enhance the accuracy and medical software of tracking equipment[7].

6.5.1 Longitudinal Analysis of Neuro-imaging Data

Longitudinal research is important to comprehend the development of AD. Deep getting-to-know methods enable the analysis of longitudinal neuro-imaging records, which include repeated MRI scans, to identify subtle adjustments associated with disorder development. Processing sequential information is properly desirable for Recurrent Neural Networks (RNNs) and has been carried out to provide a version of the temporal evolution of brain modifications in AD.
The system for an RNN cell is represented as

$$a < t >= g\left(Waaa < t-1 > +Wax < t > +ba\right) \tag{6}$$

where $a < t >$ denotes the hidden kingdom at time $x, < t >$ represents the enter at time t, Waa and Wa are the load matrices, ba is the unfairness time period, and g is the activation feature.

6.5.2 PREDICTIVE MODELLING OF DISEASE TRAJECTORIES

Predictive fashions leveraging imaging biomarkers offer precious insights into disease trajectories and aid in figuring out how sufferers can have a better experience of cognitive decline. Architectures for deep mastering, like Long Short-Term Memory (LSTM) networks, are well-perfect for time series forecasting obligations and were applied to expect AD development based on longitudinal neuro-imaging records. The formulation for computing the output of an LSTM cell is:

$$\hat{y}_i < t >= g(WYaa<t>+bY) \tag{7}$$

wherein $\hat{y}_i$ denotes the predicted output at time t, WYa was the burden matrix which was connecting the hidden state to the output, bY changed into the bias time period, and g became the activation characteristic.

6.5.3 Incorporating Clinical and Demographic Variables

While neuro-imaging biomarkers offer precious statistics, incorporating medical and demographic variables into deep mastering models complements their accuracy and clinical utility. Multimodal fashions that combine imaging records with cognitive ratings, genetic facts, and demographic factors have shown improved predictive overall performance described in Figure 6.10. The formulation for combining multimodal inputs in a deep mastering version can be represented as:

$$z\text{combined} = W\text{imaging} \cdot \text{imaging} + W\text{clinical} \cdot \text{clinical} + b \tag{8}$$

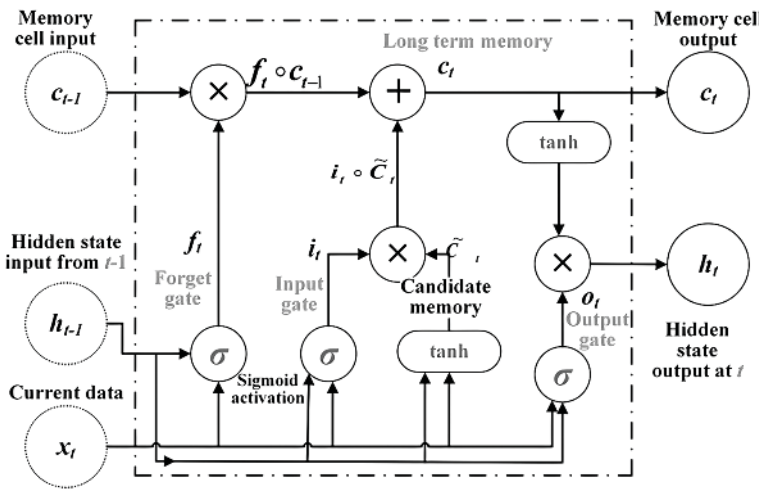

FIGURE 6.10 Illustrating a Long Short-Term Memory (LSTM) network for predicting Alzheimer's disease progression based on longitudinal neuro-imaging data.

in which *z*combined represents the mixed function vector, *W*imaging and *W*clinical are weight matrices for imaging and scientific functions, respectively, and *b* is the bias time period.

6.6 CHALLENGES AND FUTURE DIRECTIONS

Applications of neuro-imaging biomarkers and deep learning for Alzheimer's sickness (AD) prognosis and development monitoring holds first rate promise, however it is likewise accompanied by considerably demanding situations and barriers. This section identifies key challenges and discusses capability future guidelines for research and innovation in this field[8,9] described in Figure 6.11.

6.6.1 Key Challenges

Data Heterogeneity: Neuro-imaging datasets used in AD studies exhibit vast heterogeneity in terms of imaging modalities, acquisition parameters, and affected person

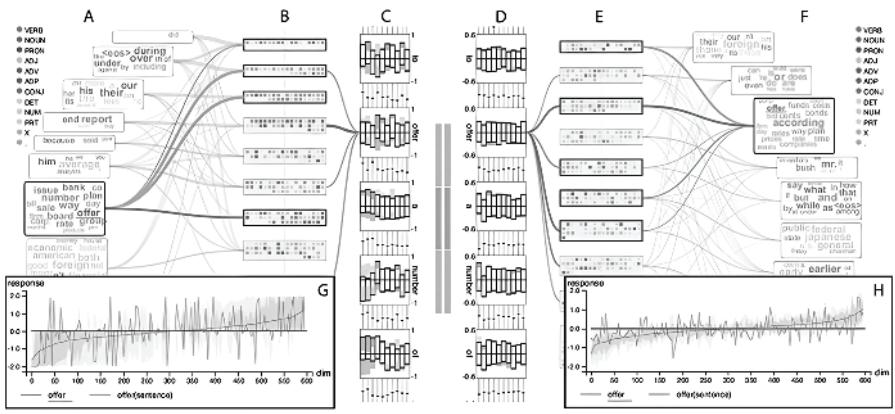

FIGURE 6.11 Comparison of RNNs, LSTMs and Multimodal Models.

TABLE 6.2
Summary of deep getting-to-know fashions and techniques for Alzheimer's Disease development monitoring

Model/Technique	Description
RNNs	Utilized for modelling temporal dependencies in longitudinal neuro-imaging statistics.
LSTMs	Employed for time series forecasting of ailment trajectories based on imaging biomarkers.
Multimodal Models	Combine neuro-imaging facts with clinical and demographic variables to enhance predictive accuracy

demographics. This diversity poses challenges for version generalization and can lead to biased or unreliable effects. Formula is defined as

$$H = -\sum_{i=1}^{N} p(xi)\log p(xi) \tag{9}$$

Model Interpretability: Deep mastering techniques are effective in identifying tricky patterns in neuro-imaging facts and absence interpretability. However, the black-container nature of those fashions prevents their considerable use in clinical settings, at the same time as interpretability is crucial for knowledge of the premise of predictions and making informed selections[10,11,12].

Ethical Considerations: The deployment of AI-based totally diagnostic gear for AD brings up ethical problems with affected person privacy, consent, and the misuse of personal clinical statistics. Moreover, the unequal distribution of access to superior diagnostic technology may exacerbate present health disparities.

6.6.2 Potential Future Directions

Integration of Multimodal Imaging Data: Future research ought to concentrate on integrating multimodal neuro-imaging data, consisting of combining structural MRI with practical PET or fMRI, to provide a complete view of AD pathology. Statistical formulas can be used to assess the correlation among one-of-a-kind imaging modalities, which include:

$$FC_{ij} = \frac{\sum_{k=1}^{N} BOLD_i(k).BOLD_j(k)}{\sqrt{\sum_{k=1}^{N} BOLD_i(k^2).\sum_{k=1}^{N} BOLD_j(k^2)}} \tag{10}$$

*Development of Interpretable Deep Learning Models***:** Researchers need to prioritize the improvement of deep mastering models that offer interpretability without sacrificing overall performance. Techniques which include interest mechanisms, saliency maps, and model distillation may be employed to enhance the transparency of version predictions[13,14,15.]

Exploration of Novel Biomarkers and Imaging Techniques: Beyond conventional neuro-imaging biomarkers, inclusive of amyloid and tau PET tracers, there's a need to discover novel biomarkers and imaging techniques which could seize early pathological adjustments in AD. For example, computational models can be used to investigate graph-based total representations of mind connectivity derived from diffusion MRI facts[16].

6.7 CONCLUSION

The combination of neuro-imaging biomarkers and deep learning represents a revolutionary approach to strengthening cybersecurity defences and enhancing threat

detection and response capabilities. By harnessing insights from human cognition and behaviour, combined with the computational power of deep learning models, researchers and practitioners have opened up new possibilities for creating digital assets and products giving business protection against cyber threats. Throughout this chapter, we have explored the synergistic potential of combining neuro-imaging biomarkers and deep learning in the context of cybersecurity, by discussing how neuro-imaging techniques such as fMRI and EEG provide a valuable point into brain activity and cognitive processes, which can be used as additional indicators of confounding activity in digital systems.

REFERENCES

[1] W. Lihua, and Z.i-P. Liu, "Detecting diagnostic biomarkers of Alzheimer's disease by integrating gene expression data in six brain regions," *Frontiers in Genetics*, vol. 10, p. 157, 2019.

[2] J. Park, H. Park, J. Lee, et al., "Hybrid Deep Learning Model for Alzheimer's Disease Diagnosis using Multimodal Magnetic Resonance Imaging," *Scientific Reports*, vol. 11, no. 1, pp. 1–13, 2021. DOI: 10.1038/s41598-021-82427-5

[3] N. Xue, K. Fu, and S. Liu, "A Deep Learning-Based Framework for the Early Detection of Alzheimer's Disease Using Resting-State fMRI," *Frontiers in Aging Neuroscience*, vol. 13, p. 692820, 2021. DOI: 10.3389/fnagi.2021.692820

[4] Y. Guo, B. Zhou, and J. Ren, "Alzheimer's Disease Diagnosis Using a Hybrid Deep Learning Model with 3D MRI Images," *Frontiers in Computational Neuroscience*, vol. 15, p. 693460, 2021. DOI: 10.3389/fncom.2021.693460

[5] B. Zhou, X. Li, and Y. Guo, "A Deep Learning-Based Method for the Diagnosis of Alzheimer's Disease Using Structural MRI Images," *Frontiers in Neuroscience*, vol. 15, p. 701368, 2021. DOI: 10.3389/fnins.2021.701368

[6] L. Yan, J. Yao, and J. Lu, "Alzheimer's Disease Classification Based on Stacked Ensemble Learning and Spatial Features from T1-Weighted MRI," *Frontiers in Aging Neuroscience*, vol. 13, p. 632999, 2021. DOI: 10.3389/fnagi.2021.632999

[7] S. Liu, Y. Lin, and C. Li, "Alzheimer's Disease Classification with fMRI Data Based on Transfer Learning," *Frontiers in Neuroscience*, vol. 15, p. 666301, 2021. DOI: 10.3389/fnins.2021.666301

[8] M. D. Ramasamy, R. K. Dhanaraj, S. K. Pani, R. P. Das, A. A. Movassagh, M. Gheisari,..., and S. Banu, "An Improved Deep Convolutionary Neural Network for Bone Marrow Cancer Detection Using Image Processing," *Informatics in Medicine Unlocked*, vol. 38, p. 101233, 2023.

[9] L. He et al., "Alzheimer's Disease Diagnosis Based on MRI Images Using Transfer Learning and Convolutional Neural Networks," *Frontiers in Neuroscience*, vol. 15, p. 721550, 2021. DOI: 10.3389/fnins.2021.721550

[10] X. Zhang et al., "Alzheimer's Disease Detection Based on Convolutional Neural Networks from T1-Weighted Magnetic Resonance Imaging," *Frontiers in Neuroscience*, vol. 14, p. 525, 2020. DOI: 10.3389/fnins.2020.00525

[11] Y. Hu et al., "Alzheimer's Disease Diagnosis Based on Multi-Modal Convolutional Neural Network and Magnetic Resonance Imaging," *Frontiers in Neuroscience*, vol. 14, p. 870, 2020. DOI: 10.3389/fnins.2020.00870

[12] C. N. Vanitha, and S. Malathy, Optimizing Wireless Multimedia Sensor Networks Path Selection using Resource Levelling Technique in Transmitting Endoscopy

Biomedical data. In *IOP Conference Series: Materials Science and Engineering* (Vol. 1055, No. 1, p. 012071). IOP Publishing, 2021, February.

[13] S. Wang et al., "Alzheimer's Disease Diagnosis Based on Multimodal Fusion of MRI Images Using Convolutional Neural Network," *Frontiers in Neuroscience*, vol. 14, p. 532, 2020. DOI: 10.3389/fnins.2020.00532

[14] S. Roobini, M. Kavitha, M. Sujaritha, & D. R. Kumar, Cyber-security threats to IoMT-enabled healthcare systems. In *Cognitive Computing for Internet of Medical Things* (pp. 105–130). Chapman and Hall/CRC, 2022.

[15] L. Ma et al., "Multi-Channel MRI-Based Alzheimer's Disease Classification Using 3D Deep Convolutional Neural Networks," *Frontiers in Neuroscience*, vol. 15, p. 617175, 2021. DOI: 10.3389/fnins.2021.617175

[16] X. Li et al., "Alzheimer's Disease Classification Based on Multi-View and Deep Learning," *Frontiers in Neuroscience*, vol. 14, p. 628, 2020. DOI: 10.3389/fnins.2020.00628.

7 A Preview of Cybersecurity Measures in Healthcare Applications Using 5G

G. Indumathi, V. Karthikeyan, and V. Arun Raj

7.1 INTRODUCTION

Out of all the previous generations of wireless network technology, 5G is a unified air interface with the objective of achieving very high capacity with minimal delay to provide enhanced services and experiences for the next generation of users. The expectation from 5G is large system connectivity with improved speed of data transfer and minimal data transfer end-to-end delay. Millimeter waves in the frequency band of 30 GHz–300 GHz are conventionally used for 5G communication.[1] The major developmental need for 5G technology is mainly due to the data intensive applications like real-time video streaming, online games, the Internet of Things (IoT), etc. Such dependable applications require very short, delayed connections and are thus able to develop smart cities, unmanned vehicles, etc. With respect to the infrastructure requirement for 5G, the most challenging part is the incorporation of tiny cellular base stations and antennas because the very high operating frequency results from the minimal structures.

The digital transformation creates a huge revolution in every sector, including the healthcare industry. Along with the development of 5G wireless networks, artificial intelligence (AI)-based approaches like big data, machine learning, deep learning, IoT, and blockchain-based security mechanisms lead to a unified network, which creates a strange opportunity, particularly in the development of healthcare systems.[2] The expectations from the implementation of 5G in smart healthcare are a discrepancy reduction in the allocation of medical resources and expedited advancements in the medical field. Similarly, online shopping, demonstrations, and the sharing of huge files through cloud services become more flexible and efficient in 5G. This implementation also enhances businesses by increasing productivity and sales. Also, new methods like the Internet of Medical Things (IoMT) and remote-operated machines are revolutionizing healthcare delivery with reduced latency and improved capacity.[3–5]

For enhanced efficiency and sustainability, 5G becomes a necessary treadle for industry. By the year 2030, the global GDP of 5G-based healthcare, manufacturing, and retail services could vary between 1.2 trillion USD and 2 trillion USD.[6] Nowadays,

 DOI: 10.1201/9781032711379-7

very widely, telemedicine is used to assess the healthcare outcomes of people suffering from chronic diseases, having less mobility, or residing in remote areas. Along with that, the Internet of Medical Things (IoMT) is also being adopted for monitoring vital medical signs, which can be operated remotely as well. As of 2022-year statistics in the USA, around 98 million people are using healthcare monitoring devices. Also, the expectation over the next five years is a 16% reduction in healthcare costs because of the adoption of IoMT devices. In India, about 33% of people are utilizing telemedicine for mental health, while 22% are using it to monitor physical health.[7]

7.2 5G USE CASES IN HEALTHCARE

Through the evolution of semiconductor industries, automotive solutions, and electronic devices, we can envisage the huge development of more reliable, robust, very high data rates, smart, and energy-efficient communication solutions through 5G. Numerous 5G applications are available in healthcare. Some of the widely adopted technologies are:

Telemedicine:
During the COVID-19 pandemic, as we all know, telemedicine helped hospitals attend to patient needs quickly. Through reliable and having fast connectivity, doctors can address patients by residing at their homes in safety. Even though such remote consultations are older than 5G, they enable built-in security and privacy-protected large video file sharing with good resolution.[8] The major benefit we observed during that pandemic period was very low end-to-end delay and large spectrum usage, which led to a good telehealth session without any consequences at a lower price.

Large Medical Data Transfer:
Commonly, the scanned medical data through CT or MRI produces enormous data and thus slows down the data transfer in the network as well. The 5G-enabled platform in many hospitals allows real-time access to the data collected from medical equipment, medical staff using electronic gadgets, notepads, mobile phones, etc., and allows the medical team to obtain the required imaging and other laboratory reports of the patients in a fraction of the previous time. Thus, it enables the doctors to treat the patients in an effective manner for a short duration.

Connected Ambulance:
With the help of 5G's capabilities, connected ambulances were implemented very effectively during the COVID-19 pandemic period. While the patient is travelling to the hospital, the connected ambulance and its staff can gather patient data and send it to the doctors via wearable technology, sensors, or live streaming of the patient's status via a high-definition video camera. This is a way to understand the patient's condition before the patient's arrival. In some situations, it allows for the provision of some paramedic guides, procedures, and diagnostic assessments to improve efficiency during emergency services.

Medical Imaging:
Normally, imaging data like CT or MRI helps the doctors analyze and provide therapy quickly to the patients. 5G advancements enable robot-assisted imaging, enabling safe treatment of patients with highly contagious diseases. With 5G technology, the MRI data can be converted into holograms so that it can be shared remotely with patients and medical specialists. This helps to identify the patient's condition more accurately without any guessing and leads to a fast and accurate diagnosis.

Inventory and Equipment Tracking:
To enhance the capacity and coverage, 5G enables the tracking of thousands of devices across the network. Hospitals use this option to track and locate the nearest life saving devices for emergency needs.

Augmented Reality:
Enormous applications are possible with augmented reality in healthcare, from monitoring to surgery. 4G allows a time lag of 20 to 50 milliseconds for augmented reality. This introduces a jitter effect between visual capture and brain processing. But with enhanced 5G network performance in terms of huge bandwidth and dependability, those limitations in 4G are eliminated.

5G Remote Surgery:
Most hospitals lack experienced surgeons in every special category. Through audio and video, doctors on the scene can consult with specialists in such circumstances. But 5G allows streaming the on-going surgery in real time to the necessary experts and getting counselling from the surgical team. 5G-enabled virtual reality and augmented reality headsets allow the specialists to provide guided remote procedures for the surgical team. This will increase the productivity of younger medical experts and speed up training as well.

Wearable for patient monitoring:
As of today, across the world, we can observe that millions of people are using wearable gadgets for preventive care and quantification. 5G is enabling patients to have medical-grade equipment, and thus clinicians can access the reliable and remote clinical information of those patients.

Healthcare Drones:
Apart from the use of drones for commercial purposes, in future with the aid of 5G technology, small indoor drones are planned to support the bedside of a patient by delivering medicine from the pharmacy, thus avoiding human interaction. This expected facility can be more rapid and less prone to error in medicinal administration.

Distraction and Rehabilitative Therapy:
For distraction and rehabilitative therapy within a hospital to provide an improved experience for the patients, AR and VR can be used. This requires 5G's low latency and huge bandwidth to enable cloud-based streaming of videos. The time lag and jitter can be reduced with the support of a low-latency feature, which thus enhances the user experience.

Behavioral Recognition through Video Analytics:
To analyze the behavior of abnormal people, this emerging 5G technology uses video analytics to identify patients who are behaving out of the ordinary. This facility is expected to be placed in hospitals, care centres, psychiatric centres, etc. The huge 5G bandwidth allows for the transfer of high-definition video for processing and analytics. The analytics can be done in real time since 5G supports low latency. With the help of the 5G slicing technique, security and reliability of patient data can be ensured.

7.3 5G ADOPTION RISKS AND RISK FACTORS

In comparison to earlier generations of mobile networks, to achieve enhanced performance, 5G utilizes higher frequencies in the range of 3 GHz to some tens of GHz. For efficient usage, 5G networks must utilize many base stations and connected devices, and beam-forming techniques are applicable for focusing the signal on the end user device. According to the World Health Organization report,[9] for these high frequencies, the overall radiation exposure is anticipated to have no consequences for public health.

To adopt the 5G network, there is a need for hardware up-gradation. But due to software's' distinctive susceptibility, 5G applications may impose a serious security problem.[10] 5G's expected adaptive software-based architecture would have more routers than the previous generation's network access points. This new structure creates a path for network attack in a risky manner. This can be avoided by complete restructuring of the existing security. The IoT devices with reduced cyber security measures can be easily hacked which allows intruders to enter the enterprise networks. This criminal activity makes it possible to intercept and modify the 5G-based sensitive communication. Also, denial-of-service attacks can affect the whole network by simply overloading a single node.

The authors in[11] suggested some useful strategies as 3Rs, namely risk-reducing tools, risk-reduction requirements, and risk-reduction design and management for observing the non-thermal effects of 5G higher frequencies. The basis for the use of 5G networks and devices is shown in Figure 7.1. The users' mobile phones must impose a strict specific absorption rate (SAR) limit, which denotes the amount of radio frequency (RF) absorbed by the body of a human. Also, it is a must to adopt some precautionary limits on RF exposure for risk reduction. One idea is proposed to announce "no RF EMF" at public gathering locations to mitigate the risk of exposure to these radiations for people who are not using a mobile phone.

Smart healthcare technologies available today accelerate the ease of care for patients by reducing treatment costs and extending the service capabilities of medical practitioners over a wide geographic area. A smart healthcare system ensures a citizen in a smart city environment can lead a healthy life with the help of facilities like the Internet of Medical Things (IoMT). This has the capability to support globally connected smart healthcare approaches. It can avoid costly hospital visits by providing accurate diagnoses and medical services. It influences the maintenance of electronic health records (EHR), transmission of patients' biomedical data to remote caretakers without any direct contact between them. For this, some sensors are used for data gathering, and smart things are used for the transmission and processing of those medical data remotely.

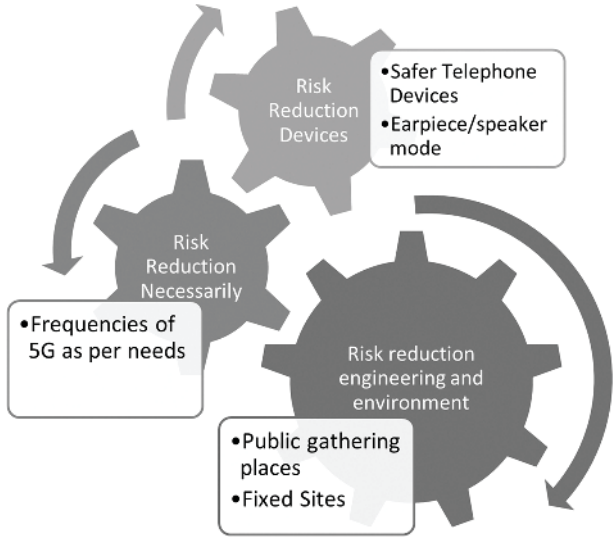

FIGURE 7.1 Basis for use of 5G networks & devices.

The speedy technological advancements in the healthcare sector allow medical devices connected through IoT and facilitate enhanced healthcare services. Along with the initiatives taken by the government, private digital technology investments create good growth in the medical sector. Hence, the global smart healthcare market is expected to generate revenues of 172.4 billion USD by the year 2030, with a 15.9% CAGR(Compound annual growth rate) from the year 2021 to the year 2030[12] as shown in Figure 7.2. At different expertise levels, healthcare services in support of IoMT for developing smart cities in a sustainable manner are rapidly evolving and have great attractions. Also, through the continuous integration of new technological developments in smart healthcare systems, improvements in precision and suitability in urban environments are witnessed. The healthcare evolution starts with version 1.0, which has limited functionality and minimal paperwork for patient diagnosis and treatment. In 2.0, the healthcare systems are interconnected locally, which allows the sharing of data between them. Whereas in 3.0, the interconnection of healthcare systems within a country is possible with the support of Hospital Information System/ Electronic Health Record, wearable devices, and interfaces with patients.

In 4.0, global smart connectivity is established with fast response and real-time tracking capability. It includes a variety of specializations like AI, analysis of big data, cloud and fog computing, edge computing, and real-time data collection and monitoring. Today we are familiar with 5.0, where a human-centred approach is considered in collaborative care and prevention. It implements integrated traditional and complementary medicinal habits.

Intelligent communication and the interconnection of enormous smart devices in the network are possible today after the emergence of IoT. In modern life, IoT has become the primary component, and in the future, it will become the vital element in the 6G network. According to "A Guide to the Internet of Things Infographic,"[13]

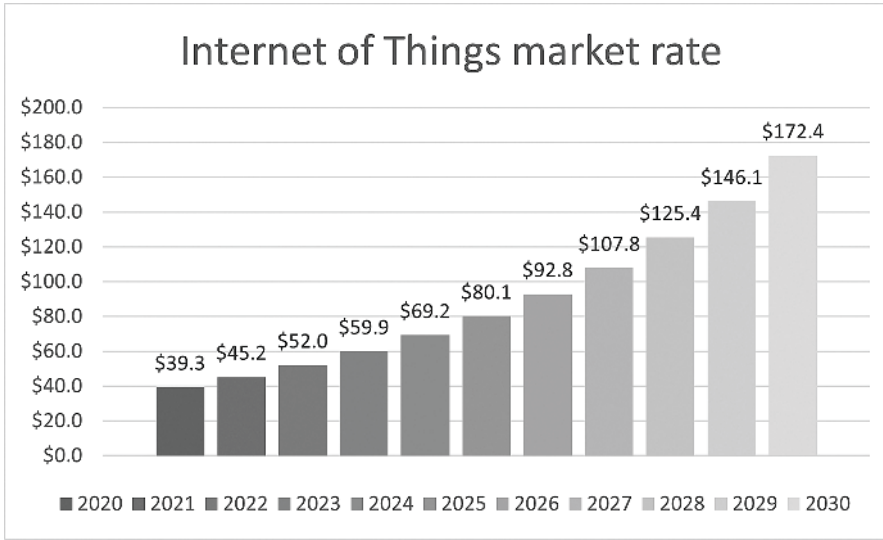

FIGURE 7.2 Internet of Things market rate, Year: 2020–2030 in USD Billion.

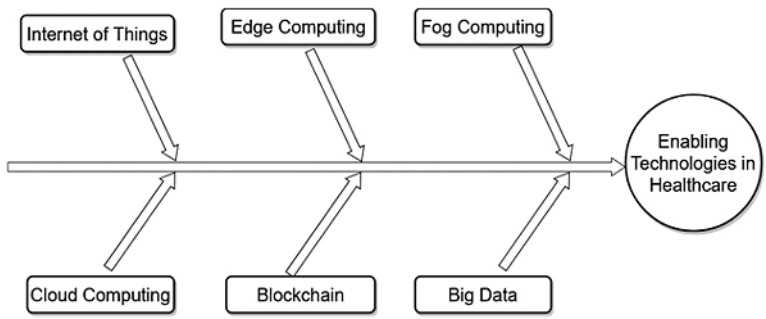

FIGURE 7.3 Emerged Technologies in Healthcare domain.

healthcare will account for around 40% of IoT technology by 2025. The emerging technologies for supporting real-time data exchange between healthcare stakeholders, including patients and healthcare service providers, are shown in Figure 7.3.

Real-time medical data exchange is allowed in the IoT to facilitate data-driven decisions and patient care quality improvement. With the use of centralized cloud computing, vast healthcare data access and storage are possible in a cost-effective manner. Decentralized Fog computing allows data processing with minimal latency and avoids the data centre requirement; thus, it leads to cost reduction. Along with the capability of fog computing, edge computing provides enhanced patient data security for its processing. To improve the precision of healthcare records blockchain technology is being developed. It gives patients privacy and authorized access to sensitive health information. The main features of blockchain technology are data attribution,

strength, distribution management, privacy, and authorization.[14,15] The incorporation of this technology needs some major funding from healthcare establishments without any validated success. Still, this technology is in an evolving stage; its adoption may lead to some risks and challenges.

7.4 5G BASED SECURE SMART HEALTHCARE MONITORING

Instead of focusing on hospitals and specialists, healthcare is increasingly moving towards a distributed model that prioritizes the patient. Several breakthroughs are propelling rapid interdisciplinary growth in medical care. Through electronic communication technology, remote and personalized healthcare is now possible. To meet present and future demands, healthcare is utilizing technology for communication, such as the 4G network, for intelligent medical solutions.[14] As a growing number of innovative healthcare applications join the network, data volumes and protocols will differ. The network is going to encounter some tough problems with data throughput, delay, and capacity. Connecting many different hospital machinery and equipment with sensor-based systems will require massive machine-type connectivity as this digital medical industry develops. Increasing numbers of application scenarios, such as tactile computing and distant activities, will necessitate critical machine-type communication with hyper-accuracy and minimal latencies.

7.4.1 Smart Healthcare

Nowadays, wireless networks are under constant and complex pressure from all the different intelligent medical activities. The 5G network is anticipated to support advanced medical applications with exceptional energy conservation, high coverage, ultra-high performance, high speed, and minimal latency. The combination of 5th Generation and IoT technologies will enhance coverage, performance, and protection in future smart healthcare networks.

According to recent reports,[16] experts project that the IoT in healthcare will be worth $125 billion in the year 2020–25. The literature suggests a plethora of intelligent medical applications that combine wireless mobile networks[17] and suggests using a 5G smartphone and the Internet of Things to continually track chronic patients. These methods enable a mobile health system to continuously evaluate and track individuals with diabetes.[18] Intelligent health services, such as remote surveillance and medical assistance that are facilitated by the Internet of Things were proposed in Xiao et al..[19] For continual surveillance of health, connected devices like sensors, smart watches, and smart clothes track vitals like beats per minute, sleep, and movement levels were suggested. The Internet of Things (IoT) has inspired the development of wireless entrances that can provide smart support in portable medical settings, allowing for remote assessment of chronic patients' health in real-time, for example.[20] One use of the Internet of Things in medicine is the remote monitoring of people with chronic illnesses.[21] One possible use of wearable technology is to enable data transfer between wearables and remote, internet-accessible "cloud" servers.[22,23] By connecting to a cloud server, wearable gadgets can transmit data on a user's heart

rate, sleep, and activity levels. Enhanced smart healthcare apps may be possible with 5G and the Internet of Things.

7.4.2 5G and Smart Healthcare: Recent Studies

There have been a number of studies that investigate the possibility that 5G could enhance smart healthcare applications. The following is a list of some of them.

Overcrowding Control mechanisms: Wireless multimedia sensor networks, which often have limited bandwidth resources, can benefit from a priority rate-based routing protocol (PRRP), as suggested in Hua.[24] Congestion of network resources is possible in low-resource capacity systems because streaming audio and video uses a lot of bandwidth. Inadequate picture and speech performance of transmitted information for medical applications (e.g., remote surgery, remote health surveillance) is a common consequence of congestion, which consumes limited resources like node energy and has impacts on the application QoS necessities.[25]

Scheduling Strategies: The presentation of network slice-based 5G wearable networks in[26] aims to improve network resource sharing and energy efficiency. The strategy intends to maximize the network's resources (O.1) and energy efficiency (O.4) through the introduction of software-defined networks (SDNs) (G.3) and network function virtualization (NFVs) (G.4). As a result of SDNs' ability to manage both the control and data planes, networks can be flown in a variety of ways.[27] NFV uses software instead of physical hardware to partition the network's operations into distinct functional domains and implements virtualization technology. The 5G small cells (femto, pico, microcells) network design can enhance the quality of service (O.2) by achieving a high data rate (P.1), as explained in Rehman et al.[28] The potential for sending a medical ultrasound video feed from a moving ambulance to a hospital uplink is investigated in this case study. We consider a heterogeneous network consisting of smaller mobile cells and stationary macro cells with eNodeB.

Routing Scenarios: Nodes can hop from one location to another and establish direct-to-direct (D2D) linkages with nearby nodes during a changeover, allowing for improved channel quality and seamless communication.[23,29] eNB manages resources, controls power, and establishes D2D sessions. The electronic network block uses the channel quality indicator (CQI) to decide whether to switch networks. In the first of three stages that make up the handover process, user equipment (UE) communicates with its serving eNB about the channel. The eNB then decides whether or not to initiate the handover based on the conditions. During the execution stage, the eNB determines whether to move UE data and behavior to another cell. As a last stage, cells acknowledge each other and update their state regarding UEs in newly formed cells.[30,31]

7.5 FRAMEWORK OF 5G NETWORKS FOR INTELLIGENT HEALTHCARE SYSTEMS

As a successor to the current 4G networks, 5G presents the next generation networks. Detailed here are 5G's specifications, characteristics, and improvements to efficiency. Pictured in Figure 7.4 is the 5G smart healthcare system configuration.

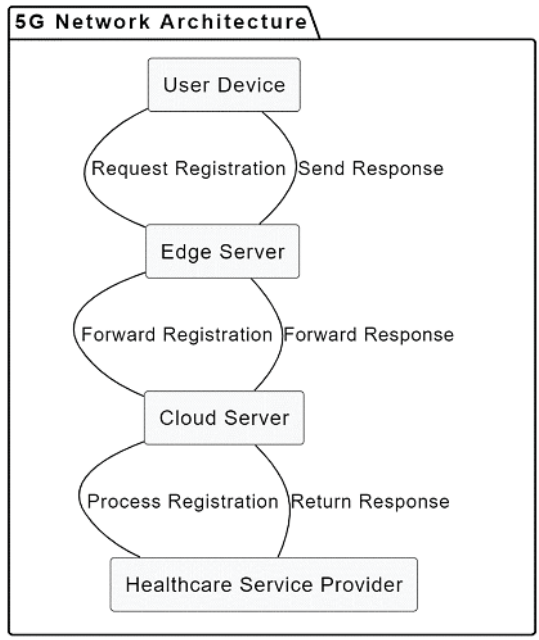

FIGURE 7.4 5G framework for smart healthcare.

5G Architecture

Small cells, which range in width from a few centimeters to a kilometer, are radon entry terminals with minimal power. 5G smart healthcare applications may rely heavily on the variety of small cells. Data speeds ranging from 137 Mbps all the way up to 1.6 Gbps are necessary for several advanced medical applications, including remote surgery. One method involves using small cells. The size of cells can vary from femto to pico to micro. In comparison to macrocells, which may reach distances of up to 20 kilometers, these cells are quite small. Coverage and capacity in tiny places, such as residences and hospitals, are enhanced by femtocells. Over 0.1 kilometers, it can accommodate up to 30 people. Better coverage and support for 100 users across 1 km are features of picocells. Picocells are a way to boost wireless and cellular coverage in tight spaces. Microcells are comparable to picocells, except they can accommodate more users and cover a larger area. Within a range of 2 kilometers, microcells can support 2000 users. The cellular network's extensive radio coverage is provided by Marcocells It covers a lot of ground and gets the job done quickly. Hence, UEs can't establish connections with either macro- or small-cell base stations at the same time. While small-cell base stations use higher frequencies to deliver high-throughput information, macro-cell base stations employ smaller frequency zones to enable connection and accessibility (the control plane).[32] In complex networks, the base units might be either macro, micro, pico, or femto.

Enhancements and Functionalities of 5G Networks

D2D, or device-to-device communication, is a method of establishing a connection between individual network nodes that does not rely on a central hub or base station (BS). Interaction between devices reduces congestion in networks.[33] D2D communication allows for the instantaneous transfer of data or the sharing of radio access links between each destination. Band 20–300 GHz for millimeter wave (mmWave) connectivity: Since there is a dearth of bandwidth under 3 GHz, 5G will have to make use of the abundantly available mmWaves band, which usually spans 20 GHz to 90 GHz. One of the many uses for small-cell mmWaves is in intelligent healthcare, where they reduce high path loss.[34] Software-defined networking (SDN): SDN provides a low-cost, highly managed, flexible, and active network architecture that can support numerous applications with high bandwidth. SDN makes use of a wide variety of network solutions to increase network agility and flexibility, which are essential for today's storage platforms, centralized computer systems, and information centres. The new networking method known as network function virtualization (NFV) uses software-based network tools that operate as virtual desktops on normal systems to substitute costly special-purpose components. Distributed computing at the network's periphery, or "edge," processes data close to its point of origin. Figure 7.5 shows the 5G architecture-based intelligent medical care system implementation.

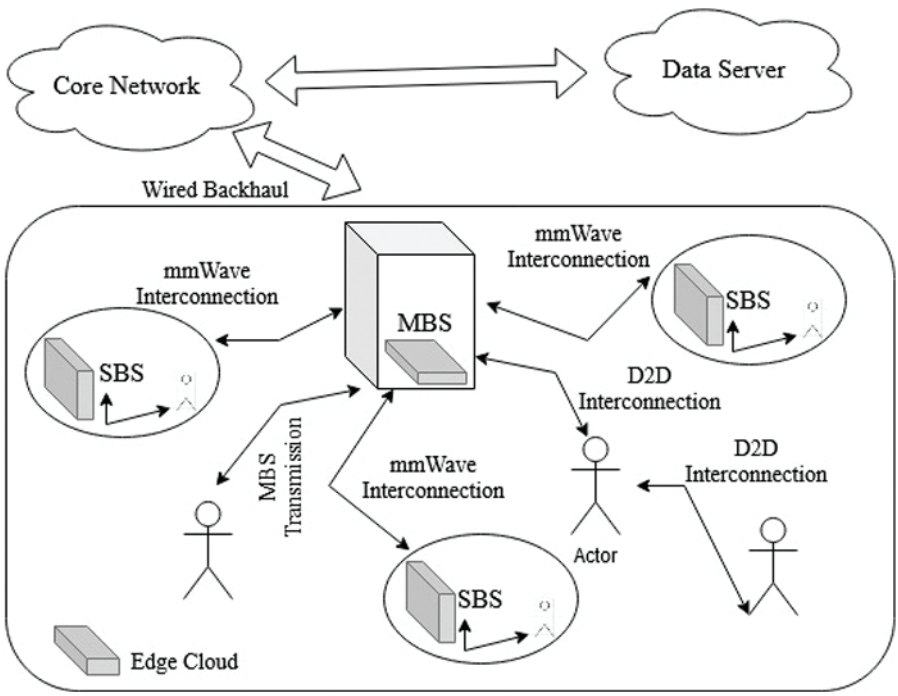

FIGURE 7.5 Intelligent medical care using 5G architecture.

5G Network's Enhanced Functionality

Table 7.1 compares traditional schemes with 5G-based methods in terms of their characteristics and efficiency improvements.[35]

- Transmission speeds up to 10Gbps are possible during peak times, with estimates of 20Gbps pending depending on the circumstances.
- We can handle services with extremely low latency specifications, defined as 1 ms or fewer.
- With this connectivity, you may reach speeds of up to 500 km/h.
- Make high-density network interaction possible and allow for huge machine-type connectivity.
- Boost the utilization of energy by ten times and spectrum effectiveness by three.

The 5G network architecture introduces several enabling technologies for intelligent healthcare, addressing restrictions in conventional medical techniques. Improved connection settings, continuous surveillance, adaptability, and encryption are all benefits of these technological advancements. 5G can completely change the way healthcare is provided, emphasizing the contrast.

Conditions for Intelligent Medical Services

To streamline procedures and enhance patient care, smart healthcare systems require technology, patient engagement, security, and interoperability. Enabling comprehensive care, interoperability facilitates the flow of patient information by allowing easy data interchange among healthcare components. Strong data security and privacy measures, such as encryption and HIPAA compliance, are necessary to protect sensitive patient data, maintain confidentiality, and build trust. Advanced analytics and AI can sift through enormous datasets for useful insights, paving the way for predictive analytics, personalized medicine, and well-informed decision-making. When it comes to managing chronic diseases, wearable sensors and technologies allow for real-time tracking, early problem diagnosis, and rapid response. More people may use telemedicine and virtual consultations thanks to secure technology, which decreases the need for in-person visits and boosts communication between patients and doctors.[31]

Integrating IoT devices enhances real-time monitoring, automates data collection, and gives a comprehensive picture of a patient's health. With 5G connectivity, large medical dataset transmission, Internet of Things (IoT) device integration, and remote surgery are all within reach. Interfaces that are easy to use enhance processes, engagement, and usefulness, which benefits both patients and healthcare practitioners. The immutability, security, and impossibility of tampering with data mean that blockchain technology provides significant advantages to healthcare transactions and information exchange. By adjusting to emerging technology, scalable infrastructure helps meet healthcare demands and future expansion. By actively involving patients, portals and mobile apps promote treatment adherence and proactive health management. For the sake of patient safety, industry norms, and the lawful and ethical use of health data, compliance with regulations is essential. Maintaining continuity, avoiding duplication, and providing a full medical history are all benefits of seamless integration with the EHR. Establishing and regularly testing feedback loops with healthcare professionals

TABLE 7.1
Advantages of 5G schemes over standard approaches

Component	Enabling Technologies	Comparison with Traditional Healthcare
User Equipment (UE)	Wearables, medical sensors, smartphones, BLE for device connectivity	Conventional approaches frequently depend on regular, face-to-face examinations, lacking the ability to monitor continuously. Wearables provide instantaneous data for the purpose of monitoring patients from a distance.
Radio Access Network (RAN)	Massive MIMO, beamforming	Conventional medical care approaches may employ regular networks that have restrictions in terms of information transmission speeds and instrument interconnectivity. 5G RAN improves connectedness and increases data transmission speeds.
Core Network (CN)	NFV, SBA	Conventional healthcare networks sometimes possess a rigid structure, which might present difficulties when it comes to accommodating evolving needs. The NFV and SBA technologies of 5G provide a high degree of adaptability and expandability.
Network Slicing	SDN, NFV	Conventional networks do not possess the ability to generate separate virtual networks. Network slicing enables the creation of dedicated segments for healthcare, guaranteeing efficient distribution of resources.
Edge Computing	Edge servers, fog computing	The use of centralized data processing in conventional healthcare has the ability to introduce latency. By bringing processing of data closer to its origin, edge computing decreases latency.
Security Measures	End-to-End Encryption, Blockchain, Authentication mechanisms	Despite the fact that they frequently rely on typical security precautions, standard medical approaches have difficulties when it comes to maintaining the safety of digital medical records. There are new and improved security protocols introduced by 5G.
Application Layer	Telemedicine Platforms (HD video codecs, reliable protocols), Health Information Systems (FHIR), IoT Integration (MQTT, CoAP)	Consultations in person and documentation in paper form are features of more conventional healthcare. 5G applications pave the way for standardized data interchange, remote consultations, and the integration of the Internet of Things.
Quality of Service (QoS)	Dynamic QoS management, Network slicing, Policy enforcement	The quality of treatment could vary since traditional medical networks don't always give priority to the treatments their patients really need. Reserved resources for vital healthcare applications are guaranteed by 5G's QoS control.

and a patient ensures the effectiveness, ease of use, and satisfaction of end users with smart healthcare solutions. Smart healthcare solutions that are effective, secure, and easy to use are essential for better patient outcomes and healthcare delivery, but only if these complicated conditions are satisfied.[36]

Challenges and Scope for Improvement of 5G in Clinical Care

Although the use of 5G offers enormous promise for the medical sector, there are quite a few major limitations.[37] Concerns about the security of individual medical records against breaches and the necessity for adhering by security laws like HIPAA are common as 5G technology improves connection and data transfer. The already tough process of attaining interoperability across diverse healthcare systems, tools, and apps is made more difficult by the lack of established protocols and data formats. Despite developments, it is still hard to maintain reliable and continuous network connections, particularly in urgent healthcare environments. Coordination is essential since there are compatibility concerns when integrating 5G with the present healthcare infrastructure.[32,38] Healthcare systems must employ complex analytics and effective methods for handling data to prevent breaking under the weight of the enormous amounts of data generated by 5G-connected medical equipment. However, the high cost of adopting new technologies and deploying 5G infrastructure might place healthcare organizations in a financial predicament. It is not trivial keeping up with regulatory compliance, which involves navigating complex systems and abiding by both regional and international laws. Healthcare professionals might want specialized training to effectively utilize 5G technology, and ethical issues, such as obtaining patients' consent for data sharing, are of extreme importance.[33–35]

Lack of coverage in rural regions and the challenge of integrating various healthcare technology owing to the lack of widely accepted norms might lead to a widening of healthcare disparities. To get over these challenges and promote adoption, we must continue working to build and maintain patient confidence in 5G-based healthcare systems and address worries about data security. Collaboration between technology suppliers, politicians, regulators, and healthcare providers is essential to ensure the safe, moral, and effective implementation of 5G in the healthcare industry. The open tasks and concerns in 5G based health care are illustrated in Figure 7.6.

7.6 BLOCKCHAIN FOR 5G HEALTHCARE APPLICATIONS

Blockchain and 5G technologies can be integrated to develop several intriguing new possibilities in the healthcare sector. When utilized alongside 5G's lightning-fast speeds and low latency, blockchain's independent and secure nature can solve a variety of challenges encountered by the healthcare industry.[39]

Convergence of Blockchain and 5G Healthcare

Every person should have access to health data since it contains essential details about our physical health. It is fundamental to the diagnosis and treatment of illnesses.[40] Medical data has become an invaluable resource in the fast-moving field of artificial intelligence, supporting the development of advanced diagnostic models and assisting medical professionals in making precise diagnoses. Although data accessibility and

FIGURE 7.6 Open Tasks and Concerns.

storage convenience have improved with the shift from traditional paper records to electronic medical records (EMR), data privacy must be given top priority.[41,42] Considering these problems, a more sophisticated database management system that is impervious to tampering and hacking is desperately required to substitute for the one that has been in use in recent years. The blockchain consideration for 5G is shown in the Figure 7.7. Enhanced data protection and the ability to interface with other IT systems, like finance and admissions, are two features that the new, creative system should offer. When blockchain technology was first presented in 2008, it essentially met each of these requirements due to its adaptability for use in a variety of banking and financial applications. A growing, uninterrupted list of data records created by the participating nodes is maintained by blockchain, a decentralized database. Data from each completed transaction is included in the information, which is kept in a public ledger.[43] In addition, blockchain functions as a kind of distributed ledger that aggregates value-exchanged transactions in a sequential manner using cryptographically linked blocks. Along with decentralization, security, privacy, and data integrity, blockchain also has the feature of being unalterable and without a middleman to regulate agreement.[44] Because blockchain is made up of an ongoing succession of blocks that include data and information, the information is transparent and unchangeable.[45–47]

FIGURE 7.7 Blockchain for 5G.

Smart Contracts: Automating Procedures to Transform Healthcare

In the constantly changing field of healthcare, where precision and efficiency are the ultimate goals, the use of smart contracts is a game-changer. Figure 7.8 represents the lifecycle of smart contracts for the automation in several healthcare facilities. The operational dynamics of the sector are being revolutionized by these self-executing contracts, which have the potential to improve patient care and streamline administrative work.[48]

Revolutionizing Healthcare: Innovative Scenarios and Blockchain-5G Solutions

Scenario 1: Several healthcare organizations, each with their own data silos, suffer from interoperability problems that impede smooth information sharing.

Scenario 2: Patient confidentiality is at risk of being compromised by security vulnerabilities in traditional health data interchange systems.

Scenario 3: Conventional systems encounter delays in data retrieval and exchange, yet prompt access to patient data is essential for efficient telemedicine consultations.

Scenario 4: Inefficiencies, insufficient information, and a lack of openness constitute typical problems related to conventional medical study processes.

Scenario 5: Illegal drugs and inefficiencies in the pharmaceutical supply chain constitute a threat to individual patient safety.

Scenario 6: Due to potential misuse of already present E-health records, patient histories may be incorrect.

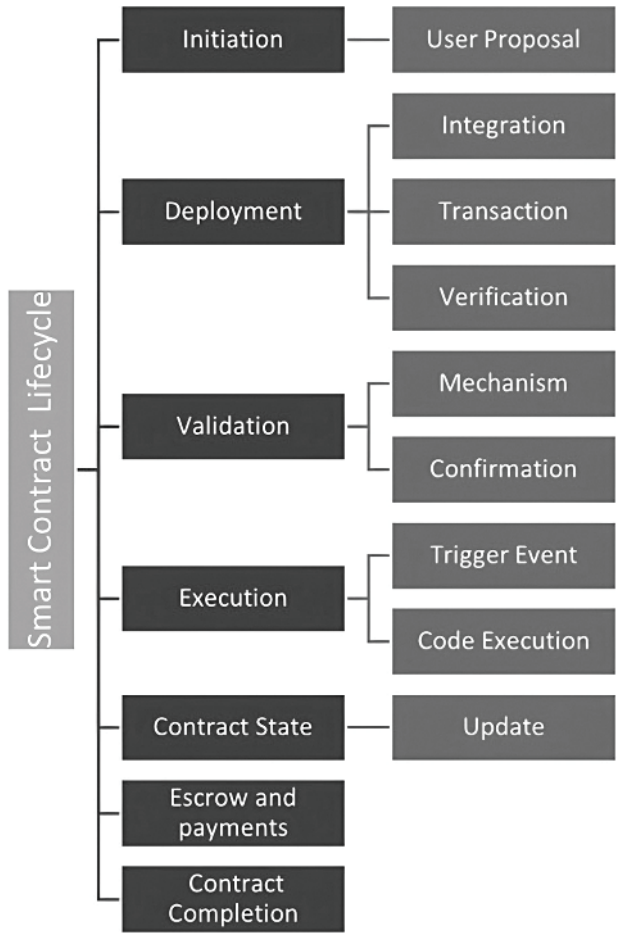

FIGURE 7.8 Smart Contract Lifecycle.

Blockchain and 5G networks work together to give healthcare supply chains continuous monitoring, improve security and traceability while eliminating the risk of counterfeiting from happening. Immutability assures that patient data is unchanging and impenetrable, which is essential for the security of health information. It is a way to entirely reinvent healthcare delivery as well as implement small-scale improvements. It envisions a day where patient-centric, protection, and intelligence all work together to create a smarter and efficient medicare environment. When blockchain's robust encryption and 5G's low latency interconnection combine to guarantee sharing of data remains safe, clinical data exchange safety worries become less of an issue. Clinical trials are changing dramatically as decentralized systems powered by 5G real-time connectivity and blockchain transparency simplify, improve, and promote global inclusion in research projects.[49]

7.6.1 High-level Representation of Blockchain in 5G Healthcare Applications

Input: Health data file (HDF), Hash (H1), Patient details (PD), Access Records (AR)
Output: Record Access

- Initiate Blockchain()
- Authenticate Users Devices()
- function Verify Transaction(Tx):
  - Verification logic
  - return is Valid
- function Consensus Mechanism(Tx):
  - Consensus logic
  - return agreed
- Execute Smart Contract(Contract)
- function Encrypt Data(Data):
  - Encryption logic
  - return encrypted Data
- function Form Block(Block, Previous Block):
  - Block formation logic
  - return new Block
- function Distribute Ledger(Node1, Node2, ..., NodeN):
  - Ledger distribution logic
  - Distribute Ledger()
- function Real Time Transmission(Data, Speed):
  - Transmission logic
  - Transmit Data(Data, Speed)
- function Immutable Record(Record):
  - Ensure immutability
  - return immutable Record
- Trigger Event(Event)
- function Regulate Data Access(Node, Access Control):
  - Access control logic
  - Regulate Access(Node, Access Control)
- function Continue Consensus(Block, Nodes):
  - Consensus continuation logic
  - Continue Consensus(Block, Nodes)
- function Monitor Network(Latency, Reliability, Security):
  - Monitoring logic
  - Monitor Network(Latency, Reliability, Security)
- Finalize Transaction(Tx)

This representation algorithm is suitable for all kinds of applications and the logic of the applications depends on the user perspective usage and can be altered to suit their needs.[50]

7.7 CONCLUSION

Here we have provided an overview of present research and future directions for study regarding the networking components of 5G and the Internet of Things (IoT) as they pertain to smart healthcare. In the first part of our presentation, we laid out the framework for 5G smart healthcare and the key technologies that will make it possible, including direct-to-device connectivity, small cells, software-defined networks, network function virtualization, millimeter waves, and edge computing. Second, we laid out the 5G smart healthcare taxonomy and examined the new goals and needs for this technology, including resource optimization, improved quality of service, reduced interference, and increased energy efficiency, as well as ultra-high reliability, high bandwidth, and high battery lifetime. Our third contribution was a comprehensive overview of the current state of, and potential future directions for, research into network layer solutions for 5G smart healthcare based on the Internet of Things (IoT). This included topics such as scheduling, routing, and congestion control. It was challenging to cover every possible strategy due to the ever-changing and expanding nature of computer networks, but we did our best to cover all the important ones. As a conclusion, we provided a high-level overview of the current and potential obstacles to 5G smart healthcare.

REFERENCES

1. M. Zohrehvand, O.A. Dobre, A. Abdi, and M. Zolghadri, "5G networks: Opportunities and challenges," *IEEE Trans. Internet Things*., vol. 7, no. 11, pp.10229–10249, 2020.
2. D.S.W. Ting, H. Lin, P, Ruamviboonsuk, T.Y. Wong, and D.A. Sim,. "Artificial intelligence, the internet of things, and virtual clinics: Ophthalmology at the digital translation forefront," *Lancet Digital Health*., vol. 2, no. 1, pp. e8–e9, 2020.
3. D. Li, "5G and intelligence medicine—how will the next generation of wireless technology reconstruct healthcare?" *Precis. Clin. Med*., vol. 2, no. 4, pp. 205–208, 2019.
4. H.N. Qureshi, M. Manalastas, S.M.A. Zaidi, A. Imran, and M.O. Al Kalaa, "Service level agreements for 5G and beyond: Overview, challenges and enablers of 5G-healthcare systems," *IEEE Access*, vol. 9, pp. 1044–1061, 2020.
5. S. Dananjayan, and G.M. Raj, "5G in Healthcare: How fast will be the transformation?" *Int. J Med. Sci*., vol. 190, no. 2, pp. 497–501, 2021.
6. www.mckinsey.com/br/en/our-insights/all-insights/ciberseguranca-e-condicao-para-destravar-potencial-da-saude-com-5g,Available online- September 14, 2022.
7. www.statista.com/statistics/1344086/india-usage-of-telemedicine-among-consumers/ Available online- Feb 9, 2024
8. E. Liu, E. Effiok, and J. Hitchcock, "Survey on health care applications in 5G networks," IET Commun., vol. 14, no. 7, pp. 1073–1080, 2020.
9. www.who.int/news-room/questions-and-answers/item/radiation-5g-mobile-networks-and-health. Available online- Feb 27, 2020
10. V. Yeruva, Why 5G networks are disrupting the Cybersecurity Industry, Forbes Technology Council, October 2021. www.forbes.com/sites/forbestechcouncil/2021/10/29/why-5g-networks-are-disrupting-the-cybersecurity-industry/?sh=762299ae1fe9.

11. S. Jain, and P.K. Jain, "5G Technology for healthcare and its health effects: Wonders, dangers, and diligence", *J. Family Med. Prim. Care*, vol. 11, no. 11, pp. 6683–6686, 2022. Doi: 10.4103/jfmpc.jfmpc_1426_22.
12. Internet of Medical Things Market. Available online: www.precedenceresearch.com/internet-of-medical-things-market (accessed on 14 April 2023).
13. www.intel.com/content/www/us/en/internet-of-things/overview.html (accessed on 13 March 2023).
14. P. Mishra, and G. Singh, "Internet of medical things healthcare for sustainable smart cities: current status and future prospects," *Applied Sciences*, vol. 13, no. 15, p. 8869, 2023.
15. T.T. Kuo, H.E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *J. Am. Med. Inform. Assoc*., vol. 24, pp. 1211–1220, 2017.
16. T.J. McCue, $117 Billion Market for Internet of Things in Healthcare by 2020. Forbes Tech. [Online], Apr. 2015. Available https://www.forbes.com/sites/tjmccue/2015/04/22/117-billion-market-for-internet-of-things-in-healthcare-by-2020/.
17. J. Lloret, L. Parra, M. Taha, and J. Tomás, "An architecture and protocol for smart continuous eHealth monitoring using 5G," *Comput. Netw*., vol. 129, pp. 340–351, Dec. 2017.
18. M. Chen, J. Yang, J. Zhou, Y. Hao, J. Zhang, and C.-H. Youn, "5G-smart diabetes: Toward personalized diabetes diagnosis with healthcare big data clouds," *IEEE Commun. Mag*., vol. 56, no. 4, pp. 16–23, Apr. 2018.
19. F. Xiao, Q. Miao, X. Xie, L. Sun, and R. Wang, "Indoor anti-collision alarm system based on wearable Internet of Things for smart healthcare," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 53–59, Apr. 2018.
20. J. Santos, J.J.P.C. Rodrigues, B.M.C. Silva, J. Casal, K. Saleem, and V. Denisov, "An IoT-based mobile gateway for intelligent personal assistants on mobile health environments," *J. Netw. Comput. Appl*., vol. 71, pp. 194–204, Aug. 2016.
21. I. Chiuchisan, I. Chiuchisan, and M. Dimian, "Internet of things for ehealth: An approach to medical applications," in *Proc. IEEE Int.Workshop Comput. Intell. Multimedia Understand. (IWCIM)*, 2015, pp. 1–5.
22. M. Chen, Y. Ma, Y. Li, D. Wu, Y. Zhang, and C.-H. Youn, "Wearable 2.0: Enabling human-cloud integration in next generation healthcare systems," *IEEE Commun. Mag*., vol. 55, no. 1, pp. 54–61, Jan. 2017.
23. L. Tshiningayamwe, G.-A. Lusilao-Zodi, and M.E. Dlodlo, "A priority rate-based routing protocol for wireless multimedia sensor networks," in *Advances in Nature and Biologically Inspired Computing*. Cham, Switzerland: Springer, 2016, pp. 347–358.
24. S. Hua, "Congestion control based on reliable transmission in wireless sensor networks," *J. Netw*., vol. 9, no. 3, pp. 762–768, 2014.
25. W. Chen, Y. Niu, and Y. Zou, "Congestion control and energy-balanced scheme based on the hierarchy for WSNs," *IET Wireless Sensor Syst*., vol. 7, no. 1, pp. 1–8, 2016.
26. Y. Hao, D. Tian, G. Fortino, J. Zhang, and I. Humar, "Network slicing technology in a 5G wearable network," *IEEE Commun. Stand. Mag*., vol. 2, no. 1, pp. 66–71, Mar. 2018.
27. R. Chaudhary, N. Kumar, and S. Zeadally, "Network service chaining in fog and cloud computing for the 5G environment: Data management and security challenges," *IEEE Commun. Mag*., vol. 55, no. 11, pp. 114–122, Nov. 2017.

28. I.U. Rehman, M.M. Nasralla, A. Ali, and N. Philip, "Small cell-based ambulance scenario for medical video streaming: A 5G-health use case," in *Proc. 15th Int. Conf. Smart Cities, Improving Qual. Life Using ICT IoT (HONET-ICT*), Oct. 2018, pp. 29–32.
29. A. Orsino, M. Gapeyenko, L. Militano, D. Moltchanov, S. Andreev, Y. Koucheryavy, and G. Araniti, "Assisted handover based on device-todevice communications in 3GPP LTE systems," in *Proc. IEEE GLOBE- COM Workshops*, Dec. 2015, pp. 1–6.
30. Y. Xing, and H. Seferoglu, "Device-aware routing and scheduling in multi-hop Device-to-Device networks," in *Proc. Inf. Theory Appl. Work-shop (ITA)*, Feb. 2017, pp. 1–7.
31. G.A. Akpakwu, B.J. Silva, G.P. Hancke, and A.M. Abu-Mahfouz, "A survey on 5G networks for the Internet of Things: Communication technologies and challenges," *IEEE Access*, vol. 6, pp. 3619–3647, 2018.
32. W.H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun*., vol. 21, no. 2, pp. 106112, Apr. 2014.
33. F. Jameel, Z. Hamid, F. Jabeen, S. Zeadally, and M.A. Javed, "A survey of device-to-device communications: Research issues and challenges," *IEEE Commun. Surveys Tuts*., vol. 20, no. 3, pp. 21332168, 3rd Quart., 2018.
34. N. Al-Falahy, and O.Y.K. Alani, "Millimetre wave frequency band as a candidate spectrum for 5G network architecture: A survey," *Phys. Commun*., vol. 32, pp. 120–144, Feb. 2019.
35. A. Bazzi, G. Cecchini, M. Menarini, B.M. Masini, and A. Zanella, "Survey and perspectives of vehicularWi-Fi versus sidelink cellular-V2X in the 5G era," *Future Internet*, vol. 11, no. 6, p. 122, 2019.
36. Z. Qi, J. Liu, and G. Zhao, "Towards 5G enabled tactile robotic telesurgery," *arXiv preprint arXiv:1803.03586* (2018).
37. M. Agiwal, N. Saxena, and A. Roy, "Towards connected living: 5G enabled Internet of Things (IoT)," *IETE Tech. Rev*., vol. 36, no. 2, pp. 190–202, 2019.
38. T.Q. Duong, X. Chu, and H.A. Suraweera, Eds., Ultra-Dense Networks for 5G and Beyond: Modelling, Analysis, and Applications. Hoboken, NJ, USA: Wiley, 2019.
39. J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large- scale health data," *IEEE Internet Things J*., vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
40. P. Xi, X. Zhang, L. Wang, W, Liu, and S. Peng, "A review of blockchain-based secure sharing of healthcare data." *Appl. Sci*., vol. 12, pp. 7912, 2022.
41. J. Adamu, R. Hamzah, and M.M. Rosli, "Security issues and framework of electronic medical record: A review," *Bull. Electr. Eng. Inform*., vol. 9, pp. 565–572, 2020.
42. Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *J. Med. Syst*., vol. 43, no. 1, p. 5, Jan. 2019.
43. K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, A blockchain-based approach to health information exchange networks. HealthIT.gov. 2016
44. P. Zhang, J. White, D.C. Schmidt, and G. Lenz, "Applying software patterns to address interoperability challenges in blockchain-based healthcare apps." ArXiv Preprint posted online on June 5, 2017
45. R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *J. Econ. Perspect*., vol. 29, no. 2, pp. 213–238, May 01, 2015.

46. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," *IEEE Access*, vol. 6, pp. 11676–11686, 2018.
47. A. Margheri, M. Masi, A. Miladi, V. Sassone, and J. Rosenzweig, "Decentralised provenance for healthcare data," *Int. J. Med. Inform.*, vol. 141, pp. 104197, 2020.
48. H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Jul. 2019, pp. 44–51.
49. M.R. Bataineh, W. Mardini, Y.M. Khamayseh, and M.M.B. Yassein, "Novel and secure blockchain framework for health applications in IoT," *IEEE Access*, vol. 10, pp. 14914–14926, 2022.
50. Z. Zulkifl et al., "FBASHI: Fuzzy and blockchain-based adaptive security for healthcare IoTs," *IEEE Access*, vol. 10, pp. 15644–15656, 2022.

8 Ensemble Based Feature Selection Method for DDoS (EBFM-DDoS) Attack Detection of Healthcare Data in the Cloud Environment

A. Somasundaram, S. Devaraju, V.S. Meenakshi, S. Jawahar, M. Manimaran, and M. Thenmozhi

8.1 INTRODUCTION

DDoS attack results in an unacceptable and extended unavailability of cloud facilities for genuine users. The impetus behind DDoS attack may be related to political, emotional, financial, commercial, or personal gain, such as competition, hacking, cyber warfare and exploitation resulting from stress, among other factors. There exist two distinct classification categories for the credentials of DDoS attacks, namely misuse detection and anomaly detection. Identifying attacks based on misuse entails the examination of network traffic through the utilization of predetermined patterns. Conversely, the lateral approach involves detection of such attacks by meticulously scrutinizing data derived from customary usage.[1]

However, the finding and grouping of attacks from normal traffic start from the feature mining and assortment phase. Any initial step in creating a model starts from the collection or extraction of data. For the DDoS detection model, various parameters from network traffic are to be extracted which is crucial as the network data contains numerous information about source and destination hosts. It is imperative to acknowledge that not all mined features are essential for the finding or classification of DDoS attacks. Mostly, it contains irrelevant and redundant data, the handling of which handling may take excessive time to train prototypical and test them appropriately.[2]

Additionally, processing the inappropriate attributes does not only increase the time and complexity of the overall defense system and considerably reduce detection accuracy.[3] It is obvious that the caliber of the yield is contingent upon the caliber of the input that is introduced into the system model. To ensure the simplicity, comprehensibility and rationality of the prototypical, it is imperative to minimize the

DOI: 10.1201/9781032711379-8

number of features included therein. Consequently, it is incumbent upon us to identify features that are pertinent to the study at hand.

Feature selection has become the most extensively used, significant and vital method in several applications including image and pattern recognition, text categorization, bioinformatics, clustering, rule mining, statistical and machine learning and even system and network monitoring specifically for identifying irrelevant and redundant attributes. These irrelevant and redundant attributes are also termed outliers and thus outlier mining is essential in all fields.

Feature selection focuses on identifying the best subset of a feature set that represents the entire feature set based on which the learning model is built. The technique for selecting features might be characterized into three primary classifications within supervised learning, specifically filter techniques, embedded techniques and wrapper techniques.

The filter method utilizes statistical analysis to appraise the importance of attributes related to the target variables. The process mentioned above assesses each attribute and assigns a rank to it based on various metrics, including distance, the correlation among the attribute and the class variable and information gain.[4] This method has fit for great dimensional data as it offers the best results with high performance, less computational complexity and high speed.

Wrapper methods employ a search algorithm that assesses all feasible feature subsets by means of learning quality. The subset of optimal features that yields superior learning quality is chosen to train this model. This method is effective when the predictive accuracy is predominant and the underlying serious applications are not interested in computational speed and simplicity as they are time-consuming.[5]

Embedded techniques utilize wrapper and filter methods and employ iteration to determine the most advantageous features while simultaneously reducing computational expenses. However, in contrast to filter methods, wrapper and embedded techniques trust a specific classification algorithm to find significant features from subset.

At beginning of feature selection model evolution, single feature selection models are highly utilized for selecting significant attributes connected to the study. Notwithstanding, the emergence of novel concepts and the conduct of extensive investigations in the arena of feature selection have led to the increased significance of integrating feature selection models to select attributes pertinent to the study. This is attributed to the enhancement of the overall performance of learning models. The main idea behind combining the models for selecting features is that it utilizes the advantages of all models used in the combination to eliminate the redundant and irrelevant attributes.

The utilization of multiple models in lieu of a single model to attain an effective outcome by enhancing the overall precision of the entire learning model is commonly referred as the ensemble model. The idea is to combine several frail apprentices to form a strong learner. This knowledge of grouping different methods is also signified as meta-algorithms. The Model of Ensemble is a grouping of different methods employed by gathering the output formed in healthcare at the cloud environment by every method with the following targets:

1. Reducing the model errors
2. Maintaining generalization

The end outcome of the different methods can be combined in numerous methods namely sum, weighted average, simple and count.

Section 8.2 provides an algorithm for the selection of feature which depend on an ensemble base, which improves the efficiency of identifying DDoS attacks. The present method introduces the Ensemble based Feature Selection Framework (EBFM-DDoS), a hybrid technique used to select the useful features which combines filter, wrapper and embedded methods. The EBFM-DDoS works with embedded methods such as Gains Ratio (GR) and Chi-Square Approach (CSA).

8.2 PROPOSED ENSEMBLE BASED FEATURE SELECTION (EBFM-DDOS)

This section presents a selection of features with the help of selection models that have been exactly shaped to distinguish and select remarkable features that hold significance. The procedure of feature selection involves the recognition of a suitable subcategory of features which can proficiently ascertain traffic as either typical or anomalous. The proposed process for choosing features has been validated through the use of a classification model in order to determine its efficacy in improving performance in healthcare at the cloud environment.

This hybrid model capitalizes on the advantages of various feature selection methods, namely, wrapper, hybrid and filter to attain optimal results. Figure 8.1 shows the workflow of proposed ensemble-based architecture

At the outset, the traffic data is gathered from the network, encompassing diverse attributes pertaining to both regular and malicious traffic. Subsequently, the collected traffic data undergoes normalization to adjust the values to a suitable scale for subsequent processing. The model proposed employs statistical normalization.

Next, the salient characteristics pertinent to the investigation are carefully chosen and subsequently employed in prevention and detection procedures to ensure the efficient execution of attack detection. The EBFM-DDoS is a hybrid methodology that amalgamates diverse feature selection methods.

The present study employs the Chi-Square Approach (CSA) and Gains Ratio (GR) methods from the filtering technique, Recursive Feature Elimination (RFE from the wrapper technique, and Least Absolute Selection and Shrinkage Operator (LASSO) from the embedded technique. The aforementioned approaches are utilized to choose a subcategory of significant features, which are subsequently combined. To calculate the efficacy of the proposed selection progression, the selected attributes are fed into various standard classifiers, and results are subjected to further analysis.

8.2.1 Statistical Normalization

After the collection of traffic data from the network, the subsequent step involves data normalization. This is a crucial preprocessing step that must be undertaken in any data mining application, its significant impact on accuracy of classification or prediction results. The input data of good quality will always effectively contribute to the quality result. Specifically, data normalization plays a major role in data preprocessing in which the given range of input data is normalized or scaled

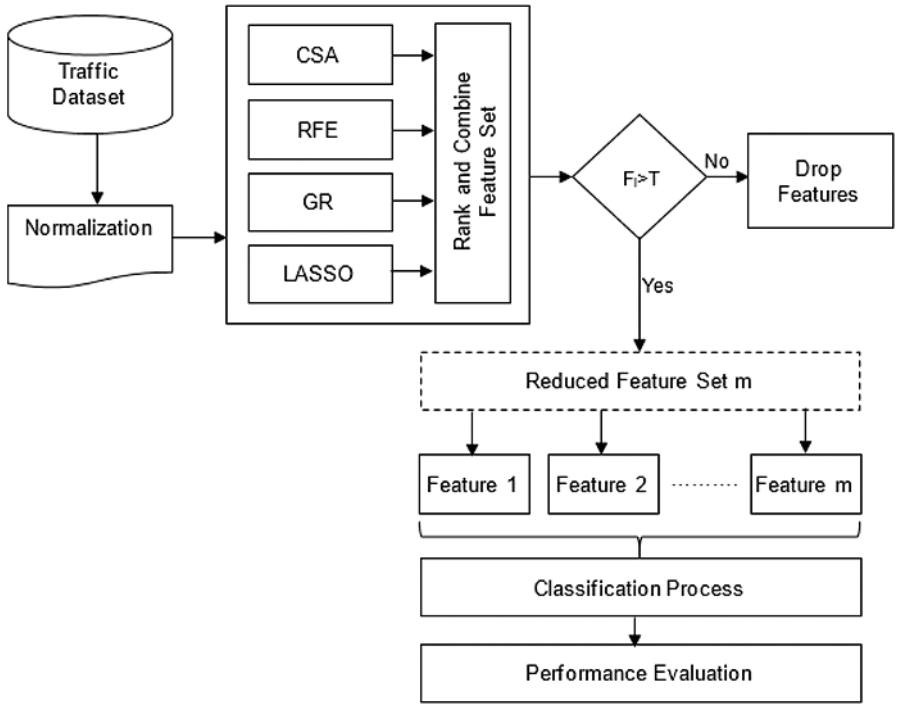

FIGURE 8.1 Overall Process of Proposed Ensemble-based Feature Selection.

to a particular form such that the effect of one data will not affect another. Many network-related datasets are not normalized, however, it is proved in literature that features normalization is vital for any detection-based applications in healthcare at the cloud environment.[5]

Owing to the significance of feature normalization in detection or mining, there exist various types of data normalization in literature such as:

1. Min-max or mean range [0, 1] normalization
2. Statistical or standard normal distribution-based normalization
3. Ordinal or rank-based normalization
4. Frequency or count-based normalization

The next question to be answered is which type of normalization should be chosen for the underlying detection model. Specifically, network traffic data, the standard data normalization, is proved to be effective as it increases the detection process accuracy precisely for the large dataset.[6] Thus, the proposed model exploits the use of statistical normalization for effective results.

The procedure of statistical normalization entails the modification of the given input value through the conversion of data found from a normal distribution to the

standard normal distribution. The general expression can be articulated, as exemplified in Equation (1).

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}} e^{\frac{-1}{2}\left(\frac{x-\mu}{\sigma}\right)^2} \tag{1}$$

In the present context, the symbol μ denotes the statistical measures of central tendency, namely the mean, median, mode, or expectation of the distribution. The parameter σ signifies the standard deviation, which is related to the variance as σ^2.

The standard normal distribution has been defined as a particular type of normal distribution. This distribution arises when the mean is zero and the variance is one ($\mu = 0$ and $\sigma = 1$). Equation (2).

$$\varphi(x) = \frac{e^{\frac{-x^2}{2}}}{\sqrt{2\pi}} \tag{2}$$

Thus, the statistical normalization for the input data can be performed as in Eq. (3).

$$x'_A = \frac{x_A - mean(x_A)}{std(x_A)} \tag{3}$$

Here $mean(x_A)$ represents the average of n values for attribute A and $std(x_A)$ represents the standard deviation of which the value is computed as in Eq. (4).

$$std(x_A) = \sqrt{\frac{1}{n}\sum_n (x_A - mean(x_A))} \tag{4}$$

The constraint for using statistical normalization is that the attribute values must be normally distributed and records specified as n must be larger concerning the central limit theorem.[7] Also, the range of values of an attribute after applying statistical normalization mostly lies between [-3, +3] which is different from other normalizations such as min-max normalization that lies between [0, 1].

8.2.2 Recursive Feature Elimination (RFE)

The RFE method is applied to eliminate features which measured unimportant and extract the most important features of a prototype RFE arranges features in a specific order based on their rank and eliminates the feature with the lowest rank. In the event that function becomes disabled, due to RFE, it will reinstate and eliminate the feature that holds the least significance in healthcare at the cloud environment. The aforementioned procedure is iterated until a pre-established quantity of characteristics, as

delineated in citation,[8] are obtained. The RFE technique operates by minimizing the cost function as presented in Equation (5):

$$J = \frac{1}{2}\alpha^T \mathrm{H}\alpha - \alpha^T l \tag{5}$$

The matrix H is defined as having values *yiyjK(xi, xj)*, while l represents an l-dimensional vector consisting entirely of ones.

The cost function can be updated after removing an attribute f, then computing the matrix H which os characterized as *H(-f)* and *(-f)* specifies the removal of an attribute f. The variations in the cost function can be computed as in Eq. (6):

$$\Delta J\left(f\right) = \frac{1}{2}\alpha^T \mathrm{H}\alpha - \frac{1}{2}\alpha^T \mathrm{H}\left(-\mathrm{f}\right)\alpha \tag{6}$$

Thus, technically, the features having minimum cost function $\Delta J\left(f\right)$ implies that the feature is not significant and thus can be removed. In the proposed model, the ranks are assigned to features based on their values obtained from the cost function with the least ranks for the higher values and vice versa.

8.2.3 Chi-Squared Approach

The Chi-Square test, denoted by the symbol ($\chi 2$), is a statistical technique employed for the analysis of categorical data and the assessment of the correlation between two variables. The $\chi 2$ statistic is utilized to ascertain the level of independence among individual feature and objective variables. Furthermore, it identifies features which possess the highest $\chi 2$ scores.[9] The test utilizes data variables, namely the observed count O and the expected count E, to mathematically determine the extent of deviation in healthcare at the cloud environment. The formula for computing the Chi-Square measures is presented in Equation (7):

$$\chi_{\mathrm{c}}^2 = \Sigma \frac{\left(O_i - E_i\right)^2}{E_i} \tag{7}$$

In the realm of statistical analysis, the variable denoted as c represents DoF, while O signifies detected value between o and E denotes predictable value of s.

With this mathematical logic for selecting significant features, the Chi-Square Approach (CSA) identifies the deviation between the dependent attributes and the independent attributes called predictors or target class. The characteristics are evaluated and ordered according to the degree of interdependence among the two variables. As the interdependence degree between the attribute and the target class variable increases, the attribute's ranking as per its efficacy for classification purposes

decreases. Consequently, a rise in the level of interdependence among attribute and target class variables specifies that the anticipated and observed values are in close proximity, resulting in a minimal Chi-square score.

The common steps in performing Chi-Square test are:

- Outlining null hypothesis that attribute and class attribute are independent and alternative hypothesis that the attribute and class attribute are dependent.
- Constricting the contingency table based on unique values of the attributes with one representing the row and other representing the column. Each element represents the count of records with the specific values of the attributes.
- The determination of the degrees of freedom (df) as achieved by multiplying the alteration among number of rows (n) and one, and the alteration among number of columns (m) and one, in the contingency table.
- Constructing the contingency table to hold expected values. The expected value at each cell *i* is computed as $E_i = c\ X\ p$, where the variables *c* and *p* indicates the total instance count and possibility of two variables with specific values as $p = p(a)\ X\ p(t)$. *p(a)* and *p(t)* refer to the probability of the specific values of an attribute and the target attribute.
- The Chi-Square value is ascertained by utilizing the formula provided in Equation (7).
- Finally, the Chi-Square critical value can be computed at 95% confidence level and computed degree of freedom *df*. The acceptability of the hypothesis can be established if the Chi-Square value calculated is below the critical region, thereby indicating that the computed value lies within the acceptance region. If the hypothesis is accepted, then specific attribute *a* is not depending on the class attribute *t* and thus it can be eliminated.

8.2.4 Least Absolute Selection and Shrinkage Operator (LASSO)

LASSO is a commonly employed tool in both statistical analysis and machine learning methodologies. This regression-based model is designed to address the challenge of high dimensionality data by incorporating information that minimizes overfitting and enhances the precision of prediction and interpretation in healthcare at the cloud environment. The efficacy of LASSO in selecting a significant subset of features is contingent upon a constraint.

The regression model is limited through utilization for the sum of squares of weights. LASSO employs *l1* normalization, wherein the tuning parameter served to measure shrinkages.[10] Thus, the objective of the LASSO is to minimize the standard least square technique as a function given in Eq. (8):

$$\min_{\theta} \frac{1}{2} \left\| (Z - \Phi\theta) \right\|_2^2 \tag{8}$$

The above equation can be rewritten in its Lagrange form as in Eq. (9):

$$\min_{\theta} \frac{1}{2} \left\| (Z - \Phi\theta) \right\|_2^2 + \lambda \left\| \theta \right\|_1 \tag{9}$$

Here, $\|.\|_2$ represents the *l2* Euclidean norm form and $\|.\|_1$ denotes the *l1* norm.

The regularization parameter λ that lies between λ_{min} and λ_{max} controls the adjustments between error and sparseness. It improves the accuracy in terms of prediction. The method seemed to be effective for identifying the reduced set of attributes for further processing.

8.2.5 Gain Ratio Approach

The Gain Ratio (GR) is metric indicating the proportion of information obtained in relation to the intrinsic information. The Information Gain (IG) algorithm aims to mitigate the issue of multi-valued attributes in healthcare at the cloud environment. This approach considers both the quantity and magnitude of branches when selecting attributes. The GR technique employs the calculation of intrinsic information, which involves entropy distribution and instance distribution, to modify the IG and accommodate splitting.[11] The calculation of GainRatio as specified feature x and feature y may be articulated and demonstrated in Equation (10):

$$GainRatio = \frac{Gain(x, y)}{inherent\_info(x)} \tag{10}$$

where the information gain *Gain(x,y)* and the *inherent_info (x)* are computed as in Equations (11), Equation (12) and Equation (13) respectively:

$$Gain(x, y) = Entrop(S) - \sum \frac{|S_i|}{|S|} E(S_i) \tag{11}$$

$$Entrop(S) = \sum_i - p(c_i) \log_2 p(c_i) \tag{12}$$

$$inherent\_Info(x) = - \sum \frac{|S_i|}{|S|} * Log_2 \frac{|S_i|}{|S|} \tag{13}$$

where |S| represents the total count of potential values for a given feature x, $|S_i|$ denotes the specific functional value of feature x, and $p(c_i)$ signifies the likelihood of a class c_i.

The GR model biases the decision tree besides allowing for the features to have a large number of unique values and resolves the downside of information gain.

8.2.6 Constraint Based Majority Voting

On applying the models such as Chi-square, GR, RFE and LASSO, the model results in a set of ranks $\{R_1, R_2, \ldots . R_n\}$ for all the attributes from each specific model. These ranks are to be processed in such a way to make the decisions on identifying the significant attributes for feature selection. The results can be combined in various ways such as majority voting, applying weights and so on. A proposed model and the statistical examination have been conducted for computing the significance of an attribute and constraint-based majority voting for selecting the attributes.

For each specific method, the selected features that meet the given threshold are selected as significant features for further study. Thus, for a feature to be selected as a significant one, then it is available at least in *m* models with the top *k* ranks. Here *m* is the quantity of methods applied in the proposed ensemble method i.e. four (CSA, GR, RFE and LASSO).

To conduct the experimental analysis by computing the ratio of total features (*tf*) present in the given dataset to the quantity of (*m-1*), the formula to compute the value of top rank *k* is given in Eq. (14):

$$k = \frac{total\ features}{(m-1)} \tag{14}$$

Thus, *m* is the model number in the ensemble-based methods and the threshold is set as three fourth of techniques (*m*) used in model (three out of four methods).

The algorithm pseudocode for the proposed ensemble-based feature selection model with constraint-based majority voting is presented in Figure 8.2.

Comprehensive examination is to assess efficiency of the EBFM-DDoS method. The preliminary examination entailed application of the NSL-KDD dataset, which encompasses 41 distinct features. The proposed model was subjected to this dataset, and the JRip classifier was used to select 13 highly significant features from the list. The outcomes derived from the suggested model were juxtaposed with those of alternative ensemble models, including CSA, RSE, LSSO and GR. The EBFS model demonstrated superior results of various factors like accuracy, false positive, sensitivity and specificity, with an improvement of approximately 2% over the other individual models. Although the proposed model consumed more time, approximately 0.71 seconds more than other individual classifiers, the performance metrics were optimally matched from existing models.

Additionally, to showcase the effectiveness of EBFM-DDoS, a metaphorical examination has been experimented among the outcomes derived from datasets NSL-KDD, KDD and those obtained from other extant feature selection models, namely correlation-based model, filter-based model utilizing correlation, consistency, INTERACT, gradual feature removal, linear correlation-based model, and ensemble-based Multi-filter. The findings specify that the EBFM-DDoS surpasses

Input: A dataset comprising with n features $X = \{f_1, f_2, f_3, \ldots, f_n\}$;

$FSA_m = \{CSA, LASSO, GR, RFE\}$;

Output: Dimensionally reduced data set $X' = \{f_{(1)}, f_{(2)}, f_{(3)}, \ldots f_{(r)}\}$, where $r < n$.

Procedure feature_select()

Begin

1. $Rank_i = \{\}$, $X' = ?$
2. Apply training dataset having n features
3. For each FSA method in FSA_j
4. Set the cross-validation fold as 10
5. Compute R_{ij} ranks for all the features in the given dataset.
6. Sort the features $\{f_1, f_2, f_3, \ldots, f_n\}$ based on their ranks
7. End For
8. Compute the value of k for selecting top k features as $k = n / (m-1)$
9. Compute the threshold T as (3/4) x m
10. For each ranked list R_j
11. Select the top k ranked list
12. Compute feature_count(f_n), the occurrence of each feature f_n from the top k ranked list
13. End For
14. For each feature i from 1 to n
15. If feature_count(f_i) > T then
16. $X' = X' \cup f_i$
17. End If
18. End For
19. Return reduced feature set X'

End Procedure

FIGURE 8.2 Algorithm for Proposed Ensemble-based Feature Selection.

the aforementioned models as per computation time and accuracy, as it selects an optimized number of significant features.

8.3 ENSEMBLE BASED FEATURE SELECTION METHOD (EBFM-DDOS)

An experimental investigation was conducted to calculate the efficacy of the EBFS-DDoS model. The experiments were conducted utilizing hardware and software resources, characterized by an Intel Core i3-4005U CPU @ 2.00GHz, 8GB RAM and a 64-bit Windows OS. The analysis employed an EBFM-DDoS to extract the most relevant features in healthcare data at the cloud environment.

The prototypical proposed significant features selection have been subjected to evaluation using various classifiers to identify performance of EBFM-DDoS in

healthcare data at cloud infrastructure. The investigation was conducted by employing version 3.9.3 of the Weka tool. Weka is a free-open-source application which provides the tools for data preprocessing, application of diverse ML algorithms and visualization of outcomes.[12]

8.3.1 Dataset Used for Initial Analysis

For the purpose of an initial assessment, the proposed model has undergone analysis utilizing the NSL-KDD dataset. Every feature had been characterized as either conventional or unconventional, or designations enumerated in Table 8.1. The basic feature group includes features related to the TCP/IP link, while operational features indicate the environment is considered as mistrustful or not. The traffic characteristics are evaluated through use of a connection window, which enables analysis of properties.

For evaluation of the proposed system, 20% of Train 20 records are used for training data from the NSL-KDD database and the Train+ training set. The circulation of classes namely Normal, DoS, Probe, R2L and U2R in the dataset shown in Table 8.2 shows total entries in each train, 20%, train + and test + sets.

Thus, from the statistical analysis, NSL-KDD comprises 52.1% of Normal traffic, 9.42% of Probe attacks, 36.08% of DoS attacks, 0.074% of U2R and 2.36% of R2L attacks respectively. This analysis displays that DoS attacks are the most common and

TABLE 8.1
Categorization of Attacks in NSL-KDD Dataset

Attack Types	Classification of attacks
Denial of Service Attack – DoS	back, pod, neptune, smurf, land, teardrop
Probing attack – Probe	warezclient, warezmaster, ftp_write, imap, multihop, phf, guess_passwd,spy
User to Root Attack – U2R	rootkit, loadmodule, buffer_overflow, perl
Root to Local attack – R2L	portsweep,ipsweep, satan, nmap

TABLE 8.2
Classification Distribution of NSL-KDD

	Instances Number					
Category	**Total**	**Normal**	**Probe**	**DoS**	**U2R**	**R2L**
Train 20%	25192	13449 (53%)	2289 (9.16%)	9234 (37%)	11 (0.04%)	209 (0.8%)
Train+	125973	67343 (53%)	11656 (9.11%)	45927 (37%)	52 (0.04%)	995 (0.85%)
Test+	22544	9711 (43%)	2421 (11%)	7458 (33%)	67 (0.29%)	2887 (12.8%)
Total	173709	90503 (52.10%)	16366 (9.42%)	62619 (36.08%)	130 (0.07%)	4091 (2.36%)

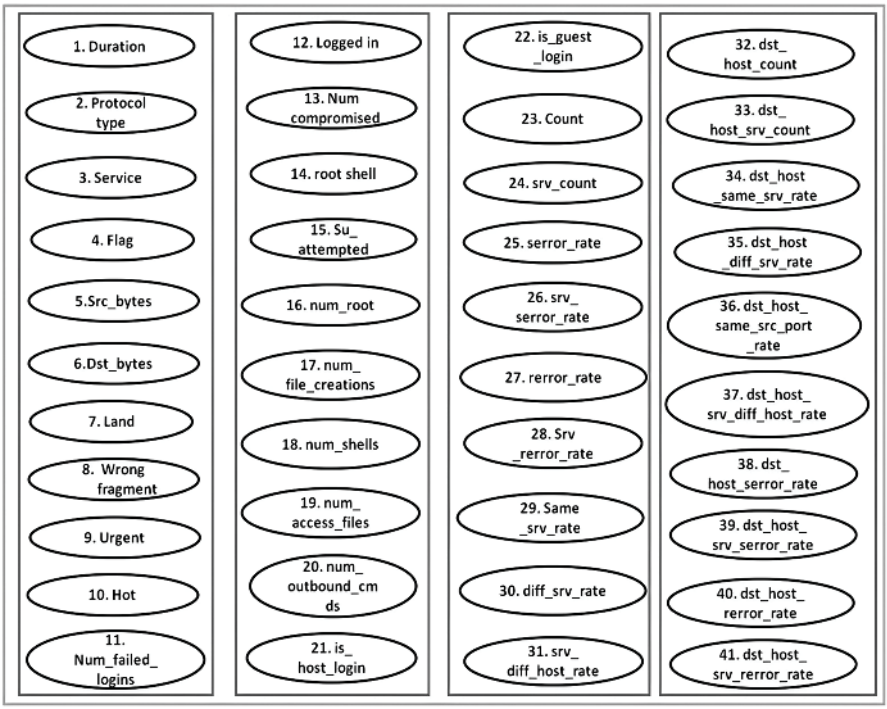

FIGURE 8.3 Features List in NSL-KDD Dataset.

frequently occurred in the network traffic. Also, the rate of training samples applied for analysis is 87% whereas the remaining 13% is applied as a test sample for which the model will identify the attack from normal traffic.

The NSL-KDD categorical and numerical features are itemized in Figure 8.3.

8.3.2 Experimental Analysis for DDoS

The proposed prototypical outcome for feature selection is under consideration, which incorporates statistical normalization and an ensemble-based feature selection algorithm, demonstrating a diminished dataset comprising 12 noteworthy features. This was achieved by implementing the constraint-based majority voting technique, which satisfies the predetermined threshold value, based on the outcomes obtained from diverse filtering, wrapper, and embedded approaches, namely CSA, LASSO, GR and RFE in healthcare data at cloud environment.

Table 8.3 displays the ranked features based on their significance using the four feature selection approaches with significant features selected as output after applying the constraint-based majority voting. In the proposed model, the k for the top k features is computed as 41/3 which is equal to 13. Thus the top 13 features were designated for further examination in which the number of occurrences of each attribute in the four-feature selection method is computed. The threshold value is

TABLE 8.3
Features Ranked in Order for Various Methods

Filter Method	Ranked Features	Top k Features
CSA	2, 40, 3, 39, 33, 4, 38, 6, 37, 29, 5, 23, 32,25, 1, 20, 26, 35, 22, 31, 24, 28, 30, 21, 34, 7, 10, 19, 9, 27, 16, 11, 13, 8, 12, 41, 36, 18, 17, 14, 15	2, 40, **3, 39, 33, 4, 38, 6,** 37, **29, 5, 23,32**
RFE	25, 34, 32, 22, 30, 38, 23, 16, 20, 5, 6, 21, 9, 24, 36, 2, 39, 37, 3, 27, 28, 18, 14, 4, 17, 15, 13, 11, 26, 29, 35, 1, 7, 33, 12, 41, 40, 10, 8, 30, 19	25**, 34**, **32**, 22, **30, 38, 23**, 16, 20, **5, 6,** 21, 9
LASSO	29, 33, 39, 34, 25, 26, 30, 23, 32, 4, 3, 28, 41, 36, 9, 20, 37, 24, 38, 22, 31, 27, 21, 1, 5, 3, 19, 16, 7, 8, 2, 11, 40, 10, 13, 6, 15, 17, 18, 14, 12	**29, 33, 39, 34,** 25**,** 26, **30, 23,32**, **4, 3,** 28, 41
GA	2, 3, 34, 39, 4, 33, 38, 37, 27, 5, 29, 30, 6, 25, 35, 22, 32, 23, 26, 20, 31, 28, 1, 24, 40, 7, 10, 19, 9, 21, 16, 11, 13, 8, 12, 41, 17, 18, 14, 36, 15	2, **3, 34, 39, 4, 33, 38,** 37, 27, **5, 29, 30, 6**
Selected Features	*3, 4, 5, 6, 23, 29, 30, 32, 33, 34, 38, 39*	

computed as (3/4) x m where the variable m is the amount of techniques employed in the model and so the threshold value T is set as 3.

Thus, the attributes that occurred in at least three feature techniques used in the study at the top k positions are selected as the significant attributes.

It is noteworthy that the proposed ensemble model employs conventional yet potent techniques, namely CSA, LASSO, GR and RFE. Nevertheless, it can be expanded to incorporate any number of techniques to enhance the model's performance. The proposed algorithm identifies features that appeared in 75% of the techniques utilized in the model as significant for the study.

The EFSM algorithm that has been proposed selects a total of 12 features, namely 3, 4, 5, 6, 23, 25, 29, 30, 33, 34, 38 and 39, which meet the computed threshold value of 3. The performance characteristics is delineated in Table 8.4.

8.3.3 Result Analysis for EFSM

The assessment of performance is an essential instrument utilized to appraise the classification process, guaranteeing the dependability and the precision of its outcomes in detecting attacks. A preliminary analysis was conducted to estimate the reduced dataset using the JRip classifier, a proposed rule learner called Iterative Recursive Intersection to Produce Error Reduction (RIPPER).[13]

The efficacy of various feature selection methods, namely the Chi-Square Approach (CSA), Recursive Feature Elimination (RFE), Gain Ratio (GR), Least Absolute Selection and Shrinkage Operator (LASSO), and proposed model, has been assessed using the JRip classifier in healthcare data at the cloud environment. The results of experimental outcomes pertaining to security parameters, encompassing

TABLE 8.4
Description of Nominated Features from NSL-KDD Dataset

Attributes	Description
F.no.3-service	Destination coverage network
F.no.4-flag	Link Status – nominal error
F.no.5-src_bytes	Number of bytes sent between beginning and end
F.no.6-dst_bytes	Amount of single bytes sent between end and beginning
F.no.23-count	No. of connections similar host at the older two seconds
F.no.29-same_srv_rate	Percentage of similar service connections
F.no 30-diff_srv_rate	Percentage of dissimilar services connections
F.no.32-dst_host_count	No. of similar destination host IP address connections
F.no.33-dst_host_srv_count	Percentage of connections similar facility, aggregated in the destination host count
F.no.34-dst_host_same_srv_rate	Percentage of different services connections, aggregated in destination host count
F.no.38-dst_host_serror_rate	% of SYN errors from same host to the destination host connections
F.no.39-dst_host_srv_serror_rate	% of with SYN errors from same service to destination host connections

TABLE 8.5
Performance Evaluation of Individual and Collective Feature Selection

Feature Selection Techniques	Accuracy (%)	Detection Rate (%)	False Positive (%)	Sensitivity (%)	Specificity (%)	Time in (in Seconds)
No feature selection	97.22	97.17	2.83	97.26	97.15	1.28
CSA	98.23	98.24	1.76	98.23	98.42	2.29
RFE	98.02	98.13	1.87	98.01	98.09	2.53
LASSO	98.27	98.31	1.69	98.26	98.47	2.47
GR	98.33	98.15	1.85	98.33	98.47	2.27
Proposed Ensemble	99.79	99.82	0.18	99.79	99.82	2.98

false-positive rate, detection rate, sensitivity and specificity, along with performance parameters namely evaluation time, have been scrutinized and the findings are depicted in Table 8.5.

In every feature selection scheme, namely, the Chi-Square Approach (CSA), is accompanied by a presentation of sensitivity, accuracy and specificity values in Table 8.5. The aforementioned values are also visually represented in Figure 8.4 with the intention of facilitating comprehension. The investigation reveals that the proposed prototypical collective feature selection outperforms the individual classifiers of sensitivity, accuracy and specificity. The proposed model exhibits an approximate 2% increase in performance matched to the other individual models.

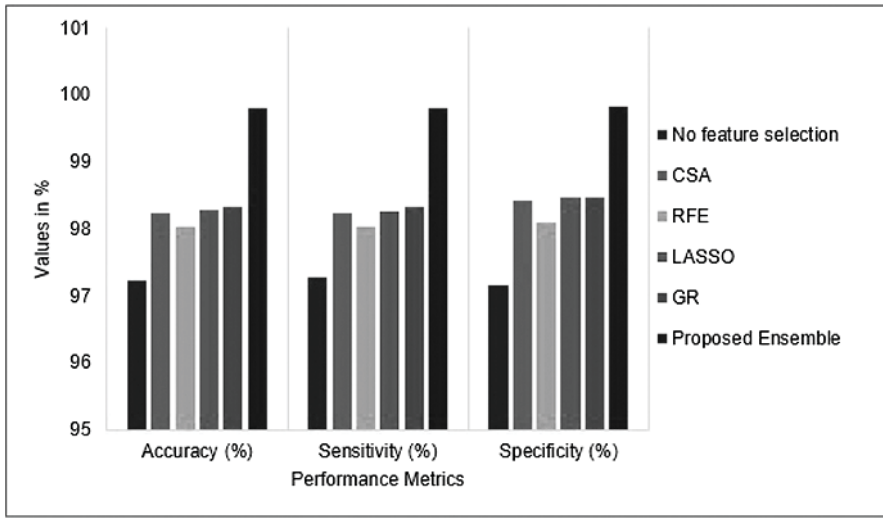

FIGURE 8.4 Performance Comparison with Individual Feature Selection.

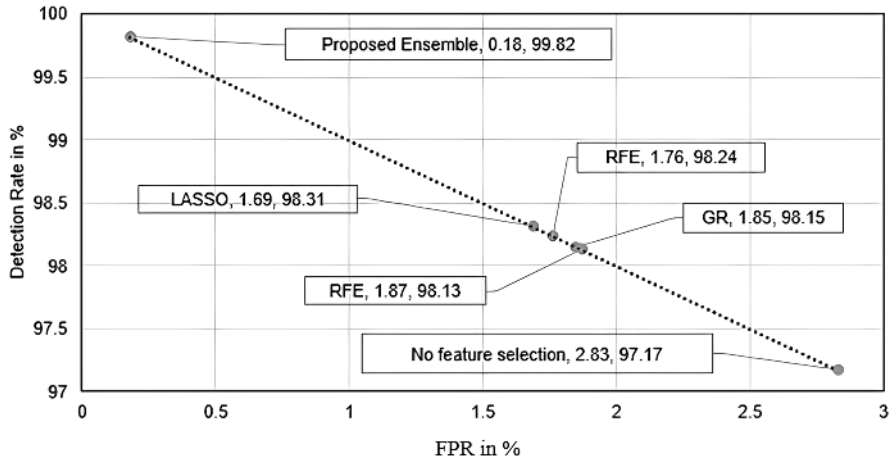

FIGURE 8.5 FPR Vs. DR Comparison with Individual Feature Selection.

Comparison of false-positive rate (FPR) vs. detection rate for a proposed model is matched with individual feature selection methods and without features selection technique in which the proposed model has minimum FPR and maximum detection rate which are critical metrics to be satisfied for any attack detection model in Figure 8.5.

Also, when the performance analysed the execution time in the proposed model, it consumes 22% and other individual feature selection such as CSA, RFE, LASSO, and GR consume 17%, 18%, 18% and 16% respectively whereas the training process consumes 9s of the training time in seconds, as shown in Figure 8.6.

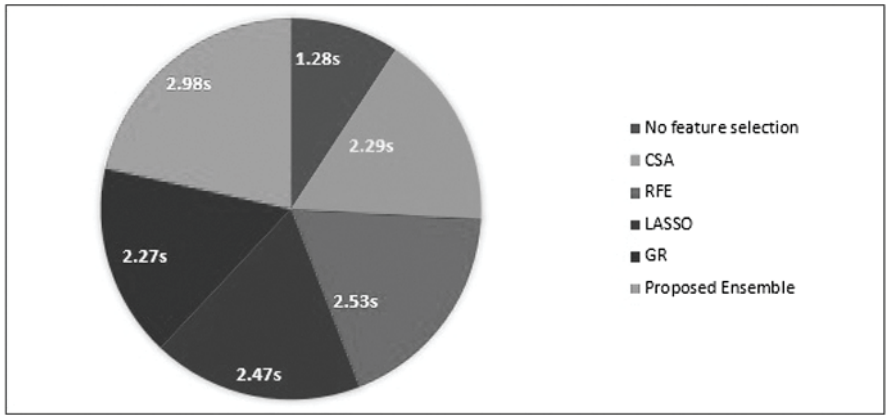

FIGURE 8.6 Execution Time Comparison with Individual Feature Selection.

Upon conducting an analysis, it is obvious that the proposed model requires a greater amount of time, approximately 3%, equating to roughly 0.71 seconds, in comparison to other individual classifiers for training purposes. However, the proposed model achieved the better performance for various parameters compared to other classifiers.

In a subsequent stage of analysis, the proposed ensemble model is subjected to a comparative evaluation in other models. The models utilized for the purpose of comparison include Correlation-based feature selection,[14] Filter based with correlation, consistency and INTERACT,[15] Gradual feature removal,[16] Linear correlation-based,[17] Ensemble-based Multi filter,[3] and Ensemble-based 7 feature selection.[18] The accuracy and build time of the proposed prototypical are matched with existing values. The performance comparison is presented in Table 8.6.

After conducting a comparative analysis, it is determined that the Ensemble based Multi filter, correlation based, and linear correlation feature selection approaches yield superior results that are on par with the proposed ensemble-based feature selection method, it boasts an accuracy rate exceeding 99%. Nevertheless, the proposed model still delivers satisfactory outcomes by selecting an optimized number of significant features. A graphical representation of accuracy rates of both existing and proposed feature selection models is presented in Figure 8.6.

An experiment had been examined on the suggested feature selection, it is based on ensemble. As stated by reference,[19] the assessment of performance has solely been executed on DoS records, as the model proposed and the existing model being compared concentrate on the detection of DDoS attacks.

Therefore, for the purpose of analysis, a grand total of 142,404 samples were collected for evaluation, comprising 87,832 instances of normal traffic and 54,572 instances of DoS attack instances, encompassing a range of DDoS attacks, including smurf, neptune, teardrop, pod, land, and back.[20] Similar to the NSL-KDD dataset, KDD ’99 dataset consists of a total of 41 features (Figure 8.7).

TABLE 8.6
Performance Comparison Using NSL-KDD Dataset

Approach	Classifier	No. of Features	Accuracy (%)	Time to Build the Model (s)
Correlation-based (CFS)	C4.5	NA	99.13	NA
Filter based using correlation, consistency and INTERACT (CCInteract)	HNB_PKI_INT	7	93.72	NA
Gradual Feature Removal (GFR)	Clustering, Ant Colony and SVM	19	98.62	NA
Linear correlation based (LCFS)	C.45	17	99.1	12.02
Ensemble based Multi-filter (EMFFS)	J48	13	99.67	0.78
Ensemble based 7 feature selection (EnFS)	Decision Tree	11	97.1	NA
Proposed Ensemble based Hybrid (EFSM)	JRip	12	99.79	2.98

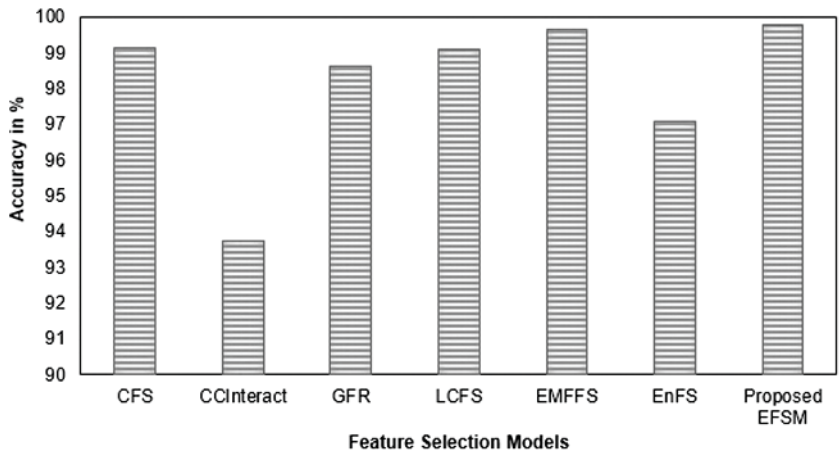

FIGURE 8.7 Accuracy Comparison of Proposed and Existing Models.

This model under consideration selects 16 features from a total pool of 41 features given in KDD cup '99 datasets. The accuracy is measured using the JRip classifier. A comparative examination is done in the proposed method with other existing models. The derived values are tabulated in Table 8.7, which includes specific values for a number of designated features and model accuracy.

TABLE 8.7
Performance Comparison Using KDD cup '99 Dataset

Approach	No. of Features Selected	Accuracy (%)
All features with JRip Classifier	41	99.990
IG and CFS with ANN classifier[21]	25	99.93
Feature Selection with SVM classifier[22]	25	99.5
Mutual Information-Based Hybrid Feature Selection Method[23]	Unknown	98.61
Mutual Information based feature selection[24]	Unknown	99.00
Singular value decomposition with SVM[17]	Unknown	99.25
IR and GR based intersection[19]	19	99.992
Proposed Ensemble based Hybrid (EFSM)	16	99.93

Upon conducting an in-depth analysis of the feature selection phase, it is determined that the proposed model yields superior outcomes compared with numerous existing models utilized for the purposes of comparison.

8.4 CONCLUSION

This work introducing the proposed feature selection prototypical depends on ensemble techniques, which integrate filtering, wrapper and embedded feature selection methods, including the Chi-Square Approach, Gains Ratio, Recursive Feature Elimination, and Least Absolute Selection and Shrinkage Operator, to achieve optimal outcomes in healthcare data at the cloud environment. To combine results of the aforementioned models, the model employs constraint-based majority voting, and an algorithm for the proposed model is presented. The feature selection algorithm proposed in this study was found to efficiently select 13 and 16 important features for NSL KDD and KDD CUP '99 database to accurately identify network traffic as normal or attack. The results are obtained and indicate that the proposed model has yielded an accuracy of 99.79% and an improved detection rate of 99.82%, surpassing the performance of other individual feature selection models as well as many existing models.

REFERENCES

1. Singh, S, Jeong, Y.S., & Park, J.H, "A survey on cloud computing security: Issues, threats, and solutions", *Journal of Network and Computer Applications*, vol. *75*, pp. 200–222, 2016.
2. Peng, J, Choo, K.K.R, Ashman, H, "Bit-level n-gram based forensic authorship analysis on social media: Identifying individuals from linguistic profiles", *Journal of Network and Computer Applications*, vol. 70, pp. 171–182, 2016.
3. Osanaiye, O, Cai, H, Choo, K.K.R, Dehghantanha, A, Xu, Z, Dlodlo, M, "Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing", *EURASIP Journal on Wireless Communications and Networking*, vol. 2016, no. 1, pp. 1–10, 2016.

4. Wang, X, Chen, M, Xing, C, Zhang, T, "Defending DDoS attacks in software-defined networking based on legitimate source and destination IP address database*", IEICE Transactions on Information and Systems,* vol. 99, no. 4, pp. 850–859, 2016.
5. Wang, B, Zheng, Y, Lou, W, "DDoS attack protection in the era of cloud computing and software-defined networking", *Computer Networks*, vol. 81, pp. 308–319, 2015.
6. Wang, W, He, Y, Liu, J, Gombault, S, "Constructing important features from massive network traffic for lightweight intrusion detection", *IET Information Security*, vol. 9, no. 6, pp. 374–379, 2015.
7. Durrett, R, "Probability: Theory and Examples", Wadsworth, Pacific Grove, California, 1991.
8. Masotti, M, "Exploring ranklets performances in mammographic mass classification using recursive feature elimination", In *Sixteenth Signal Processing Society Workshop on Machine Learning for Signal Processing*, IEEE, pp. 265–270, 2006.
9. Moradkhani, M, Amiri, A, Javaherian, M, Safari, H, "A hybrid algorithm for feature subset selection in high-dimensional datasets using FICA and IWSSr algorithm", *Applied Soft Computing*, vol. 35, pp. 123–135, 2015.
10. Kukreja, S.L, Löfber, J, Brenner, M.J, "A least absolute shrinkage and selection operator (Lasso) for nonlinear system identification", *IFAC Proceedings*, vol. 39, no. 1, pp. 814–819, 2006.
11. Karegowda, A.G, Manjunath, A.S, Jayaram, M.A, "Comparative study of attribute selection using gain ratio and correlation based feature selection", *International Journal of Information Technology and Knowledge Management*, vol. 2, no. 2, pp. 271–277, 2010.
12. Mishra, A, Gupta, B.B, Peraković, D, Peñalvo, F.J.G, Hsu, C.H, "Classification based machine learning for detection of DDoS attack in cloud computing", In *International Conference on Consumer Electronics*, IEEE, pp. 1–4, 2021.
13. Cohen, W.W, "Fast effective rule induction", In *Machine learning proceedings*, Morgan Kaufmann, pp. 115–123, 1995.
14. Sathyamoorthy, M, Kuppusamy, S, Nayyar, A, Dhanaraj, R.K, "Optimal emplacement of sensors by orbit-electron theory in wireless sensor networks", *Wireless Networks*, vol. 28, no. 4, pp. 1605–1623, 2022.
15. Koc, L, Mazzuchi, T.A, Sarkani, S, "A network intrusion detection system based on a Hidden Naïve Bayes multiclass classifier", *Expert Systems with Applications*, vol. 39, no. 18, pp. 13492–13500, 2012.
16. 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 Systems with Applications*, vol. 39, no. 1, pp. 424–430, 2012.
17. Dhiviya, S, Malathy, S, Monikha, M, "Enhancing the network lifetime using on demand tree based routing protocol for MANET", In *2018 4th International Conference on Computing Communication and Automation (ICCCA)*, IEEE, pp. 1–6, 2018, December.
18. Das, S, Venugopal, D, Shiva, S, Sheldon, F.T, "Empirical evaluation of the ensemble framework for feature selection in DDoS attack", In *Seventh International Conference on Cyber Security and Cloud Computing (CSCloud)*, *Sixth International Conference on Edge Computing and Scalable Cloud (EdgeCom)*, IEEE, pp. 56–61, 2020.
19. Nimbalkar, P, Kshirsagar, D, "Feature selection for intrusion detection system in Internet-of-Things (IoT)", *ICT Express*, vol. 7, no. 2, pp. 177–181, 2021.
20. Aanjanadevi, S, Palanisamy, V, Aanjankumar, S, "An improved method for generating biometric-cryptographic system from face feature", In *2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI)*, IEEE, pp. 1076–1079, 2019.

21. Dhanaraj, R.K, "A review paper on fog computing paradigm to solve problems and challenges during integration of cloud with IoT", In *Journal of Physics: Conference Series* (Vol. 2007, No. 1, pp. 012017). IOP Publishing, 2021, August.
22. Horng, S.J, Su, M.Y, Chen, Y.H, Kao, T.W, Chen, R.J, Lai, J.L, Perkasa, C.D, "A novel intrusion detection system based on hierarchical clustering and support vector machines", *Expert Systems with Applications*, vol. 38, no. 1,pp. 306–313, 2011.
23. Liu, Q, Shi, S, Zhu, H, Xiao, J, "A mutual information-based hybrid feature selection method for software cost estimation using feature clustering", In *Thirty Eighth Annual Computer Software and Applications Conference*, IEEE, pp. 27–32, 2014.
24. Amiri, F, Yousefi, M.R, Lucas, C, Shakery, A, Yazdani, N, "Mutual information-based feature selection for intrusion detection systems", *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1184–1199, 2011.

9 An Analysis of Identity Management for Digital Healthcare and the Importance of the Medical Internet of Things

A. Sirajudeen, Senthilnathan Palaniappan, Ilayaraja Venkatachalam, S. Saravanan, and T. Anitha

9.1 INTRODUCTION TO IOMT: REVOLUTIONIZING DIGITAL HEALTHCARE

The healthcare segment has recently experienced an important change, driven by more advanced technologies, mostly the smart Medical Internet of Things (IoMT). This invention has essentially changed the digital method of healthcare by creating a network system of unified and interconnected medical approaches and applications offered via the Medical Internet of Things. IoMT enables continuous assortment, exchange and real-time study of health-related information, utilizing devices like wearable fitness trackers, smart insulin pumps, remote patient monitoring systems and implantable sensors to enhance patient care and healthcare outcomes. IoMT relies on data-driven decision-making and continuous real-time nursing, permitting healthcare professionals to remotely observe the patient's vital signs, medication and its adherence and the complete health position. This endless flow of information permits early disease finding, personalized action plans and timely involvements, ultimately refining patient outcomes and lowering healthcare costs. Additionally, IoMT enhances healthcare efficiency by enabling proactive management of chronic conditions and prevention of complications through daily health parameter monitoring by patients and remote patient monitoring by healthcare providers.

Figure 9.1 illustrates the role of smart IoMT in connected healthcare, where data integrity is ensured through encryption for long-lasting performance and

DOI: 10.1201/9781032711379-9

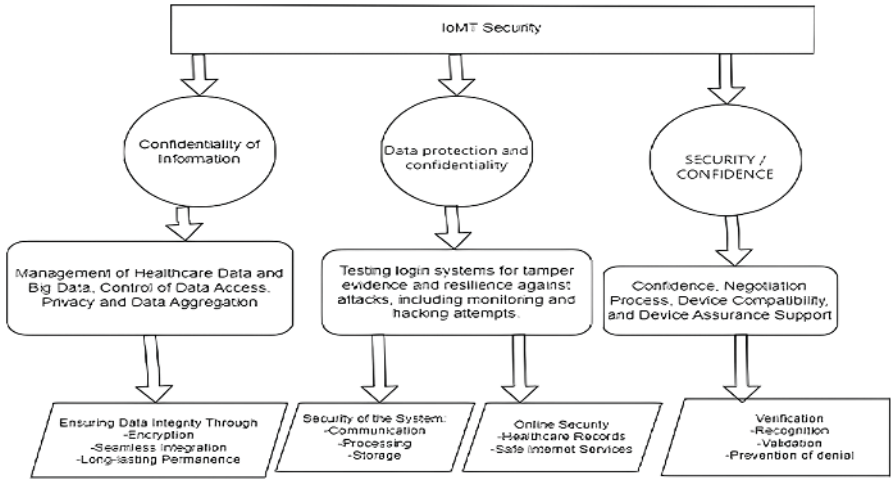

FIGURE 9.1 Role of smart IoMT in connected healthcare.

confidentiality of information from IoMT security offers management of healthcare data. IoMT security's data protection and confidentiality offer resilience to attacks and hacking attempts, testing login systems, and improved processing storage of all, which increase system security. Device compatibility and assurance support are provided by IoMT security, which will enable denial attack detection, identification and prevention. The integration of predictive analytics and machine learning algorithms into healthcare through IoMT provides valuable insights into disease patterns, treatment effectiveness and patient behavior. This data-driven approach supports evidence-based decision-making, fuels medical research and drives innovation, leading to advanced treatments and therapies. However, the extensive adoption of IoMT increases concerns around data safety and confidentiality. To safeguard complex patient data collected by various medical plans, healthy cybersecurity trials such as encryption, secure verification protocols and steady security checks are important. Healthcare management's necessity is to contribute in these trials to preserve the choice and veracity of patient information, and preserve and guard against illegitimate access and cyber uncertainties. IoMT specifies a modal shift in healthcare engineering, transmuting patient care through unified devices and real-time data study. Strengthening and enhancing healthcare facilities not only provides better medical service but also empowers distinct persons to proactively take charge of their health and wellbeing[1,2]. For implementing successful operation of smart IoMT processes has efficiently challenged cooperation between patient healthcare occupations and healthcare technology effectively to indicate a dominant challenge and it is critical to have paramount collaboration. This associated partnership method is crucially geared to modernize to a unified adaptation of combined and most advanced medical measures, which allows patient healthcare to enter effective and safe healthcare facilities for all professional experts.

9.2 NAVIGATING THE IOMT LANDSCAPE: CHALLENGES AND OPPORTUNITIES

In the operation of smart Internet of Medical Things (IoMT) the whole technology works on sophisticated, prearranged medical measures and the structures are intentionally designed for patient healthcare data exchange. This innovative technology holds huge potential for improving patient healthcare in an optimum way to streamline patient healthcare data and and deplete its cost. Further, it also meaningfully positions many challenges that necessitate significant attention. One prime and prominent challenging task in smart IoMT involves certifying combined connectivity across many devices and platforms with medical devices of diverse origin from various combined manufacturers to differentiate various communication protocol standards, to efficiently employ for data investigation and pose recommendation methods to a significant value [3].

The secure way of essential data exposure of patient healthcare data makes a prime mark for handling the cyber-attacks, the necessity for robust safety protection like confound observance and safe confirmation to implement strong HIPAA (Health Insurance Portability and Accountability Act) rules. Steering and handling the multifaceted complex interaction web of approaches and ethics in the patient healthcare industry offers additional challenges. Varied divergence regulations for patients' healthcare information across various countries pose an additional challenge for patient healthcare providers and smart IoMT developers aiming secure systems and also offer innovative additional and secure challenges. The massive amount of data generated for patient healthcare by smart IoMT systems, which establish proficient monitoring of patients and multifaceted measurement with distributed systems for real-time data processing, meaningful analysis and storage, are thus proving a formidable and daunting task. Advanced cutting-edge analytics and machine learning schemes play an essential and crucial role for extracting meaningful actionable insights from information influx [4]. With the more advanced capabilities of smart IoMT skills, ethical debate considerations regarding patient healthcare, patient data ownership and utilization response of AIML (Artificial Intelligence and Machine Learning) usage has become more increasingly significant. The unresolved ongoing issue of reconciling innovative ethical rules is one that poses an imperative ethical principle that investigating councils and innovative healthcare establishments must tackle and address.

Despite the challenges, the IoMT landscape offers numerous opportunities for the healthcare industry. IoMT enables real-time patient monitoring, allowing healthcare providers to remotely track vital signs and manage chronic conditions. This facilitates timely interventions, reduces hospitalizations and enhances patient outcomes data, which can be utilized for predictive analytics, enabling healthcare providers to forecast ailment outbreaks, improve resource provision and make action plans based on distinct patient information. Collaborating IoMT claims empower patients to actively contributein their healthcare. Wearable devices and mobile apps give patients access to their health data, encouraging appointments and developing healthier lifestyles. IoMT solutions optimize healthcare processes by automating tasks, reducing administrative overheads and enhancing overall efficiency. This optimization leads to cost savings and increased patient satisfaction.

9.3 THE EVOLUTION OF IDENTITY MANAGEMENT IN HEALTHCARE

The transformative journey of self-management in the healthcare domain summarizes an advanced and complete service of the systems and practices employed to validate and administer people's identities in the evolution of identity management in the healthcare sector. The implication of identity management in healthcare is supreme, driven by various requirements such as protection, the confidentiality and security of enduring patient data, agreement with regulatory outlines and facilitating seamless and official access to healthcare services.

The landscape of patient healthcare management has evolved in a complex way by spanning various critical dimensions. Traditional ancient methods relying on manual procedures like paper-based records and physical ID (Identifier) cards have given way to significant transformation. The advent of improved numerical technology and capabilities has necessitated and undergone the adoption of automated framework systems such as electronic health records (EHR) and digital authentic verification methods. The integral emergence of EHRs has fundamentally spurred the adoption of an automated reshaped framework, including EHR and digital authenticated systems. The integral of EHR has fundamentally reshaped the identity domain in the healthcare sector, facilitating secure and efficient ways to access streamlined patient data for authorized patient healthcare securely[5]. Employing calculations for identity management in patient healthcare systems can access control over ethically protected patient information and user activities within healthcare settings. An essential advancement in this progression is widespread iteration of adopting biometric validation techniques like iris scan, facial recognition and analysis of fingerprints. Leveraging these biostatics enhances security protocol measures and protects against unrecognized access to sensitive patient healthcare documents. This dynamic mode of robust authentication enhances the accuracy of patient scrutiny, mitigating the potential risk by reducing the threat of identity theft.

Figure 9.2 illustrates Identity Management in IoMT, where healthcare professionals carry small sensor- and tracker-equipped medical equipment which is connected to an access point and can be stored and controlled in software systems using intermediate software. Through streamlining, the rationalized verification process enables Single Sign-On (SSO) credentials to empower patient healthcare experts to gain the

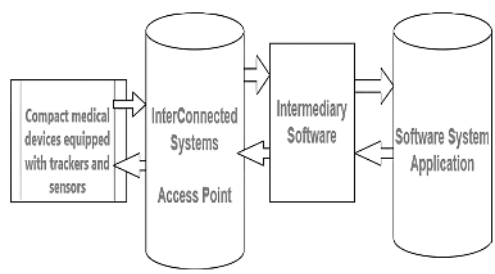

FIGURE 9.2 Identity management in IoMT.

numerous common resources and applications via a set of shared document identification systems, thereby optimizing improved system organizing arrangements and security enhancements by reducing and handling the numerous password keys. In essential patient healthcare management, Role Based Access Control (RBAC) involves assigning specific permissions and roles to distinct tasks in the patient healthcare environmen[6]. This crucial and pivotal function ensures that users are able to access only the task relevant to their patient healthcare roles by mitigating patient risk of data disruptions. Through logical structuring of the Single Sign-On (SSO) verification process, credentials empower patient healthcare professionals to access numerous commonplace resources and applications resources using a shared unified identification document. This streamlines not only organizing system arrangements by reducing the need for individuals to juggle various encrypted password keys, integrally central to patient healthcare identity management, but also Role Based Access Control (RBAC) involves the allocation and assigning of specific, precise roles and permits some roles by particular distinct tasks in the patient healthcare environmental setting. This commendable approach ensures that users exclusively access tasks and information pertinent to their relevant roles, thereby mitigating breaches in the data.

Pondering the existing shift towards patient-centered care, there is a superficial leaning in permitting patients to attain their healthcare information. This development involves the operation of identity administration solutions permitting patients to firmly access and regulate their health records, with a steadfast commitment to privacy and safety. The development of identity management in healthcare indicates a profound change from manual and paper-centric procedures to digital, automatic and cultured systems. The predominant objective is to reinforce security actions, rationalize workflows, ensure supervisory amenability and adapt to the active terrain of healthcare technology.

9.4 THE CRITICAL ROLE OF IDENTITY MANAGEMENT IN IOMT

The fast developments in skills have enabled the blending of assorted devices into healthcare, generating the smart Medical Internet of Things (IoMT). IoMT signifies the system of medical approaches and submissions of reliable consistency via the internet, allowing data exchange to progress patient care and to improve health related processes. Managing individualities is pivotal in this unified network to safeguard the protected and effective operation of IoMT strategies and systems. Identity management within IoMT includes processes and skills to identify, validate and approve users and devices within the system. It manages digital characters, safeguarding that only official persons or systems can access sensitive and complex healthcare data and control medicinal plans and strategies. This is most critical in healthcare, wherever safeguarding patient data is of utmost highest importance.

Figure 9.3 illustrates patient-centered care in smart IoMT, where healthcare providers must respect and regard the patient's dignity in a comfortable physical setting in order to empower the patient's mental worth and improve their mental well-being. Involving the patient's family and friends in the healthcare process and requiring them to offer emotional support and encouragement is a requirement for healthcare professionals. This guarantees the patient's simple access to

FIGURE 9.3 Patient-centered care in smart IoMT.

the treatments they need. Comfort and improved hospital-centric care result from healthcare professionals providing continuous and reliable patient care. A major trial in smart IoMT lies particularly in the throng of hardware and software applications, each having separate identities and entrée requirements. Actual identity management solutions tackle this trial by applying standard protocols and verification methods, allowing uninterrupted interaction between hardware infrastructure and platforms. The identity management enhances the security protocols of the smart IoMT setup by permitting restricted access to solely authenticate the approved users[7]. Additionally, actual identity restricts this method by encompassing validation medical devices, confirming support of the software and hardware grade to protect the accuracy to sustain defense against having uninterrupted changes. By applying a separate identity and entrée requirements in patient healthcare, an improved switching mechanism permits privacy and effectively prevents hateful potential threats such as information breach, and devises medicinal strategies and plans which authorize further, identity

management procedure by streamlining and protecting numerous patient information for user directorial management and device permission.

9.5 PRIVACY CONCERNS IN IOMT: SAFEGUARDING PATIENT INFORMATION

Now currently, there is a distinguished concealed spike in privacy issues within the smart Medical Internet of Things (IoMT). This will increase growth in an essential core future trait for the patient healthcare segment, which improves multiple interconnected fused approaches to direct patient healthcare behavior by supervising healthcare behavior. The smart Internet of Medical Things (IoMT) integrates various corrective medical techniques in a Digital IT (Information Technology) infrastructure, for attractive real-time healthcare treatment and delivery.

One of the primary key interests in smart IoMT is the confidential protection of patient privacy. Biomedical devices like insulin pumps and therapeutic gadgets are examples of gadget devices that gather complex dedicative types of sensitive information about patient healthcare and active information securely. Unauthorized entry to this data could entail a potential risk and could create fatal life-threatening events and phishing impersonation. In order to challenge this anxiety apprehension, device manufacturers need to pay attention and patient healthcare administrators must approve safety measures. Fundamental techniques should employ access technique procedures to encode the control devices to implement the secure spread of data between patient healthcare systems and surveillance monitoring devices.

One primary concern and foremost freight in smart IoMT revolves around core apprehension of patient information. Strategies like medical healthcare gadgets and sensor-based technologies gather sensitive confidential information about patient healthcare and activity engagements. Intrusion access to this data may endanger individual unique risks like theft, scam or even some kind of critical life-threatening event during hazard conditions. To challenge these confronting anxieties, patient healthcare equipment developers and healthcare medical operations must implement protective strategies. Critical methods like incorporation of encoding procedures can authenticate fundamental aspects of access control devices which ensure the safe and protected distributed data sets and healthcare systems. Periodic software improvements and updates are also robust to address susceptibilities and protect against potential cyber threats[8].

Healthcare specialists and patients play vital roles in safeguarding patient data in IoMT. Medical staff need correct training to handle related devices firmly and should be attentive to IoMT-related hazards. Patients must receive instruction about privacy situations on their plans, be encouraged not to inform passwords frequently and counseled to enable multi-factor verification for improved safety. Monitoring the legal and governed frameworks, like Smart Responsibility and Transferability in Health Insurance Act in the USA, are in house to protect Individual patient, client privacy and to switch the use of healthcare information. Understanding these rules and strategies is required for health care employees and device developers to promise the legitimate and ethical usage of patient data.

9.6 DATA INTEGRITY IN IOMT SYSTEMS: A CRUCIAL ASPECT OF IDENTITY MANAGEMENT

The smart Medical Internet of Things (IoMT) creates a structure of prearranged medical plans and schemes planned and organized together, to transmit, exchange and distribute healthcare data. Confirming data integral schemes within smart IoMT schemes is vital as it directly affects the exactness and reliability of medical decisions and treatments. A data integral scheme, within this outline, means ensuring that healthcare data remains accurate and coherent across the entire storing of data structure, communication or processing. Efficiently handling the individual personalities and entrée panels of various devices and users offers a substantial challenge in smart IoMT systems. Identity management is the process of implementing and authorizing access to gain patient entry to comprehensive patient healthcare data.

Smart IoMT breaches in data integrity have serious consequences including inaccurate diagnosis, tangled permissions and compromised patient safety. Malicious cyber attackers could exploit and manipulate medical information resulting in procedural errors and incorrect interventions. In the future, it will be necessary to implement robust, reliable strategies like multifactor confirmation and biometric authentication to improve smart IoMT infrastructure. Employing encryption techniques like SSL/TLS (Secure Socket Layer / Transport Layer Security) guarantees secure and safe transmission of data to interface or preventing unauthorized access during crucial communications, emphasizing the implementation of significant reinforcement measures especially in implementation of the HIPAA in the United States of America. This adheres to regulatory standards of protecting patient information, emphasizing the integrity and protection to safeguard patient information. Authenticating these methods not only offers access to legal compliance but also nurtures a culture of safety and data authenticity in smart IoMT intelligent systems.

9.7 UNDERSTANDING EXISTING IDENTITY MANAGEMENT FRAMEWORKS IN HEALTHCARE

Effective identity management can play a pivotal role in protecting patient healthcare information by enhancing adaptability and flexibility and by eliminating unauthorized access through the collective collaborative sharing of patient data across numerous patient healthcare systems. HLT (Healthcare Life Science Terminology) in FHIR (Fast Healthcare Interoperability Resources) stands out as a valuable tool for distributing microelectronic and nano electronic patient healthcare data safely and offers a robust framework for identity management, which it ensures by facilitating authorized information exchange among approved entities. OpenID link widely employs a secure authentication protocol that enables secure login enhancements and enables access to genuine users for medicinal health records[9].

This fundamental framework allows secure authorization measures, allowing healthcare-associated applications to contribute limited entrée rights to third-party needs, thus helping to maintain data safety and security. SAML (Security Assertion Markup Language), created on XML (Extensible Markup Language), allows the secured data conversation and agreement among party identity workers and service

workers to come together, making secure solitary sign-on (SSO) contributions in healthcare. Particularly despite the existence of these service type frameworks, healthcare individual management faces trials such as data outbreaks, identity theft and emerging cybersecurity threats. The inclusion of these keys among a variety of healthcare IT systems may increase in complexity and challenges in the process.

Supervision of individuals in an administrative network exceeds mere oversight; it also requires a comprehensive method of recognizing and verifying positive access permissions. In the healthcare sector, the implication of identity management is augmented by maintaining patient information and protecting the secured data that only the staff document to possess entrées is vital for observing stringent and prescribed guidelines, for instance the Answerability and Compactness in Health Insurance Accountability and Portability Act (HIPAA). This essential process includes identifying and gathering related information about users, creating the groundwork for succeeding phases of personal management. Substantiation of user identity over frequent approvals such as usernames, passwords, biometric scans or multi-factor authorization enhances additional security measures[10]. Allocation of suitable types of entrée rights to authentic users founded on the exact persons and the everyday tasks safeguards that the correct persons have access to the correct data. Recording, nursing and monitoring user actions not only guarantees agreement but also assists as a robust implement for safety and issue resolution.

Extensively accepted for national identity management, LDAP (Lightweight Directory Access Protocol) upholds a complete almanac of user information and IDs. In healthcare, LDAP supervises access to serious systems, including electronic and microelectronic health records (EHRs). Some OAuth (Open Authorization) facilitates authorization, allowing third-party requests to access assets securely. OpenID (Open Identification) Link, building on OAuth (Open Authorization), ensures user authentication, enabling secure data entrée between various assorted systems. Critical for single sign-on (SSO) and cross-type of domain enabled authentication, SAML (Security Assertion Markup Language) rationalizes access to numerous applications and amenities within the complex healthcare system. By merging FHIR, a healthcare cross compatibility specification, with OAuth, SMART (Substitutable Medical Applications and Reusable Technologies) on FHIR (Fast Healthcare Interoperability Resources) creates a robust outline for creating healthcare requests, allowing safe third-party access to health information.

Mixing identity management systems across various healthcare IT surroundings remains an important trial, requiring advanced solutions. The continuous concern of conservation in patient data from unofficial entrée or disruptions necessitates enduring observance and robust safety trials. Corresponding stringent safety measures with a user-friendly crossing point are essential for the implementation of identity management schemes among healthcare experts. Some healthcare systems are discovering the potential of blockchain to start secure and translucent leveraging biostatistics such as pattern and facial acknowledgment, joined with constant verification methods, which improves the complete safety attitude.

Thoughtfully applying actual identity management outlines in healthcare is crucial for safeguarding data safety, supervisory compliance and rationalized access for official employees. As skill grows, healthcare administrations must ensure well-informed

methods of developing frameworks and skills, familiarizing their identity management plans to address in cooperation current and upcoming challenges. In summary, identity management in healthcare is a complicated but energetic feature of preserving data safety and controlling agreement, where existing backgrounds provide a dense foundation but frequent invention and enhancement are imperative.

9.8 INTEROPERABILITY AND STANDARDIZATION IN IOMT (MEDICAL INTERNET OF THINGS)

Interoperability and calibration within the realm of the smart Medical Internet of Things (IoMT) affect the continuous exchange and understanding of data across a various array of medicinal strategies, systems and to entitlement to its applications. Interoperable compatibility is a key component which ensures that disparate IoMT strategies can cooperate concordantly, sharing dynamic info and communicating efficiently, irrespective of their source or creator. Attaining the interoperability technique smooths healthcare providers in retrieving complete patient data from numerous sources, which leads to well-informed conclusions and improves patient care.

For instance, data from a fitness supporter can be flawlessly combined into a patient's electronic or microelectronic patient health record (EHR) scheme, which provides a complete indication of the patient's health position. This interoperable allows multidisciplinary healthcare teams by allowing real-time entrée to related patient data, nurturing effective relationships in analysis and handling various planning techniques. Further, interconnectivity in smart IoMT strategies allows actual and safe enhancing healthcare facilities by converting data, reducing errors and by minimizing redundancy tests[1,11]. Patient approval is another significant consequence of compatibility procedures, as it empowers affected roles to access healthcare data. This entrée allows their patients to manage their health conditions and also to track advancement and energetically promote in their healthcare organization, which leads to improved healthier outcomes. Inter-adaptable technique in a smart IoMT plan plays a dynamic role in isolated patient treatment and monitoring agendas, allowing healthcare workers to monitor dynamic indications on screens, to track medical adherence and also access other relevant information distinctly, thus streamlining timely interventions and depleting the availability of numerous healthcare appointment schedules.

The standardization process involves creating and establishing shared protocols, including Bluetooth and Wi-Fi (Wireless Fidelity) along with specialized patient healthcare standards like DICOM (Digital Imaging and Communication) and IEEE (Institute of Electrical and Electronics Engineers) 11073(x73) to promote and establish a consistent framework in smart IoMT strategies irrespective of the source origin. It also encompasses defining uniform data setups and architectural structures to generate and promote interoperability among smart IoMT devices. By adopting uniform configuration setup facilitates the seamless exchange of information flow across the different systems, allowing the accurate comprehension and analysis of healthcare patient data. Further, cybersecurity measures initiate the protection of patient healthcare information against breaches of patient information by unauthorized access and manipulation of healthcare data[12].

Ensuring compliance with submission protocol criteria is achieved by upholding reliable protocols and by providing endorsement procedures and promoting innovation in the development and growth of reliable smart IoMT devices. Constructors of IoMT may have the capacity to focus on optimized device performance and enhance their features while upholding familiar ethical standards, moral principles, promoting innovation while protecting and ensuring specifications in the current patient healthcare framework and system arrangements. Consistency and standardization in smart IoMT are critical for making a related, effective and patient-centered healthcare system. Unified data distribution is enabled by interoperable compatibility, thereby refining patient healthcare and association between healthcare experts. Concurrently, calibration ensures constancy, security and control, fostering novelty and scalable expandability within the smart IoMT landscape. These joint efforts contribute significant to the progression of digital healthcare, thereby growing patient outcomes and exciting the overall excellence of healthcare facilities.

9.9 SECURING PATIENT DATA IN THE IOMT ERA

The conversion of individuality management within the healthcare sector outlines a substantial journey considered by the alteration and progression of classifications and procedures planned to oversee and validate the characteristics of individuals involved in the healthcare sector. The essential position of identity supervision in healthcare originates from a gathering of aspects, encompassing the safety of patient data, observance of regulatory orders and the simplification of unified access to healthcare facilities for duly authorized societies. An investigation into the protuberant aspects defining the growth of identity management in healthcare discloses a change-over from predictable, physical procedures, such as physical copy or paper-based record-keeping and tangible ID (Identifier) cards, to a modern landscape conquered by computerized and electronic identity management schemes. This design shift is emphasized by the addition of cutting-edge numeral technologies, including electronic or microelectronic health records (EHRs) and progressive digital verification procedures[13].

At the essential core of this growth lies the predominant inspiration of Electronic Health Records (EHRs), acting temporarily as a substance enabling significant changes in individuality management. The digitalization of patient healthcare information over EHRs not only enables effective and safe entry for official healthcare workers but also commands the occurrence of identity management outcomes to manage access, screen user activities and support the truthfulness of patient information. Alternatively distinguished measurements in biometric authentication methods are progressively widespread within healthcare administrations as part of the evolutionary development. Finger imprint, face verification and iris image scans function as formidable barriers to prevent unauthorized entry into complex healthcare data to attract the exactness of patient ID and mitigate the threats related with individual holdup. The growth of Single Sign-On (SSO) elucidations is a required chapter in the described story, explaining the verification process for healthcare authorities. By permitting admission to frequent applications and concepts containing a unified array of credentials, SSO not only supplements workflow skills but also reinforces security

by facilitating the essential need for operators to achieve a multitude of significant keywords[14]. Important to the growing identity management landscape is the representation of Role-Based Access Control (RBAC) in healthcare sectors. This intentional context contains assigning of detailed roles and supports to entities created on their tasks, protection that only users enter evidence and features associated to their people role and lessening the vulnerability to data outbreaks.

This growth consistently highlights interoperability and incorporation with numerous schemes. This strategic consultant enables unified information interchange among numerous healthcare units while preserving difficult identity confirmation measures. Navigating the complicated guidance, the growth of identity management in healthcare places a significant stress on proposals with simple rules and policies, such as the responsibility and probable transportability in the Health Insurance Act (HIPAA) in the United States of America. This accentuates a promise to protect patient privacy and endorse the safety of medical information in the limits of legal frameworks. Associated with the increasing drift of patient-centered care, the progress concludes in a permitting attitude for patients to attain their health information. Identity management enlightenments are custom-made to approve patients' data, providing secure entry and switching over their health records, all while upholding the values of confidentiality and security. The evolutionary pathway of identity management in healthcare designates a deep change from ancient, physical procedures to a digital, robotic and cultured pattern. The key objective is to strengthen safety, justify workflows, protect supervisory plans and to explain the active arrangement of healthcare skills.

9.10 BLOCKCHAIN TECHNOLOGY: A PARADIGM SHIFT IN IOMT IDENTITY MANAGEMENT

Blockchain technology represents a significant shift in IoMT Identity Management, exploring its transformative impact within the smart Medical Internet of Things (IoMT) ecosystem. IoMT, comprising unified medical devices and structures, has become integral to healthcare, but managing device identities and security is challenging due to the sensitivity of medical data and evolving cyber threats. Originally designed for cryptocurrencies like Bitcoin, blockchain offers a revolutionary solution. Unlike centralized systems, it operates on a distributed network of nodes, validating and recording connections securely, transparently and tamper-proof. This decentralization enhances security and trust.

9.10.1 In IoMT Identity Management, Blockchain provides Key Advantages

Blockchain uses cryptanalytic techniques, making unlawful data access or changes nearly unfeasible. Transactions form unchallengeable blocks, making a tamper-resistant chain. Once on a distributed ledger, blockchain, information can't be retrospectively changed, ensuring patient historic records and device info truthfulness, aiding reviews for healthcare workers and regulators. Blockchain cryptographic ledger permits safe information mixing among various smart IoMT device platforms,

enhancing healthcare productivity through real-time, official patient information allocation. The blockchain cryptographic ledger supports self-executing smart agreements, auto-mechanical processes like insurance dues, increasing effectiveness and lowering managerial overheads. It allows secure health data management, letting patients control medicinal record access, attractive privacy and data proprietorship. This pioneering innovative technique challenges the complexity of smart IoMT identity management, which contributes to the development of an efficient, patient focused and patient centered healthcare system.

Figure 9.4 illustrates the Blockchain of Smart IoMT Architecture, a centralized process of live statistical monitoring, with health professionals submitting patient reports, which makes it comfortable for a physician to oversee the patient reports and provide guidance from a distant location. This centralized process enables secure communication with care takers and also monitors patients' remotely using body sensors. The implementtion rollout of the smart Medical Internet of Things (IoMT) has revolutionized patient healthcare services by integrating sensors and intelligent smart techniques into the medical ecosystem network. Further, the proliferation of connected devices has sparked concerns about identity management and patient-focused data security. Traditional and conventional methods of identity management are often overlooked by prompting the emerging and game changing challenges in blockchain cryptographic ledger technology as an emerging solution in smart IoMT identity management. The IoMT refers to a system of unified medical approaches, wearables and sensors that communicate and exchange health data. This system improves patient monitoring, enables remote healthcare and enables more tailored treatment plans. Nevertheless, with the cumulative volume of delicate health data being produced and shared, safeguarding the individuality and truthfulness of the aspirants in this ecosystem becomes crucial.

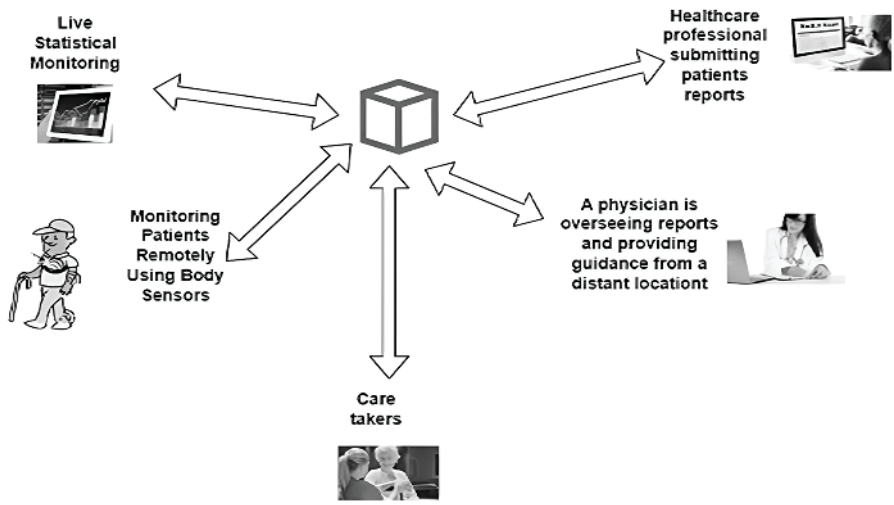

FIGURE 9.4 Blockchain of smart IoMT architecture.

Outdated identity management schemes typically rely on central establishments, such as hospitals or health institutes, to validate and approve users' plans and strategies. This concentration encourages security risks, as a single point of failure and could compromise the complete system. Furthermore, the deficiency of transparency in these schemes may lead to questions of trust among contributors. In blockchain cryptographic ledger technology, the groundwork of cryptocurrencies like Bitcoin offers a dispersed and transparent method to identity management. In a blockchain cryptographic ledger, dispersed ledger accounts and infrastructures opens across a network of nodes; protection of information is tamper-resistant and available to all official applicants.

Blockchain crypto ledger abolishes the need for a vital authority, allocating identity management through the network. This reduces the risk of a solitary point of letdown absence of success and raises the system's protection and security. Once data is verified on the blockchain crypto ledger, it cannot be altered or deleted. This feature safeguards the truth of persistent data and offers a dependable assessment path for every communication within the smart IoMT ecosystem. Smart contracts are self-operating contracts with the families of the contract and are written directly as a cipher. In smart IoMT, smart arrangements can automate identity confirmation procedures, protection that means only official strategies and users enter the system. Blockchain cipher ledger supports privacy through cryptanalytic techniques. Users can switch over their data and stake it selectively, upholding privacy while still contributing to the smart IoMT network.

Blockchain crypto ledger promotes interoperability through the application of a standardized, secure context for data conversation between various smart IoMT plans and systems. This safeguards unified announcement and teamwork across the healthcare environment. In the smart IoMT network process the expandability of blockchain systems becomes a concern. Inventors must deliberate the competence and speed of contacts to lodge the cumulative capacity of data produced by medical plans. Adherence to healthcare guidelines and data fortification laws is critical. Integrating blockchain crypto ledger into smart IoMT identity management needs a careful consideration of agreements with local and global standards. The accomplishment of blockchain crypto ledger in smart IoMT identity management is contingent on user reception[14]. Healthcare authorities and patient roles must be well-educated about the reimbursements and feature capabilities of blockchain to safeguard extensive implementation. Blockchain crypto ledger technology presents a model shift in IoMT identity management, and addresses the safety and confidentiality hearings related to the cumulative unified healthcare landscape. By dispersing identity confirmation, confirming data integrity and helping interoperable compatibility, blockchain crypto ledger improves the whole efficiency and safety of the smart IoMT ecosystem, flagging the way for a safer and patient-centric imminent healthcare.

9.11 INNOVATIVE APPROACHES TO ENHANCE IDENTITY MANAGEMENT IN IOMT

Protection of healthcare data is supreme in the province of the smart Medical Internet of Things (IoMT). This system, containing unified medical methods and schemes, also collects, shares and examines healthcare data. To improve identity

management inside smart IoMT, advanced methods are significant to promise the safety, pleasure and truthfulness of patient information approaches. One advanced method includes the use of biometric scan verification methods such as fingerprint or facial appreciation for retrieving medical plans and patient information. Individually customized biometric scan details serve for each individual as a notable tool for confirming identity, maintaining confidentiality of patient data, thwarting effectively unauthorized entry and ensuring maintainability of patient information in smart IoMT devices[12].

The innovative and revolutionary realm of blockchain cryptanalytic in smart IoMT establishes an immutable, unalterable blockchain ledger which is decentralized to secure and manage patient identities and to control permission access comprehensively. Each agreement contract request is accurately documented in a block precisely by creating and ensuring a transparent definitive ledger. This confirmation affirms the significant sustainability of patient healthcare identity integration and also prevents alterations. Further, machine learning processes are essential for refining identity management systems in smart IoMT environment settings. This protocol procedure examines the user performance trends and deviations in Realtime and swiftly identifies any deviations. By continuously monitoring user interaction actively in real-time medical data systems, machine learning models flag and detect certain behavior to activate uncertain behavior to prompt alarms, potentially preventing safety breaches and facilitating rapid response. In the framework of highly intelligent, smart IoMT systems, the submission of the zero-trust security framework has grown more common. Irrespective of where they are in the framework, no discrete number chips or devices is always authorized to allow everything within this framework to function and operate. Each user, irrespective of rank, must obtain consent and verify their identification for access to any resources. Each individual significantly lowers the probability of illegal access by means of this asset by emphasizing the continuing verification of ongoing documentation instead of being contingent on a single documentation and validation.

Within the dominion of the smart medical Internet of Things (IoMT), authenticated identity management leadership offers a valuable standard protocol for yielding authorized use and managing health information resources through the large, multi-site healthcare environmental location by means of modern technologies and cultured tactics to manage the trials brought about by the dependence on the scientifically progressive smart Internet of Medical Things (IoMT) and the need to protect persevering healthcare information. Adaptation, participating and engaging the use of identity keys through blockchain crypto ledger expertise proficiency and becoming a vital strategy in promoting confidentiality, increases and promotes crucial security by giving essential control of patient health information to relevant authorized entities. This approach not only decreases the risk of unauthorized access but also sets out to establish improved safety in smart IoMT communities.

The gathering of smart arrangements accumulates the intelligent arrangements in the blockchain crypto ledger hub which enables and facilitates verification of program identity enforcement and enhances predefined rules for access agreements and the authorization agreement process. This ensures guaranteed individuals with

proper engagement of smart IoMT plans thereby engaging valid data and ultimately secure and improved communications. Employing biostatics studies for ongoing verification facilities helps to ensure uninterrupted secure access over an extended time. The system pattern authenticates user behavior through announced gait stride movements. Actions to improve the overall safety procedures employ strategic deliberation through the implementation of micro-segment techniques within the accessibility of network architecture, inhibit constraints. Access for specific resources is allocated to each device by allowing restricted access by diminishing the potential demand for requiring additional support and mitigating security breaches in overall flexibility. Real-time risk analysis provides insight guides for establishing consent user behavior to the adaptive nature of access permission that encompasses the entire system[15].

The implementation of dynamic methods reinforces the implementation of security measure modification and enhancement in emerging threats by incorporating a compatible identity system that facilitates formation of fostering patient healthcare standards and promotes efficient data by enabling seamless administrations in healthcare and smart IoMT devices. Through the integration of various identity management, users can firmly enter resources across different patient healthcare fields by employing coherent and unified sets of credentials by ensuring safety and smooth efficient performance. Streamlining the integration of user participation in single sign-on (SSO) ensures the process of user participation is accomplished by enabling users only to authenticate access to various smart IoMT suggestions and recommendations, by mitigating, effectively reducing, the risk associated with numerous sets of credentials. The utilization of artificial intelligence in learning interactively detects notable unique irregularities in user or performance device behavior by triggering immediate prompt alerts through comprehensive examination and strengthening overall safety and security through proactive potential threat management. Engaging the active involvement in machine learning enhances the effectiveness of system capacity to detect and address responses to emerging threats.

Attractive FHE (Fully Homomorphic Encryption) permits intentions on programmed data without interpreting and improving privacy through data exemption. Complex health data remains intimate through a complete computational process, confirming a healthy privacy framework. Combining various suppression techniques confirms individual confidentiality by combining and examining healthcare data [12,14]. The introduction of noise or randomization prevents the document identification of a specific person, further emphasizing that the method respects privacy. All in all, the protection of identity management in the smart IoMT needs a combination of progressive technologies—blockchain crypto ledger, biometrics scans, integrated identity management in a zero-trust safety framework, AI (Artificial Intelligence)-powered malfunction detection and privacy-preserving approaches. This approach forms the groundwork of a robust, reliable and privacy-focused method to identify a management schedule for the combined dominion of medical devices and healthcare data.

9.12 REGULATORY PERSPECTIVES: ENSURING COMPLIANCE IN IOMT IDENTITY MANAGEMENT

The conversation about Regulatory Perspectives in smart IoMT (Internet of Medical Things) Identity Management emphasizes observance to loyalty and agreement standards is fundamental to safeguarding. It inspects trials related through management behaviors in the area of associated medical devices and healthcare suggestions, accentuating the serious nature of this level owing to its contribution to composite patient data. The inspiration is on protecting patient privacy and safety, demanding agreement with various procedures and values.

In the smart IoMT context, identity management includes procedures and skills for validating users, devices and submissions retrieving healthcare systems and information. Perspectives from a supervisory position in this field include laws, standards and measures recognized by healt care administrators and information associations for protection. These strategies aim to make a secure condition for storing, assigning and processing healthcare data. Confirming agreement in smart IoMT identity management comprises numerous crucial structures[16]. First, monitoring plans direct healthy actions such as encoding and decoding, entrée panels and endangered message settlements to guard patient information from unlawful and unsanctioned admission or disruptions. Second, suitable verification mechanisms, including multifactor validation and consent protocols, are essential to confirm user and device individualities, protection that only recognizes personnel information that can recognize sensitive and medical information. Third, measures like the Responsibility and Portability in Health Insurance Portability and Accountability Act (HIPAA) in the United States of America and the entire and Universal Data Information Safety Regulation (GDPR) in Europe smart devices has severe guidelines on arranging, storing and delivering of patient data, emphasizing the inference of patient privacy.

Additionally, smart IoMT devices often need to argue information with various healthcare systems, demanding compliance morals to ensure unified communication while following safety and privacy necessities. Moreover, supervisory perspectives strain the position of detailed inspection trails, tracking information access and assisting surveys in the event of safety occurrences. Lastly, healthcare administrations are required to conduct regular amenability audits to evaluate smart IoMT systems, including safety events, data handling practice and user entrée controls, to safeguard arrangement with procedures.

9.13 IOMT AND TELEMEDICINE

The combination of smart Medical Internet of Things (IoMT) strategies with telemedicine has resulted in an adaptation era in healthcare delivery, basically reforming the landscape of inaccessible patient monitoring and healthcare supervision. Telehealth, a cutting-edge method that connects progressive telecommunication assemblies, allows healthcare facilities to be provided from a distance. By perfectly integrating smart IoMT devices into telehealth platforms, the choice and accomplishment of remote healthcare have been deliberately augmented, giving rise to a new type of tailored and real-world healthcare services.

9.13.1 The Integration of IoMT Devices in Telemedicine

Telehealth, driven by continuous technological creation, surpasses outdated healthcare limitations by joining smart IoMT devices such as wearable sensors and incessant presentation tools into its context. This methodology is composed in accord, enhancing patient tolerance and remote distinctness in frequent disturbed behaviors. Smart IoMT, with the help of organized capable devices like wearable sensors and continuous monitoring organized devices, enables patients with vital signs and conditions like heart disease or diabetes to wear organized devices that continuously monitor the vital signs. The complete comprehensive program enables complete programs for patient healthcare experts to access real-time health informatics which allows facilitating timely interventions in case of involving indiscretions[22]. Various advanced sensors in smart IoMT include advanced imaging devices and electronic audited technology equipment which supports and facilitates simulated examinations and continuous visual inspections. Through the inclusion of additional mixture blends, it is feasible to conduct precise detailed examinations meticulously without the physical presence for improving accessibility and enhancing suitability for patients.

Smart IoMT devices such as efficient innovative pill organizers, dispensers and applications for medical adherence, meticulously oversee patient routine medication schedules. Telehealth enhances this platform technique which plays a crucial role to promote adherences, send timely alerts and inform healthcare professionals of particular deviations from the prescribed regimen and guide ongoing pathways employing and utilizing smart IoMT strategies, so that healthcare providers establish data dissemination platforms for telehealth phases allowing systematically analysed and accurately organized methods. Through leveraging the use of progressive metric computation and artificial intelligence, healthcare professionals enhance and gain a deeper understanding of improved healthcare approvals and informed rational analysis.

9.13.2 Remote Patient Monitoring and IoMT

Utilizing and integrating smart IoMT devices enables the Remote offshore Presentation Monitoring (RoPM) initiative extending patient healthcare accessibility by monitoring patients beyond traditional boundaries and by accessing continuous monitoring in patients' homes. This innovative forward-thinking traditional approach enhances patient-centric care by monitoring and managing chronic conditions and post-surgical recovery aids. Smart IoMT approaches, by precisely monitoring vital signs like average blood glucose levels for three months (Haemoglobin A1C), heart rate consistency, blood pressure and oxygen saturation in the blood enable and support complete health arrangements. This constant analysis permits patient healthcare practitioners to personalize maintenance, facilitating specific interventions and personalized maintenance. The use of smart IoMT strategy to keep observation is monitoring displays, identifying subtle deviations from normal guided standards and allowing the early detection of patient health issues[9]. Addressing these issues by taking actions based on the findings and creating improved patient

enhancement therefore increases the quality of patient care outcomes. Enhanced Patient Appointment and smart IoMT-facilitated remote intensive maintenance and monitoring actively includes patients in their healthcare exploration. Real-time data encourages patients to display their growth, make well-informed conclusions and deciding whether to carry on living, thus striking observance to conduct action plans and educating complete outcomes.

Post-discharge of smart IoMT strategies continues to monitor patients, safeguarding faithfulness to agreed actions. Healthcare workers remotely track patients' recovery growth, prevailing promptly to avoid difficulties. This practical approach openly reduces the probability of rehospitalizations, promoting a unified variety of attention. The amalgamation of smart IoMT skills into telehealth and distant patient monitoring surpasses predictable healthcare limitations, forcing the commercial trade towards a forthcoming practice branded by modified, efficient and active healthcare services. This integration and mixing empowers healthcare workers to deliver incomparable care, ultimately concluding in improved patient results and unmatched healthcare involvements.

9.14 ADDRESSING THE ADVANCED SECURITY CONCERNS IN SMART IOMT-ENABLED HEALTHCARE SYSTEMS

The fast growth of smart Medical Internet of Things (IoMT) knowledge and Technology has transformed healthcare, growing patient telehealth care, monitoring and conducting treatment. However, these developments pose challenges, predominantly in safeguarding smart IoMT-enabled healthcare systems. It is imperative to guard patient secrecy, confirm data integrity and uphold system reliability[16].

A major alarm in smart IoMT safety revolves around information confidentiality. Smart IoMT devices gather complex patient data, including medical histories and vital signs. Protecting the confidentiality and the honesty of data needs to be more energetic to avoid unauthorized entrance and possible misuse. Healthy and strong encoding protocols and access controls are important to preserve patient confidentiality. Another significant problem is the introduction of smart IoMT approaches to susceptible cyber-attacks. Security exposures can be exploited by hackers to improve unauthorized entry or to circulate essential information. Healthcare management is crucial to implement severe cybersecurity protocols, with regular software updates and the interruption of recognition arrangements, so as to minimize the hazard of weak cyber-related attacks. It is serious and vital to protect the ethics and legitimacy of data spread between smart IoMT strategies and healthcare actions. Techniques like digital signatures and blockchain crypto technology can validate the data cause, making it secure and dependable. Nonstop monitoring and actual examination of system traffic can promptlyAccurate and rapidly sense and answer to doubtful actions.

Imminent physical security concerns are too important, as strategies and plans can be erroneous or restricted, exposing risks to patient information. Implementing procedures similar to utilizing device trailing and evident covers has the volume to decrease these hazards and progress the complete safety of the system arrangements. Safeguarding smart IoMT-enabled healthcare organizations demands a broad

approach. Healthcare administrations must arrange data privacy, implement strong cybersecurity measures for robust telehealth devices, confirm data integrity and address concerns related to physical security. This utilization of addressing techniques enables the required benefits of smart IoMT technology while protecting patient information and healthcare service integrity.

9.15 PATIENT-CENTRIC IDENTITY MANAGEMENT: EMPOWERING INDIVIDUALS IN IOMT

In the proactive outlook approach of healthcare, the smart Internet of Medical Things (IoMT) has accommodated an enhanced and essential concept, concerning frequent medical methods and arrangements to enhance patient telehealth technology care. Essential to this type of method is Patient Centric Personal Identity Management (PCPIM), a preliminary element that allows people to safeguard unified healthcare schemes. This chapter examines the fundamentals of PCPIM in the smart IoMT framework, highlighting its position and inspiration on the healthcare segment. PCPIM incorporates a holistic approach for managing patient identities and info within smart IoMT systems, organizing patients throughout their healthcare journey. It involves the secure and effective management of patient information, safeguarding exactness, privacy and availability. Unlike traditional healthcare schemes where patient information is scattered across numerous platforms, PCPIM combines and shortens this information, presenting a unified view of the patient's medical history, behavioral treatment and preferences.

PCPCIM hires robust verification methods such as biometrics, two-factor confirmation and blockchain crypto ledger technology to validate patients' features, safeguarding first that official persons are able to access the smart delicate medical information. PCPIM combines information from various sources, including wearables, medical approaches, electronic means of health historic records (EHRs) and patient-reported information. This kind of complete dataset trains healthcare providers with appreciated insights into a patient's telehealth status, enabling adapted personal health care delivery. PCPIM promotes interoperability among healthcare systems, enabling seamless discussion of patient data among healthcare clinics, pharmacies and other healthcare entities. This inspires synchronized healthcare and decreases the risk of medical-related errors.

PCPIM allows patients to resist their information over explicit condense mechanisms. Individuals can fund or revoke entrée to their information, fostering visibility cum transparency and building hope between patients and healthcare providers. PCPIM reassures patients to actively contribute to their healthcare decisions. Access to their whole medical records allows individuals to understand their circumstances better, ask informed questions and engage in meaningful discussions with healthcare experts. By leveraging the data combined through PCPIM, healthcare providers can tailor treatments and involvements based on individual requirements. Personalized care aligns actions with patients' unique healthcare outlines and preferences, leading to better results. Through information security and privacy, PCPIM orders the safety and privacy of patient data. Through encryption, decentralized storage and safe communication systems, it

shields complex and sensitive data from cyber-related threats, fostering patients' trust in smart IoMT applications.

9.16 FUTURE TRENDS IN IOMT AND IDENTITY MANAGEMENT

The union of the smart Internet of Things (IoT) and healthcare, usually known as the smart Medical Internet of Things (IoMT), has significantly advanced the healthcare industry. This addition of medical devices and technology skills has not only enhanced patient care but also paved the way for upcoming revolutions. Identity management authentication has played an active role in protecting the safety, security and secrecy of individual patient information. Inspecting trends in smart IoMT and identity management authentication delivers valued insights into the future of healthcare information.

9.16.1 Future of Connected Healthcare Network

The future of smart IoMT envisions a highly combined healthcare network where medical devices like biomedical equipment, patient and healthcare workers seamlessly collaborate. This interactivity enables real-time surveillance of patient health, simplifying timely involvements and personalized actions. Therefore, the quality of healthcare services is predicted to see a considerable enhancement. Integration in Artificial Intelligence (AI) and advancement in Computerized Machine Learning (ML) system information are collected to transform smart IoMT devices. AI procedures can examine widespread patient information, which contributes actionable understandings for healthcare experts. Prognostic and anticipatory analytics based on AI can predict potential healthcare issues, authorizing healthcare providers to take preventive actions, thereby reducing hospital readmissions and educating overall patient outcomes.

9.16.2 Implementation of Enhanced Security Measures

The explosion of smart IoMT approaches underscores the importance of safeguarding patient data security. Emergent trends indicate the implementation of progressive security measures such as blockchain technology and distributed identity management systems. These inventions enhance data integrity, ensuring the patient information remains private and tamper-proof. The smart IoMT enables personalized medicine modified by tailoring treatments methods based on distinct patient information. Through complete remote patient monitoring, healthcare workers can detect vital signs and other healthcare limitations in real time. This kind of method has not only restored patient convenience but it also permits data-driven results by healthcare experts, leading to more timely and personalized actions. As smart IoMT advances, moral concerns related to patient confidentiality, consent and data proprietorship become dominant. Upcoming trends in identity credential management include the expansion of robust ethical and moral frameworks and regulatory supervised policies. Ensuring and safeguarding the protection of patient rights and mirrored type clear, transparent, accountable information usage will be vital in building public faith in smart IoMT technologies.

9.17 COLLABORATIVE EFFORTS: INDUSTRY AND ACADEMIA IN ADVANCED IOMT IDENTITY SOLUTIONS

In the modern recent times, the nodal intersection of technology and healthcare has rushed creative keys, particularly the smart Medical Internet of Things (IoMT). This Smart IoMT comprises unified medical plans and its demand for requests that collect and communicate health data through online platforms. To ensure safeguarding measures in the integrity of this data is most important, which leads to the essential need for an advanced identity type of authorized solutions in smart IoMT frameworks. This requirement has driven association between industry and academia, combining practical industry knowledge with academic information to improve smart IoMT identity solutions. Industry brings practical challenges, exploiting its expertise and marketplace insights, while academia delivers theoretic information skills, research abilities and advanced standpoints. The collaboration among these sections fuels revolution in smart IoMT identity and valid services. The prime focus of this association revolves around emerging secure verification approaches. Validating the smart IoMT devices is vital as efforts are made to confirm the legality of communicated and established information. Industry-related associates offer valued insights into the user presentation and market location needs, though academic related, and to explore blockchain crypto ledger algorithms, biometric scan confirmation and an artificial intelligence sector to create robust verified confirmation systems.

The business partnership places significant importance on data honesty and confidentiality, it also identifies the responsiveness of medical information. Industrial specialists pay their knowledge in information strategy which outlines and plans by safeguarding compliance with secured standards like HIPAA rules. Concurrently, academia explores the implementation of encryption strategies like crypto ledger technology and decentralized identity growth solutions to improve security for smart IoMT schemes against information breaks and unauthorized entree. Continuing search examination and growth create another dynamic feature of this association. Collaborations between industry and academia enable the exchange of thoughts and resources, leading to the development of models and evidences of the healthcare sectors. These inspirations are vital dynamics for challenging the possibility, expandability and growth potential of smart IoMT identity resolutions, endorsing a favorable situation for authorities and scientists to learn and renovate the inventions. These collective activities between industry and academia play an essential role in advancing smart IoMT identity key solutions. By combining practical knowledge with academic knowledge, these partnerships drive novelty, and ensure the development of secure, real and secure authentication methods within the smart IoMT landscape. This teamwork boosts the current healthcare infrastructure and prepares the way for a safer and more unified future in medical technology skills.

9.18 FUTURE TRENDS AND INNOVATIONS IN DIGITAL HEALTHCARE IDENTITY MANAGEMENT

In modern times, the nodal intersection of technology and healthcare has rushed creative keys, particularly the smart Medical Internet of Things (IoMT). This smart IoMT comprises unified medical plans and its demand of requests that collect and

communicate health data through online platforms. To ensure safeguarding measures in the integrity of this data is most important, which leads to the essential need for advanced identity types of authorized solutions in smart IoMT frameworks. This requirement has driven association between industry and academia, combining practical industry knowledge with academic information to improve smart IoMT identity solutions. Industry brings practical challenges, exploiting its expertise and marketplace insights, while academia delivers theoretical information skills, research abilities and advanced standpoints. The collaboration among these sections fuels revolution in smart IoMT identity and valid services. The prime focus of this association revolves around emerging secure verification approaches. Validating the smart IoMT devices is vital as efforts are made to confirm the legality of communicated and established information. Industry-related associates offer valued insights into the user presentation and market location needs, though academic related, and to explore blockchain crypto ledger algorithms, biometric scan confirmation and the artificial intelligence sector to create robust verified confirmation systems.

In the domain of digital healthcare, identity authentic management is undergoing a significant transformation, driven by the unified incorporation of Artificial Computerized Intelligence (ACI) and advancement in Machine Computerized Learning (MCL). The innovative and revolutionary talent expertise does not only transform or modify the core fundamentals of identity security management within the patient healthcare domain, presenting a multi-layer complex strategy at the forefront of transformative revolution in the application of identity authentication systems, wherein AI and ML play a pivotal role for enhancing the performance in individual identity validation procedures. By offering comprehensive analysis of complex design, including elements such as speed and precision, capturing is perfectly enhanced by comprehensive and exhaustive study which results in forming refined and sophisticated biometric profiles. This planned approach executes effective and proactive measures, converting entrée to equally motivational effort and engaging more complex patient healthcare information.

The seamless integration and implementation of ACI and the identification of consistent identification adds augmented skilled credentials through dynamic aspects and also by integrating individual identity by improving and by detecting irregularities by closely examining and inspecting the user behavior design which demonstrates an innovative system aiming to enable swift and speedy detection of abnormalities and which enables quick execution and triggering alarms or necessary safety measures as needed. The proactive security segment exhibits protective vigilance in detecting breaches in security and utilizing ML and AI in predictive analytics which enables patient healthcare administration to effectively anticipate potential safety threats and hazards. Through the review of historical data, these competence abilities differentiate strategies and plans in user performance by streamlining implementation of active security measures and reinforcing safety protocols. Natural Language Processing (NLP) is a component which contributes to AI and enhances individual credentials by analyzing unstructured data like Natural Language Processing (NLP) which contributes to unstructured data like communication logs and patient records. By decoding human language, NLP advances identity confirmation over the removal of applicable data, confirming comprehensive patient ID and accurate record matching.

The AI and ML algorithms play a vital role in scam recognition, to highlight the implications in the field. Over the use of power to scrutinize large groups of data, these skills are important for recognizing fake and immoral actions such as protecting scam-induced fraud theft. By discriminating against a distinctive design in insurance protection claims, expenditures or employer performance, AI and ML advance fraud finding mechanisms by confirming the financial safety of both patients and healthcare employees. Surpassing the customary limits of AI and ML, the addition of emerging services improves the dissertation's survey of security in the advanced framework with the smart Medical Internet of Things (IoMT) and blockchain crypto ledger technology, by its safe and absolute repository for healthcare records and to identify credential management, to disperse information storage. Patient individualities are saved in the medicinal chronic records by securing data integrity, promoting transparency and authorizing patients to have control over their information by locating it inside a tamper-proof blockchain cipher ledger on a wireless network system. In the realm of smart IoMT, edge computing depletes the latency and permits prompt data analysis by investigating and refining the allocation of information back to its source. This technique progresses both data security and patient privacy by reducing the necessity of large storages on central servers. Quantum computing is a transformative force in encrypting methods. Although traditional encrypting faces trials from quantum occurrences, the quantum crypto method delivers advanced robust security measures for data encoding and communication, promising the secrecy and integrity of patient information in contradiction of influential digital cyber risks. The widespread implementation of 5G Technology converts dynamic engagement between user and the system for smart IoMT strategies, permitting real-time protected and secured data communication. This evolution enables unified remote patient monitoring, the telehealth deliberations and the suitable information examination, concluding better healthcare competence and patient health care outcomes.

The progression of handling digital healthcare identity permits identity credential management with AI and progression of ML, fusion of blockchain crypto ledger skills.. Leveraging these novelties permits healthcare managements to reinforce safety actions and improve patient documentation actions, and pledges prioritizing choice and integrity of patient data. Its importance is a healthcare scheme marked by better effectiveness, sharp safety and a patient-centric determination.

9.19 CONCLUSION

To a digitally protected and patient-centered health care environment, the vital requirement for a healthcare arrangement that assembles both safety and customer-centered care in the electronic world realm is emphasized. In today's technology-driven era, the healthcare sector is quickly progressing to digital platforms to grow efficiency, adaptive access and the overall patient involvement. Nevertheless, this shift presents trials, particularly in protecting sensitive patient data and safeguarding a personalized healthcare approach. This conclusion highlights the vital need of robust security actions in digital healthcare systems. Digital healthcare also supports the execution of advanced encoding techniques, multi-factor authentic validation and regular cum systematic security audits to shield and secure patient information from

cyber intimidations and unauthorized access. Creating a secure digital ambience not only conserves patient privacy but also fosters trust between healthcare providers and patients, inspiring greater use of digital facility services.

The conclusion highlights the status of a patient-focused method in the design and execution of technological healthcare solutions. Personalization in healthcare includes tailoring provision to distinct patient needs and preferences, including intelligible interfaces, in-built design and unified integration of numerical tools into the patient's healthcare drive. By arranging patient expediency and fulfilment, discreet healthcare platforms can improve patient appointment and compliance to treatment plans, which eventually leads to enhanced healthcare performance. The assumption highlights the consequence of interoperability among various discreet healthcare structures. Smooth data discussion between various platforms and healthcare providers is crucial for complete patient care. Interoperable compatibility ensures secure allocation and access to patient data across several healthcare situations, enabling synchronized and effective healthcare distribution. The decision advocates for a complete approach that participates in severe security procedures, patient-concentrated design and interoperable compatibility in discrete healthcare systems. By speaking about these key features, healthcare engineering can create a secure, effective and patient-centered discrete environment that meets patient requirements and improves the complete quality of healthcare services.

The smart Medical Internet of Things (IoMT) plans are used in the healthcare industry and the safety protocols are applied to safeguard these strategies and the data they switch. Smart IoMT devices are medicinal strategies and the claims are linked to cyberspace, allowing them to collect, argue and examine healthcare material. These strategies encompass wearable approaches, remedial sensors, monitoring type of apparatus kit and other healthcare-related appliances that can communicate data over cyberspace for healthcare purposes. Security procedures for smart IoMT devices entail sensibly made rules and actions planned to support the confidentiality, integrity and availability of data exchanged between these policies and associated systems. Due to the complex nature of healthcare data, it is imperative to create strong safety measures to safeguard patient info and preserve the functionality of medical devices. Significant aspects of smart IoMT Devices and safety protocols are incorporated as per the following:

Smart IoMT devices empower various validation methods to authenticate user individualities and limit access to authorized personnel. Entrée control devices and their machinery ensure that only genuine manipulators can cooperate with the devices and enter patient information. Smart IoMT devices employ encoding methods to secure information transmission, averting unauthorized access or interfering. Encoding algorithms encode data, making it understandable only by official ways of collecting and having the suitable decoding solutions, thus preserving the safe communication. The smart IoMT strategies are processed to secure communication actions like engaged HTTPs (Hypertext Transfer Protocol Secure) and preserve snarled and genuine networks. These actions guarantee the security of informed switching between devices and engagement throughout communication.

Security actions incorporate technologies to confirm data honesty, confirming that data remains complete or genuine during the effective communication. Common

methods for essential checks comprise using hash determinations and discrete signs on connected secured information. Fixed updates to trick firmware and software are energetic in addressing safety obligations. Manufacturers release updates and the protection known as contacts, gaining the overall safety of smart IoMT devices. These smart IoMT strategies often contribute secure boot events and hardware-based safety erections to stop unauthorized variations to the device's software. These activities protect that the device boots and runs only important software mechanisms. **Submission with governing standards:** Smart IoMT devices must follow healthcare strategies and ethics such as the accountability and Portability in Health Insurance Act (HIPAA) in the United States of America or the Comprehensive General Data Protection Regulation (GDPR) in the European Union. Numerous arrangements with these standards, which protect patient data, are moved and protected in consensus with legal provisions. These services and practices are effective to guard smart Internet of Medical Things devices, by protecting the privacy, honesty and accessibility of healthcare data while allowing unified data chat in discreet healthcare circumstances.

Ensuring the privacy of patient data, preserving the privacy and upholding compliance with regulation values are important aspects of the healthcare identity management system. Patient data, which includes personal facts like medical history and remedial strategies must be handled with extreme care. Appropriate identity management promises that solitary approved healthcare authorities can admit this info, evading breaks, individual robbery and misconduct consequences. Encoding techniques are used to save patient information through program and storing, making it incomprehensible to unauthorized parties. Effective identity administration correspondingly has a key role in avoiding medical integrity theft. It also includes strong patient validation methods that assist in handling consents, authorizing patients control over who can admit their medical record, and also contains information about what purpose a patient has admitted. Specific linkage of evidence is to exact patient aids, so the healthcare providers avoid errors in identifying treatments and prescriptions, thereby improving patient safety. Arrangement with trials such as HIPAA rules in the United States of America and GDPR in the European Union is vital in healthcare. This arrangement needs clear patient consensus, notifying patients about their rights and increasing security functions. Failure to achieve can result in severe consequences and legal drawbacks.

Industry morals like HL7 (Health Level Seven) and FHIR (Fast Healthcare Interoperability Resources) highlight the position of identity management guidelines for secure allocation of patient information among healthcare systems and providers. Detecting these moralities ensures detailed, protected and available patient information. In conclusion, actual identity management guidelines in healthcare are energetic in shielding patient info, preserving confidentiality and fulfilling guidelines. They not only measure sensitive data but also find trust with patients, maintaining the privacy and confidentiality of medical data and depleting the risks of unauthorized entry.

REFERENCES

1) Jain, S., Nehra, M., Kumar, R., et al. "Internet of Medical Things (IoMT)-Integrated Biosensors for Point-of-Care Testing of Infectious Diseases." *Biosensors and Bioelectronics*, Volume 179, 2021, https://doi.org/10.1016/j.bios.2021.113074, 2021.
2) Joyia, G. J., Liaqat, R. M., Farooq, A., Rehman, S. "Internet of Medical Things (IoMT): Applications, Benefits, and Future Challenges in Healthcare Domain." *Journal of Communication*, Volume 12, no. 4, 2017, pp. 240–247, https://doi.org/10.12720/jcm.12.4.240-247.
3) Hatzivasilis, G., Soultatos, O., Ioannidis, S., Verikoukis, C., Demetriou, G., Tsatsoulis, C. "Review of Security and Privacy for the Internet of Medical Things (IoMT)." In *Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Santorini, Greece, 29–31 May 2019.
4) Aanjanadevi, S., Palanisamy, V., Aanjankumar, S., Poonkuntran, S. "A Secure Authenticated Bio-Cryptosystem Using Face Attribute Based on Fuzzy Extractor." In *New Trends in Computational Vision and Bio-inspired Computing: Selected works presented at the ICCVBIC 2018*, Coimbatore, India, 2020, pp. 379–384.
5) Lin, T. W., Hsu, C. L., Le, T. V. "Smartcard-Based User-Controlled Single Sign-On for Privacy Preservation in 5G-IoT Telemedicine Systems." *Sensors*, Volume 21, 2021, pp. 2880, https://doi.org/10.3390/s21082880.
6) Vanitha, C. N., Malathy, S., Anitha, K., Suwathika, S. Enhanced Security using Advanced Encryption Standards in Face Recognition. In *2021 2nd International Conference on Communication, Computing and Industry 4.0 (C2I4)* (pp. 1–5). IEEE, 2021, December.
7) Srivastava, J., Routray, S., Ahmad, S., Waris, M. M. "Internet of Medical Things (IoMT)-Based Smart Healthcare System: Trends and Progress." *Computational Intelligence and Neuroscience*, Volume 2022, 2022, Article ID 7218113, https://doi.org/10.1155/2022/7218113.
8) Chuquimarca, L., Roca, D., Torres, W., Amaya, L. "Mobile IoT Device for BPM Monitoring in People with Heart Problems." In Conference, IEEEXplore, 12–13 June 2020, Istanbul, Turkey, https://doi.org/10.1109/ICECCE49384.2020.9179293.
9) Yaacoub, J. P., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., Chehab, A. "Securing Internet of Medical Things Systems: Limitations, Issues, and Recommendations." *Future Generation Computer Systems*, Volume 105, 2020 pp. 581–606, https://doi.org/10.1016/j.future.2019.12.028.
10) Alsubaei, F., Abuhussein, A., Shandilya, V., Shiva, S. "IoMT-SAF: Internet of Medical Things Security Assessment Framework." *Internet of Things*, Volume 8, 2019, https://doi.org/10.1016/j.iot.2019.100123.
11) Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., Qadir, J. "Security and Privacy of Internet of Medical Things: A Contemporary Review in the Age of Surveillance, Botnets, and Adversarial ML." *Journal of Network and Computer Applications*, Volume 201, May 2022, pp. 103332.
12) Malviya, R., Sundram, S., Dhanaraj, R. K., Kadry, S. (Eds.). Digital Transformation in Healthcare 5.0: Volume 2: Metaverse, Nanorobots and Machine Learning. Walter de Gruyter GmbH & Co KG, 2024.
13) Kang, S., Baek, H., Jung, E., Hwang, H., Yoo, S. "Survey on the Demand for Adoption of Internet of Things (IoT)-Based Services in Hospitals: Investigation of Nurses' Perception in a Tertiary University Hospital." *National Library of Medicine - National Center for Biotechnology Information*, Volume 47, June 2019, pp. 18–23, https://doi.org/10.1016/j.apnr.2019.03.005.

14) Kamalov, F., Pourghebleh, B., Gheisari, M. "Internet of Medical Things Privacy and Security: Challenges, Solutions, and Future Trends from a New Perspective." *Sustainability,* Volume 15, Issue 4, 10 February 2023, https://doi.org/10.3390/su15043317.
15) Krishnasamy, L., Tamilselvi, A., Dhanaraj, R. K. An innovative outcome of internet of things and artificial intelligence in remote centered healthcare application schemes. In *Healthcare 4.0* (pp. 245–265). Chapman and Hall/CRC, 2022.
16) Verikoukis, C. "Review of Security and Privacy for the Internet of Medical Things (IoMT): Resolving the Protection Concerns for the Novel Circular Economy Bioinformatics." In *Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, Santorini, Greece, 29–31 May 2019, pp. 457–464.

10 Authentication and Access Control Protocols in Digital Health and Wellness

Strengthening Security with Quantum-Resistant Cryptography

D. Elavarasi and R. Kavitha

10.1 INTRODUCTION

This section clearly explains the fundamental roles of authentication and access control protocols in digital health and wellness for a better understanding of the upcoming trends.

10.1.1 Background and Significance

The primary emphasis is on the increasing significance of cyber security in health and digital aspects. Due to the rapid use of technology in healthcare, cyber security is a critical factor. This chapter is crucial in addressing the fundamental questions and solutions related to protecting private health information, as well as its significance for the field's future[1].

10.1.2 Purpose of the Chapter

This chapter covers the regulations and guidelines related to cyber security that impact digital health and wellness. The purpose is to emphasize the importance of rules and regulations in ensuring patient privacy and security. The chapter guides healthcare professionals, policymakers and researchers on navigating the intricate cyber security environment that entails evolving principles, regulations, methods, procedures, best practices, etc.

DOI: 10.1201/9781032711379-10

10.1.3 Overview of the Digital Health and Wellness Landscape

Digital health and wellness space has seen the entrance of new technologies that include wearables, telemedicine and health monitoring systems. One section outlines a chapter summary that focuses on how digital health can improve healthcare delivery. The chapter acknowledges the advantages but notes that their operations pose potential cybersecurity threats due to acquiring confidential patient information.

10.2 EXISTING WORK

These articles summarize key privacy and security issues in the health and related technology sectors. A privacy authentication system and a key agreement mechanism were developed for securing remote healthcare services across dozens of servers in privacy based systems. A review of QKD, the quantum key distribution, reveals that it provides secure key exchange through quantum states, but has limitations in terms of data rate[2,3]. It focuses on IoT security and wireless sensor networks by employing the SEKCA (Security Key Certificate Authority) for encrypted data transmission. Privacy protection[4] is discussed, as key agreement and authentication in multi-server healthcare systems, highlighting the use of a privacy-based system. In Raich and Gadicha[5], a proposal was made to overcome the need for secure digital health passports (DHPs) through a distributed analysis and privacy approach addressing privacy concerns. A robustly distributed architecture uses SSL/TLS encryption, role-based authorization, and token-dependent identity to offer security from multiple threats on all data. They have an architecture that keeps both health records and research data together.

10.3 AUTHENTICATION AND ACCESS CONTROL

This section clearly explains the fundamental roles of authentication and access control protocols in digital health and wellness for a better understanding of the upcoming trends.

10.3.1 Access Control and Monitoring

This section clearly explains the access control monitoting function in different organization for ensuring the security.

10.3.1.1 Concepts and Significance

The rise of analytics and access control is influencing digital health. For authentication, only authorized users can access sensitive health data. After gaining approval to view certain resources and information, the access control process stipulates various activities authorized people can do. These thoughts must protect healthcare facilities, which manage patient data from any unauthorized use or exposure to these ideas above (Sutradhar et al., 2024)[6].

10.3.1.2 Role in Digital Health

Data privacy and security are among the main aspects on which digital health depends. Implementing these tools allows medical staff to access EHRs, telemedicine

systems, and smart medical devices without permission, ensuring they can modify patient information. Additionally, they support patient access to health records while complying with GDPR and HIPAA regulations. Access control and audits are significant ways of safeguarding digital health information, thus increasing trust and safety in the health sector[7].

10.4 QUANTUM COMPUTING AND ITS THREAT TO CRYPTOGRAPHY

This section clearly explains the fundamental Quantum Computing and Its Threat to Cryptography for a better understanding of the upcoming trends.

10.4.1 Introduction to Quantum Computing

According to an article[8], the advent of quantum computing is viewed as a significant revolution in computer technology. Different from classical systems that employ bits as 0s and 1s, qubits play a crucial role in quantum computers. Quantum computing, with superposition and entanglement, allows rapid processing of certain types of calculations. Among the many fields that can be transformed by quantum computing are cryptography, optimization an simulation. Still it offers opportunities, particularly in cyber security and cryptography that are not currently accessible through conventional methods[9,10].

10.4.2 Vulnerabilities of Traditional Cryptography

Traditional cryptography, based on mathematical problems such as integer factorization and unique logarithms for security, faces major disadvantages during compilation[11,12]. Shor's Algorithm, developed by Peter Shor in 1994, proved that quantum computers can handle large numbers efficiently, a function that forms the basis of many encryption methods, including RSA. Grover's algorithm, another numerical algorithm, can speed up the search process in unstructured databases and can break symmetric encryption. These advances challenge the security foundations of classical cryptographic agreement principles and require the development of post-quantum cryptography to prevent quantum computing threats.

10.4.3 Quantum Algorithm for Secure Data Encryption

1. Start from scratch to create both conventional and quantum registers.
2. Handle input data for quantum privacy, such as patient medical records.
3. During the encryption procedure, use quantum gates:
   a. Include a quantum gate, such the BBM92 or E91 series, for the distribution of quantum keys.
   b. To guarantee encryption, configure quantum keys.
   c. Make use of quantum mechanics to perform encryption.
4. Keep data encrypted with quantum encoding safe by keeping it in a secure database.

5. Ensure that only authorized medical personnel are given the quantum key, which they can use to decode it.
6. The imposition of authoritative agents: the usage of quantum gates; The quantum encryption key returns. Use quantum gates to retrieve the encrypted data stored at the quantum level. In order to fully establish the relationship between the two entities, private patient health records can be acquired.
7. Utilize anonymized data for participation in research studies or healthcare initiatives.
8. After completing the process, it is important to dispose of the quantum key securely.
9. The aim of this research is to investigate the prospects of using quantum security methods for managing digital health information.

10.5 KYBER: A QUANTUM-RESISTANT CRYPTO-ALGORITHM

This section clearly explains the fundamental of Kyber: A Quantum-Resistant Crypto-Algorithm for a better understanding of the upcoming trends.

10.5.1 Features and Advantages

Kyber encryption methods were developed to address emerging cryptography and quantum computing threats. Its most important aspects are its post-quantum security, efficiency and flexibility. After the task is completed, the quantum key is disposed of in a secure manner. Cryptosystems are susceptible to cryptographic compromise due to quantum attacks, so lattice-based cryptography forms the basis of Kyber's security. Due to its excellent combination of security and speed, the algorithm is well suited for a variety of applications, including digital health. Its value lies in protecting private information, such as medical records, and it can be used in post-quantum environments while maintaining its highest performance levels[13,14].

10.5.2 Applications in Digital Health

Kyber's endurance makes it ideal for improving the security of digital health systems. Kyber is an important component of digital health as it ensures patient integrity and privacy. The system is compatible with patient monitoring systems, telemedicine platforms, secure electronic health records and other health data transmission methods. Kyber noted that patient information remains encrypted and vulnerable even in the face of such a threat[15,16]. The company can protect personal medical information by integrating Kyber with digital health applications, providing privacy and security for patients and healthcare providers.

Kyber's Pseudocode: A Crypto-Algorithm Resistant to Quantum

1. Establish the initial digital health security resource system.
2. Evaluate the attributes of users, such as patients and medical professionals, using conventional research methods.

3. For safe key exchange, utilize Kyber quantum resistance cryptography:
   a. Establish a distinct pair of Kyber keys to facilitate safe communication.
   b. Disseminate the stakeholders' Kyber Public Keys.
4. Use krypton encryption to safeguard private health information:
   a. Determine which particular data needs to be protected.
   b. Apply the Kyber approach to encrypt specific data.
5. Ensuring the receipt and transmission of confidential health information:
   a. Provide data in encrypted form to authorized recipients.
   b. Decrypt the data that was received using the relevant Kyber encryption key.
6. Monitor for weak points or security lapses.
7. For the audit trail, keep thorough records of all conversations and data access activities.
8. Use strong security measures to thwart threats that don't risk privacy, such intrusion detection systems.
9. To stop emerging security threats, patch and upgrade the system often.

10.6 ADVANCED ENCRYPTION STANDARD IN GALOIS/COUNTER MODE (AES-GCM)

10.6.1 Introduction and Significance

Galois/ Counter Mode (GCM) and Advanced Encryption Standard (AES) are recommended algorithms in network security. Galois/Counter Mode (GCM) is used by AES-GCM for encryption and authentication, while AES is used for verification. This combination of algorithms makes it possible to store and transfer data in an effective manner. Due to its unique ability to do encryption and analysis, it is a vital tool for secure sensitive information hence it is used in various industries like healthcare, medicine and finance. The Advanced Encryption Standard algorithms matching round count, block size and key length are listed in Table 10.1.

Table 10.1 shows the different AES algorithms with key length, block size and number of rounds it took.

TABLE 10.1
Key-Block-Round combinations

	Key Length (32-bit word)	Block Size (32-bit word)	Number of Rounds
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

10.6.2 Data Encryption and Authentication

An AES-GCM[8] encryption key can access the information encrypted through a data encryption method. Galois/Counter Mode keeps track of everything that happens during the analysis process to ensure the security of the data while in storage or in transit. The preservation of patient records, medical data and communications is crucial in digital health applications due to the importance of these two functions. The availability of AES-GCM encryption capabilities makes it the most secure and dependable method for encrypting private health information in the 21st century.

AES-GCM (Advanced Encryption Standard in Galois/Counter Mode) is an architecture that combines the AEC encryption algorithm and in Galois/Counter Mode for data encryption and authentication, as demonstrated in Figure 10.1.

The arithmetic component of Galois field multiplication is significant in GCM. A population reduction function is employed to determine the authentication code, which can also be called message authentication (MAC). The Galois/Counter mode is used with the AES encryption method in the Advanced Galossary/Comander Encryption Standard (AES-GCM). AES-GCM coding and analysis involve several stages.

Key Notation:
K: Secret encryption key (128, 192, or 256 bits)
IV: Initialization Vector (usually 96 bits for GCM)
P: Plaintext
C: Ciphertext
A: Additional authenticated data (optional)

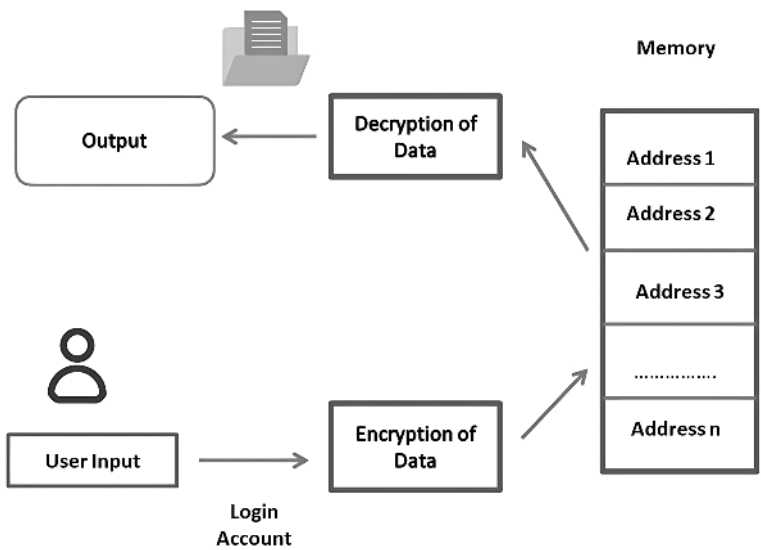

FIGURE 10.1 Overall architecture of AES-GCM.

H: Hash subkey
EK: AES encryption function with key K
GFMul: Galois Field multiplication

High-Level Encryption and Authentication Steps:

a. Initialization:
   Expand the K key if needed.
   Connect IV to the counter to create the initial counter block, J0.
   For every block of plaintext Pi.
b. Galois/Counter Mode Encryption:
   If needed, the K key can be expanded with Galois/Counter Mode encryption.
   Connect IV to the counter, and you have a first counter block J_0.
   By increasing the block count of plaintext P_i by J_{i+1}, a block counter is created for each block.
   The J_i block can be encrypted by using the K key while utilizing AES encryption.
   The cipher block C_i can be obtained by computing the plaintext block's length using Pi and XOR the resulting crypt text.
c. Finalization and Authentication:
   If needed, alter the K key. The first counter J_0 is generated by connecting the IV to the corresponding counter.
   J_i block counters are created by doubling the value of the counter, where 1 is J_{i+1} .J_i blocks can be encrypted using K-key while being encrypted using AES.
   Transform the plaintext block into a pair and get the resulting ciphertext. The identification code of the block cipher C_i is P_i, which regulates the T test label.
   J_{final} is a cryptographic block counter that differs in taking into account the length of the written text and the value of its final counter. XOR J_{final} is used to protect the last block of encrypted ciphertext.
   To obtain T, multiply the result by the hash subkey H acquired from the AES cipher for the empty block.
   AES-GCM has become a widely accepted standard for secure communications due to its ability to provide efficient authentication and encryption.

10.7 ENHANCING AUTHENTICATION AND ACCESS CONTROL IN DIGITAL HEALTH

This section clearly explains the fundamental of Enhancing Authentication and Access Control in Digital Health for a better understanding of the upcoming trends.

10.7.1 Integration of Kyber and AES-GCM

The integration utilizes AES-GCM for efficient data encryption and authentication, and Kyber for secure key exchange method.

Key Exchange using Kyber:

Secure communication by using multiple Kyber keys. Disclose the personal Kyber public keys belonging to the members.

Mathematical formula for AES-GCM:

Algorithms for AES-GCM include the XOR function for encryption and combing multiple Galois fields and polynomial reduction for analysis. Although the details are complex, the secure combination of AES encryption and GCM analysis is the key.

Table 10.2 shows the comparative study of the algorithms and it describes algorithm strengths and weaknesses.

$$GF\left(2^{128}\right) Multiplication : a * b = \sum_{i=0}^{127} c_i \, x^i \tag{1}$$

where ci = ai* b + ai − 1* b* x + … + a0* b* x 127 − i

The formula provided is a representation of Galois Field Multiplication in the context of AES-GCM, which is used for the authentication component of the algorithm. Here's an explanation of the key components:

GF(2^{128}): This refers to the Galois Field with 2^128 elements, which is used in AES-GCM for the authentication process.

*: Represents multiplication in this Galois Field.

a and b: The binary polynomials being multiplied.

$\sum_{i=0}^{127} 0$: The summation is performed over 128 terms, representing the bit positions in the binary polynomials.

c_i: Coefficient of the polynomials to appear.

x: The primitive element of the Galois Field.

Explanation:

The Galois field in the AES-GCM must be amplified to create analytical tags. The application of arithmetic and bitwise operations on Galois fields is also covered. The polynomial c and the integer called ic are obtained by multiplying two binary numbers, a and b, with 127 as their degree and maximum.

TABLE 10.2
Comparative study of the algorithms with strengths and weaknesses

Algorithm	Strengths and Weaknesses of the algorithms
Kyber + AES-GCM	Strengths: Post-quantum security, effective encryption. Weaknesses: can be calculated on the surface.
RSA + HMAC	Strengths: Well accepted and demonstrated safety. Weaknesses: Vulnerable to quantum attacks.
ECC + ECDSA	Strengths: Strong security with short key lengths. Weakness: Quantum is weak.
Lattice-based Cryptography	Strengths: Post-quantum security. Weaknesses: Limited adoption, potential performance issues.

The way polynomials are represented in binary is important for calculating numbers that then get multiplied with XOR and AND. This method is vital to checking that AES-GCM encryption works correctly and keeps data safe. The Galois field used in the crypto process decides the starting x factor. This Galois field boils down to XOR and AND in binary, giving a ballpark idea of how much computing power matters for this big piece of AES-GCM works[15].

10.7.2 Strengthening Security Protocols of Kyber and AES-GCM

Cryptographic algorithms are essential in the cyber security area to improve security protocols. The combination of Kyber, AES-GCM and quantum-resistant cryptography improves security measures in various domains.

AES-GCM: effective data encryption and analysis

By integrating the Kyber and AES-GCM algorithm, the approach which strengthens the security in digital and wellness data. In order to overcome attacks from quantum computers, Kyber is a post-quantum key exchange technique. Kyber could be able to overcome the existing public-key cryptographic algorithm like RSA and ECC. The proposed technology minimizes the possibility of quantum attacks by utilizing Kyber for secure key exchange and ensuring the data integrity and security.

AES-GCM provides effective encryption and authentication by ensuring the transmitted data's confidentiality, integrity and authenticity. Hence, the combination of Kyber and AES-GCM provide an extensive approach to secure digital assets, even though it's essential to implement and manage these cryptographic techniques to improve their effectiveness and also mitigate the potential threats.

The development of the digital sphere will necessitate the integration of advanced cryptographic techniques to ensure the protection and availability of sensitive data. AES-GCM and Kyber's collaboration highlights the potential of new cryptographic techniques to enhance security standards[16.]

10.8 PERFORMANCE METRICS AND OBSERVATIONS

Assessing the effectiveness and efficiency of the proposed model involves examining various methods, particularly about quantum resistance cryptography (QRC)[8–10]. The model's security and computing load, key generation, encryption and decryption speed should be evaluated. Below, the observations and insights from evaluating the performance of QRC models for these parameters are presented in tabular form.

10.8.1 Performance Metrics Table

A general analysis of the QRC model shows that although it provides a significant improvement in quantum resistance protection, there are changes in computational performance, as shown in Table 10.3. The computational overhead, slower key generation, and encryption/decryption speeds are areas of consideration. However, the inherent security strength against quantum attacks positions QRC as a crucial solution for securing digital health and other sensitive data in the era of advancing quantum computing.

TABLE 10.3
Metrics of algorithm and its observations

Metric	Observations
Computational Overhead	Higher computational overhead due to complex mathematical operations in quantum-resistant algorithms.
Key Generation Speed	Slower key generation compared to traditional cryptographic models.
Encryption Speed	Encryption speed may be slower due to intricate mathematical operations in quantum-resistant algorithms.
Decryption Speed	Decryption speed may be slower, requiring optimization efforts for real-world applications.
Security Strength	Strong resistance to quantum attacks, providing a higher level of security.
Usability and Integration	Integration challenges into legacy systems; ongoing research to enhance usability and compatibility.

TABLE 10.4
Kyber vs. AES-GCM performance comparison

Evaluation Metrics	Kyber Encryption	AES-GCM Encryption
Key Generation Time (ms)	20	12
Encryption Time (ms)	60	50
Decryption Time (ms)	80	65
Key Size (bits)	256	256
Cipher text Size (bytes)	1600	1568
CPU Utilization (%)	20	16
Memory Utilization (MB)	12	10
Throughput (Mbps)	120	140
Security Level (bits)	256	128

Table 10.3 shows the performance metrics of QRC model with its different observations. The ongoing optimization, research, and development efforts aim to address these performance challenges, making Quantum-Resistant Cryptography a promising avenue for ensuring the long-term security of digital health systems and other critical applications. As technology advances, streamlining security and performance will be critical to QRC's success in diverse IT environments.

The Quantum Resistance Cryptography Performance Comparison table compares the Kyber crypto-algorithm to AES-GCM, including evaluating various criteria such as security, speed and performance.

The following is a performance comparison of AES-GCM and Kyber:

Table 10.4 highlighted the difference between the encryption methods of the two cryptographic algorithms such as Kyber and ES-GCM. The table shows the strength

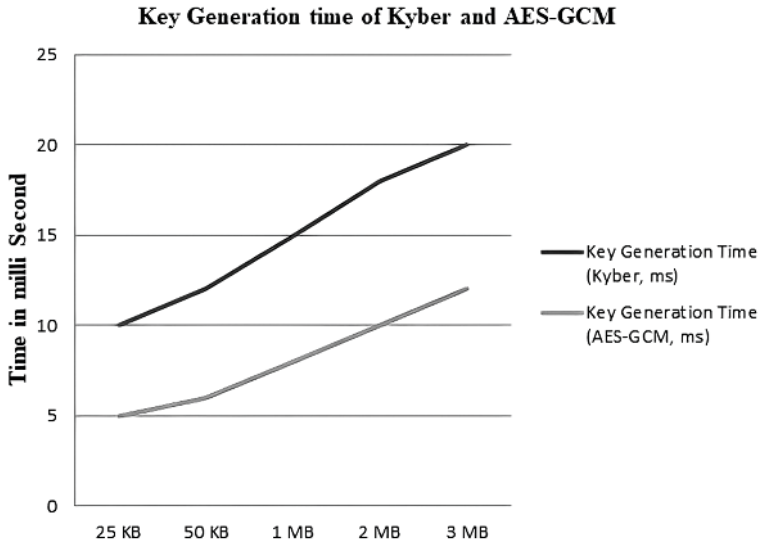

FIGURE 10.2 Comparison of key generation time in ms.

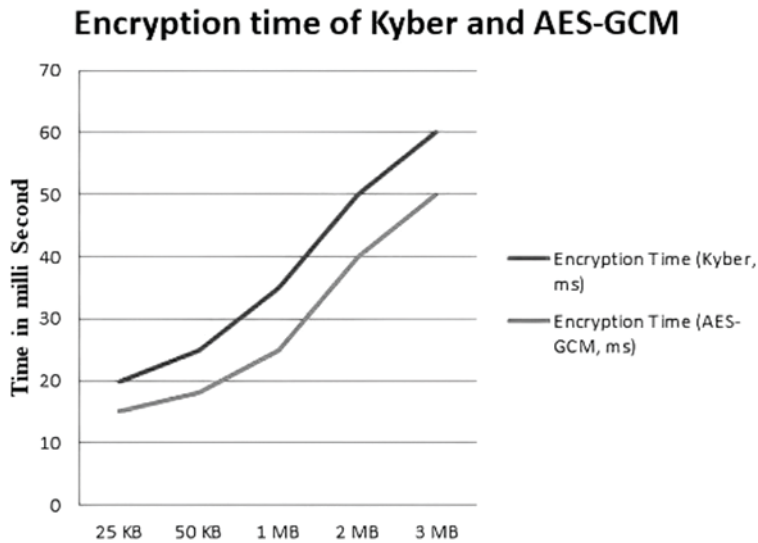

FIGURE 10.3 Comparison of encryption time in ms.

and weakness of the two algorithms in terms of security, latency, key generation times, resource usage and processing speed.

Figure 10.2 compares key generation times (ms) for Kyber and AES-GCM at different file sizes (25 KB to 3 MB). In Figure 10.3, we look at the encryption time (ms) for Kyber and AES-GCM for different file sizes (25 KB to 3 MB).

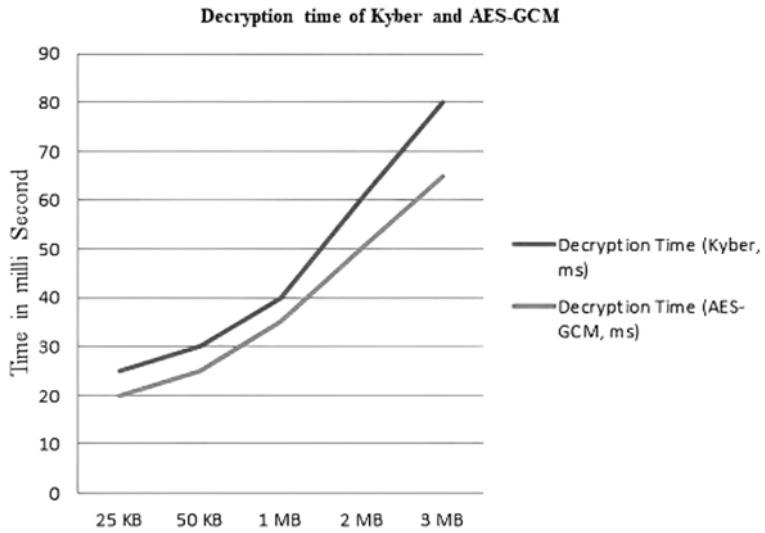

FIGURE 10.4 Comparison of decryption time in ms.

Kyber exhibits significantly higher generation times than AES-GCM, showing a computable difference. This information is important for evaluating the effectiveness of core generation, supporting AES-GCM in fast-paced scenarios.

Notably, Kyber exhibits significantly longer encryption times than AES-GCM, suggesting a possible trade-off between the algorithms in terms of computational efficiency. This information helps to understand their different types of work.
Here we examine the decryption times (ms) for AES-GCM and Kyber at various file sizes (ranging from 25 KB to 3 MB) in Figure 10.4.

Notably, there is a calculable difference between the two encryption methods since Kyber shows more excellent decryption times than AES-GCM. This study offers insightful information on their relative performance traits[17].

10.9 FUTURE-PROOFING SECURITY MEASURES

Enhanced monitoring and control of access is achieved through biometric authentication, which enhances the security of password-based systems.

Employ Blockchains: Utilize blockchain technology to produce unmodifiable, centralized health records that are both transparent and traceable.

By utilizing AI and machine learning, threat detection can be enhanced through the use of predictive analytics. They encourage collaboration and impartiality; create a robust health information exchange (HIE) infrastructure that facilitates the transfer of uniform health data across platforms[18].

Maintaining a focus on human values through education and awareness campaigns is crucial in helping healthcare workers reduce the risk of insider attacks.

Supporting the exchange of cyber security information among healthcare institutions is key to enhancing online safety.

10.10 CONCLUSION

Securing digital health data is an innovation with challenges. The approaches provided in this chapter are developing quantum-resistant encryption as a reliable and adaptable solution in the digital security model. The healthcare industry uses quantum resistance measures to strengthen its security and ensure its privacy, integrity and access to healthcare data in more secure way. By integrating advanced cryptographic rules, it makes digital healthcare data more secure and shielded from unauthorized access.

REFERENCES

[1] Dhinakaran, D., Srinivasan, L., Sankar, S. U., & Selvaraj, D. (2024). Quantum-based privacy-preserving techniques for secure and trustworthy internet of medical things an extensive analysis. *Quantum Information and Computation*, 24(3&4), 227–266.

[2] Saberi Kamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, 10(10.

[3] Wazid, M., Das, A. K., & Park, Y. (2024). Generic quantum blockchain-envisioned security framework for IoT environment: Architecture, security benefits and future research. *IEEE Open Journal of the Computer Society*, 5, 248–267, 2024, doi: 10.1109/OJCS.2024.3397307.

[4] Nagpal, S. et al. (2024). Quantum computing integrated patterns for real-time cryptography in assorted domains. *IEEE Access*. doi: 10.1109/ACCESS.2024.3401162

[5] Raich, A., & Gadicha, V. (2024). Enhancing authentication security against MITM attacks through bioinspired identity management & blockchain-enhanced protocols. *International Journal of Intelligent Systems and Applications in Engineering*, 12(10s), 468–476.

[6] Sutradhar, K., Venkatesh, R., & Venkatesh, P. (2024). Smart healthcare services employing quantum internet of things on metaverse. In Healthcare Services in the Metaverse (pp. 170–189). CRC Press.

[7] Daniel, S. A., & Victor, S. S. (2024). Emerging trends in cybersecurity for critical infrastructure protection: A comprehensive review. *Computer Science & IT Research Journal*, 5(3), 576–593.

[8] Batista, E., Lopez-Aguilar, P., & Solanas, A. (2024, June). Smart health in the 6G era: bringing security to future smart health services. In *IEEE Communications Magazine*, vol. 62, no. 6, pp. 74–80. doi: 10.1109/MCOM.019.2300122.

[9] Aithal, P. S. (2023). Advances and new research opportunities in quantum computing technology by integrating it with other ICCT underlying technologies. *International Journal of Case Studies in Business, IT and Education (IJCSBE)*, 7(3), 314–358.

[10] Jaime, F. J., Muñoz, A., Rodríguez-Gómez, F., & Jerez-Calero, A. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare. *Sensors*, 23(21), 8944.

[11] Chengoden, R., Victor, N., Huynh-The, T., Yenduri, G., Jhaveri, R. H., Alazab, M., ... & Gadekallu, T. R. (2023). Metaverse for healthcare: a survey on potential applications, challenges and future directions. *IEEE Access*, 11, 12765–12795

[12] De Roure, D., & Santos, O. (2023). NLP, the BB84 quantum cryptography protocol and the NIST-approved quantum-resistant cryptographic algorithms. Authorea Preprints.

[13] Hernández-Álvarez, L., Bullón Pérez, J. J., Batista, F. K., & Queiruga-Dios, A. (2022). Security threats and cryptographic protocols for medical wearables. Mathematics, 10(6), 886.

[14] Dadhich, M., Tiwari, H. (2022). Quantum blockchain for smart society: applications, challenges, and opportunities. *Advancements in Quantum Blockchain With Real-Time Applications*. 178–198.

[15] Aanjanadevi, S., Aanjankumar, S., Ramela, K. R., & Palanisamy, V. (2023). Face attribute convolutional neural network system for data security with improved crypto biometrics. *Computer Systems Science & Engineering*, 46(1), 2353–2362.

[16] Aanjanadevi, S., Palanisamy, V., Aanjankumar, S., Poonkuntran, S., & Karthikeyan, P. (2022). Independent Automobile Intelligent Motion Controller and Redirection, Using a Deep Learning System. In Object Detection with Deep Learning Models (pp. 165–178). Chapman and Hall/CRC.

[17] Xu, D., Wang, X., Hao, Y., Zhang, Z., Hao, Q., Jia, H., ... & Zhang, L. (2022). Ring-explwe: A high-performance and lightweight post-quantum encryption scheme for resource-constrained iot devices. *IEEE Internet of Things Journal*, 9(23), 24122–24134.

[18] Negro-Calduch, E., Azzopardi-Muscat, N., Krishnamurthy, R. S., & Novillo-Ortiz, D. (2021). Technological progress in electronic health record system optimization: Systematic review of systematic literature reviews. *International Journal of Medical Informatics*, 152, 104507.

11 ECG-Based Authentication System with Enhanced Security Using Modified CNN Classifier

S. Sureshkumar, A.V. Santhosh Babu, Joseph James, R. Priya, and B. Sakthivel

11.1 INTRODUCTION

ECG plays a vibrant part in the biomedical signal field that process a heart's electrical activity over time where signal serves as a fundamental diagnostic tool in cardiology.[1] The individual pattern that presents in ECG allows for higher security in clinical assessments. An authentication system achieves a substantial transition in all fields by using various biometric innovations like fingerprints, facial features and even cardiac patterns etc.[2] These authentications are used to improve security and convenience compared to conventional methods like passwords.[3]

Recently, ECG authentication patterns possess unique specific traits that offer a high level of individuality similar to fingerprints.[4] The ECG signals are used as an authentication system that has higher security. Furthermore, the DL model has applied to ECG signal patterns to enhance security. The DL model exhibits unparalleled process in extracting intricate features and patterns from ECG signals.[5] The DL models perform preprocessing, feature extraction and classification to reduce complexity.

This work presents an advanced ECG authentication system using deep learning models. Initially, the system uses a hybrid feature extraction module to extract key features from ECG signals. This module integrates LSTM combined with an autoencoder for feature extraction. Subsequently, a modified CNN method is used to extract a feature. The hyperparameters of this modified CNN are optimized using the Cuckoo Search optimization to improve performance.

The work is organized as follows: related works are given in Section 11.2. The preliminary part is described in Section 11.3. Next, ECG classification is discussed in Section 11.4 and Section 11.5 carries a result that discusses the proposed model. Section 11.6 discusses a conclusion followed by its references.

DOI: 10.1201/9781032711379-11

11.2 RELATED WORKS

S. K. Cherupally et al.[6] proposed an authentication algorithm for wearable devices using ECG signals. The modified deep-learning models are used for training the ECG signals. Experimental results on hardware devices show that the proposed deep learning model-based algorithm shows lower error rates on ECG data sets.

J. S. Arteaga-Falconi, et al.[7] developed an ECG authentication system for mobile applications. This model uses a DL algorithm for the classification of signals that attained a higher accuracy. S. J. Kang[8] presented a cross-correlation analysis for ECG authentication. The correlation between signals is used to match the signals. The proposed algorithm is implemented in hardware devices and analysed based on rejection rates and false acceptance.

The four-step model for ECG authentication is proposed by Dhanush M. et al.[9] This step involves peak detection, noise filtering, extraction and autocorrelation. The combined autocorrelation and filtering model improves the accuracy of the model by 5%.

Recently, the body area network gained more attention due to its IoT-enabled features. The security of this type of system is very important due to its sensitive data handling. Kiranyaz et al.[10] proposed an authentication system for body area networks using ECG. The hash functions for encryption algorithms are generated using ECG features.[11]

For classification, the CNN-based models show higher accuracy. However, the CNN models suffered from high hardware costs. The optimized CNN model is proposed by G. Wang et al.[12] for ECG authentication. The features from ECG signals are extracted using CNN for further processing. The complexity of the CNN model is reduced by using binarization-based optimizations with 96.5% accuracy.

Y. Chu et al.[13] proposed a residual network mutual ECG authentication system. The residual network shows higher accuracy by using skip connections that allow the model to learn the features deeply. Experimental results on the Arrhythmia database show a less equal error rate when compared to other models.

The hybrid model-based ECG authentication system is proposed by S. K. TR et al.[14] This model combines Alex net with inception net for ECG classification. Experimental results on the PhysioNet database show an accuracy of 95.6% and an error rate of 2.56%. A. S. Kassab et al.[15] developed a two-step authentication model for an ECG-based biometric verification system. Initially, the noises from ECG signals are removed using an autoencoder. Then, the filtered signals are classified using the CNN model, increasing accuracy by 5.4%.

D. Jiang et al.[16] proposed a stage antieducation model for IoT-enabled systems. This model combines both iris and ECG for verification. Initially, the image processing techniques were applied to verify the iris of the person using a deep learning model. Then, the ECG signal of the person is verified for confirmation for accessing resources. This dual-factor model improves the security of the system with two levels.

The VGG model with attention mechanism is proposed by V. Narayana et al. [17] for ECG signal processing. The attention mechanism of the VGG model introduces multipath feature learning to increase classification accuracy. Results on the Arrhythmia Database show that the VGG model achieves a higher accuracy of 95.6%.

N. Raheja et al.[18] introduced an ECG encryption algorithm for authentication. The features like peaks in an ECG signal are used for encrypting data in algorithms. The proposed model is applied in a triple advanced encryption algorithm and verified for different bit sizes.

The new model using an echo state network for ECG processing is proposed by N. Ibtehaz et al.[19] This echo state model uses reservoir concepts to learn the features. The reservoir is the group of neurons which extract multiple features from the ECG signals. S. I. Safie et al.[20] developed a new feature extraction for ECG authentication systems. This system uses pulse width modulation to extract the features from ECG signals. Compared to other approaches, the pulse width modulation approach extracts all levels of features and improves classification accuracies.

The hybrid authentication system is proposed by M. Derawi et al.[21] This system combines human gait with ECG for verifications. The gait of the person denotes the walking pattern which is unique to every person. The gait model combined with ECG shows higher accuracy without any model complexities.

S.-K. Kim et al.[22] presented an ECG authentication model. The time interval between the peaks of the ECG signal is used as a feature for verification. Experimental results on ECG databases show higher accuracy and precision rates.

R. Salloum et al.[23] constructed an authentication model using RNNs as a feedback connection to process the data. The RNN allows the authentication models to store the features for higher accuracy. The modified KNN model is proposed by S. Safie et al.[24] for ECG authentications. This modified KNN model combines pulse width modulation with KNN for accurate feature extractions. The proposed model is verified in the PhysioNet database with varying time sequences.

11.3 PRELIMINARY

This section presents an autoencoder, LSTM and Cuckoo Search optimization for biometric authentication.

11.3.1 Autoencoder

An autoencoder is a neural network designed for unsupervised learning that aims to reconstruct its input data that has an encoder module as ‘E’ and a decoder module as ‘D’. An input data is mapped into a lower-dimensional latent in an E module. The module ‘D’ reconstructed the original input from this reduced character. The reduction between an input and the output compressed data representation is to be achieved.

The encoder f(x) is represented with an x to a latent symbol z.

$$z=f(x) \tag{1}$$

The decoder g(z) reconstructed input as x’ from z from an encoder.

$$x'=g(z) \tag{2}$$

The Autoencoder reduced an error among x and x' based on the loss function i.e, mean squared error (MSE):

$$MSE=MSE=n1\ i=1\Sigma n\ (xi-x'i)^2 \tag{3}$$

The network parameters are optimized to reduce the error. This is achieved through backpropagation and gradient descent algorithms.

11.3.2 LSTM

The LSTM structure given in Figure 11.1 is designed to tackle the capturing long-term dependencies problems in sequential data.[11,25] It's capable of learning and remembering over long sequences making it well-suited for sequential tasks. It presented a memory cell to store data over long sequences and it updated through a set of gates. These gates allow information to be retained or forgotten selectively. It has a Forget Gate (FG), Input Gate (IG) and Output Gate (OG) where FG has data to be discarded from the cell state. The IG controls new data to the cell state. The OG manages the data to be output based on the cell state. It maintains a hidden state that is passed between time steps and acts as a short-term memory.
The LSTM gate outputs can be represented as:

$$f_t=\sigma\left(W_{xf}.x_t+.W_{hf}.h_t-1+b_f\right) \tag{4}$$

$$i_t=\sigma\left(W_{xi}.x_t+.W_{hi}.h_t-1+b_i\right) \tag{5}$$

$$\overline{c}_t=tanh\left(W_{xc}.x_t+.W_{hc}.h_t-1+b_c\right) \tag{6}$$

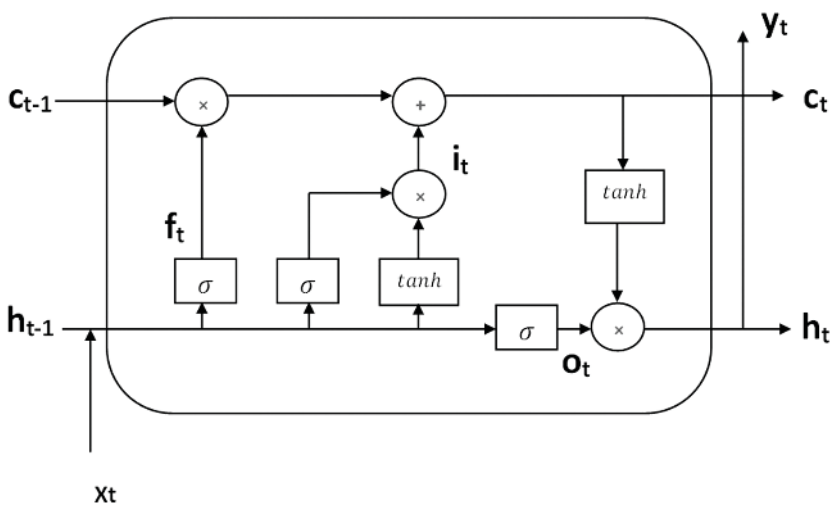

FIGURE 11.1 LSTM structure.

$$c_t = f_t * c_{t-1} + i_t * \overline{c}_t \tag{7}$$

$$O_t = \sigma\left(W_{xo}.x_t + W_{ho}.h_t - 1 + b_o\right) \tag{8}$$

$$h_t = O_t * \tanh \tag{9}$$

$$y_t = \sigma\left(W_{hy}.h_t + b_y\right) \tag{10}$$

$$\sigma(x) = \frac{1}{1+e^{-x}} \tag{11}$$

Where f_t, i_t, O_t represents the FG, IG and OG functions with weights W_{xf}, W_{xi}, W_{xo} and b represents the bias values.

Cuckoo Search Algorithm (CSA)

The CSA is a nature-inspired optimization model based on the breeding nature of cuckoo species that lay their eggs in other birds' nests. The CSA is used to emulate the cuckoo's behaviour to evaluate an optimal solution to provide an objective function. In optimization, a nest represents a candidate solution to the optimization problem. Each nest is characterized by a set of parameters or variables. Based on the objective function, a function evaluates how good or bad a solution (nest) is. The CSA includes five stages: Initialization, Egg Laying, Egg Destruction and Replacement, Local Search and Termination

In initialization, generate an initial population of nests (solutions) randomly or using a specific strategy. In Egg Laying (Exploration stage), each cuckoo lays eggs (new solutions) in a randomly chosen nest based on a levy flight or a random walk.

Initialize N nests randomly: Xi for i=1,2,...,N

$$s=\text{Levy}(\lambda)\cdot u\ 1\ \cdot s'1 \tag{12}$$

$$S = Levy(\lambda).\frac{1}{u^{1/2}}\frac{1}{s'} \tag{13}$$

where λ indicates a scaling factor with the step size of 's' and 'u' represented as a random number and s′ is presented as a step size obtained from Levy flight.

In the Egg Destruction and Replacement stage, evaluate the fitness of new solutions (eggs) against the existing ones. Replace the nest with the new egg if the new result is improved. Optionally, some eggs may be discarded to maintain diversity. Evaluate the fitness of nests:

$$f(Xi) \text{ for } i=1, 2,...,N \tag{14}$$

Fitness function f assesses the quality of each solution.

In local search (Optional), perform a local search around the best solutions to fine-tune them and enhance exploitation.

$$X_i = \begin{cases} X_{new}, & if \quad f\left(X_{new}\right) < f\left(X_i\right) \\ X, & otherwise \end{cases} \tag{15}$$

Replace the existing nests with better solutions based on their Fitness function f assesses. In the termination stage, the algorithm Stop is based on predefined criteria (maximum iterations, reaching a certain solution quality, etc.). Termination occurs after a specified number of iterations or upon reaching a certain solution quality. The Cuckoo Search Algorithm iteratively applies these steps, updating nests through Levy flights, evaluating fitness, and replacing nests with better solutions until termination conditions are met.

11.4 PROPOSED SYSTEM

The feature extraction is performed by a hybrid model and modified CNN for classification. The autoencoder and LSTM architecture integrates for ECG signal analysis that capitalizes both neural network models as shown in Figure 11.2. The autoencoder extracts intricate features by compressing input data into a latent representation. The LSTM captures temporal dependencies within ECG data. The raw ECG signal is subjected to feature extraction by an autoencoder in the proposed model. The use of an autoencoder increases the model's ability to detect important patterns inherent in the data. These encoded features are fed into an LSTM network that allows the long-range temporal subtleties and dependencies which present in a sequence of ECG signal.

The modified CNN classification is performed next of feature extraction that accommodates the extracted feature from an autoencoder LSTM. This hybrid model

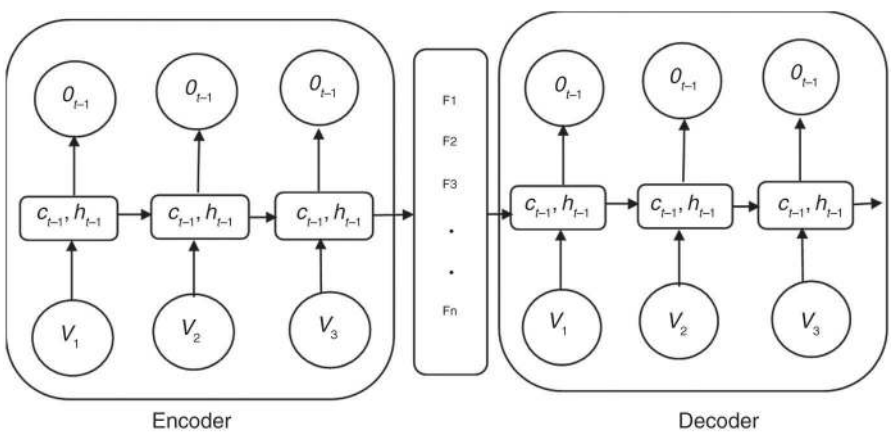

FIGURE 11.2 Proposed system.

is used to enlarge its capacity to discriminate among ECG signal. The CSA method fine-tunes the CNN's hyperparameters of learning rates, kernel sizes and filter counts. This optimization used to enhance the CNN's efficacy in accurately categorizing ECG signals.

11.4.1 Hybrid Model

The LSTM and autoencoder model are integrated and known as a hybrid model. The autoencoder model has an encoder/decoder process for a dimensionality reduction. The raw ECG signals into a short latent space by learning the hardest features that reduce reconstruction error. In this way the LSTM identifies complex patterns and significant features over time in ECG processing. This hybrid model extracts high from the ECG signal from the hand held devices then process them by a combination of compressed illustrations using autoencoder with a sequential learning capability of LSTM. It enhances the ability to interpret the fundamental patterns in the ECG signals.

Features:
The hybrid LSTM autoencoder is given in Figure 11.3 which comprises two distinct LSTM layers. The initial LSTM layer serves as the autoencoder segment to transform input data into a condensed vector representation. Subsequently, the second LSTM layer utilizes the output from the encoder to reconstruct the original input data. The model undergoes pre-training for 200 epochs, during which it learns to generate a representative encoding and accurately reconstruct the input.

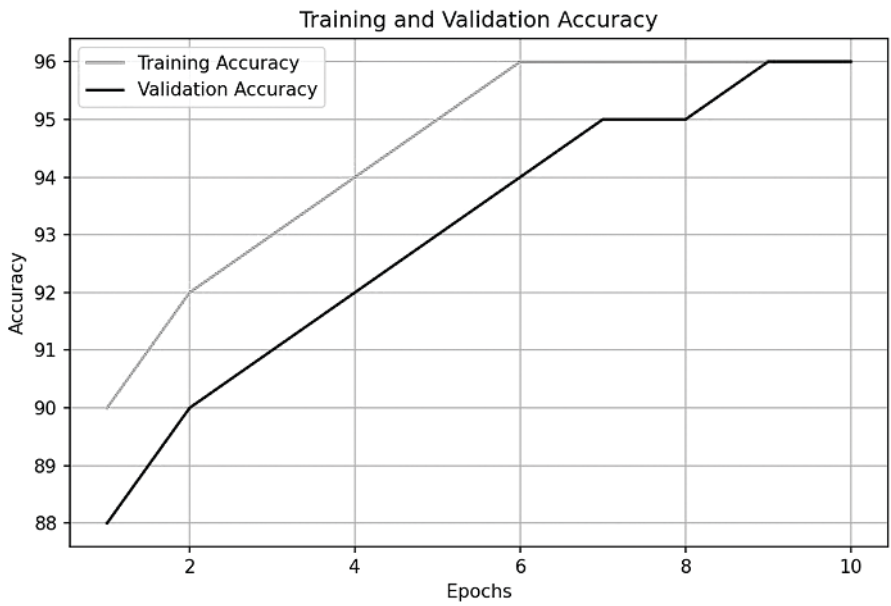

FIGURE 11.3 LSTM autoencoder.

Upon achieving the desired proficiency, the decoder component of this model is eliminated, streamlining the architecture to solely encompass the encoder's functionality. The features extracted from ECG signals using combined autoencoder and LSTM models can include various characteristics that capture important aspects of the cardiac cycle. Some of the features commonly extracted are R-peak intervals, Morphological Features, Heart Rate Variability (HRV) Features, Waveform Patterns, and Complex Time-Domain and Frequency-Domain Features.

The R-peak time duration among successive R-peaks provides information about heart rate variability and rhythm irregularities. The Morphological Features are a measure of the height and width of ECG waveforms (P, Q, R, S, T waves). The Waveform Patterns include shape, duration, and abnormalities in the P-wave and T-wave patterns.

The Complex Time-Domain and Frequency-Domain Features are Wavelet Transform Coefficients and Statistical Entropy Measures. The Wavelet Transform Coefficients extract information at different scales and resolutions. The Statistical Entropy Measures quantify signal irregularity and complexity. These features are derived from ECG signals via a combination of autoencoder-based extraction and LSTM-based temporal learning.

11.4.2 Hyperparameter Tuning

Hyperparameters Tuning of CNNs is crucial to achieving optimal performance and generalization on a given dataset. CNNs have several hyperparameters such as the number of layers, kernel size, number of filters, pooling size, etc. The different architectures can significantly impact the network's capacity to learn complex patterns. Hyperparameters influence the network's ability to generalize well on unseen data. Incorrectly chosen hyperparameters might lead to overfitting. The size and number of filters in convolutional layers determine the patterns/features learned. The larger kernel sizes might capture more complex features, but they increase computational costs. The pooling operations reduce the spatial dimensions of the feature maps. The layers and the width of layers affect the model's capacity to learn hierarchical representations. The proposed CNN tuning using CSA is given below:

```
# Pseudocode for CNN Hyperparameter Tuning
# Define functions to create, train, and evaluate CNN models
def create_cnn_model(parameters):
    # Create a CNN model based on the given hyperparameters
    # Return the compiled model
def train_and_evaluate(model, train_data, validation_data):
    # Train the model using training data and validate using validation data
    # Return the validation accuracy or any metric for evaluation
# Define Cuckoo Search Algorithm specific functions
def initialize_nests(num_nests):
    # Initialize a population of nests with random hyperparameters
    # Return a list of nests
def levy_flight():
```

```
    # Implement Levy flight for exploration
    # Return a step size for the Levy flight
def replace_nest(nests, new_nest):
    # Replace a nest in the population with a new nest if it's better
    # Return updated nests
# Cuckoo Search Algorithm for CNN hyperparameter tuning
def cuckoo_search_cnn(max_iterations):
    # Initialization phase
    num_nests = 10
    discovery_rate = 0.25
        # Open phase
    train_data, validation_data = load_data()  # Load and split dataset
        # Initialize nests
    nests = initialize_nests(num_nests)
        for iteration in range(max_iterations):
        # Exploration phase
        for nest in nests:
            step_size = levy_flight()
            # Generate new solutions (hyperparameters)
            new_nest = explore_with_levy_flight(nest, step_size)
                # Evaluation phase
            new_nest_accuracy = train_and_evaluate(create_cnn_model(new_
                nest), train_data, validation_data)
                # Replacement phase
            if new_nest_accuracy > nest_accuracy:
                nests = replace_nest(nests, new_nest)
        # Select the best solution (hyperparameters)
    best_solution = select_best_solution(nests)
    return best_solution
# Usage example
best_hyperparameters = cuckoo_search_cnn(max_iterations=100)
print("Best hyperparameters found:", best_hyperparameters)
```

The pseudocode of CSA tuning hyperparameters in CNNs initiates by loading and splitting the dataset to train and validate. The population of nests are initialized with random hyperparameters, then iteratively exploring new solutions using Levy flights and evaluating these solutions by training CNN models. Then, replace existing nests with better-performing solutions before selecting the best hyperparameters based on the achieved accuracy or metrics

11.5 RESULT AND DISCUSSION

The proposed system is coded Python IDLE and verified in the ECG data set (www.kaggle.com/datasets/bjoernjostein/ecgid-database) The dataset utilized in this study comprises 310 ECG recordings sourced from a group of 90 individuals. Each

TABLE 11.1
Performance of feature extraction model

Peak	Precision	Recall	Accuracy	F1 Score	Peak
R	85.20	82.50	88.90	91.25	R
P	90.80	88.90	87.50	89.40	P
Q	82.70	84.60	81.80	83.10	Q
S	91.20	92.40	94.10	93.70	S
T	92.50	94.20	96.50	97.10	T

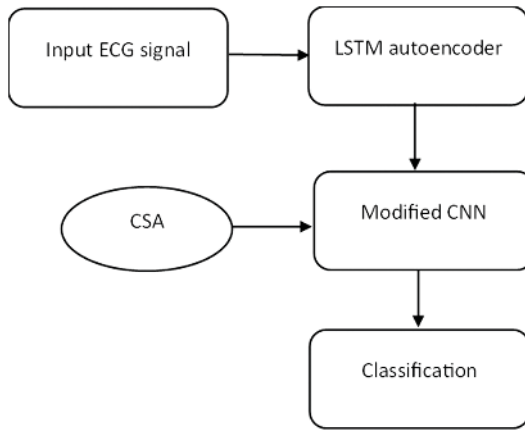

FIGURE 11.4 Performance analysis.

recording, lasting 20 seconds, is characterized by ECG Lead I information, featuring a 500 Hz digitized sampling rate, 12-bit resolution, and a nominal ±10 mV voltage range. Within each recording, 10 beats are annotated, showcasing unaudited R-wave and T-wave peak detections acquired through an automated detector. This dataset stands as a collection that offers an avenue for thorough analysis and exploration of cardiac activities within the study cohort. With its focus on R-wave and T-wave annotations, it presents valuable insights into cardiac rhythm and morphology, representing a significant asset for ECG signal processing research and the development of algorithms pertaining to arrhythmia detection. Table 11.1 shows the performance of feature extraction proposed for a various peak annotation (R, P, Q, S, T) within ECG recordings

From Table 11.1, Precision scores an accuracy of positive predictions that range from 85.20% to 92.50%. The Recall rate shows identification of true positive instances that range from 82.50% to 94.20%. Accuracy shows overall model correctness that varied from 81.90% to 96.50%. Additionally, F1 scores indicate a mean of precision and recall that ranges from 91.25% to 97.10%. The performance analysis shown in Figure 11.4.

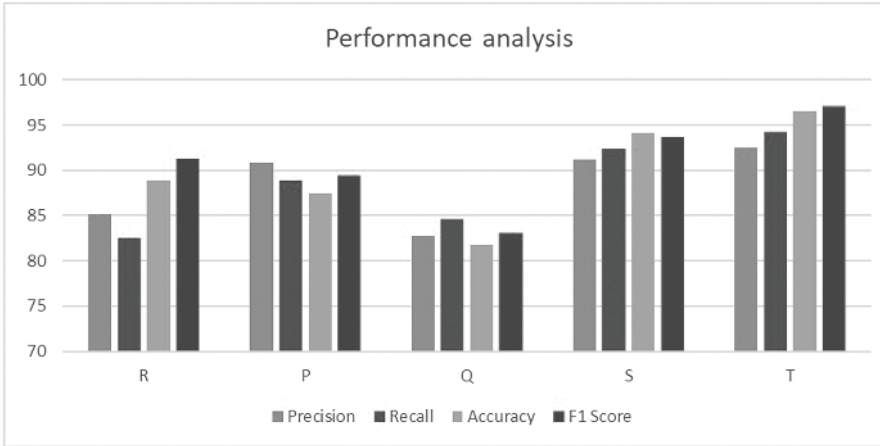

FIGURE 11.5 Training and validation of model.

TABLE 11.2
Performance analysis

Method	Accuracy	F1 Score	Precision	Recall
SVM	0.75	0.68	0.72	0.65
CNN	0.92	0.88	0.90	0.86
ESN	0.90	0.86	0.88	0.84
Hybrid model	0.92	0.89	0.91	0.87
LSTM with CNN	0.91	0.88	0.90	0.86
Proposed	0.96	0.94	0.95	0.93

The graphs Figures 11.5 and 11.6 illustrate the performance trends of a CNN model across multiple epochs during the training and validation phases. The training accuracy represents the accuracy of the CNN model on the training dataset across consecutive epochs. The increasing trend in the training accuracy demonstrates the model's ability to learn from the training data, steadily improving its predictive capability with each epoch. The validation accuracy depicts the accuracy of the CNN model on a separate validation dataset throughout the training process. The rising trend in validation accuracy indicates the model's generalization and ability to perform well on unseen data, validating its learning capacity beyond the training dataset.

The performance of the proposed model given in Table 11.2. The proposed LSTM-CNN hybrid model shows superior performance across multiple evaluation metrics. The proposed model shows the accuracy of 96% which significantly surpasses the accuracy rates achieved by traditional methods like SVM (75%), CNN (92%), ESN (90%), Hybrid models (92%), and LSTM with CNN (91%). Moreover, its F1 Score of 94% demonstrates a balanced trade-off between precision and recall, indicating a robust ability to accurately classify authentic ECG

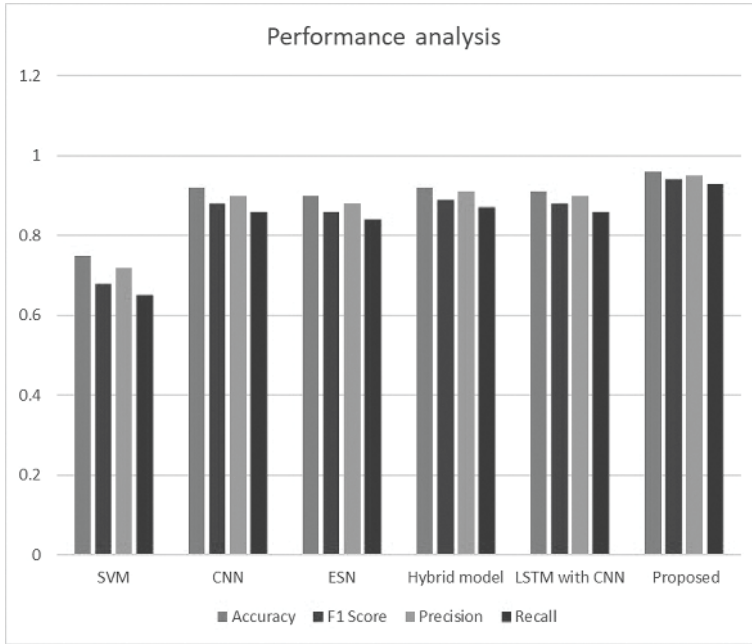

FIGURE 11.6 Performance analysis.

instances while minimizing false positives and false negatives. In terms of precision, the proposed model achieves 95%, exhibiting a high ratio of accurately identified authentic instances among positive predictions which overcomes all other methods. Additionally, its recall rate of 93% signifies its capability to effectively capture most positive instances out of the total actual positives, which dominates alternative methodologies. This collective superiority establishes the proposed LSTM-CNN hybrid model as a promising solution for ECG-based authentication. The results are graphically shown in Figure 11.6.

The confusion matrix outlines the performance evaluation of a classification model used in an ECG authentication system as shown in Figure 11.7. Among the recorded instances, the model correctly identified 93 instances of actual positive cases. This result proves the model's proficiency in recognizing authentic ECG recordings and accurately predicting them as positive. Impressively, the model displayed no instances of misclassifying actual negative cases as positive. These results indicate a robust capability to avoid falsely categorizing non-authentic instances as authentic. However, the model encountered challenges in identifying a small subset of authentic ECG recordings by misclassifying seven instances of actual positive cases as negative. While excelling in authenticating positive cases, these misclassifications highlight a potential area for improvement in accurately recognizing all genuine ECG recordings. The number of true negatives representing correctly identified non-authentic instances is not explicitly provided but is inferred to encompass all actual negative instances excluding any falsely predicted positives. It overall maintains a

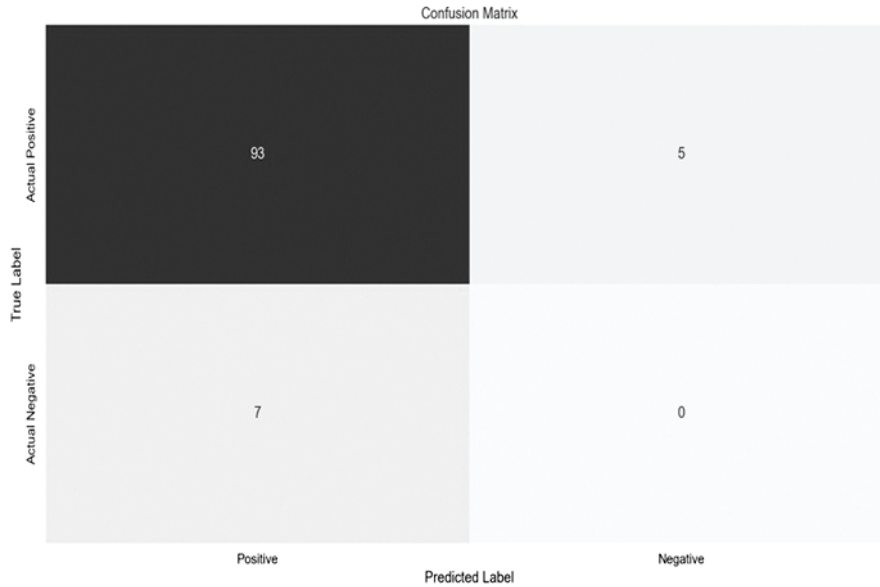

FIGURE 11.7 Confusion matrix.

high accuracy in recognizing non-authentic cases. This evaluation provides valuable insights into the model's strengths and areas for enhancements.

11.6 CONCLUSION

In this work, the ECG authentication is presented using an LSTM autoencoder for feature extraction and modified CNN for classification. The LSTM autoencoders are used as feature extraction that shows superior performance in capturing complex patterns within electrocardiogram signals. The model's ability to encode and decode ECG data extracts crucial features with minimized noise. Moreover, a modified CNN with an optimization algorithm demonstrates a significant classification stage using CSA. When compared to other models, the proposed optimized model achieves improved accuracy and efficiency in differentiating and classifying ECG features that ensure more effective authentication functions.

REFERENCES

1. M. Abo-Zahhad, S. M. Ahmed and S. N. Abbas, "Biometric Authentication Based on PCG and ECG Signals: Present Status and Future Directions," in *SIViP,* vol. 8, pp. 739–751, 2014.
2. A. Page, A. Kulkarni and T. Mohsenin, "Utilizing Deep Neural Nets for an Embedded ECG-Based Biometric Authentication System," In *Proceedings of the 2015 IEEE Biomedical Circuits and Systems Conference (BioCAS)*, Atlanta, GA, USA, 22–24 October 2015; pp. 1–4.

3. A. Santos, I. Medeiros, P. Resque, D. Rosário, M. Nogueira, A. Santos, E. Cerqueira and K. R. Chowdhury, "ECG-Based User Authentication and Identification Method on VANETs," In *Proceedings of the 10th Latin America Networking Conference*, Association for Computing Machinery (LANC'18), New York, NY, USA, 3–4 October 2018; pp. 119–122.
4. H. P. da Silva, A. Fred, A. Lourenço and A. K. Jain, "Finger ECG signal for user authentication: Usability and performance," In *Proceedings of the 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, Arlington, VA, USA, 29 September–2 October 2013; pp. 1–8.
5. S. Y. Chun, J. H. Kang, H. Kim, C. Lee, I. Oakley and S. P. Kim, "ECG Based User Authentication for Wearable Devices Using Short Time Fourier Transform," In *Proceedings of the 2016 39th International Conference on Telecommunications and Signal Processing (TSP)*, Vienna, Austria, 27–29 June 2016; pp. 656–659.
6. S. K. Cherupally et al., "ECG Authentication Neural Network Hardware Design with Collective Optimization of Low Precision and Structured Compression," In *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, Sapporo, Japan, 2019; pp. 1–5, doi: 10.1109/ISCAS.2019.8702308.
7. J. S. Arteaga-Falconi, H. Al Osman and A. El Saddik, "ECG Authentication for Mobile Devices," in *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 591–600, March 2016, doi: 10.1109/TIM.2015.2503863.
8. S. J. Kang, S. Y. Lee, H. I. Cho and H. Park, "ECG Authentication System Design Based on Signal Analysis in Mobile and Wearable Devices," in *IEEE Signal Processing Letters*, vol. 23, no. 6, pp. 805–808, June 2016, doi: 10.1109/LSP.2016.2531996.
9. M. Dhanush, A. Jain, S. C. Moulyashree, A. Melkot and A. V. Manjula, "ECG based authentication using Autocorrelation and Artificial Neural Networks," In *2016 International Conference on Computing, Analytics and Security Trends (CAST)*, Pune, India, 2016; pp. 238–243, doi: 10.1109/CAST.2016.7914973.
10. S. Kiranyaz, T. Ince and M. Gabbouj, "Real-Time Patient-Specific ECG Classification by 1-D Convolutional Neural Networks," in *IEEE Transactions Biomedcine Engineering*, vol. 63, no. 3, pp. 664–675, 2015.
11. T. Cuong-Le, H.-L. Minh, S. Khatir, M. A. Wahab, M. T. Tran and S. Mirjalili, "A Novel Version of Cuckoo Search Algorithm for Solving Optimization Problems," *Expert Systems with Applications*, vol. 186, p. 115669, 2021.
12. G. Wang, D. John and A. Nag, "Low Complexity ECG Biometric Authentication for IoT Edge Devices," In *2020 IEEE International Conference on Integrated Circuits, Technologies and Applications (ICTA)*, Nanjing, China, 2020; pp. 145–146, doi: 10.1109/ICTA50426.2020.9332012.
13. Y. Chu, H. Shen and K. Huang, "ECG Authentication Method Based on Parallel Multi-Scale One-Dimensional Residual Network With Center and Margin Loss," in *IEEE Access*, vol. 7, pp. 51598–51607, 2019, doi: 10.1109/ACCESS.2019.2912519.
14. T. R. Satish Kumar and T. L. Purushottama, "ECG Authentication Reinforced by Pretrained Convolutional Neural Networks," In *2023 International Conference on Network, Multimedia and Information Technology (NMITCON)*, Bengaluru, India, 2023; pp. 1–6, doi: 10.1109/NMITCON58196.2023.10275834.
15. A. S. Kassab, S. Banou, D. Roy and K. Chowdhury, "FERST: A Full ECG Reception System for User Authentication using Two-stage Deep Learning," In *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*, Rio de Janeiro, Brazil, 2022; pp. 873–878, doi: 10.1109/GLOBECOM48099.2022.10001694.
16. D. Jiang, G. Zhang, O. W. Samuel, F. Liu and H. Xiao, "Dual-Factor WBAN Enhanced Authentication System Based on Iris and ECG Descriptors," in *IEEE*

Sensors Journal, vol. 22, no. 19, pp. 19000–19009, 1 Oct 2022, doi: 10.1109/JSEN.2022.3198645.

17. V. Narayana, A. K. Vobbilisetty, S. Mantripragada, V. Merugu and K. Prakash, "ECG Based Biometric Authentication System using Deep Learning Methods," In *2022 3rd International Conference for Emerging Technology (INCET)*, Belgaum, India, 2022; pp. 1–4, doi: 10.1109/INCET54531.2022.9824792.
18. N. Raheja and A. K. Manocha, "An Efficient Encryption-Authentication Scheme for Electrocardiogram Data using the 3DES and Water Cycle Optimization Algorithm," In *2021 6th International Conference on Signal Processing, Computing and Control (ISPCC)*, Solan, India, 2021; pp. 10–14, doi: 10.1109/ISPCC53510.2021.9609415.
19. N. Ibtehaz et al., "EDITH: ECG Biometrics Aided by Deep Learning for Reliable Individual Authentication," in *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 6, no. 4, pp. 928–940, Aug. 2022, doi: 10.1109/TETCI.2021.3131374.
20. S. I. Safie, J. J. Soraghan and L. Petropoulakis, "ECG biometric authentication using Pulse Active Width (PAW)," In *2011 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications (BIOMS)*, Milan, Italy, 2011; pp. 1–6, doi: 10.1109/BIOMS.2011.6052382.
21. M. Derawi and I. Voitenko, "Fusion of Gait and ECG for Biometric User Authentication," In *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*, *Darmstadt, Germany*, 2014; pp. 1–4.
22. S. -K. Kim, C. Y. Yeun and P. D. Yoo, "An Enhanced Machine Learning-Based Biometric Authentication System Using RR-Interval Framed Electrocardiograms," in *IEEE Access*, vol. 7, pp. 168669–168674, 2019, doi: 10.1109/ACCESS.2019.2954576.
23. R. Salloum and C. -C. J. Kuo, "ECG-Based Biometrics Using Recurrent Neural Networks," In *2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, New Orleans, LA, USA, 2017; pp. 2062–2066, doi: 10.1109/ICASSP.2017.7952519.
24. S. Safie, M. I. Yusof, K. Kadir, H. Nasir and L. Petropoulakis, "Multiple pulse K-Nearest Neighbors authentication for Malay ECG based class attendance system," In *2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T)*, Kuala Lumpur, Malaysia, 2014; pp. 156–160, doi: 10.1109/ICE2T.2014.7006238.
25. P. Zhang, J. Cheng, and Y. Zhao, "Classification of ECG Signals Based on LSTM and CNN," In *Artificial Intelligence and Security: 6th International Conference, ICAIS 2020, Hohhot, China, July 17–20, 2020, Proceedings, Part III 6* (pp. 278–289). Springer Singapore.

12 Ransomware and Risk Management in Digital Health and Wellness Security

M. Arun Anoop, P. Karthikeyan, and A.P. Chaithanya

12.1 INTRODUCTION

A software outbreak known as ransomware silently infiltrates your computer and prevents you from accessing the system or from encrypting your information. Encryption methods are used by many ransomware infestations to render your files unreadable. Ransomware infestations aim to extort you for bitcoin in exchange for access to your files.

Ransomware definition Payoff malware, or ransomware, is a kind of malware that keeps users from getting to their system or individual files and requests a recovery instalment to recapture access.[1]

- ✓ You can be infected when you unwittingly download ransomware from compromised websites, spam messages, or other malware.
- ✓ How does information abduction go?
  Shows up on the user's computer.
  Ransomware locks the screen.
  Crypto-ransomware tracks down specific records and encrypts them.
- ✓ How does the record encryption function?
  - When inside a framework, crypto-ransomware interfaces with haphazardly produced spaces to download a public key.
  - It looks for significant efficiency records like .doc,.xls, .xls, and .pdf
  - It creates a key for each record and, at that point, encrypts them.
  - The crypto-ransomware then composes the encoded key toward the start, everything being equal.[2]
  - Displays the ransom note.
- ✓ How is the ransom paid?
  - The victim receives a ransom note with instructions on the most proficient method to pay through Bitcoin. The victim purchases Bitcoin and transfers it to the attacker's Bitcoin address. The victim sends the transfer ID to the

 DOI: 10.1201/9781032711379-12

attacker as verification of payment. Once the transaction is complete, the attacker will send the decryption instructions to the person in question.

✓ Ransomware families:
- Petya can modify, overwrite, or wipe files.
- Maze is a combination of an attack and a data breach.
- Crypto-locker fooled targets into downloading malignant connections sent through emails.
- Stop-crypt
- Wannacry spreads itself by exploiting a weakness in the Windows Server Message Block (SMB) convention.
- Morris-crypt
- Tesla-crypt
- Lockbit ransom requests involve financial payment in exchange for decryption.
- Bad rabbits bypass user account control and gain elevated administrative privileges.
- Cerber is a utility that any hacker can access.
- Conti targets Microsoft products.
- Gandcrab targets consumers and businesses with computers running Microsoft Windows, and it can be avoided with the help of a spy-hunter tool.
- Crypto-wall uses advance techniques to hide from its victims.
- Locky distributed via malicious .doc files.

Your machine may be harmed by ransomware.[3] Ransomware is malicious software designed to prevent access to your computer or files until a ransom is paid. Ransomware can also corrupt data, destroy files, and damage your system, resulting in the irreversible loss of important files. It can prevent you from using your computer or accessing your data by encrypting and blocking your files are displayed in Figure 12.1 and Figure 12.2.

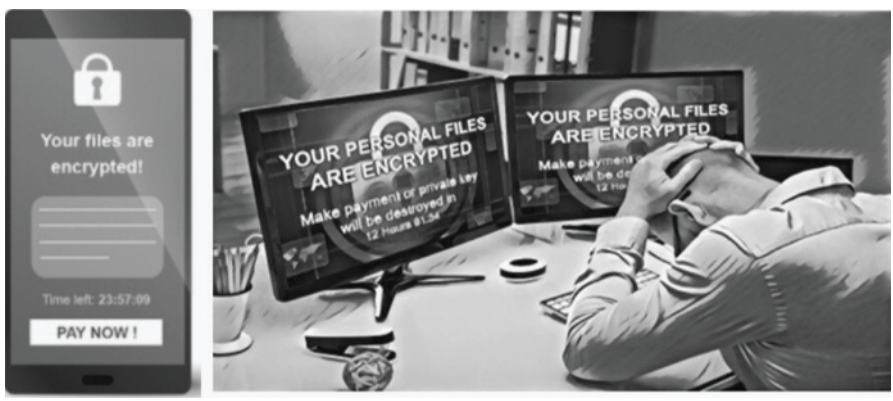

FIGURE 12.1 Ransomware encrypted message.

FIGURE 12.2 Ransomware bitcoin message.

Wannacry or wcry[4] malware has a self-duplicating nature, this is a worm-like nature that spreads through internal networks over the public internet. Furthermore, it finishes by exploiting a weakness in the Microsoft cut-off message block protocol. One of the exploit names is 'MS17-100 Eternal Blue'. W-cry has two parts predominantly, which are ransomware usefulness and proliferation. Proliferation has the advantage of being able to empower SMB exploitation capacities. W-cry, following expansion like wcry, .wry, .wncry, .wnry, .wncryt, and decryption apparatus which costs around $300–400 USD. W-cry typically uses TOR channels for order-and-control correspondence.

Also, paying the ransom[5] doesn't ensure that your data will be recuperated and better options are backup arrangements and anti-malware software to get rid of these attacks. The most ideal way to do this is to guarantee your PC framework utilizes a respectable backup of important files, use a firewall and anti-malware software, and refrain from downloading files you're not sure about. It's also crucial to protect your passwords and to refrain from downloading programs or accessing websites that you don't know or trust.

The steps for spreading ransomware are the following,

- Installation: Set keys in the Windows registry to start it while booting your system, it will load on the lock screen.
- Contacting headquarters: It communicates with the owner remotely.

- Handshake and keys: two keys they have, one in the infected machine and the other in the owner's machine.
- Encryption: Once infected all the system files get encrypted.
- Extortion: Displays a time limit and Bitcoin payment details for decryption keys.

Ransomware[6] spreads in computers by being sent through phishing messages, containing virus connections, and getting a ransomware contamination by downloading through torrents. Even healthcare sessions are also being affected by these ransomware infections, so pharmacy people must take care that their systems are not being attacked by remote agents.

Furthermore[7] keep in mind that malware such as ransomware can also introduce Trojan horses and keyloggers, which can steal user accounts and passwords. Your computer will be protected and these virus components removed if you run a scan on it with reputable anti-malware software. You can notify the local police authorities if a ransomware infection has infected your computer.

Indeed, ransomware[8] can influence WIFI organizations, as malignant entertainers can utilize it to deal with the organization, take private data, and lock out users. If a ransomware assault is effective, it could prompt a deficiency of administration as well as data, and at times, monetary misfortunes. WMIC orders can go through Windows PowerShell administrator mode is displayed in Figure 12.3.

12.2 RELATED WORKS

A prototype based on the RESTCONF protocol was constructed by Eunsoo Kim et al. in 2018,[3] demonstrating the applicability of the suggested framework for ransomware prevention, DDoS mitigation, and network separation in real-world circumstances.

Golev et al.[9] employed GonnaCry, a crypto-ransomware. The database of the website is installed in a WordPress instance on the compromised Linux Debian server. The information is synchronized and kept on the private cloud. It has been demonstrated that it is possible to recover the compromised files via a bash script and the private cloud web interface.

Yépez et al.[10] investigated to determine whether the University of Guayaquil, a public institution, has the appropriate safeguards in place to address this escalating threat. To do this, computer administrators were surveyed to determine how well-prepared they were for an assault of this kind.

The most attack-prone and vulnerable malware has been the subject of research by Kalphana et al. in 2024.. The writers made an effort to address a few malware detection techniques.[11]

The evolution of cryptovirus in Linux is examined by Rosen Hristev et al.,[12] who also shows how to use a private cloud to recover data arrays following a ransomware outbreak on Linux.

For the Silhouette Coefficient for FCM and K-Means Clustering Based on SSDEEP & SDHASH Similarity Scores for Ransomware Corpora and FCM Clustering Performance Evaluation Based on SSDEEP & SDHASH for Wannacry Ransomware Corpus, Naik et al.[13] employed cluster sizes of 2, 3, 4, 5, 6, 7.

Windows API calls were used by Yuuki Takeuchi et al.[14] to detect ransomware using support vector machines.

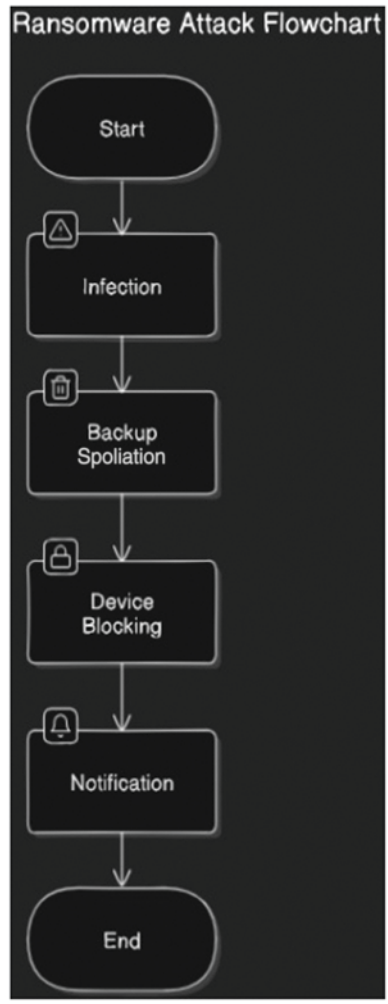

FIGURE 12.3 Phases of ransomware attack.

Table 12.1 is mainly a comparison between affected type and ransomware types. Different ransomware types have been identified and their affected region-based details have been attached to this article. Affected types in the sense that some parameters have been collected for showing the fields that were affected by ransomware. As we know ransomware once infected through any medium, encrypts and set timer and bitcoin contact details. Even a paying person could not identify the destination person or identity. The timer will get activated at the same time as ransomware activation and it will warn the user to collect the decryption key by collecting crypto currency bitcoins. Bitcoins not brought or making any delay may destroy data.

In Table 12.2, different affected types discovered and identified different ransomware attacks. Its detailed information is also processed in Table 12.2. Affected

TABLE 12.1
Related works summary

Related works	Description
[2]	Used gain ratio for feature selection and random forest for classification.
[3]	Used cuckoo sandbox and trained using different supervised methods for evaluation performance calculation.
[4]	The two-stage mixed method means the Markov chain is used for the first stage and the random forest is used for the second stage.
[5]	Features collection, sliding window, backup, and 12 families considered.
[6]	Seven families and their variants considered.
[7]	Class and non-class frequencies were evaluated based on six classifiers.
[8]	Accuracy and missing rate calculated based on ransomware and goodware data.
[9]	Captured network initially. After that TCP/IP features filtered and extracted.

types discovered mainly are country-wise, Network, healthcare, IoT devices, Operating systems, and Android devices. In the description section, where each attack is targeted or primarily targeted, those details are mentioned. Some attacks have more than one functionality also shared in Table 12.3.[15]

LazyPredict is a software that classifies machine learning models based on likelihood of suitability. You can forecast binary and continuous variables, respectively, using the LazyClassifier and LazyRegressor that are both included in the LazyPredict.

In Figure 12.4, dataset attribute details have been mentioned and the last column is for identifying labels or name. Anyway, during evaluation we will not consider Serial number or File Name as a feature. Features 2–16 can consider features or attributes. Feature or column or attribute a 17th column keeping it as a prediction. This prediction can be done based on a supervised machine-learning classification algorithm. Initially, different classifiers have been processed. Here a package named LazyPredict (can download or mount using PIP command) or LazyClassifiers also have processed for different machine learning models. In Table 12.4, it is very clear PIP package is an easy research tool for identifying different classifiers to predict the classification accuracy. Parameters Accuracy, Balanced Accuracy, ROC AUC value, F1-score, and Time Taken are also measured by the help of AI or ML techniques.[16]

In Figures 12.5 and 12.6, the first and second stage evaluation results are attached. It shows results based on accuracy score and testing accuracy. Different colour-wise results are shown to identify each classifier and its accuracy values to show the efficiency.

The evaluation step plotted different classifiers based on their accuracy and among that bagging classifier accuracy achieved is better than any other we presented. In Table 12.5, a preliminary evaluation of processed machine learning algorithms is mentioned. In Table 12.6, evaluation metrics details are mentioned. Tables 12.5–12.23 are completely added based on the evaluation results.[3,9,17,18]

TABLE 12.2
Ransomware and affected regions

	Affected type			
	Network	**IT Companies**	**Healthcare**	**Country wise**
Ransomware type	1) Network-Based Ransomware 2) Remote Desktop Protocol (RDP) Attacks 3) Phishing and Social Engineering 4) Supply Chain Attacks 5) Man-in-the-Middle (MitM) Attacks 6) Zero-Day Attacks	1) File-Encrypting Ransomware a) WannaCry b) CryptoLocker c) Locky 2) Locker Ransomware a) Police-themed ransomware 3) Ransomware-as-a-Service (RaaS) is a model where cybercriminals provide ransomware tools and infrastructure to other individuals to execute attacks. 4) Mobile Ransomware a) SLocker b) Android FileCoder 5) Ransomware a) WannaCry b) NotPetya 6) In DDoS Ransomware, attackers threaten to launch a DDoS attack on the victim's systems or website if the ransom cryptocurrency is not paid.	1) File-Encrypting Ransomware 2) Medical Device Ransomware 3) Data Breach Ransomware 4) Distributed Denial of Service (DDoS) Ransomware 5) Phishing and Social Engineering 6) Targeted Attacks	1) The WannaCry ransomware attack in 2017 affected organizations worldwide, with notable impacts in countries like the United States, United Kingdom, Spain, Russia, and India. 2) The Petya/NotPetya ransomware attack in 2017 targeted Ukrainian institutions, Russia, the United States, and Denmark. 3) The Ryuk ransomware has been associated with targeted attacks in the United States. 4) The SamSam ransomware has primarily targeted organizations in the United States, including healthcare providers, government agencies, and educational institutions. 5) The GandCrab ransomware campaign was widespread globally, affecting organizations in multiple countries.

TABLE 12.3
Affected types and ransomware attacks

Affected Types	Ransomware attacks	Description
Country-wise	CryptoLocker	primarily targeted users in the United States, Canada, and European countries.
	Locky	was distributed through massive spam email campaigns and primarily targeted English-speaking countries, including the United States, Canada, the United Kingdom, and Australia.
	Cerber	It affected users worldwide, with notable impacts in the United States, Germany, France, and Japan. Cerber was often distributed through exploit kits and spam emails.
	WannaCry	It targeted vulnerabilities in the Windows operating system and caused significant disruptions, with notable impacts in the United Kingdom, Russia, Spain, India, and the United States.
	Ryuk	Ryuk ransomware has been associated with targeted attacks on organizations, particularly in the United States.
	GandCrab	It primarily targeted English-speaking countries, including the United States, Canada, the United Kingdom, and Australia.
Network	SamSam	specifically targeted networks of organizations in sectors such as healthcare, government, and education.
	Ryuk	targeted attacks on organizations, particularly in the financial and healthcare sectors.
	Maze	targets corporate networks, particularly those of large organizations where the attackers not only encrypt the data but also threaten to release it publicly if the ransom is not paid.
	LockBit	targets corporate networks and organizations and distributed through phishing emails and exploit kits, aiming to encrypt files on network shares and compromise backups.
	Dharma/CrySiS	targets networks of small to medium-sized businesses which spreads through remote connections or malicious email attachments.
	Sodinokibi/REvil	targets networks of various organizations, including law firms, IT service providers, and manufacturing companies and distributed through phishing mails.

(*continued*)

TABLE 12.3 (Continued)
Affected types and ransomware attacks

Affected Types	Ransomware attacks	Description
Healthcare	WannaCry	It affected hospitals, clinics, and healthcare systems, disrupting patient care and operations.
	Ryuk	observed targeting healthcare organizations.
	Samsam	specifically targeted the healthcare sector, including hospitals and medical centres.
	Maze	targeted healthcare organizations as part of its broader campaign.
	Locky	It typically spreads through phishing emails and malicious attachments, targeting users within healthcare organizations and encrypting critical data.
Operating systems	Windows	WannaCry and Locky primarily affected Windows users and spread through malicious email attachments.
	MacOS	KeRanger is a first variant that distributed through a compromised installer of a legitimate software application.
	Linux	Linux encoder or encoder1 is a variant which encrypted files on Linux servers and demanded a ransom for decryption.
IoT device	BrickerBot	targets IoT devices, specifically those with insecure configurations or default credentials.
	Silex	IoT-targeting malware that aims to compromise and disable IoT devices.
	Mirai	IoT malware that utilizes infected IoT devices to create botnets which are used to launch various attacks, including ransomware campaigns.
Android devices	Android/Filecoder.C	ransomware variant specifically targeted Android devices.
	DoubleLocker	is an Android ransomware that gained attention for its unique behavior.
	Charger	targeted Android devices by masquerading as a legitimate battery-saving app.
	Svpeng	a banking Trojan, Svpeng evolved into a ransomware variant targeting Android devices.
	Simplocker	early ransomware variants specifically targeting Android devices.

```
RangeIndex: 62485 entries, 0 to 62484
Data columns (total 18 columns):
 #   Column              Non-Null Count  Dtype
---  ------              --------------  -----
 0   FileName            62485 non-null  object
 1   md5Hash             62485 non-null  object
 2   Machine             62485 non-null  int64
 3   DebugSize           62485 non-null  int64
 4   DebugRVA            62485 non-null  int64
 5   MajorImageVersion   62485 non-null  int64
 6   MajorOSVersion      62485 non-null  int64
 7   ExportRVA           62485 non-null  int64
 8   ExportSize          62485 non-null  int64
 9   IatVRA              62485 non-null  int64
 10  MajorLinkerVersion  62485 non-null  int64
 11  MinorLinkerVersion  62485 non-null  int64
 12  NumberOfSections    62485 non-null  int64
 13  SizeOfStackReserve  62485 non-null  int64
 14  DllCharacteristics  62485 non-null  int64
 15  ResourceSize        62485 non-null  int64
 16  BitcoinAddresses    62485 non-null  int64
 17  Benign              62485 non-null  int64
dtypes: int64(16), object(2)
```

FIGURE 12.4 Dataset features (1–16) and 17th column is Label for supervised machine learning prediction.

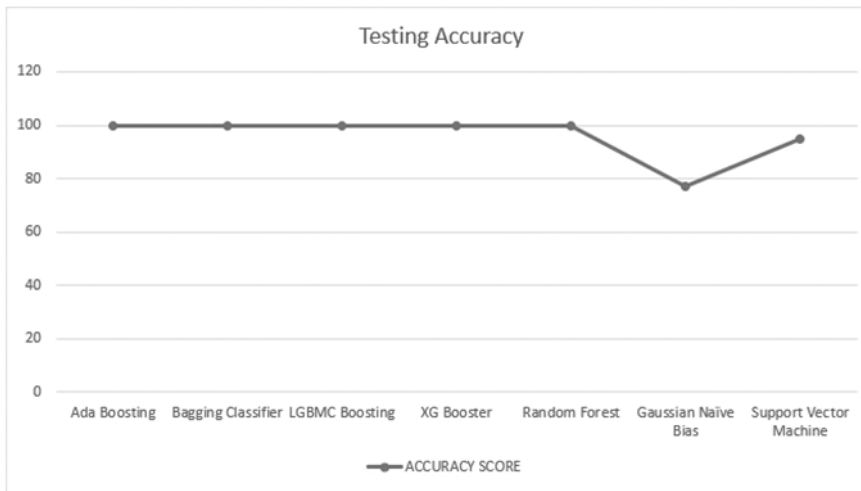

FIGURE 12.5 Second stage results.

TABLE 12.4
Evaluation results based on Lazy-Predict PIP package (Lazy Classifier)

Model	Accuracy	Balanced Accuracy	ROC AUC	F1 Score	Time Taken
AdaBoostClassifier	100	100	100	100	0.93
BaggingClassifier	100	100	100	100	0.34
LGBMClassifier	100	100	100	100	0.38
XGBClassifier	100	100	100	100	0.29
RandomForestClassifier	100	100	100	100	1.22
DecisionTreeClassifier	100	100	100	100	0.1
ExtraTreesClassifier	0.96	0.96	0.96	0.96	0.87
KNeighborsClassifier	0.96	0.96	0.96	0.96	0.35
LabelPropagation	0.96	0.96	0.96	0.96	4.68
LabelSpreading	0.95	0.95	0.95	0.95	6.36
SVC	0.95	0.95	0.95	0.95	2.73
LogisticRegression	0.93	0.93	0.93	0.93	0.15
CalibratedClassifierCV	0.93	0.93	0.93	0.93	4.79
NuSVC	0.92	0.93	0.93	0.92	7.71
LinearSVC	0.92	0.92	0.92	0.92	1.28
ExtraTreeClassifier	0.92	0.92	0.92	0.92	0.04
SGDClassifier	0.9	0.9	0.9	0.9	0.12
QuadraticDiscriminantAnalysis	0.84	0.84	0.84	0.84	0.07
RidgeClassifierCV	0.93	0.93	0.93	0.93	0.09
LinearDiscriminantAnalysis	0.93	0.93	0.93	0.93	0.17
RidgeClassifier	0.93	0.93	0.93	0.93	0.06
BernoulliNB	0.8	0.79	0.79	0.8	0.04
GaussianNB	0.77	0.76	0.76	0.77	0.04
Perceptron	0.66	0.66	0.66	0.66	0.05
NearestCentroid	0.58	0.59	0.59	0.58	0.05
PassiveAggressiveClassifier	0.55	0.55	0.55	0.55	0.06
DummyClassifier	0.55	0.5	0.5	0.38	0.03

12.3 MACHINE-LEARNING ALGORITHMS DETAILS

Following are the machine learning algorithms used for this article.

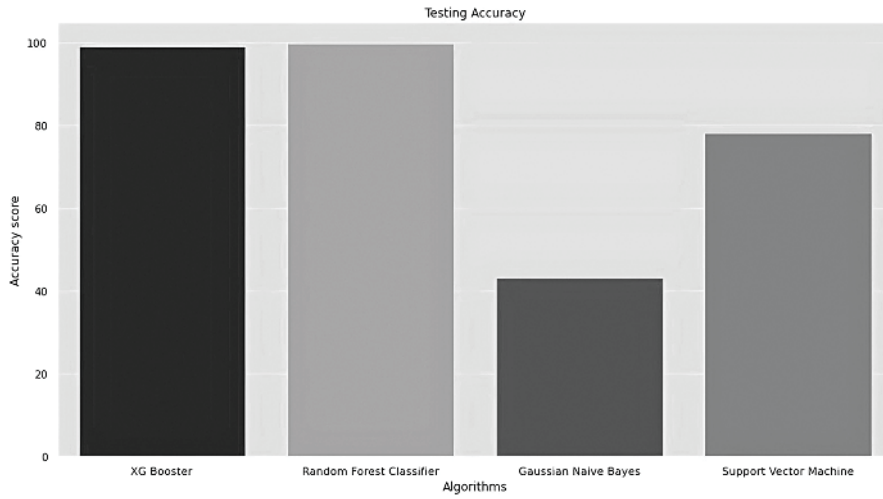

FIGURE 12.6 First stage results.

TABLE 12.5
Classifiers description

Classifiers	Description
ADA Boosting	AdaBoost algorithm, short for Versatile Boosting, is a boosting procedure that is utilized as an Ensemble Strategy in Machine Learning.
Bagging classifier	A bagging classifier is a broadly useful ensemble strategy that can be utilized with a wide range of base models, for example, decision trees, neural-networks, and direct models.
CAT Boosting	CatBoost is an algorithm for gradient boosting on decision trees.
XG Booster	XGBoost means "Extreme Gradient Boosting" and it is an execution of Gradient Boosted decision trees.
Random Forest	It is a classification algorithm comprising numerous decision trees.
Gaussian Naïve Bayes	Gaussian Naïve Bayes is a probabilistic classification algorithm in light of applying Bayes' hypothesis with solid freedom suppositions.
Support Vector Machine	Support Vector Machine (SVM) is a supervised machine learning algorithm utilized by researchers for both classification and regression purposes[10].

TABLE 12.6
Evaluation metrics

Metrics	Description
Precision	$Precision_{\_ransomeware}$ = Correctly Identified / (Correctly Identified + Incorrectly Identified)
Recall	$Recall_{\_ransomware}$ = Correctly Identified / (Correctly Identified + Skipped Data)
Accuracy	$Accuracy_{\_ransomware}$ = Correctly Identified / All data

{Correct Answer = P, Incorrect Answer = N, Correctly Answered Questions = TP, Incorrectly Answered Questions = FP, Skipped Data = FN, Recall = TP / (TP + FN), Precision = TP / (TP + FP), Accuracy = TP / (TP + FP + TN + FN)}

TABLE 12.7
Classifiers evaluation based on accuracy

Classifiers	Accuracy
ADA Boosting	98.57%
Bagging classifier	99.92% Train
	99.75% Test
CAT Boosting	99.0%
XG Booster	99.1%
Random Forest	99.98% Train
	99.71% Test
Gaussian Naïve Bayes	43.47%
	43.13%
Support Vector Machine	78.81% Train
	77.96% Test

TABLE 12.8
Classifiers evaluation based on different metrics

Classifiers	Precision (%)	Recall (%)	F1-score (%)
CAT Boosting	98.82	**99.51**	99.16
Bagging classifier	**99.90**	99.14	**99.42**
XG Boosting	99.54	98.47	99.01
ADA Booster	98.65	98.03	98.34
Random Forest	**99.88**	**99.48**	**99.68**
Gaussian Naïve Bayes	43.10	**99.88**	60.219
Support Vector Machine [19]	85.11	59.22	69.84

TABLE 12.9
CAT boosting (P, R, F1-score) for .EXE files

CAT Boosting	Precision (%)	Recall (%)	F1-score (%)
	98.82	**99.51**	99.16

TABLE 12.10
CAT boosting (P, R, F1-score) for .DLL files

CAT Boosting	Precision (%)	Recall (%)	F1-score (%)
	97.20	**99.59**	98.76

TABLE 12.11
Bagging classifier (P, R, F1-score) for .EXE files

Bagging classifier	Precision (%)	Recall (%)	F1-score (%)
	99.90	99.14	99.42

TABLE 12.12
Bagging classifier (P, R, F1-score) for .DLL files

Bagging classifier	Precision (%)	Recall (%)	F1-score (%)
	97.95	98.34	**99.10**

TABLE 12.13
ADA boosting (P, R, F1-score) for .EXE files

ADA Boosting	Precision (%)	Recall (%)	F1-score (%)
	98.65	98.03	98.34

TABLE 12.14
ADA boosting (P, R, F1-score) for .DLL files

ADA Boosting	Precision (%)	Recall (%)	F1-score (%)
	98.16	97.23	96.04

TABLE 12.15
XG boosting (P, R, F1-score) for .EXE files

XG Boosting	Precision (%)	Recall (%)	F1-score (%)
	99.54	98.47	99.01

TABLE 12.16
XG boosting (P, R, F1-score) for .DLL files

XG Boosting	Precision (%)	Recall (%)	F1-score (%)
	99.51	98.40	98.51

TABLE 12.17
Random Forest classifier (P, R, F1-score) for .EXE files

Random Forest classifier[11]	Precision (%)	Recall (%)	F1-score (%)
	99.88	**99.48**	**99.68**

TABLE 12.18
Random Forest classifier (P, R, F1-score) for .DLL files

Random Forest classifier	Precision (%)	Recall (%)	F1-score (%)
	99.47	**99.24**	**99.01**

TABLE 12.19
Gaussian Naïve Bayes (P, R, F1-score) for .EXE files

GNB	Precision (%)	Recall (%)	F1-score (%)
	43.10	**99.88**	**60.219**

TABLE 12.20
Gaussian Naïve Bayes (P, R, F1-score) for .DLL files

GNB	Precision (%)	Recall (%)	F1-score (%)
	42.31	**98.52**	**59.34**

TABLE 12.21
Support Vector Machine (P, R, F1-score) for .EXE files

SVM	Precision (%)	Recall (%)	F1-score (%)
	85.11	**59.22**	**69.84**

TABLE 12.22
Support Vector Machine (P, R, F1-score) for .DLL files

SVM	Precision (%)	Recall (%)	F1-score (%)
	84.01	57.20	67.04

TABLE 12.23
Performance evaluation

Article	Features	Precision
[17]	13	RF (96.10%)
[18]	1000-7000	RF (97.74%)
[19]	Dynamic	RF (94.59%)
Proposed System	17	RF (.EXE 99.88%, .DLL 99.47%)

12.4 CONCLUSION

Malware detection can be checked using signature, anomaly, and change based on data encrypted and ransomware is a big threat in multimedia data transmission which has already affected many countries, especially different companies in each country, and has resulted in the battle between the development and detection of new malicious behaviour. WannaCry ransomware spread recently; it affected many companies' systems and the creators demanded bitcoins to give decryption keys. Here, we have evaluated different ransomware functionalities and also shared some evaluation results based on wmic, vssadmin, and sc. After that, we have evaluated machine learning-based performance evaluation and have considered seven supervised classifiers. The bagging classifier achieved high accuracy and precision values out of the seven classifiers we have utilized here. Training and testing accuracy, we have identified and tested accuracy collected as classification accuracy of the utilized dataset. Utilized dataset (repeated stratified or stratified cross-validation, 10% of testing split, total number of data 62,485, training input data 56,236 and testing input data 6249) consists of exe and dll based files and we have also evaluated precision, recall and f1-score metrics. Our next work will be based on different families of ransomware and especially Petya, Maze, Crypto locker, Stop crypt, Locky,

Wannacry, Morris crypt, Teslacrypt, Lockbit, Bad rabbit, Cerber, Cryptowall, Conti, and Gandcrab. Finally it is very clear that fine-tuning utilization of different classifiers performed well and model stacking results in 99.75% accuracy noticed while processing bagging classifier.

REFERENCES

1. Alhawi, O.M.K., Baldwin, J., & Dehghantanha, A. (2018). Leveraging machine learning techniques for windows ransomware network traffic detection. In *Cyber Threat Intelligence* (pp. 93–106). Springer: Cham, Switzerland.
2. Mohammed, B. (2020). Ransomware detection using random forest technique. *ICT Express*, 6, 325–331. doi: 10.1016/j.icte.2020.11.001.
3. Kim, E., Kim, K., Lee, S., Jeong, J., & Kim, H. (2018). A framework for managing user-defined security policies to support network security functions. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3164541.3164569
4. Herrera-Silva, J., & Alvarez, M. (2023). Dynamic feature dataset for ransomware detection using machine learning algorithms. *Sensors*, 23, 1053. https://doi.org/10.3390/s23031053.
5. Hwang, J., Kim, J., Lee, S., & Kim, K. (2020). Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wireless Personal Communication*, 112, 2597–2609.
6. Shaukat, S. K., & Ribeiro, V. J. (2018). RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. In *Proceedings of the 2018 10th International Conference on Communication Systems & Networks (COMSNETS)*, Bengaluru, India, 3–7 January 2018 (pp. 356–363). IEEE: Piscataway, NJ, USA.
7. Hirano, M., Hodota, R., & Kobayashi, R. (2022). RanSAP: An open dataset of ransomware storage access patterns for training machine learning models. *Forensic Science International: Digital Investigation*, 40, 301314.
8. Bae, S. I., Lee, G. B., & Im, E.G. (2020). Ransomware detection using machine learning algorithms. *Concurrency and Computation: Practice and Experience*, 32, 1–11.
9. Golev, A., Hristev, R., Veselinova, M., & Kolev, K. (2022). Crypto-ransomware attacks on Linux servers: A data recovery method. *International Journal of Differential Equations and Applications*, 21(2). https://doi.org/10.12732/ijdea.v21i2.2
10. Yépez, J., Alvarado, J., Ortíz, M., & Acosta, N. (2017). Análisis y prevención del Ransomware en la Universidad de Guayaquil. *Revistaespirales.Com*, 1(11), 68–72.
11. Hristev, R., Veselinova, M., & Kolev, K. (2022). Ransomware Target: Linux. Recover Linux Data Arrays after Ransomware Attack. *Eurasia Proceedings of Science, Technology, Engineering and Mathematics*, 19. https://doi.org/10.55549/epstem.1219172
12. Kalphana, K.R., Aanjankumar, S., Surya, M. *et al.* (2024). Prediction of android ransomware with deep learning model using hybrid cryptography. Sci Rep 14, 22351. https://doi.org/10.1038/s41598-024-70544-x
13. Naik, N., Jenkins, P., Savage, N., & Yang, L. (2019). Cyberthreat hunting-part 2: Tracking ransomware threat actors using fuzzy hashing and fuzzy c-means

clustering. In *2019 IEEE international conference on fuzzy systems (FUZZ-IEEE)*, pp. 1–6. IEEE.

14. Takeuchi, Y., Sakai, K., & Fukumoto, S. (2018). Detecting ransomware using support vector machines. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3229710.3229726
15. Takeuchi, Y., Kazuya Sakai, K., & Fukumoto, S. (2018). Detecting ransomware using support vector machines. In *Workshop Proceedings of the 47th International Conference on Parallel Processing*, pp. 1–6.
16. Narudin, F.A., Feizollah, A., Anuar, N.B., & Gani, A. (2016). Evaluation of machine learning classifiers for mobile malware detection. *Software Computing*, 20(1), 343–357.
17. VSSAdmin. Available: www.windows-commandline.com/enable-disable-system-restoreservice/#:~:text=Disable%20System%20restore%20service%20from%20command%20line%20We,command%20line%20you%20can%20run%20the%20below%20command.
18. WMIC. Available: www.cyberithub.com/20-useful-wmic-command-examples-in-windows-cheat-sheet/Ransomware, Available: www.sensorstechforum.com/ransomware-virus-what-is-it/
19. Roseline, S., Abijah, & Geetha, S. (2021). A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks. *Computers & Electrical Engineering*, 92, 107143.

13 Wellness Management Using Incident Response Strategies and Recovery Tools

Practices and Proposal in Healthcare

Jay Prakash Maurya, Monoj Kumar Muchahari, Mansi Bakhshi, Vinesh Kumar, and Rajesh Kumar Dhanaraj

13.1 INTRODUCTION

In the past few years, significant work has been carried out in healthcare industries, to potentially increase incident acknowledgment and response strategies towards wellness management practices. A lot of service schemes and their effective functional nature in India are the reflection of improvements in the healthcare sector and resilient incident response strategies.[1,2] The paradigm shift is from the conventional healthcare system model towards a reinforced method that prioritizes wellness promotions and prevention. This reinforced method seeks input from recent research findings, trends from news, and the scope of the problem and type. Reinforced method design and development is supported by technologies like machine learning and artificial intelligence which also makes it a frontier in healthcare research.[3] Previous research outcomes in wellness management are published on websites or yearly reports issued by the government. Case studies in this sector fill the gap between identification and effectiveness for active policies and loopholes in implemented incidence response plans. The COVID-19 pandemic situation is the best example of aligning the gap between conventional and reinforced paradigms to handle and prepare an improvement policy over critical, proactive, rapid disaster response methods and change/decision-making systems in the healthcare sector. For instance, a study published in the *Journal of Healthcare Management* demonstrated that early intervention through data-driven wellness programs reduced hospital readmissions and healthcare costs while enhancing the quality of patient care.[4] The evolving concept of wellness management places a strong emphasis on the early identification and prevention of

 DOI: 10.1201/9781032711379-13

health issues rather than merely reacting to established medical conditions. Recent research findings in preventive healthcare have shown a direct correlation between early interventions and positive health outcomes.[5] The most impactful domain of the healthcare management field is shown in Figure 13.1. Additionally, these findings are driving the integration of incident response strategies as a proactive approach to incident prevention. Introductory areas of interest related to this article as below.

13.1.1 Healthcare Management

In the ever-evolving sector of healthcare, excellent management is necessary to offer quality patient care, operational efficiency, and regulatory compliance. The intricacy of healthcare systems, from patient data protection to the delivery of critical services, demands a diverse approach to management. This introduction lays the foundation for a deep analysis of healthcare management, looking into the essential components that drive this field. New ideas about infrastructure or policy matters under government / NGO / service-owned organizations refer to healthcare management.[1,6]

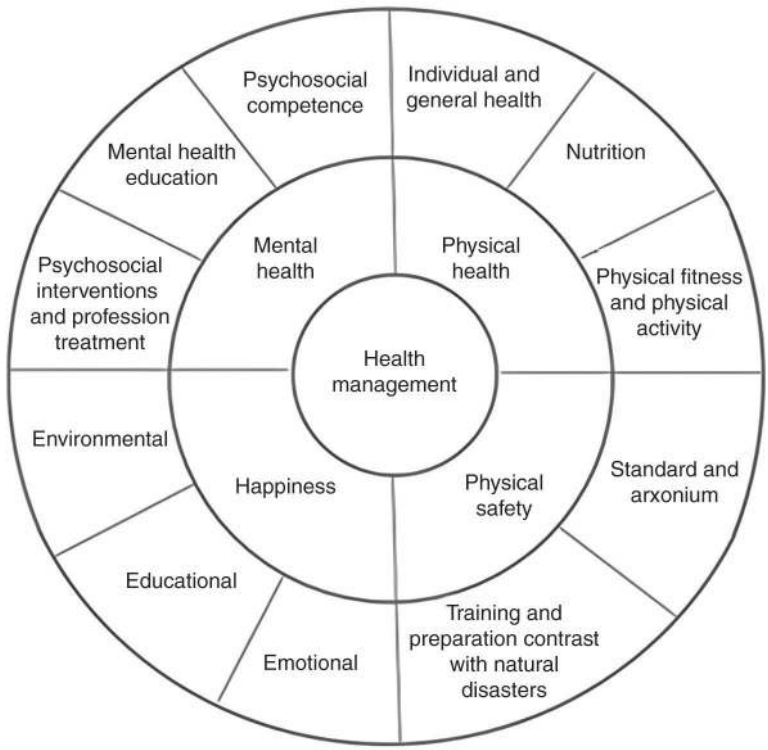

FIGURE 13.1 Health Management Impact Domain.

13.1.1.1 Wellness Management in a Real Environment

Wellness management is not confined to theoretical ideals but extends into the practical reality of healthcare systems. In real-world healthcare scenarios, wellness management takes on a dynamic dimension, involving the delivery of holistic healthcare services, the preservation of patient well-being, and the response to emergent crises. This section presents the concept of wellness management within the context of practical healthcare facilities. Thought-level integration to be healthy can be said to be a prime objective of wellness management. This idea in a real environment is possible through the activation of awareness and education about healthcare in elementary to higher levels.[7]

13.1.1.2 Incident Effecting and Response in India (in Wellness Management)

India's healthcare landscape is marked by unique difficulties and opportunities. A vital aspect of this setting is the management of accidents and crises within the wellness management framework. This portion explains the specific events and dynamics that dictate incident reactions in Indian wellness management. It acts as a predecessor to the consideration of how technology may strengthen these efforts.

13.1.1.3 Supported Technology and Stack

The implementation of technology plays a significant role in increasing incident response and management in healthcare. The technology and infrastructure stack can support incident response activities to reach among the population. By assessing the tools, methods, and resources available, we wish to understand how technology may be leveraged to fortify incident response in the Indian wellness management scenario.

Figure 13.2 shows the overall connected constructs of wellness and the directive research field to conclude the degree of wellness. Recent research in the field of predictive analytics has enabled healthcare institutions to anticipate patient needs more accurately. For instance, a study in the *Journal of Medical Internet Research* reported that predictive analytics allowed for early identification of patients at high risk for specific health conditions, enabling personalized interventions that reduced the incidence of chronic diseases. Recent studies highlight the significance of incident response and recovery not only in the face of crises but also as fundamental components of

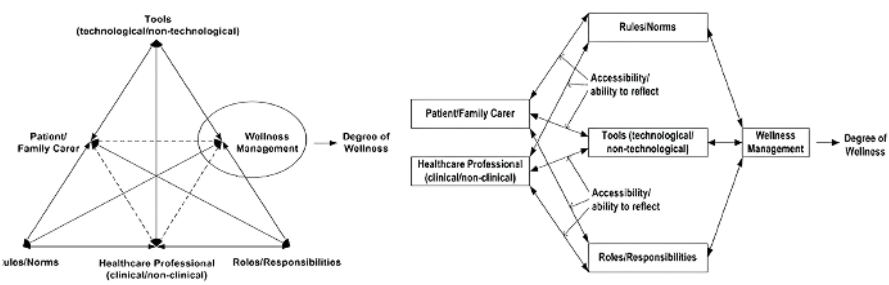

FIGURE 13.2 Overall Wellness Management construct.

day-to-day healthcare operations. Strategies credit a good impact on wellness management and actively contribute toward handling emergencies.[8] Case studies in the *Journal of Healthcare Informatics* show the impact of incident response practices on handling adverse events and patient safety in clinical workflow. Similar types of trends and published articles from different journals/conferences or books gave a critical idea that was taken to draw research highlights and directive pathways for the research society and public involvement.[9] Some of the included related research findings are discussed below:

a) Balancing healthcare costs over improving outcomes of wellness programs was showcased well in "Wellness Programs: A Review of the Evidence," by Mattke et al. (2013). The author also mentioned healthcare's progressive and proactive involvement in response strategies to address trending healthcare risks.[10]
b) The paper "Clinical Incident Management Systems: A Systematic Review" by Kallarakkal et al. (2022) focuses on the importance of the reporting system and raises the importance of judging clinical errors. Minimizing clinical errors in the healthcare ecosystem is a good factor in active wellness management strategies.[11]
c) Chekati et al. (2022) gave directions for discussing disasters and crises to improve healthcare operations disaster recovery plans. The authors also focused on the instrument's properties towards resilience.[12]
d) Asadgol et al. (2019) provide scope for predictive analysis in chronic disasters from diseases. The authors reported and showcased results from various significant tools for proactive intervention in data-driven wellness management programs.[13]

13.1.2 Real-time Tools' Usages

There are numerous incident response strategies and tools that can be utilized and enhance wellness management in healthcare. Electronic Health Records (EHR) Systems is one such tool that enables preemptive health management. It allows healthcare staff to have access to patient data in real time which facilitates early detection of health issues. These systems make incident response simpler by providing a standardized platform for recording and addressing medical incidents.[14]

Predictive analysis software is another tool that is used to identify potential health hazards. It continuously evaluates patient data and supports the creation of data-driven wellness programs. Additionally, incident reporting and monitoring software can be implemented to collect incident data and categorize them, therefore initiating quick incident response procedures. Cloud-based backup solutions ensure that critical medical information is accessible in real time for recovery in the event of a system failure or data breach. Communication and collaboration platforms that provide seamless information exchange are used to facilitate efficient collaboration when responding to incidents. All of these tools and strategies enable healthcare businesses to manage wellness proactively and react quickly to incidents, hence making them more resilient in this dynamic healthcare environment.[15]

13.1.3 Objective

- Deep understanding of emergency and critical situations to predict and prepare response plans and strategies for dynamic change in situations.
- To propose a dynamic landscape of wellness management within the healthcare sector using modern tool integration.
- Modern and innovative ideas to optimize the healthcare system for proactive resilience.
- Awareness and involvement of patients and industry in wellness management programs.

13.2 CHALLENGES IN HEALTHCARE AND WELLNESS MANAGEMENT

Challenges for the healthcare and wellness management field are a complex issue for a government in any country and dependent on country artifacts.[16] Every country has its own way and involved authority and functional system structure for incidence response. Here the Indian artifact was taken to identify significant challenges in the healthcare sector and discussed the following:

- Linguistic variety
- Public awareness deficiency
- Fragmented information
- Emerging dangers
- Resource disparities

The above challenges are not limited; these may lead to several more threats that need to be kept in mind. Apart from rapid improvement in supply chain management interconnectivity and the global healthcare market, the involved organization must focus on finding the following:

1. Finding underserved rural areas to strengthen healthcare infrastructure.
2. Competent healthcare professionals to address the scarcity.

Moreover, national and international institutions or organizations can build collaboration or exchange programs to find talent from other countries. These types of collaborations between parties may screen out the need for education and training programs, especially in rural areas. Rural healthcare resource empowerment as a local community must be part of medical service with external healthcare specialists.[17]

13.3 PRACTICE STRATEGIES AND METHODS FOR INCIDENT RESPONSE

There are varied difficulties that occur when ensuring patient care and safety. Healthcare management finds a major obstacle to work against prevention and control for infections. It may lead to higher expenses and serious consequences if morbidity

and mortality are high. Control practices like hand hygiene, sterilization, disinfection protocols, and evidence-based control practice can help in compliance and may contribute for holistic health management.[7]

13.3.1 Tool-based Support

Real-time incidence response and response co-ordination in an optimal way can be possible through technology integration only. Data analysis helps as a key factor to find minimum dependency, and allocate external resource for any effective prediction. Healthcate professionals and supporting local communities may push towards building tool using machine learning that can support for incidence response and medical services. Example of one very popular initiative of the Government of India is the Arogya Setu app to handover services on a digital platform. This tool can predict disease using questioners and also help the user using location sharing in a critical situation like COVID-19. The government has also implemented telemedicine services that allow patients to seek medical guidance from doctors over the mobile phone or video chat irrespective of the distance

The government has incorporated many modern technologies in their processes that identify and enrol qualified people for healthcare systems. Artificial and advanced data analytics are two of these tools that have made it easier to choose healthcare personnel based on their medical history and demographic data. By enforcing these policies, the government hopes that anyone in need of these benefits can access them without any obstacles.[18]

13.3.2 Educational Programs

The simplest way to propagate any awareness community or major population is by reaching out to educational institutions from necessary to higher education. Approx. 76% of the population is connected to different institutions and from these approx. 42% are active either by ongoing education or by alumni-connecting methods. Incorporating awareness for wellness in the curriculum or through training programs, annual functions, alumni meetings, or through parties applying over-scope areas is a proactive method to integrate every citizen as a social responsibility.[19] Additionally, training programs under the departmental educational programs can help build competency in employees using their initiative to maintain health as a wealth environment in the organization.[20] Some of the government and NGOs are already participating and connected to work on wellness using awareness and education involvement as mentioned:

- NHM (National Health Mission)
- NGO (Non-government organizations like Blood bank clubs)
- IMA (Indian Medical Association)
- PHFI (Public Health Foundation of India (PHFI))
- RBSK (Rastriya Bal Swasthya Karyakram)
- PMJAY (Pradhan Mantri Jan Arogya Yojana) [also known as Ayushman Bharat]

These projects have played a significant role in promoting holistic well-being and ensuring patient data security.

13.3.3 Government Strategies

Government involvement provides the maximum effort in wellness management for the establishment of protocols and financial management. Setting up a centralized authoritative system for advertising, involvement, reliability, and incidence response mechanisms can help to design a good system. An expert or healthcare professional must reach or identify issues in the crisis response preparedness areas. Routine identification of available resources for a population sample must be seen frequently and public participation can improve this through feedback methods direct to the implementing authority to permit faster or more efficient response mechanisms on strategies.[21] In addition, data analytics and AI can help to provide a future view of incidences on roads or disasters for proactive strategy design.[17] As per the 2022–23 wellness plan, Table 13.1 shows strategies and the concerned responsible ministry for implementation.

13.3.4 Awareness Schemes

Different strategies for public awareness were already functional in India through media, community interaction, digital platforms, and the release of government schemes.[22] Identification, measures, and potential impact of these strategies are needed through reaction measures. Raising implementation faults or feedback from stakeholders may have a huge impact on the optimal strategy plan in wellness scheme implementation. The National Disaster Management Authority (NDMA) is one of the key organizations holding responsibilities to measure the Hospital Safety Index. Frequent audits and directional guidelines are the key functional methods for handling

TABLE 13.1
Wellness management strategies in India and functional Government Department

Management Strategy	Government Department
Employee Health	Ministry of Health
The mental health of society	Ministry of Health
Wellness program and advertisement	Ministry of HR
Ergonomic Improvement in Workplace	Ministry of Labor
Training program for employee safety	Ministry of Labor
Flexible Leave Policies	Department of Human Resources
Telecommuting Options	Department of Human Resources
ROI Analysis of Wellness Programs	Ministry of Finance
Monitoring Healthcare Costs	Ministry of Finance
Chronic Disease Prevention	Ministry of Health
Nutrition and Healthy Eating	Ministry of Health
Smoking Cessation Programs	Ministry of Health
Health Risk Assessments (HRA)	Ministry of Health
Supportive Work Culture	Department of Human Resources

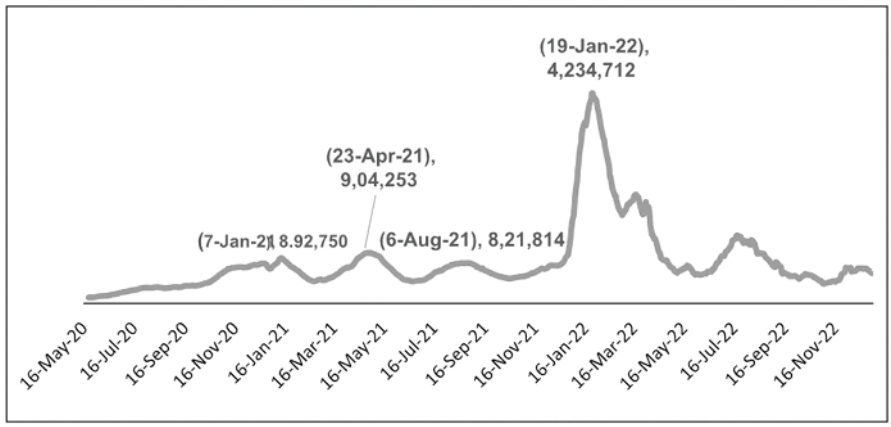

FIGURE 13.3 Month wise COVID-19 case trajectory (India Report).

disaster management. The hospital's welfare schemes like the "Swasthya Raksha Programme", issued by the Ministry of Health and Family Welfare, are important schemes that need to reach every person in the country. This scheme provides guidelines to be well and control methods in regular programs conducted by the health department and other societies for handling disaster situations.[23] Apart from scheme awareness, social responsibility for an individual must be a key point. Institutional awareness schemes can help to involve student teams to work with disasters with active participation of their moral concern through mock drills[7] (Figure 13.3).

13.3.5 Imperfection with States in Incidence Response

State and Central ministry affairs sometimes create a barrier in implementation of clinical ads and strategies. Non-implementation of services provides hurdles / delay or excessive burdens to employ human resource for functional services. Citizens have the right to be educated in the awareness of conveying and understanding clinical acts and functional implementation for their rights and needs in case of incidents. There is public healthcare loss due to policies not being properly propagated over regions due to non-communicable, or mental factors, in factious infectious diseases and pandemics, challenges to behavioral change because of limited access to healthcare resources. In addition, the absence of proper regulation and policy will create a gap in access to healthcare system and people. Society will not tolerate services when vulnerable people are affected significantly.

This can further add to social inequities and complicate efforts to obtain universal healthcare coverage. Furthermore, without effective laws, there is a greater danger of healthcare fraud and abuse, which not only wastes resources but also affects patient safety.[24] Therefore, governments need to emphasize the establishment and implementation of comprehensive healthcare legislation to safeguard the well-being of their citizens and retain public trust in the healthcare system.

13.4 PROPOSED METHOD AND REGULATION (PROPOSAL FOR PRACTICES)

Building a healthy nation is the responsibility of every human being in the nation. The existing environment in India suffers from discrete information on different platforms and reporting schemes for responding to existing response mechanisms. Moreover, a person's mindset for being healthy must promote being healthy as the first priority of life. Supporting the previously discussed point of Section 13.3, a proposed incidence response plan is suggested as a web framework that would need government support for sharing information, collecting data, sharing incidents, and the response management process. This web platform should move through a given cycle. The incident response must follow the incidence response cycle shown in Figure 13.4. Steps within this cycle will support the existing infrastructure and collectively come across people to support incident response. Each layer's attributes and involvement are explained below.

Detailed inclusion of services and partnership information for the suggested web platform are explained below. This inclusion will support existing infrastructure and provide a new platform for the information flow cycle and resource management. This functional system will support wellness management if collective efforts in this domain are driven by the government. Figure 13.5 suggests the stepwise execution of any incidence response chain for all types of incidences in the healthcare field.[25]

- **Preparation:** Planning of handling incidence framed through
  - **Government scheme:** The web platform must have statewide/central-wide schemes and available infrastructure from rural to urban areas.
  - **Healthcare service automation:** Quick response mechanism through automation with the help of available resources.
  - **Process and directives:** Supported tools and the importance of using available schemes and service automation scheme directives.

FIGURE 13.4 Generalized Incident response cycle.

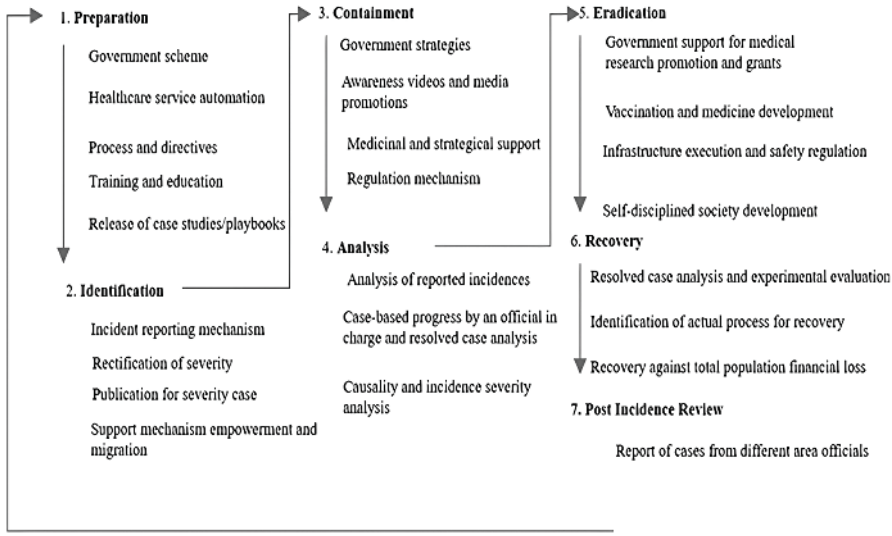

FIGURE 13.5 Proposed Method for Wellness Management.

- **Training and education:** Education for all rules for healthcare from door to workplace through interactive mechanisms. Propagation of health support using training of individuals as health workers for society.
- **Release of case studies/playbooks:** Case study report to inspire execution steps.

- **Identification:** Potential points to cover under identification
  - **Incident reporting mechanism:** Attributes of incidence happening and related case concerns cause method identification.
  - **Rectification of severity:** propagation or severity from previous histories or released publications. Professional healthcare persons' involvement for severity identification.
  - **Publication for severity case:** Publication of severity, precautionary measures, individual support and immediate supported services
  - **Support mechanism empowerment and migration:** Immediate training tools support on the web platform to train health professionals against severe situations.
- **Containment:**
  - **Government strategies:** strategies for operations and guidelines for nation or containment region.
  - **Awareness videos and media promotions:** Floating awareness through impactful media.
  - **Medicinal and strategical support:** Low budget and available supported medical facility to all.
  - **Regulation mechanism:** Regulation framework for operational assets in situations.[25]

- **Analysis:**
  - **Analysis of reported incidences:** Region-wise reported case analysis by web system
  - **Case-based progress by an official in charge and resolved case analysis:** each reported case must be tracked on the web platform about health progress using automation tools.
  - **Causality and incidence severity analysis:** Causality and incidence severity based on thresholds of casualties.
  - **Health Index infection mechanism:** Infection must be reported to all over the health index of the county if recovery from an incidence disaster.
- **Eradication:**
  - **Government support for medical research promotion and grants:** The government must promote research grants according to severity.
  - **Vaccination and medicine development:** Medine development by pharma companies and private research evaluation.
  - **Infrastructure execution and safety regulation:** On behalf of severity precaution from any incidence, safety regulation plays a vital role before medicinal support.
  - **Self-disciplined society development:** Persons self-disciplined about their own health are the prime eradication factor for any incidence and response too.
- **Recovery:**
  - **Resolved case analysis and experimental evaluation:** Medicine effectiveness on reported cases and mutated variant, feedback to concerned medical research domain.
  - **Identification of actual process for recovery:** Government officials must track each research progress on the population sample of incidence to keep interest in this role.
  - **Recovery against total population financial loss:** Must track loss and recovery against incidences.
- **Post Incidence Review:**
  - **Report of cases from different area officials:** A review of the total involved cases for future readiness.[26]
  - **Identification of effective, optimal support from plan and medicine:** Outcome reports, comparison of alternatives, recognition mechanism of plan and appointed persons.

13.5 RESULTS AND CONCLUSION

Statistical results of ambulance conditions and emergency case consideration in India have been presented for incidences for future reference of severity. Its data was collected from over 10 cities, 1000 samples of ambulances and over 1500 samples of incidence in 1 year of time period. These graphs in different categories of types of ambulance conditions redirect to the actual area of concern for incidence response and the gap in real scenarios over statistical parameters forces real-time updating of information and new web platform development that integrates

TABLE 13.2
Past 10 years automation initiative on available users against information sharing type

Year	Automation Initiatives	Percentage of Users
2023	- Implementation of a digital document management system.	75%
	- Introduction of an online service portal for citizens.	80%
	- Expansion of e-voting systems for elections.	45%
2022	- Deployment of a unified data-sharing platform for departments.	70%
	- Enhancements in online tax filing and payment systems.	90%
2021	- Launch of an integrated healthcare information portal.	60%
	- Introduction of AI-powered chatbots for citizen support.	40%
2020	- Implementation of a secure online public records archive.	65%
	- Rollout of e-permitting and licensing services.	85%
2019	- Development of a centralized citizen feedback and engagement platform.	50%
	- Expansion of e-learning platforms for students.	70%
2018	- Introduction of e-identity authentication for government services.	30%
	- Implementation of e-procurement systems.	75%
2017	- Deployment of an online emergency services reporting platform.	40%
	- Enhancements in online court case management.	55%
2016	- Expansion of online payment gateways for government fees.	80%
	- Development of a centralized employment registration system.	60%
2015	- Launch of an e-governance portal for access to government documents.	45%
	- Introduction of an e-booking system for government appointments.	70%
2014	- Implementation of an online public transportation booking system.	50%
	- Expansion of online public information services.	60%

all things in one.[27] The automation initiatives in the government organization over the past 10 years and the percentage of users using these platforms or services are shown in Table 13.2. This analysis was completed on the Kaggle environment and shown as a graph image here in Figures 13.6 and 13.7. Specific initiatives and user adoption rates will vary depending on the government organization's goals and the impact of each initiative. Table 13.3 shows the 10-year data of the changed platform on the web platform showing an interest of the user in the use of automation practices and habits. Automaton initiatives in government departments are increasing day by day and it is also important for data availability for all needed, so it needs to be confidential and integrity is also a factor in the effect of using all data concerned.

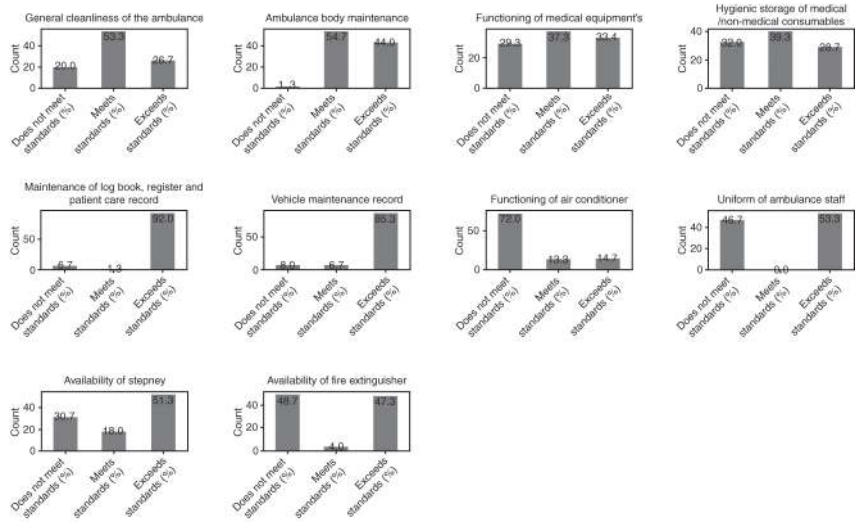

FIGURE 13.6 Statistical analysis of ambulance conditions on different attributes.

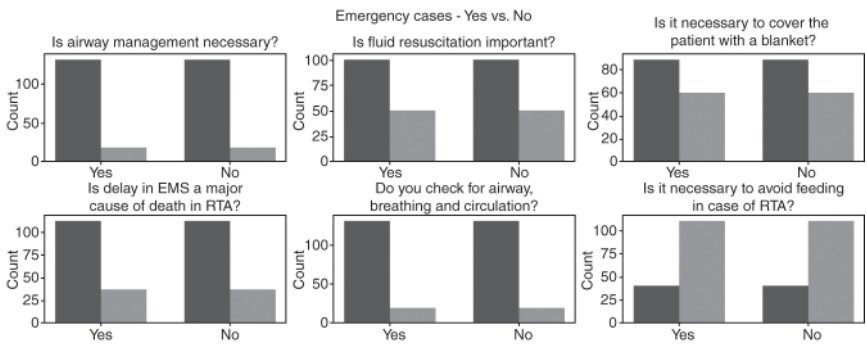

FIGURE 13.7 Emergency case over statistics for incidence.

Regarding the favourable effects and implications of using an incident management automation online platform in the healthcare profession, specific outcomes and advantages may vary based on the platform's functionality, the demands of the organization, and the amount of user engagement and compliance. These findings show the advantages of automation in enhancing incident management in healthcare, including faster reaction times, improved data security, and greater regulatory compliance (Table 13.4).

Using a web platform for incident management in the medical field may become a wise financial decision. It has enhanced patient care, data security, and overall operational efficiency in addition to incident response and resolution. Healthcare

TABLE 13.3
Percentage of platform change in the last 10 years

Year	Percentage of Platform Change
2023	20%
2022	15%
2021	25%
2020	10%
2019	30%
2018	20%
2017	15%
2016	25%
2015	10%
2014	5%

TABLE 13.4
Expected result of the inclusion of web platform

Aspect	Description	Expected Results
Incident Resolution Time	Reduction in the time taken to resolve incidents.	The average incident resolution time decreased by 30%.
Incident Response Efficiency	Improvement in the efficiency of the response process.	50% increase in the number of incidents resolved per week.
Compliance and Reporting	Enhanced ability to meet regulatory compliance requirements and reporting.	Achieved 100% compliance with healthcare regulations and reporting standards.
Data Security and Privacy	Better protection of patient data and privacy.	Zero data breaches reported in the past year.
Scalability and Adaptability	Flexibility to adapt to changing needs and scalability for future growth.	Easily scaled to accommodate a 20% increase in incident volume.
User Satisfaction	Improved satisfaction among healthcare staff.	90% of users reported increased satisfaction with the incident management process.
Cost Reduction	Reduction in operational costs related to incident management.	Achieved cost savings of 15% in incident resolution expenses.
Data Analysis and Trend Identification	Enhanced data analysis for identifying incident trends.	Predictive analytics helped in proactively addressing potential issues.
Staff Training and Knowledge Sharing	Improved training and knowledge sharing among staff.	75% of staff reported that the platform facilitated knowledge sharing and training.
Integration with Other Systems	Efficient integration with other healthcare systems.	Seamlessly integrated with electronic health record systems and alert mechanisms.
Real-time Reporting	Availability of real-time incident reporting.	Real-time incident reports improved situational awareness and response times.

companies that use automation and digital incident management systems are better equipped to handle the changing demands of the healthcare industry as technology develops. Overall performance will depend on interactivity, and scalability, government regulation, response mechanism, and many more factors discussed in this article. But for the success of a good platform continuous improvement and user feedback for the projected sample population will be needed.

REFERENCES

1. Balarajan Y, Selvaraj S, Subramanian SV. Health care and equity in India. *Lancet*. 2011;377:505–15.
2. Banerjee SK, Andersen KL, Warvadekar J, Pearson E. Effectiveness of a behavior change communication intervention to improve knowledge and perceptions about abortion in Bihar and Jharkhand, India. *Int Perspect Sex Reprod Health*. 2013;39:142–51.
3. von Lubitz D, Wickramasinghe N. Network-centric healthcare and bioinformatics: Unified operations within three domains of knowledge. Expert Syst Appl. 2006;30(1):11–23, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2005.09.069.
4. De M, Taraphdar P, Paul S, Halder A. Awareness of breastfeeding among mothers attending antenatal OPD of NRS medical college. *IOSR J Dent Med Sci*. 2016; 15:3–8.
5. Emanuel EJ, Emanuel LL. What is accountability in health care? *Ann Intern Med*. 1996;124:229–39.
6. Gulliford M, Figueroa-Munoz J, Morgan M, Hughes D, Gibson B, Beech R, et al. What does 'access to health care' mean? *J Health Serv Res Policy*. 2002;7:186–8.
7. Vanitha CN, Malathy S, Shenbagavalli P, Krishna SA, Kavin, K. (2022, May). Detecting turmeric Taphrina Maculans disease using machine learning algorithms. In *2022 International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 431–436). IEEE.
8. https://social.niti.gov.in/uploads/sample/health_index_report.pdf. [Last accessed on 2018 Jun 18].
9. James L. A Record of Buddhist Kingdoms: Being an Account by the Chinese Monk Fa-Hien of His Travels in India and Ceylon (A.D. 399–414). Dover publications. 1991:79.
10. Mattke, S, Liu, H, Caloyeras, J, Huang, CY, Van Busum, KR, Khodyakov, D, & Shier, V.. Workplace wellness programs study. *Rand Health Quarterly*. 2013;*3*(2).
11 Kallarakkal, TG, Siriwardena, BS, Samaranayaka, A, De Silva, R, & Tilakaratne, WM. A validated predictive model for risk of nodal metastasis in node negative oral squamous cell carcinoma of the buccal mucosa and tongue. *Journal of Oral Pathology & Medicine*. 2022; *51*(5):436–443.
12. Chekati, A, Riahi, M, & Moussa, F. (2022, July). An Internet of Things-Empowered Disaster Management Framework. In *Proceedings of International Conference on Computing and Communication Networks: ICCCN 2021* (pp. 141–151). Singapore: Springer Nature Singapore.
13. Zahra, A, Mohammadi, H, Kermani, M, Badirzadeh, A. & Gholami, M. The effect of climate change on cholera disease: The road ahead using artificial neural network. *PloS one*. 2019;14(11):e0224813.
14. Krishna A, Ananthpur K. Globalization, Distance and Disease: Spatial Health meDisparities in Rural India. [Last accessed on 2018 Jun 17].
15. Mohamed T, Al-Mashari M. A new dot plot-based algorithm for genomes sequences comparison: A preliminary study. *Expert Syst Appl*. 2006;30(1): 34–41, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2005.09.043.

16. Rao KD. Situation Analysis of the Health Workforce in India. Human Resources Technical Paper I. Public Health Foundation of India. 2011. [Last accessed on 2018 Jun 17].
17. Kotwal N , Khan N, Kaul S. A review of the effectiveness of the interventions on adolescent reproductive health in developing countries. *Int J Sci Res Publ*. 2014;4:1–4. Oxford Dictionary Online. [Last accessed on 2018 Jun 15].
18. Reddy KS, Patel V, Jha P, Paul VK, Kumar AK, Dandona L, et al. Towards achievement of universal health care in India by 2020: A call to action. *Lancet*. 2011;377:760–8.
19. Malathy S, Vanitha CN, Mohanasundari M, Prasath HV. (2021, December). Improved face recognition using convolutional neural network with unaided learning. In *2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA)* (pp. 1–6). IEEE.
20. Roy S. Primary health care in India. *Health Popul Perspect Issues*. 1985; 8:135–67.
21. SRS Statistical Report, 2016. Office of the Registrar General & Census Commissioner. India: Ministry of Home Affairs, Government of India; 2016. Ministry of Home Affairs, Government of India.
22. Tamanna MZ, Eram U, Al Harbi TM, Alrashdi SA, Khateeb SU, Aladhrai SA, et al. Clinical value of leukocyte counts in evaluation of patients with suspected appendicitis in the emergency department. *Ulus Travma Acil Cerrahi Derg*. 2012;18:474–8.
23. Mittal K, Goel MK. Knowledge regarding reproductive health among urban adolescent girls of Haryana. *Indian J Community Med*. 2010;35:529–30.
24. Vanitha, CN, & Malathy, S. (2021, February). A multi-syndrome pathology for breast cancer through intelligent learning. In *IOP Conference Series: Materials Science and Engineering* (vol. 1055, No. 1, p. 012073). IOP Publishing..
25. Vinesh K, et al. (2021, October 30–31). Alert based Drowsiness detection using machine learning. In *9th International Conference on Recent trend in Computing (ICACCT 2021).* https://doi.org/10.1063/5.0125988.
26. Zoheir E. Applications of artificial intelligence in bioinformatics: A review. *Expert Syst Appl*. 2006;30(1):2–10, ISSN 0957-4174. https://doi.org/10.1016/j.eswa.2005.09.042.
27. Munjanja SP, Magure T, Kandawasvika G. (2012). Geographical access, transport and referral systems. In: Hussein J, McCaw-Binns A, Webber R, editors. *I Maternal and Perinatal Health in Developing Countries* (pp. 139–54). CAB International e books.

14 Future Trends and Directions in Digital Health and Wellness Security

V. Karthikeyan and Y. Palin Visu

14.1 INTRODUCTION

Health and wellness can be improved with the employment of advanced technology by collecting and organizing accurate data on diagnoses and treatments and by encouraging healthy lifestyle choices through apps like activity trackers[1, 2]. All of these benefits will materialize as a result of the improved capacity of computers and digital network links to gather, organize, distribute, and use digital information. Numerous of these innovations will make use of cloud computing (CC), which is based on the hosting of shared data and computations. They will also depend on wireless communications and extensive internet networks to broadcast. These technologies and others will raise concerns about data security and privacy.

The increasing development of different technologies has led to the integration of technology into our everyday lives[3,4]. The Internet of Things (IoT), AI, big data (BD), CC, etc. act as key values in these effortless, ubiquitous services for everyone, which reduce the amount of manual labor and help to ubiquitously connect everyone[5,6]. Generally speaking, the IoT is the networking of intelligent, networked physical elements, which include software, instruments, and web interconnection, to consent for information compilation and interchange[7,8]. The Internet of Things is currently influencing and changing the business and consumer worlds and permeating every worldwide business and consumer domain. Furthermore, it is being utilized in various other sectors, including healthcare, agriculture, smart cities, and the military[9].

Table 14.1 highlights the multifaceted reasons why data security and privacy are crucial in electronic health records, encompassing legal compliance, patient trust, identity protection, and the overall integrity of healthcare data.

14.2 LITERATURE SURVEY

Researchers have taken an interest in medical data sharing as a means to develop new methods of treating patients. Professionals accessing medical data remotely, along with digitalization and electronic storage, form the foundation of the assertion mentioned by Lang (2011)[10]. The electronic health records that patients get from

 DOI: 10.1201/9781032711379-14

TABLE 14.1
Need for Security and Privacy for the Medical Data

Reasons for Data Security and Privacy in HER	Explanation
Patient Confidentiality	Protection of sensitive patient information to maintain trust and confidentiality in healthcare interactions.
Legal and Regulatory Compliance	Adherence to laws and regulations such as Health Insurance Portability and Accountability Act (HIPAA) to avoid legal consequences and ensure patient rights are protected.
Prevention of Unauthorized Access	Safeguarding against illegal admission, confirming that accredited persons can view or adjust patient records.
Identity Theft Prevention	Protection against theft of personal information for fraudulent activities, reducing the risk of identity theft for patients.
Preventing Medical Fraud	Minimizing the risk of fraudulent activities, including false insurance claims and unauthorized access to healthcare services.
Maintaining Patient Trust	Building and maintaining trust between patients and healthcare providers by assuring the safety and confidentiality of their health data.
Preventing Discrimination and Stigmatization	Protecting patients from potential discrimination based on their health information, promoting equitable healthcare treatment.
Data Integrity and Accuracy	Ensuring that patient data is accurate and has not been tampered with, maintaining the integrity of health records.
Research and Analytics Security	Protecting patient data used in medical research and analytics to prevent misuse or unauthorized access to sensitive information.
Preserving Professional Reputation	Safeguarding the reputation of healthcare providers and institutions by preventing data breaches and privacy violations.

hospitals following their visits become the sole proprietors of such records[11,12]. Data sharing offers intriguing value from still-opening perspectives, thanks to the advent of that technological era and the successive capture of massive amounts of information in the BD era. Businesses that collect, process, interpret, store, and share the right kind of data with other connected people have sprung up because of how important medical data is and how it fits in with distribution[13,14]. Several businesses have taken notice, particularly those whose focus is on data analytics, data derivation, cloud storage and processing, and the capacity for existing businesses to rely on the data available for their growth and longevity. It was with the intention of providing end-users with cross-domain, flexible, and controlled medical data exchange and data searching capabilities that cloud service providers (CSPs) were established[15].

The critical nature of medical data makes it imperative to guarantee its security, privacy, and integrity. Consequently, a safe and effective system for managing data was necessary[13]. The negative risks associated with disclosing their data's information prompted the CSP to challenge the requirement of collaboration in medical data sharing[16]. According to Ferrag (2020)[17], the real risk for data managers and masters comes from receiving data that is accessible to attackers. Numerous cryptographic methods for the safekeeping and transfer of sensitive medical information have been developed in response to these problems, yet they remain insufficient[18–20]. We offer these cryptographic methods keeping in mind the cloud server's inherent unreliability and the necessity to safeguard customer information. To ensure the protection of sensitive information, it is necessary to encrypt it before sending it to a remote server in the cloud. However, traditional encryption methods directly deprive customers of search functionality and result in a poor user experience[21]. Searchable encryption methods have two main configurations: the private-key and the public-key settings, both designed to protect data searches in the translated clinical information[22].

Blockchain's attractive features, such as confidentiality and decentralized governance, make it an excellent candidate for providing a reasonable solution to such problems. When it comes to handling data in the CC, the blockchain (BC) technique has proven to be a harmless and more effective substitute for traditional cryptographic approaches. Recent studies have implemented the blockchain to securely handle data[23,24]. A distributed ledger system known as a blockchain is able to link together a series of data structures called blocks to form a public and accessible web-based database. Rather than being stored midway, these blocks are transported among multiple hubs on a regular basis. Every block includes a date for its creation, a hash of the preceding block, and the information transferred: medical care supplier and patient information, as well as health information[25].

The main purpose of this chapter is to scrutinize the different BC-based safety mechanisms for cloud-based healthcare information retention and exchange in order to identify the current investigation gaps, difficulties, and prospective pathways that contribute to the development of Clinical Care 4.0.

14.3 CONFIDENTIALITY AND SAFETY OF E-HEALTH INFORMATION (NON-BLOCKCHAIN)

To ensure the security associated with medical records, organizations employ various strategies. Several investigations have utilized physical, managerial, and technological elements for this purpose. Several safety methods utilized by healthcare organizations are outlined in these instructions[26,27] to better guarantee the security and privacy of clinical data contained in electronic medical records. Figure 14.1 depicts the standards for the exchange of digital clinical care information.

A number of researchers have created cloud computing-related techniques. Despite cloud computing's broad use and many services, it still poses serious privacy and security risks. Organizations around the world have prioritized developing cloud security policies and procedures before implementing cloud solutions for

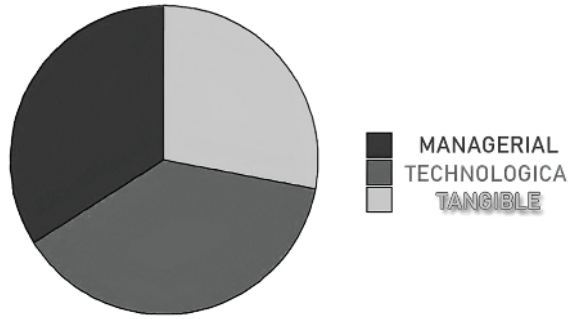

FIGURE 14.1 Digital Medical Data Transmission.

their businesses[28]. Reports indicate that cloud storage systems often store a significant amount of healthcare data. However, the rise in the number of cloud attackers necessitates the development of a method to safeguard information. The initial phase is to establish administrative protections, which include appropriate activities such as conducting examinations, designating a supervising person to ensure information security, and developing contingency plans[29]. It is worth noting that this technique may allow scientists to uncover previously unrecognized details about a certain group of individuals. The advancement of precision medicine depends on enough financing for long-term studies. Using wearable electronics and the IoT, blockchain is being utilized in clinical care to collect and amend vital medical data, such as diabetes and elevated arterial pressure[30,31].

Encryption systems have safeguarded digital health records (DHR). Cryptography has greatly enhanced the protection of medical data, during both storage and transmission. Organizations must typically record the communication mechanism when cryptographic features can be enabled or deactivated in order for information regarding patient transmission techniques to adhere to guidelines set by specifications[32]. Antivirus defense, cloud computing, radio frequency identification (RFID), employing an executive data safety agent, and translators for the initial risk assessment are all typical safety measures[33].

Because of the proliferation of Internet-connected devices, a lot of studies have focused on cloud apps that integrate with EHR. Hybrid computing's design makes it easy to "have to rent" resources like CPU and memory, and it also makes it easy to share and allocate digital assets and information, since this distributes possession, decreases operating expenses, and includes encryption technologies[34–36]. Although there is some hope for the future of cloud computing, anti-virus software is still the gold standard for online safety. Figure 14.2 depicts the approaches utilized to improve HER's safety and confidentiality. In Figure 14.2, we can see a schematic representation of the data encryption technique used in EHR maintenance. The security of information is a major concern due to the ever-increasing number of individuals utilizing gadgets connected to the Internet. Stability in a system depends on fixing various privacy and security problems[37].

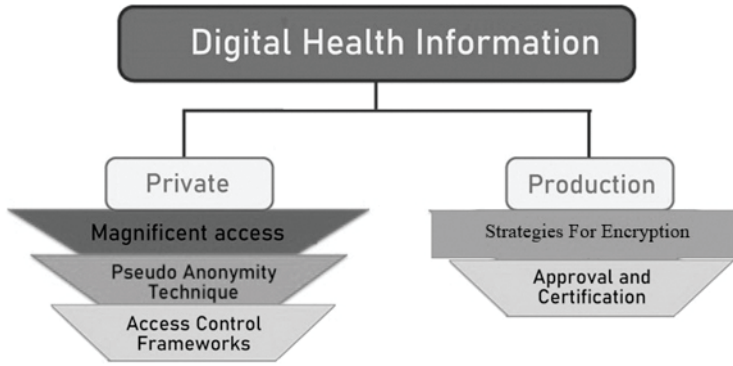

FIGURE 14.2 EHR Encryption Mechanisms.

14.4 PROTECTING THE CONFIDENTIALITY OF EHRS (USING BLOCKCHAIN TECHNOLOGY)

Public blockchains, private blockchains, and federated blockchains are the three main categories of blockchain technology.

(a) *Public Blockchain:* There is no longer a requirement for a single entity to maintain records thanks to public blockchain technology, which is a distributed ledger system that is open, reliable, and impermeable. Anyone can sign up for a public blockchain, take part in reaching a consensus, and verify transactions. While this openness promotes equality and transparency, it could pose problems with scalability, energy usage, and privacy[38].

(b) *Private Blockchain:* When only a select few individuals join a private blockchain—sometimes called a permissioned blockchain—others cannot access the system or participate in reaching a compromise. Privately distributed ledgers are intended to be utilized in a closed environment, typically by an association of companies or a single business, as opposed to open-source ones that allow anybody to join the network and confirm transactions. Implemented for specialized commercial or organizational scenarios, private blockchains provide a unique set of features not found in blockchains that are publicly accessible. Two popular private blockchain systems are Multichain and Monax[39,40].

(c) *Federated Blockchain:* It describes a blockchain design that takes the best features of public and private blockchains and merges them. Federated blockchains allow several enterprises to operate together as a consortium while also allowing each consortium member to have control of their own blockchain node[40,41]. Public blockchains allow anybody to join the network and take part in the consensus process, while federated blockchains are structured in a more restricted and permissioned way.

14.4.1 Issues with Managing Digital Health Information

HIPAA implementation has revealed several issues with clinical care record maintenance, the most pressing of which is the necessity to shield patient confidentiality as

FIGURE 14.3 Ethical Concerns in EHR.

shown in Figure 14.3. In its oversight of US healthcare execution, the Office of the National Coordinator for Health Information Technology (ONC) highlights the difficulties associated with EHR[42]. The following is the sequence in which they are listed:

- There is an increase in the amount of work involved in everyday operations due to the maintenance of patient records.
- Healthcare systems have not yet completely incorporated electronic health records due to their complexity.
- EHR accountability mechanisms do not always align with the requirements of federal funds, and data processing and extraction can be challenging.
- There is a lack of automation and scalability in the current medication regimens. The ONC has classified all of these issues as burdens on the institution.

14.4.2 Consensus Algorithms for Blockchain

A blockchain consortium uses a consensus mechanism to reach decisions, which all other participants are obligated to adhere to. For further clarification, let's examine the subsequent scenario. Suppose a group of 25 entrepreneurs convenes to deliberate about a concept. The selection process favors proposals that yield the greatest value to the majority of people. Miners are required to tackle complex theoretical riddles connected to Bitcoin in order to achieve Proof of Work (P_W) consensus and get Bitcoin incentives. The majority of blockchains employ stakeholder voting as a means to establish consensus mechanisms[43]. The key objective of consensus learning is to enable node-to-node communication for the purpose of adding valid transactions to the blockchain. Listed here are a handful of the standard consensus mechanisms:

14.4.2.1 Proof-of-Work (P_W)

In terms of reliability and popularity, P_W is the first and currently most utilized consensus method. The course of accumulation of a block to the BC begins with a miner finding and sharing a hash value that is below its difficulty threshold. But there are limitations to P_W as well. As blockchain technology gains traction, the algorithm's resource demands and computing power requirements will increase dramatically.

14.4.2.2 Proof-of-Stake (P_S)

P_S [23] is a suitable auxiliary for P_W since it resolves the main issue with P_W, namely its high CPU power usage. Unlike P_W, where every node can mine an

exchange, P_S selects miners based on their ownership interest or fortune. It is common practice to use a pseudorandom sampling technique when deciding how to distribute nodes. By letting the chosen miner retain the transaction's expense, P_S effectively removes hashing rewards. Two blockchains that utilize P_S include Polkadot and NEO5.

14.4.2.3 Delegated Proof-of-Stake *(DP_S)*

Block validation is not a requirement for vouchers or investors in DP_S. Instead, they select delegates to authorize blocks. Stakeholders are constantly kept in the driver's seat during the administrative process due to the high stakes convoluted in the event of a network failure. Participants can ballot to eliminate and replace delegates if they find an irregularity in the block construction process. Coordination among delegates is possible for the purpose of block validation and the distribution of transaction rewards.

14.4.2.4 Proof-of-Authority *(P_A)*

P_A7 is the result of combining P_W and P_S. It stresses the significance of credibility and individuality. So, a stakeholder's identity is more of an assistance system than a resource. Authentic and trustworthy customers ensure the security of the blockchain's core components. Decred is an approach that makes use of this.

14.4.2.5 Proof of Vote *(P_V)*

There is a little difference between all of the consensus algorithms and the P_V approach. Organizations need to share company data in order to form block transactions on the distributed ledger. Because of this, they decide to hire an outside team to assist them. To guarantee the distributed nature of BC, the organization will transmit the block to all businesses on the network for voting confirmation. Every once in a while, business owners will have their employees take on more work than they actually need.

14.4.2.6 Functional Byzantine Fault Tolerance (FBFT)

To ensure fault tolerance in distributed systems, even when hostile actors or components are present, Functional Byzantine Fault Tolerance (FBFT) is a consensus mechanism that is employed. A class of consensus algorithms known as Byzantine Fault Tolerance (BFT) may endure crash and Byzantine fault-related failures as well as other random failures.

14.4.2.7 Proof-of-Importance *(P_I)*

In *PoI8*, the productivity of the miner is what determines his selection rather than the quantity of work or stake he holds. Instead of rewarding users with large balances, the reward increases the volume of transactions made on the account. A trust score is assigned to every user within the P_I network. There is an inverse relationship between value and reward likelihood. This algorithm is used by NEM9 blockchain platform.

14.4.3 Managing EHR Using Blockchain

An electronic health record (EHR) stores confidential personal information, such as the healthcare accounts of individuals. Hence, the safeguarding as well as confidentiality of such information is paramount. The government establishes regulations that medical institutions in developing nations must adhere to. Storing and disseminating electronic health record (EHR) data poses significant challenges. However, electronic health record (EHR) management has numerous technical challenges. Central medical servers, for example, have limited capacity, are prone to one-point failures, and are subject to intruder outbreaks. Patients do not have precise knowledge about the specific location of their sensitive data storage and how it is shared[44,45]. Nevertheless, the significance of interconnectedness among different healthcare practitioners has increased due to the mobility of individuals in modern times, enabling more effective health recommendations.

Discussion 1: Role of blockchain in EHR management and how has it impacted the field

Blockchain revolutionizes Electronic Health Record (EHR) administration by fundamentally transforming the storage, sharing, and security of healthcare data. Blockchain guarantees the truthfulness and immutability of electronic health records by offering a dispersed and disseminated record, thereby reducing the chances of data tampering or illegal access. Blockchain presents various opportunities to address the critical issue of patient confidentiality in clinical care. It improves safety and makes it easier for healthcare organizations to share patient data. The intelligent agreements in blockchain streamline approval and data sharing procedures[46]. Blockchain gives patients more control over their health data, making healthcare more client-focused despite issues with legal compliance. Although still in its nascent phase of implementation, the capacity of blockchain to transform EHR management is apparent, offering a future healthcare environment that is more secure, streamlined, and integrated.

Discussion 2: Protocol for encoding electronic health records on the blockchain

In order to guarantee interoperability and consistent data representation, the development and adherence to industry-wide standards and formats are necessary for the standardization of storing EHRs on the blockchain. Despite the lack of consensus, several efforts are underway to create common frameworks for EHRs that are built on the BC. Health Level Seven International's Fast Healthcare Interoperability Resources (FHIR) is quickly becoming the de facto guideline for the organization of all medical-care data, including electronic health records (EHRs). The modular design of FHIR makes it easy to build adaptable and interoperable systems that can connect to blockchain networks. Integrating the Healthcare Enterprise (IHE) and similar initiatives also make use of preexisting standards like Digital Imaging and Communications in Medicine to guarantee that blockchain platforms are compatible with healthcare systems. In an effort to create a more unified and interoperable

healthcare system, these standardization initiatives are targeting problems with data accessibility, security, and consistency. In order to establish strong and broadly accepted standards for the storage of EHRs on blockchain, it is crucial that stakeholders, regulatory agencies, and standards development organizations work together continuously as the sector develops[47–49].

Discussion 3: Electronic health record-related BD

In the context of EHRs, "big data" denotes the use of sophisticated analytics and technology for the purpose of managing, processing, and drawing conclusions from massive amounts of patient records. A broad range of information types, including healthcare histories, scans, and laboratory findings, including doctors' notes, are together known as "big data" in the context of health information systems. Hospitals utilize state-of-the-art devices and platforms to handle the massive volumes, different kinds, and lightning-fast speeds of information. To efficiently handle EHRs on a large scale, businesses are turning to cloud computing solutions, which provide scalable storage and computing resources. The analytical community makes use of data lakes and warehouses to store and organize both organized and formless data. In addition, predictive measuring and ML algorithms search through this massive information for trends, make better clinical decisions, and forecast patient outcomes. A new solution that is gaining traction is blockchain technology, which can improve the reliability and transparency of EHRs by strengthening the security and integrity of huge amounts of data. While there is a great deal of promise in using big data to improve healthcare delivery and patient outcomes in the electronic health record (EHR) environment, there are still many obstacles to overcome, such as data privacy, regulatory compliance, and interoperability[44,46].

Discussion 4: Portals/blockchain techniques employed to manage EHRs

The management of EHRs has attracted the attention of multiple blockchain platforms and methods, each with its own set of advantages and disadvantages tailored to the needs of healthcare data. Hyperledger Fabric is an enterprise-ready permissioned blockchain platform with a modular design that makes it easy to manage sensitive EHRs through the usage of customizable consensus processes with privacy protections. Healthcare applications have utilized the public blockchain platform Ethereum through private or consortium networks. As a result, it's easier to manage consent and share data, and smart contracts may automate and secure the execution of predefined conditions. One such interoperability-focused platform built on the Stratis blockchain is Health Nexus. Its goal is to improve data exchange among healthcare systems and create common standards for electronic health records. To find a middle ground between the competing demands of scalability and data security in healthcare settings, several initiatives are investigating the possibility of integrating blockchain technology with off-chain storage alternatives. These include MedRec and Medicalchain. Despite the potential of these platforms, the healthcare industry is just beginning to embrace blockchain technology for EHR management. There are continuous efforts to overcome obstacles related to interoperability and guarantee compliance with regulations[45, 48, 49].

Discussion 5: Analysis of cost, confidentiality, safety storage scalability, and accessibility in blockchain-based HER

Innovations in discretion, safekeeping, packing scalability, and convenience, as well as rate examination, have resulted from the usage of BC technology in the administration of EHRs. The built-in cryptographic capabilities of blockchain help to alleviate privacy issues in healthcare data by securely storing patient information and limiting access to authorized individuals through permissioned processes. The distributed ledger technology (blockchain) increases security by lowering the probability of data breaches and eliminating potential weak points. These qualities guarantee a transparent and immutable record of patient data. Distributed and decentralized blockchain networks solve storage scalability by facilitating the easy addition of additional nodes to the network, which in turn allows for the accommodation of an ever-increasing volume of EHRs without sacrificing performance. Health Level Seven International's FHIR and other standardized data formats are finding more and more uses in blockchain-based electronic health record integration, which improves interoperability.

Improved patient care and treatment outcomes are possible because authorized entities have easy access to essential information thanks to blockchain's streamlined and secure data sharing among healthcare providers. In addition, smart contracts empower patients to have more say over their health data by letting them decide who can access their electronic health records (EHRs) via consent processes. Gains in efficiency linked to blockchain-based EHRs have a good effect on cost analysis. Some possible ways to save costs include doing away with middlemen, streamlining data sharing, and reducing superfluous administrative operations. Obstacles such as initial implementation expenses, integration with current systems, and regulatory compliance could affect the total cost analysis. To fully optimize these systems, standardize them, and navigate changing regulatory landscapes for extensive and widespread adoption across the healthcare industry, we need more research and collaboration. However, integrating blockchain into EHR management does offer promising solutions to various challenges[45–48].

The comparative Table 14.2 provides an outline of the likelihood of BC applications in EHR and the associated trade-offs. While the likelihood varies for different applications, trade-offs often involve finding the right balance between conflicting priorities, such as privacy and transparency or decentralization and scalability. The success of blockchain in EHR will depend on addressing these trade-offs while considering industry-specific requirements and regulatory constraints.

14.4.4 Important Blockchain Developments for the Long Term of Medical Care

(i) The clinical-care basis series;
(ii) the information technology rebellion;
(iii) the rapid growth of the digital market are a few of the important future developments in healthcare that will use blockchain technology.

TABLE 14.2
Use of Blockchain in HER Management

Blockchain Application in HER	Likelihood of Adoption	Trade-Offs
Patient Data Security	High	Privacy vs. Transparency: Achieving a balance between patient data privacy and the need for transparency in healthcare records. Regulatory Compliance: Ensuring adherence to healthcare regulations and standards, this may vary across regions.
Interoperability	Moderate	Standardization: Challenges in establishing standardized data formats for interoperability. Integration: Seamless integration with existing EHR systems and healthcare infrastructure.
Decentralized Access Control	Moderate	Scalability: Balancing decentralized access control with the need for scalable solutions as EHR data volumes grow. Usability: Ensuring user-friendly interfaces for healthcare providers and patients.
Smart Contracts for Consent	High	Ethical Considerations: Striking a balance between automated consent management through smart contracts and the ethical implications of automated decision-making in healthcare.
Real-time Updates	Low to Moderate	Network Latency: Addressing latency issues in real-time data updates, especially in large healthcare networks. Adoption Challenges: Overcoming resistance to change and encouraging widespread adoption among healthcare providers.

(i) Maximizing the practice of the BC concept in medicare supply chains: BC technology is crucial for the development of digital supply chains and for enhancing efficiency and transparency.

Manufacturing items along the supply chain to ensure authenticity may be recommended by medical care administrations, from makers to sellers, in high-risk environments due to signs of tampering. In the event that a builder notices an issue with a medicine or sensor, the blockchain can assist the seller in quickly recalling the information by identifying the location of the record along the data link that has to be disconnected. On occasion, it is anticipated that federal drug supply chain security will enhance the detection of dirty, misplaced, and harmful drugs. Under this law, there are just a handful of experimental programs that examine the best practices for protecting patient information. To test new technologies and improve security recommendations for medicine sources and supplies, Walmart and IBM have chosen a trial program.

(ii) Quick incorporation into the IT revolution: new technologies have been developed at a rapid pace thanks to the Internet technology revolution, which includes things like blockchain, cloud computing, and artificial intelligence. When estimating

routine needs, the innovative hybrid cloud that stores private medical data beneath initiative firewalls offers highly accessible public cloud services at client outcomes[20, 23].

a). AI: The usage of AI has the potential to revolutionize the future of managing electronic health records (EHRs). Using AI to better extract, analyze, and interpret meaningful insights from the large and complicated datasets included inside EHRs is an encouraging area of research. Improving the understanding of unstructured clinical narratives through the development of natural language processing (NLP) algorithms can lead to more efficient and accurate data extraction. Artificial intelligence has the ability to enhance digital healthcare, information privacy, and patient-centric treatment suggestions, as well as data entry for clinicians in EHRs[32]. Explainable AI uses AI frameworks to consolidate all medical information into a single file. It also affirms that adhering to the necessary rules and regulations is crucial for the ethical implementation of AI in her management.

b). Edge Computing (EC): EC is the latest trend that aims to improve the critical handling of EHRs. It also improves the speed of operation and data analysis by performing the assessments during the data collection stage itself. Several studies and physician feedback are required to improve the efficacy and reliability of EC implementation in EHR. EC performs clinical data analysis and decision-making at the network edge point itself[35]. This will reduce the workload on the processing clouds, as well as clinicians, and improve overall EHR management.

c). Internet of Medical Things (IoMT): As technology advances, secure mechanisms for EHR sharing in clinics via IoMT are required. The peer group must establish reliable information sharing between IoMT devices and EHR systems. Experts can enrich the instantaneous information collected by IoMT equipment through the application of sophisticated analytics and artificial intelligence. Concerns about data breaches and illegal access highlight the need for future research on methods to secure and protect sensitive health information as it is sent across IoMT networks. With concerns like consent management, data ownership, and patient empowerment in mind, it is imperative that we work together to develop standards and best practices for the ethical use of IoMT in EHRs[38]. Ultimately, the combination of IoMT with EHRs has the prospect of modernizing Medicare delivery by providing doctors with real-time, comprehensive visions of their patients' health and enabling prompt interventions based on data from connected devices.

By recognizing the designs and connections to the massive amounts of data stored on integrated clouds and safely organized in blockchain frameworks, artificial intelligence integrates and extracts characteristics. Blockchain technology, when coupled with Internet of Things (IoT) sensors, can reveal demographic shifts, accelerate medical development[49] and research, and improve patient outcomes.

(iii) Rapid progress in established marketplace. Most of the time, developing blockchain technology benefits high-income nations, especially those in Asia. Furthermore, by increasing blockchain copyrights, the Chinese management has set them up to dominate the BC industry. As part of its thirteenth five-year plan, the Chinese state council typically builds blockchain improvements in states. As an example, in 2019, President Xi of China recognized the importance of blockchain technology in building China's cyberpower, launching the digital economy, and creating social and economic improvements. Therefore, in 2018, the United Arab

Emirates developed a plan to improve banking, transportation, and healthcare for its citizens by utilizing blockchain technology. The plan originated in Estonia[50]. Competent medical professionals, including local organizations, technology groups, and medical specialists, display a data sharing output during the medical care stage to save and share valuation data.

14.4.5 Potential Constraints

The safety and confidentiality of EHR data encounter substantial limitations, posing problems for the healthcare sector. An important limitation is the growing complexity of cyber threats that specifically target healthcare systems[20]. Electronic health records (EHRs) are attractive to evil individuals because of the valuable patient data they contain. These individuals want to get unauthorized access to EHRs, resulting in data breaches and identity theft. Moreover, the complex and interrelated structure of healthcare ecosystems presents difficulties in upholding uniform security measures across different platforms and devices, particularly when incorporating data from Internet of Medical Things (IoMT) devices[38]. The implementation of EHR security measures poses the problem of protecting patient data while simultaneously complying with legislation[3]. Strict standards may impede information transmission that is critical for rapid patient treatment, making it difficult to strike a balance between data accessibility and good security[17, 19]. Humans introduce vulnerabilities such as insider attacks and inadequate cybersecurity training among healthcare workers[8]. To protect electronic health record data from ever-changing cyber threats, more study, funding, and cooperation are required to create and implement cutting-edge cybersecurity measures, encryption methods, and privacy-preserving technology. Ethical and responsible data handling is of the utmost importance in Medicare commerce.

14.5 CONCLUSION AND FUTURE SCOPE

Using a blockchain for smart health is the method. Blockchain is the method. As technology progresses, blockchains have the ability to handle tasks in healthcare, such as the coordination of care, security of data, and interoperability. As technology develops, processing speeds and the facility to duplicate large volumes of records will both increase. The importance of preserving healthcare data has developed in modern days owing to the growing need for more precise, efficient, and economical patient care. By fixing issues with client-server and cloud-based approaches' vulnerabilities, privacy concerns, and unique points of failure, the system might enhance medical data management. Comparative analysis describes the likelihood of blockchain applications and their trade-offs. Many challenges need to be resolved in order to develop blockchain-based services that generate profit. Developers and researchers in the medical industry play a crucial role in utilizing BC technology for the distribution of clinical records. If blockchain technology is able to gain traction in the healthcare industry, it might open up new possibilities for medical research. The neural control method utilizes blockchain technology, allowing the digital brain to store it while being observed. Machine

learning models, on the other hand, have the potential to directly boost precision and productivity. Longevity and healthcare go hand in hand. Experts in medicine might be of assistance. The report states that in the future, researchers may look at how gender, age, and experience with blockchain affect the adoption of smart healthcare systems. One such area that needs more research is figuring out what influences people to use blockchain technology.

REFERENCES

[1] Phillips, S. A., Ali, M., Modrich, C., Oke, S., Elokda, A., Laddu, D., & Bond, S. (2019). Advances in health technology use and implementation in the era of healthy living: Implications for precision medicine. *Progress in Cardiovascular Diseases*, 62(1), 44–49.

[2] Gachet Páez, D., de Buenaga Rodríguez, M., Puertas Sánz, E., Villalba, M. T., & Muñoz Gil, R. (2018). Healthy and wellbeing activities' promotion using a Big Data approach. *Health Informatics Journal*, 24(2), 125–135.

[3] Yang, C., Huang, Q., Li, Z., Liu, K., & Hu, F. (2017). Big Data and cloud computing: Innovation opportunities and challenges. *International Journal of Digital Earth*, 10(1), 13–53.

[4] Tully, C. J. (2003). Growing up in technological worlds: How modern technologies shape the everyday lives of young people. *Bulletin of Science, Technology & Society*, 23(6), 444–456.

[5] Raj, P., & Raman, A. C. (2017). *The Internet of Things: Enabling technologies, platforms, and use cases*. CRC Press.

[6] Gill, S. S., Tuli, S., Xu, M., Singh, I., Singh, K. V., Lindsay, D., ... & Garraghan, P. (2019). Transformative effects of IoT, blockchain and artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. *Internet of Things*, 8, 100118.

[7] Ali, Z. H., Ali, H. A., & Badawy, M. M. (2015). Internet of Things (IoT): Definitions, challenges and recent research directions. *International Journal of Computer Applications*, 128(1), 37–47.

[8] Atlam, H. F., Walters, R., & Wills, G. (2018). Internet of things: State-of-the-art, challenges, applications, and open issues. *International Journal of Intelligent Computing Research (IJICR)*, 9(3), 928–938.

[9] Vermesan, O., & Bacquet, J. (Eds.). (2019). *Next generation Internet of Things: Distributed intelligence at the edge and human machine-to-machine cooperatio*n. River Publishers.

[10] Lang, T. (2011). Advancing global health research through digital technology and sharing data. *Science*, 331(6018), 714–717.

[11] Mahajan, H. B. (2022). Emergence of healthcare 4.0 and blockchain into secure cloud-based electronic health records systems: Solutions, challenges, and future roadmap. *Wireless Personal Communications*, 126(3), 2425–2446.

[12] Baird, A., Davidson, E., & Mathiassen, L. (2017). Reflective technology assimilation: Facilitating electronic health record assimilation in small physician practices. *Journal of Management Information Systems*, 34(3), 664–694.

[13] Mahajan, H. B., Rashid, A. S., Junnarkar, A. A., Uke, N., Deshpande, S. D., Futane, P. R., ... & Alhayani, B. (2023). Integration of Healthcare 4.0 and blockchain into secure cloud-based electronic health records systems. *Applied Nanoscience*, 13(3), 2329–2342.

[14] Yang, G., Li, C., & Marstein, K. E. (2021). A blockchain-based architecture for securing electronic health record systems. *Concurrency and Computation: Practice and Experience*, 33(14), e5479.

[15] Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Information Sciences*, 305, 357–383.
[16] Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, 41(10), 1027–1038.
[17] Ferrag, M. A., Maglaras, L., Derhab, A., & Janicke, H. (2020). Authentication schemes for smart mobile devices: Threat models, countermeasures, and open research issues. *Telecommunication Systems*, 73, 317–348.
[18] Jin, H., Luo, Y., Li, P., & Mathew, J. (2019). A review of secure and privacy-preserving medical data sharing. *IEEE Access*, 7, 61656–61669.
[19] Yaacoub, J. P. A., Noura, M., Noura, H. N., Salman, O., Yaacoub, E., Couturier, R., & Chehab, A. (2020). Securing internet of medical things systems: Limitations, issues and recommendations. *Future Generation Computer Systems*, 105, 581–606.
[20] Kumar, P., & Lee, H. J. (2011). Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors*, 12(1), 55–91.
[21] Zhang, R., Xue, R., & Liu, L. (2017). Searchable encryption for healthcare clouds: A survey. *IEEE Transactions on Services Computing*, 11(6), 978–996.
[22] Ali, A., Pasha, M. F., Ali, J., Fang, O. H., Masud, M., Jurcut, A. D., & Alzain, M. A. (2022). Deep learning based homomorphic secure search-able encryption for keyword search in blockchain healthcare system: A novel approach to cryptography. *Sensors*, 22(2), 528.
[23] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2020). Integration of blockchain and cloud of things: Architecture, applications and challenges. *IEEE Communications Surveys & Tutorials*, 22(4), 2521–2549.
[24] Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908–164940.
[25] Fan, K., Wang, S., Ren, Y., Li, H., & Yang, Y. (2018). Medblock: Efficient and secure medical data sharing via blockchain. *Journal of Medical Systems*, 42, 1–11.
[26] Fernández-Alemán, J. L., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, 46(3), 541–562.
[27] Gaziano, J. M., Concato, J., Brophy, M., Fiore, L., Pyarajan, S., Breeling, J., Whitbourne, S., Deen, J., Shannon, C., Humphries, D., & Guarino, P. (2016). Million Veteran Program: A mega-biobank to study genetic influences on health and disease. *Journal of Clinical Epidemiology*. 70, 214–223.
[28] Alzoubi, Y. I., Osmanaj, V. H., Jaradat, A., & Al-Ahmad, A. (2021). Fog computing security and privacy for the Internet of Thing applications: State-of-the-art. *Security and Privacy*, 4(2), e145.
[29] Nagahawatta, R. T. S. (2022). Critical security and privacy related factors influencing the adoption of cloud computing in Australian small and medium-sized enterprises. (Doctoral dissertation, RMIT University).
[30] Ray, P. P., Dash, D., & Kumar, N. (2020). Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. *Computer Communications*, 160, 111–131.
[31] Kakhi, K., Alizadehsani, R., Kabir, H. D., Khosravi, A., Nahavandi, S., & Acharya, U. R. (2022). The internet of medical things and artificial intelligence: trends, challenges, and opportunities. *Biocybernetics and Biomedical Engineering*, 42(3), 749–771.

[32] Panimalar, S. P., & Gunasundari, S. (2023, February). A survey based on privacy-preserving over health care data analysis. In *International Conference on Emerging Trends in Expert Applications & Securit*y (pp. 443–456). Singapore: Springer Nature Singapore.

[33] Matullo, K. S., Amato, C. A., & Burskii, P. (2023). Use of blockchain technology for implantable medical device tracking. In *Blockchain in Healthcare: From Disruption to Integration* (pp. 201–214). Cham: Springer International Publishing.

[34] Navaz, A. N., Serhani, M. A., El Kassabi, H. T., Al-Qirim, N., & Ismail, H. (2021). Trends, technologies, and key challenges in smart and connected healthcare. *IEEE Access*, 9, 74044–74067.

[35] Zaman, U., Imran, Mehmood, F., Iqbal, N., Kim, J., & Ibrahim, M. (2022). Towards secure and intelligent internet of health things: A survey of enabling technologies and applications. *Electronics*, 11(12), 1893.

[36] Velayuthapandian, K., Karuppiah, G., Vadivel, S. R. S., & Joseph, D. R. V. (2024). Mammogram data analysis: Trends, challenges, and future directions. In *Computational Intelligence and Modelling Techniques for Disease Detection in Mammogram Imag*es (pp. 1–38). Academic Press.

[37] Taherdoost, H. (2023). An overview of trends in information systems: emerging technologies that transform the information technology industry. *Cloud Computing and Data Science*, 4(1), 1–16

[38] Anitha Kumari, K., Padmashani, R., Varsha, R., & Upadhayay, V. (2020). Securing Internet of Medical Things (IoMT) Using Private Blockchain Network. In Peng, SL., Pal, S., Huang, L. (eds) Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, vol 174. Springer, Cham. https://doi.org/10.1007/978-3-030-33596-0_12.

[39] Piccolo, A. (2017). Distributed ledger technology in the capital market: Shared versus private information in a permissioned blockchain. p. 55. www.diva-portal.org/smash/get/diva2:1120587/FULLTEXT01.pdf.

[40] Zeba, S., Suman, P., & Tyagi, K. (2023). Types of blockchain. In *Distributed Computing to Blockchain* (pp. 55–68). Academic Press.

[41] Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). Consensus in the age of blockchains. arXiv preprint arXiv:1711.03936.

[42] Act, A. (1996). Health insurance portability and accountability act of 1996. *Public Law*, 104, 191.

[43] Al Mamun, A., Azam, S., & Gritti, C. (2022). Blockchain-based electronic health records management: A comprehensive review and future research direction. *IEEE Access*, 10, 5768–5789.

[44] Zetler, J. A. (2015). The legal and ethical implications of electronic patient health records and e-health on Australian privacy and confidentiality law. Available online : http://hdl.handle.net/2123/13865

[45] Cucoranu, I. C., Parwani, A. V., West, A. J., Romero-Lauro, G., Nauman, K., Carter, A. B., ... & Pantanowitz, L. (2013). Privacy and security of patient data in the pathology laboratory. *Journal of Pathology Informatics*, 4(1), 4.

[46] Capece, G., & Lorenzi, F. (2020). Blockchain and healthcare: Opportunities and prospects for the EHR. *Sustainability*, 12(22), 9693.

[47] Cerchione, R., Centobelli, P., Riccio, E., Abbate, S., & Oropallo, E. (2023). Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem. *Technovation*, 120, 102480.

[48] Faisal, M., Sadia, H., Ahmed, T., & Javed, N. (2022). Blockchain Technology for Healthcare Record Management. In: Husain, M.S., Adnan, M.H.B.M., Khan, M.Z., Shukla, S., Khan, F.U. (eds) Pervasive Healthcare. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-77746-3_17

[49] Karthikeyan, V., Kishore, M. N., & Sajin, S. (2024). End-to-end light-weighted deep-learning model for abnormality classification in kidney CT images. *International Journal of Imaging Systems and Technology*, 34(1), e23022.

[50] Gordon, D., & Nouwens, M. (Eds.). (2022). *The digital silk road: China's technological rise and the geopolitics of cyberspace*. Taylor & Francis.

15 Case Study on Botnet Attacks in Healthcare Sector and P2P Networks

Samriddhi Tripathi, S. Aanjankumar, S. Poonkuntran, Rajesh Kumar Dhanaraj, and Malathy Sathyamoorthy

15.1 INTRODUCTION

The Internet has become a more powerful and easy tool to access technical resources in today's world market. The Internet has become indispensable in many fields, including commerce, education, and biology. Nearly all aspects of people's everyday lives have been positively impacted by the Internet throughout the past three decades. Most applications from all fields depend on the Internet. As far as the application grows usage of the Internet has also rapidly increased. At the same time, the challenges faced by the usage of the Internet have also become an issue. The two main challenging factors of the Internet are security and privacy.[1]

The multiple security characteristics of secrecy, authenticity, as well as reliability must be protected at all times while operating computer and network systems. Many hackers and third parties are involved in stealing the data and hacking the information carried through various networks. This has become a major focus area for the researchers to sort out these issues for the users depending on the network.

Currently, there is substantial motivation for cybercriminals to participate in malevolent, profit-driven unlawful operations on the Internet. Botnets have emerged as a favored tool for digital wrongdoers in today's landscape. Serving as the primary means for many coordinated cybercrimes, botnets pose a grave menace to cybersecurity. This has resulted in a proliferation of fresh botnet threats, presenting significant hurdles to the field of cybersecurity. Presently, there exists a significant incentive for cybercriminals to partake in malevolent, profit-driven illegal activities on the web. Botnets are a preferred tool among modern digital criminals, leading to an upsurge in the emergence of novel botnet threats and introducing multiple substantial challenges to the realm of cybersecurity.[2]

Traditional techniques of safeguarding a system using signature-based detection have several limitations, prompting the search for improved and more effective solutions. The objective is to tackle issues associated with conventional botnet detection approaches and develop more efficient alternatives. This research explores various phases of botnet activity to devise effective detection strategies and surmount

DOI: 10.1201/9781032711379-15

the shortcomings of conventional botnet detection methods in both Windows and Android environments.[3]

15.2 BOTNETS AND THEIR CHARACTERISTICS

In today's interconnected world, all devices share links. Botnets, often referred to as "bots" or "zombies," are responsible for distributing malware and other potentially harmful software. A botnet constitutes a network of interlinked devices, each operating one or more bots. It represents an assembly of compromised computers and other gadgets overseen by an individual, usually a hacker or cybercriminal, without the owner's consent or awareness. Botnets serve as an amplifying force for malicious actors, cybercrime organizations, and individuals seeking to disrupt or compromise their targets' systems. The owner can manage the botnet through the utilization of C&C software. The term "botnet" is a fusion of "robotic" and "network," and it typically carries a negative or malicious connotation. In recent years, it has significantly influenced the global landscape, from Ukraine to the United States. Botnets serve as tools for disseminating malware through networks, positioning them as substantial threats to corporate networks, which must consistently maintain data, applications, and services accessibility. Botnets represent the primary culprits behind Denial of Service (DOS) attacks. These attacks can impede employees' access to sensitive and confidential information stored within the networks, potentially undermining the availability of data on the system and the data handler's credibility in data management. Despite the prevalence of DOS attacks, businesses may struggle to find effective solutions to counter this threat, often attempting to evade it entirely to minimize data loss.[4]

Botnet is another type of malicious code which operates or controls the network without the knowledge of the users. Security is a major and important concern in a cloud networking environment. Most of the security threats in the cloud are based on the bots in cloud networking. Hence, the detection and mitigation of bots in the cloud is vital in cloud networking to improve the performance of the networking. The current research will provide new apps that will help in the detection of the presence of the botnets and in monitoring the network activity regarding the botnet entry in the system.

Botnets, a collection of infected computers, are one of the newest technologies in growing cybercrime. Financially motivated cybercriminals to use these viruses as a tool for cybercrime. For example, a botnet was used for Sting's DDoS ransom. Sending streams and running web services are not good for phishing attacks. Therefore, digital forensic investigators need to perform forensic analysis and reconstruction of these crimes. However, botnet developers use many tips and tricks to hide the existence of their bots. By using botnets with hundreds or thousands of devices all with their IP addresses, it is nearly impossible for hackers to prevent attacks or distinguish legitimate users from liars. Botnets are not new. Since early 2000, hackers have been using botnets to launch DDoS attacks by accessing unsecured devices, which were mostly computers at the time. But the Internet of Things is making the problem worse. Botnets are a significant cybersecurity threat, and their operators are often motivated by financial gain, ideological reasons, or other malicious intent. Efforts to combat botnets continue to evolve as both cybersecurity experts and cybercriminals develop new tactics and technologies.[5,6]

15.3 BOTNET ARCHITECTURE CYBER OBSERVATORY

This section deals with different botnet architecture. Botnet hosts can control the botnet from a central hub called a command-and-control architecture, briefly defined below.

15.3.1 Centralized Architecture

With centralized botnet architecture, botnet hosts can control the botnet from a central hub called a command-and-control architecture, which are all zombie programs.

15.3.2 Decentralized Architecture

When a decentralized botnet architecture is used, no machine in the botnet can control the bot program. Many command-and-control servers connect and communicate with robots. Figure 15.1 shows the difference between normal architecture and P2P architecture.

15.3.3 Hybrid Architecture

Hybrid style is the grouping of central and distributed architecture. There are two models of bots in hybrid architecture.

15.3.4 Client Robots and Service Robots

Botnets with hybrid architectures are more difficult to monitor and detect than centralized and distributed operations.

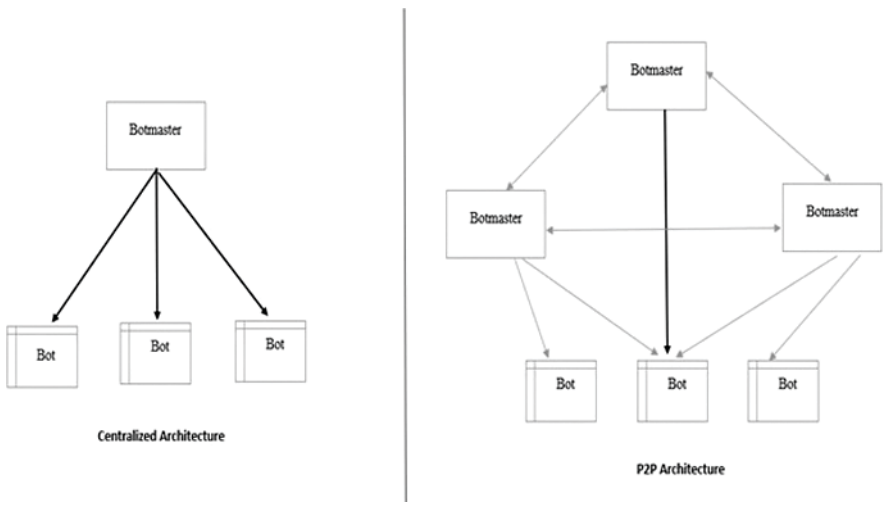

FIGURE 15.1 Difference between normal architecture and P2P architecture.

15.4 EFFECTS OF BOTNETS

i) **Viruses:** Botnets are created by infecting a large number of devices with malware that can be transferred through a variety of methods, such as phishing emails, malicious websites, or malware.

ii) **Control:** Once a device is infected and becomes part of a botnet, it can be controlled by a botnet operator. This centralized management allows business owners to issue commands to the entire network where the infected device resides.

iii) **Operations:** Botnets are used for a variety of crimes, including DDoS attacks, sending spam, spreading malware, stealing data, and even mining cryptocurrency. They may also engage in fraud by creating fake online advertisements.[7]

iv) **Distributed attacks:** DDoS attacks are a common use of botnets. In a DDoS attack, an infected device sends too much traffic to the target server or website, slowing it down or making it inaccessible to legitimate users.

v) **Hidden operators:** Botnet operators often take steps to hide their identities and locations, making it difficult for attackers to discover these.

vi) **Detection and mitigation:** Cybersecurity experts use a variety of approaches to detect and mitigate botnets, including network monitoring, intrusion detection, and security design to remove botnet malware from software.

vii) **Prevention:** To avoid becoming a part of a botnet, individuals and organizations need to have good security, keep their software and systems up-to-date, use reliable antivirus, and antimalware software, and avoid clicking on suspicious links or downloading unknown files.

viii) **Distributed denial of service:** Botnets may be used to release big-scale DDoS attacks in opposition to websites, servers, or online offerings. These assaults can crush the goal and make it unavailable to valid users.[8]

ix) **Statistics theft and privacy breaches:** Botnets can receive touchy statistics, together with personal data, login credentials, and economic statistics, from infected devices. This record is frequently used for identity theft or sold on the dark net.

x) **Junk mail and phishing campaigns:** Botnets are frequently chargeable for sending out massive volumes of unsolicited emails and phishing campaigns, attempting to mislead recipients into revealing touchy data, or downloading malware.

xi) **Cryptocurrency mining:** some botnets are repurposed for cryptocurrency mining. This may gradually bring down or overheat infected devices and boom power intake.

xii) **Click on fraud:** Botnets can be used to artificially generate clicks on online advertisements. This could defraud advertisers and artificially inflate internet site visitors' facts.

xiii) **Malware distribution:** Botnets often involve the distribution of other malware, such as ransomware and spyware, to expand the network of infected devices.[9]

xiv) **Financial losses:** Individuals and organizations may suffer financial losses for various reasons due to activities performed by botnets, including costs associated with mitigating attacks and remediating vulnerabilities.
xv) **Reputational damage:** For organizations, being the victim of a botnet attack can damage their reputation, undermine customer trust, and undermine legal and regulatory compliance.
xvi) **Resource usage:** Resource usage increases on infected devices in the botnet, which can reduce device performance and cause computer disruption.
xvii) **Network infrastructure stress:** Large-scale botnets can stress the entire network infrastructure, resulting in crashes and service outages.

It is worth noting that the effects of botnets are often problematic and illegal. Protecting against botnets involves implementing effective security measures, keeping software and systems up-to-date, and implementing network security measures to detect and prevent these threats.[10,11]

15.5 P2P BOTNET

A peer-to-peer community is a simple network of computers, first seen in the 1970s. Here each computer works as one of the shared files in the community, where every node acts as a server, so there may be no important server in the community. This lets in greater facts to be shared, and tasks are distributed equally among nodes. The capability of all connections in the network is in the same proportion. For the community to fail, all nodes ought to be stopped personally, because every node operates independently.

In shape, a peer-to-peer (P2P) network is created using greater computers connecting to every different and sharing asset without passing through the PC. The primary server is separate. A P2P network can be an ad hoc connection, which means there can be many computers connected through a worldwide bus to switch statistics. A P2P community also can be a set vicinity linked via copper cables to six computers in a small office; or, a P2P network can be a bigger community in which unique processes and packages create relationships between customers on the net.

Commercial use of P2P networks followed the introduction of standalone computers in the early 1980s. Compared to a smaller solar system, such as Wang Laboratories Inc.'s VS system, which sent processing messages and other applications from a central computer to a secret message and stored the data on the central hard disk. It has a hard drive and a built-in CPU. Smart boxes also have built-in apps, which means they can be transferred to desktop computers and used without needing to connect to the host computer. Many employees feel the sense of freedom that comes with having a computer at their desk. But they soon needed a way to share information and printers. The solution was to save the file on a floppy disk and take the floppy disk to the recipient or send it by mail.[12]

In response to attempts to identify and destroy IRC botnets, malware has been introduced into peer-to-peer networks by bot herders. These bots, like those from Gameover Zeus and Zero Access, can use digital signatures to limit control of the botnet to those with access to private keys. The latest botnets only work in

P2P networks. Instead of interacting with a central server, P2P bots follow both the client receiving commands and the server distributing them. This prevents a single point of failure from centralized botnets.P2P bots covertly test random IP addresses until they locate another compromised machine to locate other infected workstations. Information like its software version and a list of known bots are provided in the contacted bot's reply. One of the bots will start a file transfer to update if its version is lower than the others. In this way, every bot expands its list of compromised systems and keeps itself updated by corresponding with all other bots regularly.[13]

This is particularly concerning for businesses heavily reliant on digital technologies, emphasizing the need for organizations and governments across various sectors to proactively identify and mitigate cyberattacks. Among the various malware types used by cybercriminals, botnets are the most prevalent, appearing in diverse forms and serving various purposes in compromising computer assets. Botnets pose a significant threat to cybersecurity, making it essential to understand and counteract their malicious activities. Numerous strategies have been developed and recommended to address the botnet problem, yet it persists and continues to harm both businesses and individuals operating in the online domain. Detecting P2P (peer-to-peer) botnets, which have appeared as a prominent threat in network cyberspace and serve as the infrastructure for various cybercrimes, presents a unique challenge compared to conventional botnets using existing approaches. Consequently, this learning will discover multiple P2P botnets.[14]

Botnets can harm peer-to-peer (P2P) networks, particularly because they're malicious and disruptive. When botnets infiltrate P2P networks, they are able to use the most allotted and normally relied on peer-to-peer relationships for a variety of malicious purposes.

Right, here's how botnets affect P2P networks.

a) **Supply malware:** Botnets can use P2P networks to distribute malware to unsuspecting users. this will encompass sharing infected files or putting malicious code into valid documents. Customers who download files from P2P networks run the risk of unknowingly infecting their devices with malware, doubtless turning them into botnet zombies.
b) **Amplified allotted Denial of service (DDoS) attacks:** Botnets can use P2P networks to create more effective DDoS attacks. With the aid of coordinating a huge variety of infected friends, a botnet can overwhelm its goal with a massive number of malicious attacks, resulting in carrier outages.
c) **Content material pollutants:** In a few P2P structures, bots can cause terrible content by means of sending faux or malicious facts to the network. This will prevent legitimate users from seeking to get admission to or proportion information and decrease the reliability of the community.
d) **Robbery and privateness:** If a botnet breaks into a P2P network, it can intercept, eavesdrop, or thieve touchy facts sent between friends. This may result in severe privacy breaches and information theft.
e) **Abuse of believef:** P2P networks frequently depend on users agreeing with to percentage facts to believe or to omit them without seeing them. Botnets can use this belief to spread malicious content or behaviour phishing attacks.

f) **Resource usage:** peers with affected structures can eat resources and eat a lot of sources, slowing down P2P networks and inflicting performance problems for customers.
g) **Legal and regulatory troubles:** P2P networks are related to illicit and online bet sports, and the existence of botnets can exacerbate these issues. Botnets can be used to distribute unlawful content material that can be valid.
h) **Mitigate problems:** Detecting and mitigating botnets in P2P networks may be tough due to the fact they often perform in a distributed manner. conventional security measures that depend upon centralized groups or traffic tracking might not be as effective in this case.

It's very critical to use security features consisting of antivirus and antimalware to shield P2P networks from botnet associated threats regularly. and software patches to reduce vulnerabilities. Additionally, community directors need to apply community tracking gear to correctly stumble on threats.[15]

The number of botnet attacks in healthcare is alarming, jeopardizing the overall protection of affected individual records, healthcare services, and healthcare businesses. Here are some critical factors that encourage a growth in botnet attacks in healthcare:

A) **Scientific statistics:** Medical facilities; store a diffusion of affected personal facts, inclusive of clinical records, economic records, and identity numbers. This information is a chief asset to the black market, making healthcare a pinnacle goal for cybercriminals to steal and sell these records.
B) **Virtual transformation:** The healthcare organization has undergone big modifications in recent years. Digital fitness records, telemedicine, and internet of things (IoT) gadgets have become essential additives to healthcare and feature delivering prominently in the impact of cybercriminals.
C) **Loss of cybersecurity arrangements:** Hospitals always appear inside the return of cybersecurity arrangements. Many web sites using the preceding strategies and personnel might also lack safety records and education, becoming an inclined vicinity for botnet use.
D) **Ransomware and monetary guide:** Botnets are frequently used to spread ransomware in healthcare. Ransomware assaults can financially advantage cybercriminals who call for ransom to unencumber clinical statistics and systems.

Due to the sensitivity and confidentiality of clinical records, botnets exist in peer-to-peer (P2P) networks in the healthcare industry. Beneath are a few results and troubles of botnets getting access to P2P networks in the healthcare industry:

i) **Records breach:** Botnets can be used to retrieve or access affected person statistics, collectively with medical information, coverage statistics, and personally identifiable facts (PII). This could lead to vital statistics breaches and privateness breaches, leading to theft and fraud.
ii) **Patient safety:** In healthcare, well timed getting the right of entry to accurate affected men's or women's statistics is crucial to affected person care. P2P

network disruptions from botnets can disrupt access to scientific statistics and impact affected person safety and vital care.

iii) **Malware distribution:** Botnets can distribute malware to clinical P2P networks. If malware infects a medical device, it can disrupt the device's functionality and compromise affected person care and safety.

iv) **Information integrity:** Botnet attacks on P2P networks will compromise integrity of statistics. Disclosure or destruction of clinical records may additionally cause wrong clinical selections and damage to patients.

v) **Criminal tips and hints:** Healthcare companies are scenario for strict rules, such as the health insurance. The Health Insurance Portability and Responsibility Act (HIPAA) within the United States rules that data concerning botnet breaches might also result in prison and regulatory measures, together with fines and prosecutions.

vi) **Monetary charges:** Mitigating the impact of botnets in medical P2P networks can be steeply priced. This consists of investigating, notifying affected individuals, enforcing safety upgrades, and probably paying fines.

vii) **Damage to reputation:** Botnet-related facts, breaches and protection issues can damage a healthcare agency's popularity. Patients might also additionally lose self-assurance in their clinical medical doctor's competence to shield their sensitive records.

viii) **Fitness impact:** Botnets can launch denial-of-provider (DDoS) assaults on healthcare structures, rendering them quickly inaccessible. This could disrupt healthcare and disrupt patient care and operations.

ix) **Harm to medical gadgets:** A few hospitals use P2P networks for verbal exchange and facts sharing. Botnets can disrupt this equipment and put patients at hazard.

x) **Aid consumption:** Botnet-infected gadgets devour network property and degrade the performance of P2P networks. This could bring about decreased normal clinical performance and delays in affected individual care.

To defend healthcare P2P networks in opposition to botnets and their related dangers, healthcare groups ought to put in force security capabilities, mainly addressing cybersecurity, consisting of network tracking, encryption and intrusion detection systems, and security control. Normal worker schooling and industry awareness are crucial to assist employees in discovering and responding to threats. To lessen the prevalence of botnet-associated problems within the healthcare enterprise, it's absolutely essential to comply with healthcare policies and helpful protection practices.[16]

15.6 TYPES OF BOTNET ATTACKS IN HEALTHCARE

Botnet attacks in healthcare cause many risks and consequences that affect patient safety, data security, and financial health. Here is a detailed issue caused by botnets. Some sample botnet attacks details are mentioned in Table 15.1 and Figure 15.2 different types of attack with their categories.[17]

TABLE 15.1
People suffer due to botnets in time and range

Botnet Attack	Attacks per Hour	People suffer due to P2P Bots in numbers
Scanner Device attack by botnet	513	2,200,000
Keylogger	300	2,030,000
Ransomware	260	13,380,000
Hospital data loss	150	5,700,000
Manual entry digital storage loss	367	70,000

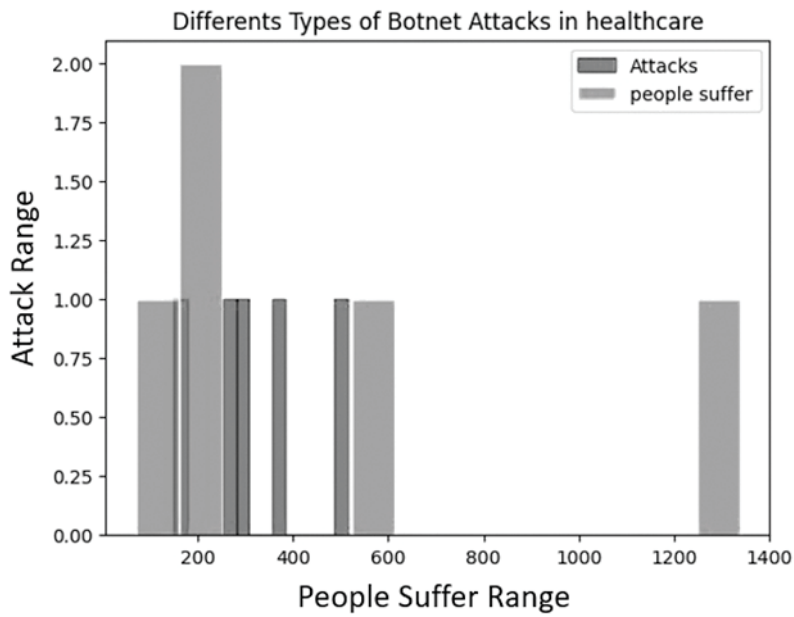

FIGURE 15.2 Different Types of Attack with their categories.

15.6.1 Data Breach

a) Patient Rights: Botnet attacks can lead to data breaches that expose sensitive information of the patient, including medical records, personal identification numbers, and financial records. This violates patient privacy and can lead to identity theft, fraud, and anxiety.

b) HIPAA Violation: In the United States, healthcare organizations are subject to the Health Insurance Portability and Accountability Act (HIPAA). Data breaches resulting from botnet attacks can result in fines and penalties for noncompliance with HIPAA regulations.
c) Lack of Belief: The patient's belief is important in treatment. A data breach can undermine a patient's trust in a doctor, tarnish his or her reputation, and cause patients to seek care elsewhere.[18,19,20]

15.6.2 Patient Safety Concerns

a) Health implications: Botnets can launch Distributed Denial of Service (DDoS) attacks that disrupt medical services. These attacks can disrupt patient care, schedule appointments, and access critical medical information.
b) Medical Device Threats: Some botnets target medical devices and Internet of Things (IoT) devices that patients care for. Damaged medical equipment can result in inaccurate readings, improper use of therapy, and patient injury.
c) Life situations: In the worst-case scenario, a botnet attack can disrupt critical systems or medical equipment and lead to life-threatening situations if timely medical attention is not given.[21,22]

15.6.3 Financial Impact

a) Extortion: Most botnet attacks involve ransomware, where cybercriminals demand a ransom to decrypt data. Healthcare organizations may find themselves in a difficult situation where they will have to pay a large ransom to operate and gain access to important patient information.
b) Operations Disruption: Botnet attacks can cause significant disruptions in operations, resulting in disruptions and increased costs. This includes scheduling appointments, investing in cybersecurity fixes, and legal fees.
c) Payment Taxes: In addition to HIPAA penalties, healthcare organizations may be subject to penalties in other areas, including class action lawsuits from affected patients.
d) Reputational damage: Financial impact causes long-term damage to the healthcare organization's reputation. Patients' trust in the institution may be lost and the consequences may take years to recover from.
e) Cybersecurity investments: After a botnet attack, healthcare organizations often need to invest in cybersecurity transformation, plans to resolve issues, and training employees; these lead to additional financial problems.

In summary, botnet attacks on healthcare can have serious consequences such as data breaches, patient safety issues, and disruptions. Healthcare organizations need to prioritize cybersecurity to reduce these risks and protect patient information and patient health.[23,24,25]

15.7 GLOBAL IMPACT OF BOTNET ATTACKS IN HEALTHCARE

These global events highlight the importance of botnet threats in healthcare and highlight the devastating impact such attacks can have. Healthcare organizations must continue to improve cybersecurity measures, update outdated systems, and increase employee awareness to mitigate these growing threats.[26]

Some important research on botnet attacks in healthcare organizations to date.

15.7.1 WannaCry Ransomware Attack (2017)

WannaCry Ransomware Attack is one of the most serious and devastating health attacks. It affected the United Kingdom's National Health Service (NHS) and many medical organizations around the world. WannaCry spread very quickly by exploiting a vulnerability in Microsoft Windows. It encrypts data on affected systems and requires a ransom to be decrypted. This strike disrupted hospital operations, cancelled appointments, and impacted patient care. This botnet-based ransomware disrupts healthcare services, rendering computers and medical equipment inoperable. The NHS had to cancel appointments and transfer patients due to the strike. The NHS had to move patients, cancel surgeries, and it had a huge impact on business. The attack highlighted the importance of cybersecurity in healthcare and led to calls for better security practices.[27]

15.7.2 Ryuk Ransomware Attack (2019)

Ryuk ransomware is related to a botnet and released a massive-scale ransomware assault in opposition to many healthcare companies inside the US and around the world. Ryuk is regularly sent by botnets which include Emotet or TrickBot. Once in the network, it encrypts facts and needs a ransom in trade for the decryption key. Ransomware causes massive economic losses within the healthcare enterprise. These assaults can lead to statistics encryption and business disruptions, and require healthcare agencies to pay big ransoms to regain access to their systems. The attacks can disrupt affected person care, impact the supply of scientific statistics, and cause extensive financial losses.[28]

15.7.3 University of Vermont Health Network (2020)

The University of Vermont Health Network (UVMHN) suffered a major cyberattack after being linked to Ryuk ransomware. This attack resulted in the disruption of essential medical services, including patient care, surgery, and appointments. As a result of the attack, the network had to use manual methods. UVMHN was forced to pay a ransom to obtain the decryption key. This shows the vulnerability in the medical industry and further compromises in improving cybersecurity measures.[29]

15.7.4 Emotet Malware (2020)

While Emotet is not itself a botnet, it is known for creating botnet patterns and has been used to spread a variety of malware, including TrickBot and Ryuk. The Emotet virus has affected healthcare organizations around the world, causing data breaches and operational disruptions.[30,31]

15.7.5 Vulnerabilities in IoT Devices (Vulnerable)

Botnets are known to exploit vulnerabilities in IoT devices in healthcare organizations. For example, unsecured IoT medical devices such as pumps, patient monitors, and even security cameras have been compromised, resulting in data loss, leakage, or interference with patient care.

These case study highlight the serious consequences of botnet-based attacks in healthcare, including data encryption, operational disruption, financial loss, and impact on patient care. They also highlight the need for cybersecurity measures and emergency plans in healthcare organizations to reduce these risks. Healthcare organizations need to be aware of new threats and continue to improve security to protect patient information and security.[32,33,34]

15.8 PREVENTION AGAINST BOTNET

Figuring out and stopping botnet interest in healthcare is important to shielding affected persons' information and continuity of care. Beneath are methods and great practices for detecting botnet hobbies, in addition to relevant technologies for preventing botnet assaults:

1. Community evaluation: Intrusion Detection gadget (IDS) and Intrusion Prevention gadget (IPS): these structures display networks for suspicious patterns and perceive botnet-related behavior. They can trigger alerts or block undesirable traffic.[35]
2. Behavioral analysis methods: errors detection: the usage of device studying and synthetic intelligence algorithms as the idea of network behavior. Deviations from this baseline may also imply botnet interest.
3. Endpoint security: Antivirus and Anti-Malware software programs: updated antivirus and anti-malware tools can come across and get rid of botnet-related malware.
4. E-mail protection Gateway: Scans emails for malicious messages which can lead to phishing attempts and botnet infections. Internet filtering: Use internet filtering to prevent getting right of entry to malicious websites recognized for use for botnet management and distribution.
5. Research and analysis: Centralized get entry to gather and analyze logs from more than one network device to identify suspicious pastimes which includes

more than one login or related records. User Analytics and vicinity conduct (UEBA): UEBA gear has a look at a person's behavior which can have a financial impact on your corporation.

6. Risk Intelligence: Subscribe to the safety program: currently informed approximately rising threats and botnet command and control servers.[36,37]

15.8.1 High-quality Safety Practices and Approaches

1. Normal Software Updates and Patch control: Ensure all software, running systems, and applications are up to date against known vulnerabilities generally exploited by way of botnets.
2. Community Segmentation: Separates important procedures from unsecured parts of the community. These boundaries restrict the motion of botnet malware throughout the network.
3. Access control: Use strong controls to restrict get right of entry to systems and information. Use multi-thin authentication (MFA) to boost protection.
4. E-mail security: Use e-mail filtering and security answers to dam phishing emails and malicious attachments, which are common distribution mechanisms of botnet malware.
5. IoT device security: Guard IoT gadgets with sturdy passwords, regular firmware updates, and community sharing to prevent botnets from disrupting gadgets.
6. Worker training: Offer employees cybersecurity education to assist them in discovering phishing attempts, suspicious emails, and the significance of password management.
7. Ransomware protection: Regularly restore critical files and maintain backups stored securely offline. Create an emergency response plan to behave quickly in the event of a ransomware attack.[38]
8. Firewall and Intrusion Detection/Prevention: Enforce firewalls and intrusion detection/prevention systems to display and filter out community visitors for botnet-associated sports.
9. Conduct based total protection: Install security solutions that examine and stumble on unusual conduct patterns among network customers and devices.
10. Hazard Intelligence Sharing: Participate in hazard intelligence sharing networks to acquire and percentage statistics about acknowledged botnet activity and rising threats.
11. Normal Safety Audits: Use ordinary behavior protection audits and vulnerability exams to discover and cope with weaknesses in the community.

With the aid of combining these detection methods and first-class prevention practices, healthcare agencies can appreciably enhance their capacity to pick out and mitigate botnet-related threats and make stronger the overall cybersecurity posture in their networks.[39,40]

15.8.2 How to Handle Botnet Attacks

Mitigating the impact of botnet attacks on healthcare groups calls for a clear reaction and recuperation plan. Here are some strategies for handling botnet assaults, inclusive of incident response and countermeasures:

1. Incident reaction Plan: Create and control an incident reaction plan for botnet assaults. The plan needs to consist of roles and responsibilities, communication approaches, and a period in between procedures to reply to the situation.[41]
2. Training: Train personnel and stakeholders to recognize the symptoms of a botnet attack. Behavior cybersecurity education and drills to ensure all of us know what to do on the occasion of an assault.
3. Early Detection: Use Intrusion Detection Structures (IDS) and Intrusion Prevention Systems (IPS) to screen network connections for signs and symptoms of botnets. Installation signals and automated responses to threats.
4. Elimination: While an attack is detected, isolate the affected system. Cast off infected devices from the community to save you similar harm and the movement of malware.[42]
5. Conversation: Set up clear conversations in the organization. make certain personnel recognize how to record incidents and have open traces of verbal exchange to raise issues.
6. Incident Containment: Compromise botnet assaults with the aid of isolating infections, blocking malicious connections, and preventing infections. This prevents the attack from spreading in addition.[43]
7. Research: Research to verify the botnet assault. Become aware of vulnerabilities and get the right of entry to factors used by attackers. Acquire proof of the crime.
8. Elimination: Remove botnet malware and related processes from affected systems. Ensure all systems are patched and updated to prevent reoccurrence.[44]
9. Statistics recuperation: Get better-unaffected facts and structures from backups. Remember to test your backups frequently and shop them securely offline to prevent them from being centered with the aid of botnets.[45]
10. Coverage and Compliance: Ensure compliance with information safety legal guidelines and policies. Record this incident and cooperate with the research.
11. Non-stop tracking: Continuously reveal the network for signs and symptoms of botnet pastime, even after the issue is resolved. The botnet can also try and regain access or release new attacks.
12. Classes found out: Conduct an incident evaluation to determine the root reason for the attack, examine the effectiveness of the response, and make essential improvements to the emergency response plan.
13. Advanced safety: Observe lessons learned from stepped-forward security. This will encompass strict controls, area management, and workforce training, as well as safety technology updates.
14. Collaborate and share threats: Collaborate with other healthcare businesses and safety groups to be the first to file botnet threats and threats. This aggregate facilitates the prevention of future assaults.

A strong incident and recovery plan is important to mitigate the effect of a botnet attack. With the aid of detecting and controlling those threats, healthcare groups can boost their security whilst decreasing the risk of damage to information and packages. To sum up, this case study provides insightful information about how cyberthreats are changing in the healthcare industry and how they relate to peer-to-peer networks. The insights gleaned from these real-world instances highlight how critical it is to proactively address these security issues in order to protect patient data, uphold the integrity of healthcare services, and guarantee the public's trust and welfare.[22,46,47]

15.9 CONCLUSION

Challenges have been identified that have exacerbated cybersecurity vulnerability and the danger to the healthcare industry. These difficulties include botnet attacks, which result from obsolete healthcare data and software; a decline in experienced IT and cybersecurity workers, which results in fewer support and patching updates; and caregiver training. This has coincided with the pandemic period and a significant increase in cybersecurity threats worldwide. Correcting these shortcomings needs improving cybersecurity, and the techniques now available will not sustain an effective cyber defence system, let alone put the healthcare sector on a level playing field with industry.

The proliferation of IoMT necessitates the establishment of regulatory agencies to oversee the design, production, and distribution of these devices, including fundamental encryption and communication protocols. Without some type of regulation, the IoMT will become a massive and insecure attack surface in an industry that commands the greatest price for data on the dark web. To stay current with threats, all software and devices, including the IoMT, must be routinely updated and patched. Without this, the attack surface is larger and more easily revealed, as evidenced in the ransomware attack on the NHS.

In future the healthcare industry should send out phony phishing emails on a regular basis. To draw attention to a possible risk, all external emails should have a banner or highlighted bar. Passwords should have a minimum strength and be updated on a regular basis with a fully new password. All of these measures will have the greatest impact since an institution's workforce is the greatest cybersecurity risk to its systems and data. All of these approaches need financing, which is woefully lacking in healthcare cybersecurity. An assault is unavoidable in the absence of this financing and the necessary competence. This case study showed the impact of P2P botnets, how to solve botnet problems, how to control future botnet attacks, and their mitigation in detail.

CONFLICT OF INTEREST

The authors declare that they have no conflict of interest.

ETHICS APPROVAL

Since no experiments are performed on humans or animals (dead or alive) in this research, therefore, Ethical approval is not required

REFERENCES

1. Aanjankumar S, Poonkuntran S. (2016, December). Peer-2-Peer Botnet manage SDT security algorithm. In *2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1–5). IEEE.
2. HM Government. *National Cyber Security Strategy 2016–2021*. London, UK: HM Government. www.assets.publi shing.service.gov.uk/government/uploads/system/uploads/attachment_data/fle/567242/national_cyber_security_strategy_2016.pdf (2016). Accessed 12 Dec 2020.
3. Verizon. 2019 Data Breach Investigations Report. www.verizon.com/business/resources/reports/dbir/2019/results-and-analysis/ (2019). Accessed 5 Jan 2021.
4. Ghafur S, Fontana G, Martin G, Grass E, Goodman J, Darzi A. *Improving Cyber Security in the NHS*. London, UK: Imperial College London Institute of Global Health Innovation. www.imperial.ac.uk/media/imperial-college/institute-ofglobal-health-innovation/Cyber-report-2020.pdf (2019). Accessed 15 Nov 2020.
5. Jalali MS, Landman A, Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. *Journal of Clinical Monitoring and Computing*. 2023;37:1123–1132.
6. Sittig DF, Singh H. A socio-technical approach to preventing, mitigating, and recovering from Ransomware attacks. *Applied Clinicial Informatics*. 2016;7(2):624–632.
7. Best J. Could implanted medical devices be hacked? *British Medical Journal (Clinical Research Ed).* 2020;368:m102. www.bmj.com/content/368/bmj.m102. Accessed 23 Feb 2021.
8. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. *Maturitas*. 2018;113:48–52.
9. Williams CM, Chaturvedi R, Chakravarthy K. Cybersecurity risks in a pandemic. *Journal of Medical Internet Research*. 2020;22(9):e23692–e23694. www.jmir.org/2020/9/e23692/. Accessed 23 Feb 2021.
10. O'Brien S. Average cost of data breach in healthcare industry hits $7.13 Million. www.securityitsummit.co.uk/briefing/average-cost-of-data-breach-in-healthcare-industry-hits-7-13-million/ (2020). Accessed 12 Dec 2020.
11. Robinson J, Zoltan M. US healthcare data breach statistics. www.privacyafairs.com/healthcare-data-breach-statistics (2021). Accessed 15 Apr 2021.
12. Ghafur S, Grass E, Jennings NA, Darzi A. The challenges of cybersecurity in health care: The UK National Health Service as a case study Comment. *Lancet Digital Health*. 2019;1(1):e10–e12.
13. Stack B. Here's how much your personal information is selling for on the dark web. www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-onthe-dark-web/ (2017). Accessed 25 Mar 2017.
14. Cyber-attack: Europol says it was unprecedented in scale. www.bbc.com/news/world-europe-39907965 (2017). Accessed 27 Nov 2020.
15. www.bmj.com/content/361/bmj.k1750.long (2018). Accessed 11 Mar 2023.
16. Department of Health and Social Care. *Lessons Learned Review of the WannaCry Ransomware Cyber Attack*. London, UK: Department of Health and Social Care. www.england.nhs.uk/wp-content/uploads/2018/02/06_pb_08_02_18-lessons-learned-review-wannacry-ransomware-cyber-attack.pdf (2018). Accessed 12 Dec 2020.

17. National Health Executive. WannaCry cyber-attack cost the NHS £92m after 19,000 appointments were cancelled. www.nationalhealthexecutive.com/articles/wanna cry-cyber-attack-cost-nhs-ps92m-after-19000-appointments-werecancelled (2018). Accessed 26 Mar 2023.
18. Whittaker Z. GE admits security faws in its hospital devices could cause patient harm. https://techcrunch.com/2019/07/09/fawsanesthesia-respiratory-devices-tampering/ (2019). Accessed 6 Mar 2023.
19. Pranggono B, Arabo A. COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*. 2020;2021(4):e247.
20. Baumgart DC. Digital advantage in the COVID-19 response: Perspective from Canada's largest integrated digitalized healthcare system. *NPJ Digitial Medicine*. 2020;3(1):1–4.
21. Looper C. What is 5G? Everything you need to know. www.digitaltrends.com/mob ile/what-is-5g/ (2021). Accessed 18 May 2021.
22. Newman LH. A new Pacemaker hack puts Malware directly on the device. Retrieved from www.wired.com/story/pacemaker-hack-malware-black-hat/ (2018). Accessed 12 Dec 2020.
23. Petrosyan A. Share of global adults who trust public Wi-Fi networks to keep info safe 2019. www.statista.com/statistics/1147501/share-adults-trust-public-location-wif-network-infor mation-safe/ (2022). Accessed 25 Mar 2023.
24. Cyberunit. Can you trust public WiFi? www.cyberunit. com/blog/can-you-trust-public-wif (2021). Accessed 25 Mar 2023.
25. Mirsky Y, Mahler T, Shelef I, Elovici Y. CT-GAN: Malicious tampering of 3D medical imagery using deep learning. Retrieved from www.arxiv.org/pdf/1901.03597.pdf (2019). Accessed 15 July 2020.
26. McNamee K. 5G – What could go wrong? [Conference Presentation]. ISC2 Security Congress 2020, Online (2020).
27. Patel H, Hassell A, Keniston A, Davis C. Impact of remote patient monitoring on length of stay for patients with COVID19. *Telemedicine and E-Health*. 2020. https://doi.org/10.1089/tmj. 2021.0510.
28. Skorobogatov S. The bumpy road towards iPhone 5c NAND mirroring. www.arxiv.org/pdf/1609.04327.pdf (2016). Accessed 27 June 2018.
29. Evans D. *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*. San Jose, USA: Cisco. www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (2011). Accessed 18 Oct 2020.
30. Ericsson. Wearable technology and Internet of things. www.ericsson.com/en/repo rts-and-papers/consumerlab/reports/wearable-technology-and-the-internet-of-things (2016). Accessed 6 Mar 2023.
31. MIT Technology Review. Security experts hack teleoperated surgical robot. Retrieved from www.technologyreview.com/2015/04/24/168339/security-experts-hack-teleoperated-surgical-robot/ (2015). Accessed 18 Oct 2020.
32. Nasajpour M, Pouriyeh S, Parizi RM, Dorodchi M, Valero M, Arabnia HR. Internet of things for current COVID-19 and future pandemics: An exploratory study. *Journal of Healthcare Informatics Research*. 2020;4(4):1–40.
33. Newman LH. Medical devices are the next security nightmare. Retrieved from www.wired.com/2017/03/medical-devices-next-securitynightmare/ (2017). Accessed 18 Oct 2020.

34. Storm D. MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. Retrieved from www.computerworld.com/article/2932371/medjack-hackers-hijacking-medical-devices-tocreate-backdoors-in-hospital-networks.html (2015). Accessed 15 Dec 2020.
35. IBM Global Technology Services. *IBM Security Services 2014 Cyber Security Intelligence Index.* Somers, USA: IBM Corporation. Retrieved from www.i.crn.com/custom/IBMSecurityServices2014.PDF (2014). Accessed 8 Mar 2020.
36. Cisco. *Defending against today's critical threats*. San Jose, USA: Cisco. www.cisco.com/c/dam/global/en_uk/assets/pdfs/en_cybersecurityseries_thrt_01_0219_r2.pdf (2019). Accessed 18 Oct 2020.
37. Infoguard Cyber Security. 5 industries that top the hit list of cyber criminals in 2017. Retrieved from www.infoguardsecurity.com/5-industries-top-hit-list-cyber-criminals-2017/ (2017). Accessed 15 Dec 2020.
38. Hadnagy C. *Social Engineering: The Science of Human Hacking*. 2nd ed. Indianapolis: Wiley; 2018.
39. Symantec. *Internet Security Threat Report*. Mountain View: USA: Symantec. https://docs.broadcom.com/doc/istr-24-2019-en (2019). Accessed 19 Jan 2021.
40. Furnell S, Shah JN. Home working and cyber security–An outbreak of unpreparedness? *Computer Fraud Security*. 2020;2020(8):6–12.
41. Shi F. Threat spotlight: Coronavirus-related phishing. Retrieved from www.blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-relatedphishing (2020). Accessed 19 May 2021.
42. Sjouwerman S. Q1 2020 coronavirus-related phishing email attacks are up 600%. Retrieved from www.blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600 (2020). Accessed 19 May 2021.
43. Kumaran N, Lugani S. Protecting businesses against cyber threats during covid-19 and beyond. Retrieved from www.cloud.google.com/blog/products/identity-security/protecting-against-cyberthreats-during-covid-19-and-beyond (2020). Accessed 20 May 2021.
44. Ronquillo JG, Winterholler JE, Cwikla K, Szymanski R, Levy C. Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information. *Journal of the American Medical Informatics Association*. 2018;1(1):15–19.
45. Gibbs S. UK government PCs open to hackers as paid Windows XP support ends. Retrieved from www.theguardian.com/technology/2015/may/26/uk-government-pcs-open-to-hackers-aspaid-windows-xp-support-ends (2015). Accessed 19 Dec 2020.
46. Zou X, ed. IoT devices are hard to patch: Here's why—and how to deal with security. Retrieved from www.techbeacon.com/security/iot-devices-are-hard-patch-heres-why-how-deal-security. Accessed 18 Oct 2020.
47. Food and Drug Administration. Cybersecurity vulnerabilities afecting medtronic implantable cardiac devices, programmers, and home monitors: FDA safety communication, 21 Mar 2019. Retrieved from www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-afecting-medtronic-implantable cardiac-devices-programmers-and-home (2019). Accessed 18 Oct 2020.

16 ETI-GCN

Explicit to Implicit Graph Convolution Network for Personalized Recommender System in e-commerce and Healthcare

Thenmozhi Ganesan and Palanisamy Vellaiyan

16.1 INTRODUCTION

In today's internet era, massive volumes of data are developed and processed in day-to-day life that cause complexity in finding the relevant information and become time consuming. To alleviate the information explosion issues, a recommender system is ascertained owing to its effectuality of suggesting appropriate information to the relevant beneficiary[1]. Traditional recommender system filtering approaches are categorized as follows: Content-based[2], Collaborative filtering (CF)[3], Demographic[2] and Hybrid filtering[3]. Among them, CF technique is a widespread and proverbial method which investigates user preference by using their implicit and explicit feedbacks. It's productively utilized by the industries including e-learning, e-commerce, entertainment and healthcare. The fundamental mechanism of the CF method is predicting the user's interest by exploiting historical user-item interaction among the like-minded people[5]. Figure 16.1 illustrates the basic functionalities of recommender system.

16.1.1 Benefits of Recommender System

(i) **Revenue** – To raise the income of online shopping sites, several researchers have studied and computed several algorithms in recommender systems which increase the sales and consumers of the sites [4].

(ii) **Satisfaction of the consumer** – By providing essential and expected products in a short period of time and least search, the recommender system has earned the user contentment[2].

(iii) **Personalization** – Recommender system offers personalized suggestions from our friends also. Friends discern our likes and dislikes better than any others.

DOI: 10.1201/9781032711379-16

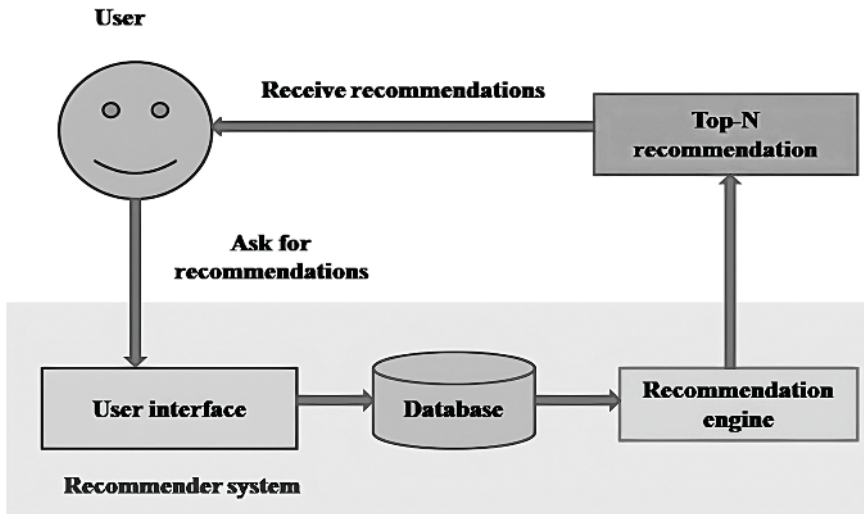

FIGURE 16.1 Basic functionalities of recommender system.

Apart from these advantages, discovery of new items to predict user preferences and generating/proving reports of the user's purchase history for future prediction are some key benefits of RecSys[3].

There are three phases in the traditional recommender systems including data collection (IC) phase, learning phase and prediction phase.

16.1.1.1 Data Collection Phase

User's relevant information such as user profile, previous purchase and views, user behaviour are gathered to build the learning and prediction model. For an enhancement of the functionality of a recommendation engine, the model generation is contemplated as a crucial factor. Without the user profile/model, it does not predict the relevant information for recommendation. Data collection is completed by three formats including explicit, implicit and hybrid feedback. Explicit response involves the user's reviews and ratings for particular items they have purchased[6]. In general, explicit feedbacks are text and non-negative numerical values from 0 to 10. Implicit feedbacks incorporate the user's earlier purchase history, time spent on shopping websites, clicks on wish-listed items, links followed by the user and email contents. To enhance the prediction performance, both methods (explicit and implicit) are collaborated. By amalgamating these two methods, the limitations of each technique are eliminated[2].

16.1.1.2 Learning Phase

Subsequently, the amassed data are fed to the learning phase in which machine learning algorithms are generated and practised on the data to convert them into the patterns. Pattern generation is a significant process of machine learning (ML) since ML prediction algorithms would not function on the raw data. These patterns are utilized by the prediction phase to produce recommendations[7].

16.1.1.3 Prediction Phase

In association with the outcome of the learning phase, the user's future preferences (what kind of suggestions they required to get) are predicted in the prediction phase with assist of ML prediction algorithms [2].

16.1.2 Techniques of Recommender System

16.1.2.1 Content-based Filtering

CB filtering utilizes features of the products and user's profile. User profiles, item description, features of previously purchased items are employed to recommend the items the user is interested in. Content-based filtering involves the following: Content analyzer, profile learner and filtering component[12].

Content analyzer – In cases where information lacks structure, such as text, a pre-processing phase is necessary to extract pertinent and structured data. The principal duty of the constituent is to display the substance of objects such as documents and web pages, product details, news, etc.[8]. Feature extraction techniques are exploited to examine data items and change the item representation from the original information space to the intended one.

Profile learner – By gathering information regarding user preferences and attempting to generalize it, this model creates a profile of the user. The generalization approach is typically implemented by ML strategies that can comprehend an improved model to predict user's preferences starting from items liked and disliked in the past[9].

Filtering component – This model finds new products that match the item list by achieving the user's data profile. It then shows the user the new product. The comparison is done by comparing the prototype vector with the item vector[10, 2].

16.1.2.2 Collaborative Filtering

The user's behavioural records including feedbacks, ratings, activities and their reviews are collected and utilized to construct the collaborative filtering recommender system. The CF method does not employ the client's profile and product description[11]. The similarity among various users and items is computed using a similarity calculation algorithm. These calculations are then exploited to recognize the users with the same preferences for the target user and item. Finally, missing records in the data are imputed with distance calculation with the predicted score to suggest items to the users. The collaborative filtering approach is classified into a couple of classes: memory-based collaborative filtering[2] and model-based collaborative filtering[3].

16.1.2.2.1 Memory-based Collaborative Filtering

As its name suggests, memory-based algorithms accumulate user-item rating features. It is simple to execute but requires massive storage space to store and retrieve the data. It exploits complete user-item rating records to calculate the similarity matrix.

It is further classified as user-user collaborative filtering and item-item collaborative filtering techniques[12].

The user-user collaborative filtering method gathers similar users with high scores (i.e. active users) for target users to predict their preferences to satisfy them with most appropriate recommendations, whereas in item-item collaborative filtering methods, similarity among active items are computed for the target item[6].

16.1.2.2.2 Model-based Collaborative Filtering

It reduces complications of handling a massive database by developing the models. These models are achieved by the ML algorithms such as clustering, dimensionality reduction, Bayesian classification, neural networks etc. The model-based approach ensures a prompt response to the user's request. Recommendations generated by this technique are static because it is burdensome to create and train the model when the choices vary rapidly[13].

(i) Clustering

Finding the patterns in data and separating them into the relevant classes is known as clustering. It is an unsupervised machine learning technique exercised to group the variables into classes without knowing the class labels. Maximum cohesion and minimum coupling are the criteria to form the ideal cluster[2], i.e. the target element should be assigned to the cluster having a higher degree of similarity with the element and other clusters should have lower similarity scores. In k-means clustering, 'k' cluster is having the group of users. k is denoted as a centre point for the cluster which is assigned randomly at first. Based on the cluster centre's similarity users are grouped into this cluster. The cluster centre is updated by cumulating the user's data within the cluster. Until convergence, the aforementioned progress is repeated[14]. Partitioning based clustering, model based, density based and grid based are the types of clustering techniques[3].

(ii) Matrix factorization (MF)

MF is one among the accepted approaches in RecSys that depends on the theory of each user and item connected with its latent features. Matrix factorization methods are highly recommended for sparse datasets which can identify the missing values. It performs flexibly for huge complex data with least computational cost. Probabilistic matrix factorization (PMF), principal component analysis (PCA), SVD, etc. take place in dimensionality reduction technique[15].

(iii) Association rule mining

Association rule mining is a significant method of data mining, which foresees appealing associations between items in a set of data. Association analysis, on the contrary, is the search for association rules that show attribute-value relationships that often co-occur in a data set[14]. It is recognized as an effective solution for a cold start issue hence user item rating matrix is not necessary.

(iv) Graph Convolutional Network
Graph convolutional network is a momentous approach in a collaborative filtering recommender system for grabbing the embeddings. A graph is a construction which is formed by nodes/vertices and edges. Nodes are the entities and the edges are correlating these entities to symbolize the relation between them. Based on the relation's directions, graphs are classified as directed graph and undirected graph[16, 17]. In directed graph, the relations are single way where as in undirected graphs have both way relations. For recommendation graphs, nodes betoken the user and item and edges are the relation between them[18].

16.1.2.3 Demographic Filtering

Demographic filtering exploits the user's demographical data to generate personalized recommendations. It involves the profile information including gender, age, profession, education background and location. It does not inspect the user's behavioral data and awareness of the item[3]. User profiles are created in DF classifying users into stereotypical descriptions that represent the characteristics of user classes.

16.1.2.4 Hybrid Filtering

This is the combination of any two aforementioned techniques. Hybrid methods are identified as a robust and effective method due to its performance. It alleviates the limitations in the traditional techniques by providing high-score recommendations[19]. It is quite complicated to form and execute the hybrid architecture owing to its multifaceted formation and expensiveness. Weighted, switching, mixed, meta, feature combination, feature augmentation and cascade are the types of hybrid recommender system techniques.

The following delineates the organization of the manuscript: Section 16.2 lists the various related works in this research. In Section 16.3, proposed methodology is discussed. Section 16.4 illustrates the experimental analysis. Experimental outcomes are demonstrated in Section 16.5 and Section 16.6 presents the conclusion.

16.2 RELATED WORKS

Graph Convolution Network (GCN) represents the next generation of collaborative filtering technology. However, little is known about the factors that contribute to its recommendation-effectiveness. Neural Graph Collaborative Filtering (NGCF)[17] incorporates the bipartite graphical formation, which pertains to user-item interrelations, into embedding procedure. NGCF generated the user-item graph formation through proliferating embeddings on it. Author-tested efficacy of method on three benchmarks of implicit datasets namely Gowalla, yelp2018 and amazon-book and performance comparison is done by various methods with recall and NDCG. Deep learning based multi-criteria collaborative filtering is studied[20] that incorporate the user's profile information with user-item rating matrix to enhance the prediction performance.

A criteria preference aware light graph convolution (LGC) recommender system is proposed[21] in which there are graph neural network aided multi-criteria along with feedbacks. It is a revolutionary lightweight multi-criteria (MC) recommendation technique that can accurately capture users' preferred criteria and the collaborative signal in MC ratings through LGC. Precision, recall and NDCG are employed for performance measures. Probabilistic matrix factorization is concatenated with Bayesian personalized ranking[22] to diminish the cold start issue by using both explicit and implicit feedback data. It requires keen and enormous observations for complex datasets.

Light graph convolution network (Light GCN) is studied[23] for collaborative filtering with neighbourhood aggregation to predict the user-item interactions. The model exploits two factors, i.e. light graph convolution and layer combination. LGC is generated with discarded feature conversion and nonlinear activation. In layer combination, concluding embeddings of the node are constructed as a weighted summation of its embeddings on entire layers. Multi-criteria collaborative filtering practising rough set theory (RST) is achieved[24] in which weight factors for every item are initialized by RST to increase prediction accuracy. Further, fusion of DNN and MF is achieved[25] to generate MC collaborative filtering to provide optimal recommendations. This fusion yields relatively high accuracy yet is quite complicated for massive dataset.

16.3 PROPOSED METHODOLOGY

Networks known as GCNs are able to recognize patterns in graph data. They have a wide range of applications, but because of their capacity to encode relationships, they are specially appropriate for recommendation systems. Traditionally, users and items are represented as embeddings in models such as matrix factorization. Furthermore, the signal that encodes the behaviour and the interaction are portrayed in the loss function; usually it would be a dot product, rather than being a component of the embeddings. It is being uncertain that these techniques are sufficient to provide acceptable embeddings for collaborative filtering, despite their efficacy. Figure 16.2 depicts the Graph convolutional collaborative filtering architecture.

In GCN architecture, NGCF is made much simpler by eliminating nonlinear activation, self-connection, feature transformation using weight matrices, and other processes simply performing the normalized summation of neighbour embeddings towards the upcoming layer. To acquire the final representations in the layer combination stage, we aggregate the embeddings at each layer rather than concatenating the embeddings. It contains user embeddings and item embedding. N numbers of layers are combined in the layer combination stage to build the GCN network for user-item relation matrix. e_u^o and e_i^o denote the user and item interaction embeddings respectively.

16.3.1 Architecture of the ETI-GCN Model

Figure 16.3 illustrates construction of the proposed ETI-GCN model. It comprises five phases including data collection, data preparation (i.e. preprocessing), modelling, and prediction/recommendation and evaluation.

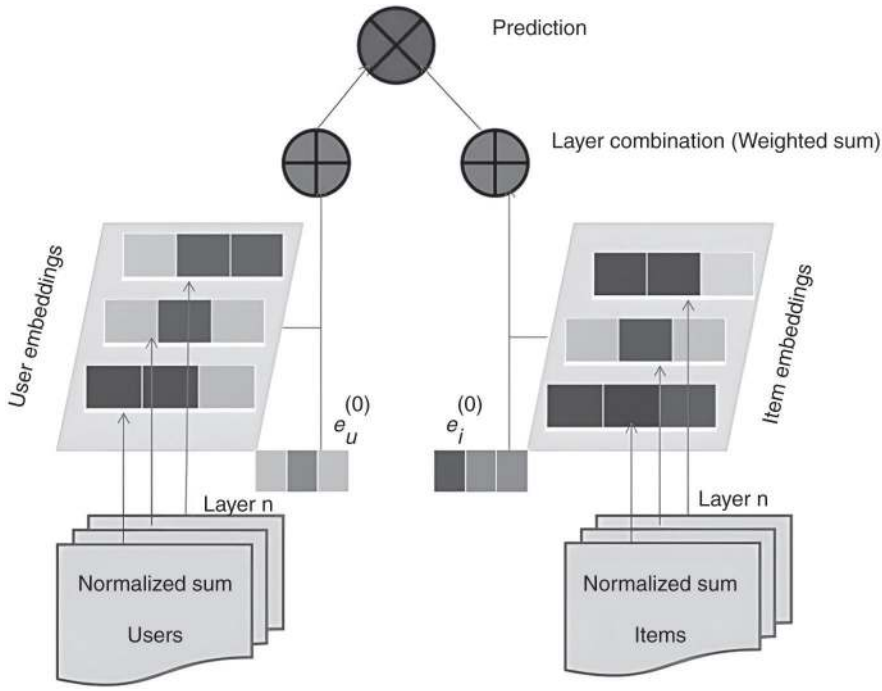

FIGURE 16.2 Graph convolutional collaborative filtering architecture with user and item embeddings for n number of layers.

(i) Data collection
The Movie lens dataset, which encompasess numerical ratings lies between 1 to 5, will be utilized. We translate Movie lens into implicit feedback for training and evaluation progress.

(ii) Data preparation
The GCN network can process implicit feedback data. For this, the explicit data are converted into the implicit feedbacks by using binarization methods in which the values above zero are converted into positive implicit data.

(iii) Data pre-processing
Data with missing values are inflexible to train the ML model. It is essential to handle them before the training process. Ensure and handle the missing values (if any) to upgrade the execution of the model by using deletion and data imputation methods.

(iv) Normalization
Normalization of adjacency is a key process of data preparation which helps to reduce unnecessary records in the data.

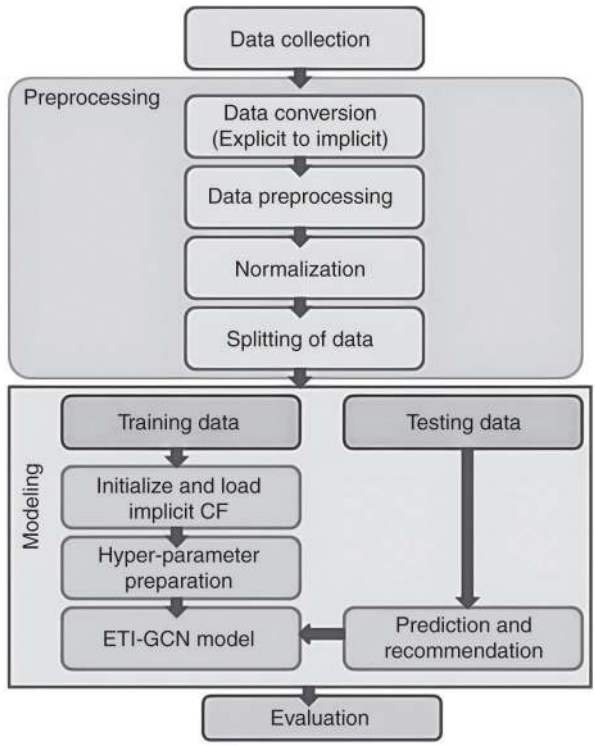

FIGURE 16.3 Architecture of the proposed explicit-to-implicit graph convolution network (ETI-GCN) model – Work flow.

(v) Splitting of data
The preprocessed data are then split into train-test data with 75% and 25% respectively. A modelling algorithm is operated on the trained data and the prediction and evaluation phases performed on the test data to experiment its efficacy.

(vi) Initialization and loading of implicit CF
The class Implicit CF loads and initializes data for the training procedure. This class initializes by re-indexing user and item IDs, converting ratings that are superior to zero towards implicit positive interactions, and creating an adjacency matrix for the user-item table.

(vii) Hyper-parameter preparation
The following are the essential parameters of an ETI_GCN model:

Data – initialized object of ETI-GCN dataset
n_layers – number of layers of ETI-GCN model
epochs – amount of training epochs

eval_epochs – The efficiency of the training model can be monitored by calculating evaluation metrics on test data for each eval epochs (if it is non-zero).
top-k – predicted items for recommendation to the target user when computing ranking metrics.

(viii) Prediction and recommendation
We use the paired loss known as the Bayesian Personalized Ranking (BPR) loss, which promotes the prediction that such an observed item will rank higher than its unobserved counterparts. During training, recommendations and evaluations were carried out on the designated test set. The model is preserved to estimate and make recommendations on different types of data after it has been trained.

(ix) Evaluation
Mean average precision (MAP), Precision, recall and Normalized Discounted Cumulative Gain (NDCG) are taken into account as performance measures to evaluate the model accuracy. These measures are calculated on the test data.

16.4 EXPERIMENTAL ANALYSIS

16.4.1 Datasets

To test the accuracy and efficacy of studied ETI_GCN model, Movie lens 100k and Movie lens 1M datasets[26] are utilized. These datasets contain explicit feedbacks with 1 to 5. To perform the GCN, both datasets are amended into implicit data by a binarization method which assumes values above 0 as a positive implicit feedback. Both datasets are non-cost and open source datasets collected from GroupLens website[26, 27]. Table 16.1 visualizes the numerical particulars of experimental datasets.

16.4.2 Comparative Methods

(i) Light GCN
By linearly propagating UI (user-item) embeddings lying on the UI interrelation graphical structure, Light GCN learns them. An eventual embedding is the weighted summation of the embeddings acquired at all levels. The logic of the basic Light GCN is analyzed from both an analytical and an empirical standpoint. This method is compared with neural graph collaborative filtering techniques. Light

TABLE 16.1
Numerical analysis of experimental datasets [26, 27, 30]

Dataset	Interaction	Movie	User	Sparsity
Movie lens 100k	100,000	943	1682	93.69%
Movie lens 1M	1,000,209	3900	6040	95.73%

GCN's fundamental principle is to learn node representations by smoothing features throughout the graph. It does this by iteratively performing graph convolution, which involves combining the attributes of neighbours to create a new demonstration of the target node[23].

(ii) Neural Graph Collaborative Filtering
Neural Graph Collaborative Filtering (NGCF) incorporates a bipartite graph-based structure, which pertains to user-item relations, into the embedding procedure. NGCF-generated UI graph structure through proliferating embeddings relies on it. By propagating embeddings on the user-item graph structure, it takes advantage of it. Consequently, transcendent connection in the user-item graph may be expressively modeled, thus explicitly acquainting the collaborative signal towards the embedding procedure[17].

(iii) Neural collaborative filtering
Within this framework, NCF expresses and generalizes matrix factorization in a generic manner. NCF modelling is the fusion of generalized matrix factorization with neural networks (multi-layer perceptron). In pursuance of incorporating non-linearities into NCF modelling, multi-layer perceptron is studied to attain user-item association. It relies on the implicit feedback to resolve the limitations in the collaborative filtering recommender system[28].

16.4.3 Performance Measures

To ensure the efficiency of the studied model, four globally accepted performance measures were investigated and compared with the existing methods. They are mean average precision (MAP), precision, recall and Normalized Discounted Cumulative Gain (NDCG) [23].

(i) Mean average precision
MAP or Mean Average Precision at k (MAP@k) is the widely accepted error metric for recommender and other ranking-related classification tasks. For recommendations presented to different users, the MAP@k metric measures the AP@k (average precision @ k) which is averaged across all queries in the dataset.

(ii) Normalized Discounted Cumulative Gain
Normalized Discounted Cumulative Gain (NDCG) is acquired to determine the accuracy of the predicted score in the ranking progress. Depending on the hit point in the recommendation list, it will manipulate and provide the end result.

(iii) Precision
The precision metric quantifies the segment of accurate predictions generated through the model. We are dividing the precision@k computation by the aggregation of items, suggested in the popular-k recommendation. Precision@k is set to 1 when zero recommendations are generated.

(iv) Recall

Recall@k provides the total pertinent items present in top k out of all relevant recommendations. k indicates the number of suggestions produced for the target user.

16.5 RESULTS AND DISCUSSION

The Explicit-to-implicit graph convolution network for personalized recommender system (PRS) is proposed and augments the effectiveness of the CF recommender system. To implement and investigate the efficiency of the studied model, Movie lens 100k and 1M datasets are utilized. The ETI-GCN architecture is implemented in python, which is open-source and high-end object oriented programming language. Tensorflow is one of the machine learning libraries of python developed for neural networks. The proposed model is set up in the most popular IDE of python named Jupyter notebook with the following hyper parameters: embed_size = 64, n_layers = 3, batch_size = 1024, decay = 0.0001 and learning rate (LR) = 0.015. MAP, NDCG, Precision and recall are the evaluation protocols taken for performance evaluation. The model surpassed traditional state-of-the art strategies even for sparse datasets.

Figure 16.4 demonstrates the efficiency of the ETI-GCN model for Movie lens 100k dataset. Table 16.2 illustrates performance comparison of the competitive models for both Movie lens 100k and 1M datasets. The studied model achieved effective outcomes with the following: MAP = 0.143201, NDCG = 0.474331, Precision = 0.401982, Recall = 0.260344 for k = 10 respectively. The obtained results are comparatively higher than the existing approaches which are clearly depicted in tables and graphs.

Figure 16.5 shows the graphical representation the competitive models for Movie lens 1M dataset. The studied model also yields the better performance for the massive

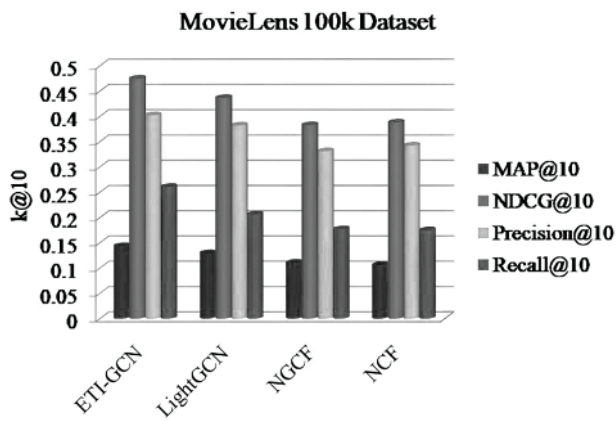

FIGURE 16.4 Bar chart of performance comparison for Movie lens 100k dataset with four bars.

TABLE 16.2
Comparative analysis of the competitive models on datasets for k=10

	Movie lens 100k				Movie lens 1M			
Techniques	**MAP**	**NDCG**	**Precision**	**Recall**	**MAP**	**NDCG**	**Precision**	**Recall**
ETI-GCN	0.143201	0.474331	0.401982	0.260344	0.081033	0.3835	0.352431	0.137419
Light GCN	0.129236	0.436297	0.381866	0.205816	0.075012	0.377501	0.345679	0.128096
NGCF	0.110591	0.382461	0.330753	0.176385	0.060579	0.299245	0.270116	0.10435
NCF	0.105725	0.387603	0.3421	0.17458	0.062821	0.34877	0.320613	0.108121

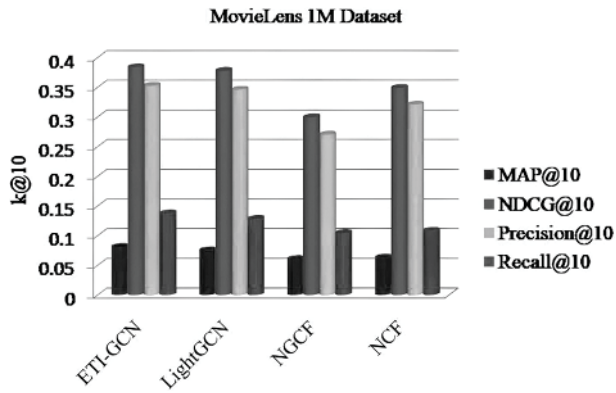

FIGURE 16.5 Bar chart of performance comparison for Movie lens 1M dataset with four bars.

dataset compared with the any other model. Apart from ETI-GCN, Light GCN achieved better results for both datasets[29]. Yet, neural graph collaborative filtering and neural collaborative filtering methods are obtained from lower performance for above experimental set up.

16.6 CONCLUSION

The recommender system is proved as an efficacious solution to alleviate the infoxication issue caused by storage and retrieval of massive volumes of data every day. Among the various techniques of RecSys, collaborative filtering is one of the broadly accepted techniques for its effectiveness and ease of use. In this study, a novel explicit-to-implicit graph convolution network is proposed to resolve the limitations in convolutional recommender system approaches. It consists of two stages, namely feature transformation and layer combination. The proposed ETI-GCN model is experimented on benchmark datasets Movie lens 100k and 1M. As an initial step, explicit feedbacks from the users is converted to implicit feedbacks thus graph convolution networks are capable of processing implicit data. The evaluation

of the proposed model is achieved by measuring MAP, NDCG, precision and recall @ k=10. The obtained results are then equated with the existing techniques to analyze the efficacy of the model. The studied model outperformed the existing approaches, which is clearly shown in comparative tables and graphical representation of evaluation protocols. Number of layers utilized here are three. By computing the user as well as item embeddings, user-item interactions are computed. Future preferences of users are predicted and suggested to the relevant users depending on this relation. Top-k predictions are suggested to the users among all the relevant predictions. In future, it is planned to increase the hidden layers to enhance the efficiency of the graph collaborative filtering. By adding more embedding layers especially for larger datasets, the dimensionality can be improved.

REFERENCES

1. Feng, X., Zhenchun P., and Rui X. E-commerce product review sentiment classification based on a naïve Bayes continuous learning framework. *Information Processing & Management*, vol. 57, p. 102221, (2020).
2. Vellaiyan, P., Rajendran, A., and Ganesan, T. A comprehensive survey on recommender system techniques. *International Journal of Computational Systems Engineering*, vol. 7, no. 2–4, pp. 145–158, (2023).
3. Anitha, T., Aanjankumar, S., Poonkuntran, S., & Nayyar, A. A novel methodology for malicious traffic detection in smart devices using BI-LSTM–CNN-dependent deep learning methodology. *Neural Computing and Applications*, vol. 35, no. 27, pp. 20319–20338, (2023).
4. Rahul, Dahiya, H., and Singh, D. (2019) A review of trends and techniques in recommender systems. In *Proceedings - 2019 4th International Conference on Internet of Things: Smart Innovation and Usages* (pp.1–8) , IoT-SIU. https://doi.org/10.1109/IoT-SIU.2019.8777645.
5. Akhilesh, K.S., Bhavna, B., Rachit, A., Suthar, D.P., Prajapati, P.G., and Atul, K. An efficient approach of product recommendation system using NLP technique. *Materials Today: Proceedings*, vol. 80, pp. 3730–3743, (2023).
6. Elavarasi, D., R. Kavitha, and S. Aanjankumar. (2023). "Navigating Heart Health with An Elephantine Approach in Clinical Decision Support Systems." In *2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS)* (pp. 1416–1423). IEEE.
7. Ganesan, T., and Vellaiyan, P. An efficient missing data prediction technique using recursive reliability-based imputation for book recommendation system. *International Journal of Computer Sciences and Engineering*, vol. 11, no. 2. pp. 8–11, (2023).
8. Wang, D., Liang, Y., Xu, D., Feng, X., and Guan, R. A content-based recommender system for computer science publications. *Knowledge-Based Systems*, vol. 157, pp. 1–9, (2018). https://doi.org/10.1016/j.knosys.2018.05.001.
9. Roy, D and Mala, D. A systematic review and research perspective on recommender systems. *Journal of Big Data*, vol. 9, pp. 1–36, (2022). https://doi.org/10.1186/s40537-022-00592-5.
10. Jain, A.F., Vishwakarma, S.K., and Jain, P. (2020). An Efficient Collaborative Recommender System for Removing Sparsity Problem. In: Fong, S., Dey, N., and Joshi, A. (eds) *ICT Analysis and Applications. Lecture Notes in Networks and Systems*, vol. 93. Springer, Singapore. https://doi.org/10.1007/978-981-15-0630-7_14.

11. Sallam, R.M., Hussein, M., and Mousa, H.M. An enhanced collaborative filtering-based approach for recommender systems. *International Journal of Computer Applications*, vol. 176, no. 41, pp. 9–15, (2020). https://doi.org/10.5120/ijca2020920531.
12. Davagdorj, K., Park, K.H. and Ryu, K.H. (2020) A Collaborative Filtering Recommendation System for Rating Prediction. In *Smart Innovation, Systems and Technologies*. Springer Singapore. https://doi.org/10.1007/978-981-13-9714-1_29.
13. Han, L., Wu, H., Hu, N., and Qu, B. (2019). Convolutional neural collaborative filtering with stacked embeddings. In Asian Conference on Machine Learning 2019 Oct 15 (pp. 726–741). PMLR.
14. Singhai, A., Aanjankumar, S., and Poonkuntran, S. (2023, May). A Novel Methodology for Credit Card Fraud Detection using KNN Dependent Machine Learning Methodology. In *2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)* (pp. 878–884). IEEE.
15. Bin, S., and Sun, G. Matrix factorization recommendation algorithm based on multiple social relationships. *Mathematical Problems in Engineering*, p. 6610645, (2021). https://doi.org/10.1155/2021/6610645.
16. Shuai, Z., Lina Y., Aixin, S., and Yi, T. Deep learning based recommender system: A survey and new perspectives. *ACM Computing Survey*, vol. 52, p. 38, (2020). https://doi.org/10.1145/3285029.
17. Wang, X., He, X., Wang, M., Feng, F., and Chua, T.-S. (2019) Neural Graph Collaborative Filtering. In Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR'19*)* (pp. 165–174). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3331184.3331267.
18. Shah, V., Anunay, Kumar, P. (2023). Recommendation System Using Neural Collaborative Filtering and Deep Learning. In Singh, Y., Verma, C., Zoltán, I., Chhabra, J.K., and Singh, P.K. (eds) *Proceedings of International Conference on Recent Innovations in Computing. ICRIC 2022. Lecture Notes in Electrical Engineering*, vol. 1011. Springer, Singapore. https://doi.org/10.1007/978-981-99-0601-7_10.
19. Liu, D., Li, J., Du, B., Chang, J., Gao, R. and Wu, Y. A hybrid neural network approach to combine textual information and rating information for item recommendation. *Knowledge-Based Systems,* vol. 63, pp. 621–646, (2021). https://doi.org/10.1007/s10115-020-01528-2.
20. Nassar, N., Jafar, A., and Rahhal, Y. A novel deep multi-criteria collaborative filtering model for recommendation system. *Knowledge-Based Systems*, vol. 187, p. 104811, (2020a), https://doi.org/10.1016/j.knosys.2019.06.019.
21. Park, J.-D., Li, S., Cao, X., and Shin, W.-Y. (2023) Criteria Tell You More than Ratings: Criteria Preference-Aware Light Graph Convolution for Effective Multi-Criteria Recommendation. In *Proceedings of the 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining (KDD '23)* (pp. 1808–1819). Association for Computing Machinery, New York, NY, USA. https://doi.org/10.1145/3580305.3599292.
22. Feng, J., Xia, Z., Feng, X., and Peng, J. RBPR: A hybrid model for the new user cold start problem in recommender systems. *Knowledge-Based Systems*, vol. 214, p. 106732, (2021). https://doi.org/10.1016/j.knosys.2020.106732.
23. Kumar, S., Aanjan, P., Karthikeyan, S., Aanjana Devi, S., Poonkuntran, V., Palanisamy, and Navatharani, V. (2024) Protecting Medical Images Using Deep Learning Fuzzy

Extractor Model. In *Deep Learning for Smart Healthcare* (pp. 183–203). Auerbach Publications.

24. Demirkiran, E.T., Pak, M.Y., and Cekik, R. Multi-criteria collaborative filtering using rough sets theory. *Journal of Intelligent & Fuzzy Systems*, vol. 40, pp. 907–917, (2021). https://doi.org/10.3233/JIFS-201073.
25. Nassar, N., Jafar, A., and Rahhal, Y. Multi-criteria collaborative filtering recommender by fusing deep neural network and matrix factorization. *Journal of Big Data*, vol. 7, no. 1, (2020b). https://doi.org/10.1186/s40537-020-00309-6.
26. www.grouplens.org/datasets/movielens/1m/
27. Manochandar, S., and Punniyamoorthy, M. A new user similarity measure in a new prediction model for collaborative filtering. *Applied Intelligence,* vol. 51, pp. 586–615, (2021). https://doi.org/10.1007/s10489-020-01811-3.
28. He, X., Liao, L., Zhang, H., Nie, L., Hu, X. and Chua, T.-S. (2017) Neural Collaborative Filtering. In *Proceedings of the 26th International Conference on World Wide Web (WWW '17). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE* (pp. 173–182). https://doi.org/10.1145/3038912.3052569.
29. Liu, H., Wang, W., Zhang, Y., Gu, R., and Hao, Y. Neural matrix factorization recommendation for user preference prediction based on explicit and implicit feedback. *Computing Intelligent Neuroscience*, (2022). https://doi.org/10.1155/2022/9593957.
30. www.grouplens.org/datasets/movielens/100k/

17 Enhancing Health Care

GAN-Based Stress Detection with Capsule Networks and Lion Optimization

P. Mahalakshmi, V. Gayathri, S. Gayathri, and R. Saranya Priyadharshini

17.1 INTRODUCTION

Electrocardiogram (ECG) signals are measure of electrical activity of the human heart[1]. This measurement contributes a major role in the medical field for health assistance. ECG signals reflect health conditions of humans with mental stress. The property of ECG signals is characterized by using the parameters of time, amplitude and frequency[2].

The concepts of machine learning and deep learning models are introduced to process the ECG signals effectively[3]. In machine learning models, the feature extraction and classification process are carried out separately. But in deep learning, the entire extraction and classification processes is carried out by the model itself. Convolutional Neural Networks (CNNs) have emerged as powerful tools for automatically extracting discriminative features from ECG data.

Compared to advantage, the DL-based ECG processings add some difficulties for processing. One primary limitation lies in the complexity of signal interpretation and feature extraction. ECG signals contain more complicated features for extraction. The proper selection of features from ECG signals leads to higher accuracy for classification. Various researchers developed a different algorithm for feature extraction and classification.

While the DL model shows promise in ECG signal processing, there's a need to address drawbacks such as over fitting, the interpretability of learned features and the requirement for large annotated datasets for model training. The development of novel methodologies that enhance feature extraction, improve model interpretability, and mitigate data scarcity issues is crucial for advancing stress detection in healthcare using ECG signals[4]. Integrating DL models by leveraging advancements in transfer learning and ensemble techniques can afford an effective accuracy and robustness of stress detection[5].

In this work, a modified GAN model is presented for stress classification using ECG signals. Also, an optimization is used as hype tuning. The proposed model has a capsule network, DenseNet and the Optimization to strengthen stress detection capabilities and also ensures adaptability and efficiency.

 DOI: 10.1201/9781032711379-17

The remaining is contributed as follow. Section 17.2 discussed the related works and preliminary works are described in the Section 17.3. Next, the proposed GAN model is discussed for stress detection in Section 17.4 and results and discussion of the proposed protocol is discussed in Section 17.5. Section 17.6 discusses a conclusion and is followed by references.

17.2 RELATED WORKS

S. Jayalakshmy et al.[6] discussed a GAN model to classify a respiratory signal. Initially, the signal is decomposed by Empirical Mode Decomposition. The signal is transformed into image for normal and abnormal classification. The accuracy is increased up to 5.3% when a GAN model is applied to the signal.

B. Liu et al.[7] presented a GAN model for the compression of signal and images. The signals are represented by latent vectors and redundant portions are compressed using the GAN model. For redundant portion identification, the iteration back propagation algorithm is used. The compressed signal is analysed in terms of signal to noise ratio (SNR) with other existing models. In[8], the authors developed a signal modulation type classifier based on GAN model. The signal is processed in time domain to calculate modulation factors. The results shows that the GAN model shows higher accuracy of 97.6% when compared to DL models.

Likewise, the authors Z. Tang et al.[9] proposed a signal modulation classifier using a GAN model. To balance a data imbalance, the GAN model is applied for data augmentation. The multiple signals generated are from a single signal from the GAN generator to solve a data imbalance issue. The SNR rate of the signal is improved to 4.5% after data augmentation. Arrhythmias are abnormal heart rhythms that can be classified based on the processing of signals. The hybrid arrhythmias classification algorithm is proposed by T. Lan et al.[10] using recurrent neural network and a GAN model. The data imbalance issues are solved using a GAN model with fast Fourier transform. Then, the recurrent neural network is used for classification.

Similarly, in[11], the arrhythmias' signals are classified using a conditional GAN model. In a conditional GAN model, the noise level generated is produced in a controlled manner. Compared to conventional GAN, the conditional GAN model shows higher accuracy in arrhythmias' signal classification. S. Janbhasha et al.[12] developed a new ECG signal classification approach based on long short-term memory. The unbalancing in heart signal is balanced using a GAN model and short-term memory network is used for classification.

N. H. Trinh et al.[13] developed a Pathological Speech Classification using GAN models. Initially, the signals are pre-processed using wavelet decomposition. The GAN model is applied for classification. The concept of a dual learning model in GAN is introduced by S. Jang et al.[14]. The dual ResNet model is used in generating part of the GAN model to classify the environmental signal. The environmental signal is processed by the dual generator for synthetic signal generation and classified as noise or noise free signals.

In[15], the authors proposed a wavelet decomposition combined GAN model for audio signal classification. The signal is transformed from time domain to frequency domain and processed by feature extraction-based wavelet transform. To improve the

accuracy of GAN models, the modified GAN model is proposed by Q. Zhang et al.[16] for signal classification. The layers of the GAN model are modified with different layers to learn the features deeply.

X. Wang et al.[17] designed an ECG signal noise filter using GAN models. The auto encoder-based generator is used to generate multiple signals for learning noises in signal. The discriminator includes multiple convolutional layers for the discrimination of signals. Compared to wavelet and other techniques, the GAN model shows higher SNR rates. The classification of snore signal is a difficult task due to its data availability. Z. Zhang et al.[18] proposed a GAN model to generate multiple snore signals to balance the data insufficiency. In addition, ensemble model is used to enhance the GAN model.

L. Xia et al.[19] proposed a long short-term memory model with attention mechanism to classify the EEG signal for stress. The attention mechanism is transferred from one to the other to output layer to learn the features deeply. The hybrid model of fuzzy and deep learning-based stress detection in ECG signal is proposed by M. Amin et al.[20]. The concept of knowledge transfer from one layer to another layeris used to learn the features from ECG signal. The final ranking about the stress signal is provided by fuzzy logic.

S. T. Chandrasekaran et al.[21] developed an echo state network-based stress detection model as an ECG signal. The model consists of a reservoir layer which is the series connections of neurons to process the signal. Compared to a machine learning algorithm, the echo state network shows higher true positive rates. B. S. Zheng et al.[22] proposed a new feature extraction technique for ECG-based stress detection. The proposed technique uses fuzzy K means algorithm with Euclidean distance for feature importance identifications.

In[23], the author proposed a decision tree-based ECG stress classification model. Initially, the features of ECG signals are extracted using wavelet transform. Then, the decision tree model is used for stress severity classification like low, medium and high. The hybrid machine learning model-based stress classification is proposed by L. Vanitha et al.[24]. The hybrid model combines neural network and support vector machine for the stress detection.

17.3 PRELIMINARY

This section presents an explanation about the basic working procedures of LOA.

17.3.1 Lion Optimization Algorithm (LOA)

The LOA is inspired by the cooperative hunting and social structure strategy of lions[25]. This LOA used a lion's behaviour to solve complex optimization issues based on a fitness function computation. The fitness values are evaluated using a cost function. In LOA, the population of lions randomly initializes across the solution space that is designating a portion as nomads and organising the rest into prides, with each lion assigned a specific gender that remains constant throughout optimization. Females and males are dispersed within prides according to specific ratios, for development diversity within the population.

17.3.1.1 Initialization

The initialization phase establishes a population of potential solutions (represented as lions) across the solution space. Each lion's position in the solution space is random, aiming to cover a diverse range of potential solutions.

Lions are represented in an N-variate dimensional space and their fitness values are computed using a predefined cost function.

The position of the lion in the search space is represented as follows:

$$lion = \left[x_1, x_2 \ldots..x_{Nvar} \right] \tag{1}$$

The objective or fitness function can be expressed as follows:

$$fitness\ values\ of\ lion = f\left(x_1, x_2 \ldots..x_{Nvar} \right) \tag{2}$$

17.3.1.2 Hunting

Lions emulate hunting behaviours to encircle prey, wherein female lions play key roles in stalking and encircling prey from different directions. Opposition-Based Learning (OBL) guides their movements, resembling the coordinated strategy of encircling prey observed in lions. Opposite points are calculated using OBL to simulate the encircling movements of lions around prey as follows:

$$X' = \left[x_1',\ x_2' \ldots..x_{Nvar}' \right] \text{Where} \quad x_i' = a_i + b_i - x_i \tag{3}$$

The encircling prey of lions mathematically modelled as follows:

$$Hunter_0 = rand\left(2 - PREY - Hunter, PREY - Hunetr\right) \tag{4}$$

17.3.1.3 Moving Toward Safe Place

Female lions, after hunting, move toward specific areas within their pride's territory. The movement is influenced by tournament selection among the pride's territories, aiming to diversify the search space exploration. Female lions' movements are directed towards selected points within the territory based on tournament selection. The updated position of the female lion can be expressed as follows:

$$Femal\ lion_0 = Female\ lion + 2D.r1\left(0,1\right)\tan\left(\theta\right).D \tag{5}$$

17.3.1.4 Roaming

Male lions engage in roaming behaviours within their territory, conducting local searches. Nomad lions adaptively roam to escape regions deemed unsuitable for finding optimal solutions. Nomad lions' adaptive roaming helps in escaping from areas with poor solutions. The position of a nomad lion to escape can be expressed as follows:

$$Lion_{ij}' = lion_{ij} \ \text{ if } \ r_j < p_{ri} \tag{6}$$

The probability of a lion to escape can be expressed as follows

$$p_{ri} = 0.1 + \min(0.5, \left(Nomad_i - Best_{nomad}\right) / Best_{nomad} \tag{7}$$

17.3.1.5 Mating

Mating between lions facilitates information exchange and genetic diversity. Females mate with resident males to produce offspring, inheriting traits from both parents. Offspring production involves a combination of genetic material from selected females and males within the pride, along with mutation for genetic diversity. The offspring can be expressed as follows:

$$offspring_1 = \beta Female\,Lion + \left(1-\beta\right)\sum_{i=1}^{NR} S_i Male\,Lion_i \tag{8}$$

17.3.1.6 Defence

Lions defend their pride against intruding males or attempt to take over prides through aggression. This phase maintains strong solutions and allows for exploration of new territories. Strategies determine when lions fight or change prides based on success ratios and aggressive behaviours observed in lions.

17.3.1.7 Migration

Females migrating between prides helps maintain diversity and share information. Nomad females redistribute among prides, contributing to information exchange and diverse exploration. Determining the number of migrating females and redistributing them among prides maintains diversity.

Each phase in LOA mimics specific behaviours observed in lion societies, integrating mathematical models and algorithms to simulate hunting strategies, territorial movements, mating, defence mechanisms, and population dynamics. These behaviours aim to balance exploration and exploitation while maintaining diversity within the population of potential solutions.

17.4 PROPOSED SYSTEM

A GAN model is a DL model that comprises two network generators and the discriminator as given in Figure 17.1. This innovative framework is designed for unsupervised learning and focusing for generating new synthetic data that closely resembles the training data.

The generator network within a GAN learns to create realistic data instances. In contrast, the discriminator network learns to differentiate between the synthetic data produced by the generator and real data from the training set. As the two networks iteratively compete against each other, the generator strives to produce data that

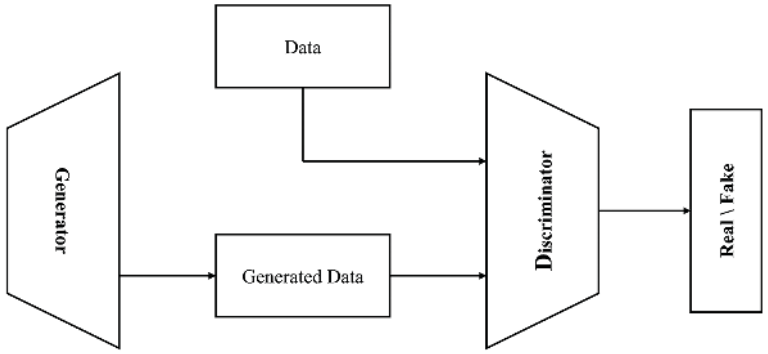

FIGURE 17.1 GAN model.

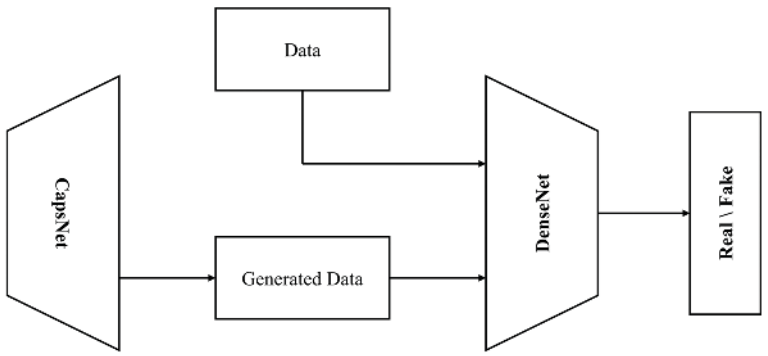

FIGURE 17.2 Proposed GAN model.

cannot be distinguished from real data by the discriminator and the discriminator aims to improve its ability to distinguish between real and generated data.

This work uses a novel strategy in a GAN model. The system integrates a generator employing capsule network models and a discriminator employing DenseNet architecture. Stress detection's criticality in healthcare cannot be overstated and impacts various medical conditions. The generator uses deep transfer learning which accurately generates stress-related physiological signals to refine the detection precision. Simultaneously, the DenseNet-based discriminator proficiently discerns between genuine and synthesized stress signals. LOA's role in fine-tuning model parameters ensures the system's optimal performance and robustness. The proposed GAN model is shown in Figure 17.2.

17.4.1 Capsule network

Capsule Networks (CapsNets) represent a paradigm-shifting neural network architecture that aims to overcome some limitations of traditional Convolutional Neural

Networks (CNNs)[26][27]. Introduced by Geoffrey Hinton and his team, CapsNets revolutionize how neural networks understand spatial hierarchies and offer promising solutions in various fields, including computer vision and pattern recognition. Traditional CNNs excel at recognizing patterns but struggle with viewpoint variations, deformation, and hierarchical representations. Capsule Networks are inspired by how the human visual system works and introduce capsules as fundamental units capable of preserving spatial relationships and pose information.

Capsules encapsulate the presence and pose of an entity in an image, preserving spatial hierarchies and relationships. Each capsule represents a group of neurons that encode various properties of a specific entity, encapsulating information about its presence, orientation, and deformation.

17.4.1.1 Routing Mechanism

Capsules communicate through dynamic routing by agreement to allow higher-level capsules to attend to lower-level capsules using agreement scores. It iteratively adjusts weights between capsules to improve an agreement among predictions and predictions of the lower-level capsules.

17.4.1.2 Transformation Matrices

Capsules used a transformation matrix to pose and instantiate parameters within the input data. These matrices encode parameters like translation, scale and orientation that is aiding in robustness against transformations in input data.

17.4.1.3 Primary and Digit Capsules

Capsule Networks used to capture lower-level features and digit capsules responsible using primary capsules for recognizing higher-level entities. It gathers features while digit capsules represent high-level entities contributing to better generalization and understanding of complex patterns.

17.4.1.4 Routing by Agreement

The agreement routing used to help CapsNets select relevant data while discarding noisy or irrelevant data to enhance robustness. Capsules are groups of neurons designed to encode different properties of visual entities. Each capsule represents a set of neurons that preserve spatial hierarchies and relationships within the data. It encapsulates the instantiation parameters (pose) of specific entities and allow the networks to understand various attributes simultaneously. Capsules explicitly encode pose information to overcome the drawback of existing models. This routing agreement reduces the overall complexity of the network and easily learns all the types of features from the datasets.

17.4.1.5 Dynamic Routing

Capsule Systems utilize energetic steering to set up associations between capsules which permit higher-level capsules to choose significant lower-level capsules for data accumulation. This permits the demonstration to memorize the spatial connections and chains of command inside information with minimal complexity. Not at all like

routine CNNs, CapsNets are an unusual kind of design that's based on the capacity of the human visual framework to progressively see objects. This design is built on the idea of "capsules" which are specialized neurons planned to speak to critical properties of objects in pictures. These capsules keep up spatial chains of command and bear data for understanding complex designs in information. The substance of this demonstration hence lies inside these capsules that encode not as it were presence but positional and instantiation parameters of particular substances inside an input picture. Thus, with this interesting design, CapsNet is able to address complex spatial connections superior to those that standard neural systems can address.

17.4.1.6 Capsule Architecture

Input Layer:
Raw pixel data or feature representations are received by the input layer. After this, the input data is fed into the network.

Convolutional Layer:
A convolutional layer processes the input data to extract basic features. This layer applies convolutional filters to identify simple patterns like edges or textures.

Primary Capsules:
The primary capsules layer receives feature maps from the convolutional layer and forms the first level of capsules. Each primary capsule represents the presence and pose of a particular part or feature in the input image. These capsules perform encoding of instantiation parameters and spatial relationships.

Capsule Layer(s):
Subsequent capsule layers consist of higher-level capsules. These capsules hierarchically represent more complex visual entities by integrating information from primary capsules. They encapsulate higher-level attributes with increased abstraction.

Routing Mechanism:
Capsule layers use dynamic routing to establish connections and compute relationships between capsules. This process iteratively refines connections between lower-level capsules and their related higher-level capsules based on agreement scores. This allows improvement of the model predicting accuracy.

Pose Matrix Calculation:
Capsules within the network compute pose matrices. This calculation encodes the information to spatial transformations. This transformation includes translation, rotation, and scale, for each identified entity or feature.

Digit Capsules:
The final layer comprises digit capsules responsible for recognizing and representing entire objects or entities. These capsules consolidate high-level features and pose information from lower-level capsules, producing output capsules that predict the presence and properties of specific entities in the input data.

Loss and Reconstruction:
Capsule Networks incorporate loss functions and reconstruction mechanisms. The loss function helps train the network, encouraging accurate predictions, while reconstruction aids in enhancing robustness by reconstructing the input data based on the learned representations.

Dynamic Routing by Agreement (Iteration):
Capsules iteratively refine their predictions through routing by agreement. This iterative process enhances agreement between capsules. This dynamic routing involves proper assigning of weights to the layers in order to reach a highest accuracy.

Each layer in the Capsule Network architecture plays a distinct role, from feature extraction to hierarchical representation, dynamic routing, and iterative refinement, ultimately enabling the network to understand spatial hierarchies, pose information, and complex relationships within the input data. The pseudocode for proposed GAN model is given below

Define GAN Components

```
generator = generator_library.create_generator_model()  # Creates the gener-
ator model
discriminator = discriminator_library.create_discriminator_model()  # Creates
the discriminator model
# Define optimizer and compile models
generator_optimizer = lion_optimizer_library.LionOptimizer()  # Initialize
Lion Optimization Algorithm for generator
discriminator_optimizer = lion_optimizer_library.LionOptimizer()  # Initialize
Lion Optimization Algorithm for discriminator
generator.compile(optimizer=generator_optimizer, loss='binary_
crossentropy')  # Compile generator
discriminator.compile(optimizer=discriminator_optimizer, loss='binary_
crossentropy', metrics=['accuracy'])  # Compile discriminator
# Training Loop
for epoch in range(num_epochs):
    # Sample real signals from the dataset
    real_signals = dataset_library.get_real_signals_batch(batch_size)  # Get
batch of real signals
    # Generate synthetic signals from noise using the generator
    noise = generator_library.generate_noise(batch_size)  # Generate noise
    generated_signals = generator.predict(noise)  # Generate signals from noise
    # Create labels for real and generated signals
    real_labels = np.ones((batch_size, 1))  # Labels for real signals
    generated_labels = np.zeros((batch_size, 1))  # Labels for generated signals
    # Train the discriminator
    discriminator_loss_real = discriminator.train_on_batch(real_signals, real_
labels)  # Train on real signals
```

```
discriminator_loss_generated = discriminator.train_on_batch(generated_
signals, generated_labels)  # Train on generated signals
    # Combine generator and discriminator for end-to-end GAN training
    noise = generator_library.generate_noise(batch_size)  # Generate
new noise
    misleading_labels = np.ones((batch_size, 1))  # Misleading labels to fool
the discriminator
    # Update the generator through GAN training
    gan_loss = gan.train_on_batch(noise, misleading_labels)  # GAN training
combining generator and discriminator
    # Display training progress (e.g., loss values, accuracy)
    print(f'Epoch: {epoch}, D Loss Real: {discriminator_loss_real}, D Loss
Generated: {discriminator_loss_generated}, GAN Loss: {gan_loss}')
# End of Training Loop
```

17.4.2 Parameter Tuning

In GAN, parameters are fundamental elements determining the model's architecture, training process, and ultimately, the quality of generated outputs. These parameters include network architectures (generator and discriminator), learning rates, batch sizes, and activation functions. The psudo code for proposed tuning is given below:

```
# Initialize GAN parameters
initialize_GAN_parameters()
# Lion Optimization Algorithm (LOA) iterations
for iteration in range(max_iterations):
    # Hunting phase - Adapt GAN parameters based on opposition-based
learning (OBL)
    adapt_parameters_based_on_OBL()
    # Moving toward safe place - Adjust parameters for exploration diversity
    move_towards_safe_zones()
    # Roaming - Adaptive parameter tuning to escape poor solutions
    adaptively_roam_parameters()
    # Mating - Combine selected parameters for diversity and inheritance
    mate_parameters()
    # Defense - Optimize parameters based on successful strategies
    optimize_parameters_based_on_strategies()
    # Migration - Redistribute parameters to maintain diversity
    migrate_parameters()
# Final GAN parameter settings after LOA iterations
final_GAN_parameters = optimized_parameters()
```

The iterative LOA unfolds within this pseudocode to dynamically fine-tune the parameters of a GAN. Similar to how lions coordinate their strategies in the wild,

each iteration emulates specific behaviours. The 'Hunting' phase adapts GAN parameters based on opposition-based learning, while 'Moving toward safe zones' fosters exploration diversity. 'Roaming' allows adaptive tuning to avoid inadequate solutions, followed by 'Mating' to blend parameters for diversity. 'Defence' optimizes successful strategies, and 'Migration' redistributes parameters to maintain diversity. This orchestrated process mirrors nature's dynamics, systematically refining the GAN's parameter settings for enhanced performance in classifying stress-related physiological signals.

17.5 EXPERIMENTAL RESULTS

The proposed GAN model is coded in python 3.7. The dataset is collected from PhysioNet website (https://physionet.org/content/ephnogram/1.0.0/)[28]. This dataset prepared for electro-phono-cardiogram (EPHNOGRAM) protects for analysing stress signals. The EPHNOGRAM project was centred on devising affordable, low-power recording devices capable of capturing simultaneous ECG and phonocardiogram (PCG) data. These devices were equipped with additional channels to capture environmental audio, enabling potential enhancement of PCG quality through signal processing. The current dataset comprises recordings from 24 healthy adults aged between 23 and 29 years. It involved 30-minute stress-test sessions where participants engaged in resting, walking, running and biking activities using indoor fitness centre equipment. It offers an intricate relationship among the mechanical and electrical components during rest and various physical activities. The dataset is publicly accessible on PhysioNet, facilitating research and exploration in the field of cardiac signal analysis and cardiac health monitoring. The proposed model was analysed in terms of accuracy, F1-Score, precision and specificity rate with other models.

The Performance of proposed model is given in Table 17.1. The F1-Score comparison across various models in their classification capabilities. Among these models, the proposed GAN stands out prominently and achieving a remarkable F1-Score of 96. This indicates the model's exceptional ability to balance precision and recall and proves the superior accuracy in discerning between positive and negative instances within the dataset. In contrast, models like the Multi-Attention CNN and DenseNet perform commendably with F1-Scores of 92.92 and 90.38, respectively. The GAN

TABLE 17.1
Performance analysis

Models	F1-Score	Accuracy	Precision	Specificity
Support Vector Machine (SVM)	89.46	84.43	87.76	78.18
Multi attention CNN	92.92	89.76	92.13	85.39
DenseNet	90.38	86.32	89.06	79.87
GAN	94.76	94.84	95.2	92.47
Proposed GAN	96	95.8	96	94.8

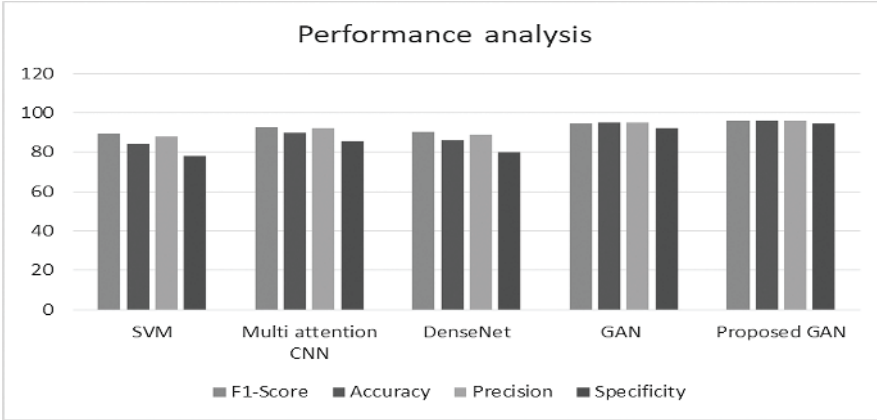

FIGURE 17.3 Performance analysis.

model also outperforms its foundational GAN counterpart and marks a substantial improvement in classification prowess. This notable performance enhancement with its high F1-Score underscores the efficacy and potential superiority of the proposed GAN in accurately categorizing and distinguishing between different classes within the dataset.

In analysis, the least performance was attained by the SVM model. This model achieved an accuracy of 84.43. The next best model is Multi attention CNN with the accuracy of 89.76. Then, the next best performance achieves by DenseNet. The model achieved the accuracy of 86.32. Then, the next model best perform in terms of accuracy is GAN.

From the results, the developed model shows the highest incremental percentage in terms of all the parameters. This model shows best suitability for all the dataset used in this work. Comparing the accuracy metrics, the proposed GAN demonstrates a notable improvement by achieving an accuracy of 95.8% compared to the existing model. This enhancement represents a substantial incremental gain of approximately 1.09%. The GAN architecture itself has proven to be effective with the high accuracy of 94.84%. However, the proposed GAN attains an even higher accuracy rate. The performance is graphically shown in Figure 17.3.

The confusion matrix of proposed model is shown in Figure 17.4. Among the 30 total normal samples, the model accurately identified 30 of them as normal (True Negatives), correctly identifying the absence of stress in these cases. However, the model misclassified 3 normal samples as stressed (False Positives), indicating instances where the model wrongly labelled normal samples as stressed. Notably, all 24 stressed samples were accurately identified as stressed (True Positives), demonstrating the model's proficiency in recognizing stress. Importantly, no stressed samples were erroneously classified as normal (False Negatives), which signifies the model's capability to avoid mislabelling stressed cases as normal. While the overall accuracy stands at 96%, examining the confusion matrix reveals specific instances of misclassification, particularly in the normal sample category, where a small proportion was inaccurately identified as stressed.

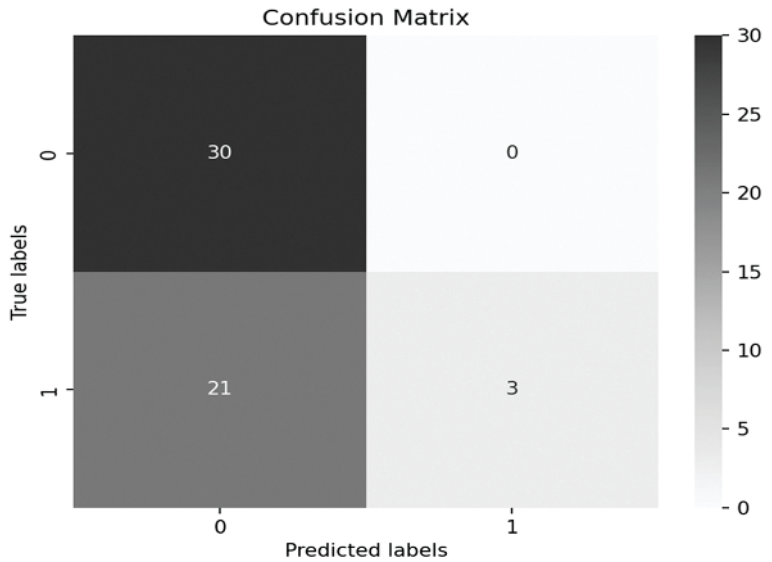

FIGURE 17.4 Confusion matrix.

FIGURE 17.5 Training and validation Loss Progress curve of GAN model.

The validation curve of model is shown in Figure 17.5 and Figure 17.6. Achieving a consistent 96% training and validation accuracy across epochs signifies a robust model that accurately learns and generalizes patterns from the data. This indicates the model's strong capacity to correctly classify instances, capturing intricate features during training. Such high accuracies imply the model's adeptness in making precise predictions not only on the training dataset but also on unseen validation data,

FIGURE 17.6 Training and validation accuracy progress curve of GAN model.

showcasing its capability to generalize well beyond the observed samples. This convergence of high accuracies suggests that the model has effectively learned essential patterns without over fitting, ensuring reliable performance on both seen and unseen data samples.

17.6 CONCLUSION

This work proposed a new approach to stress detection in healthcare by using a GAN model. The model proposes integrating capsule network-based deep transfer learning into the generator and leveraging DenseNet architecture in the discriminator. The integration different model is a GAN model achieves higher accuracy for stress signal detection. The generator's ability to create accurate stress-related physiological representations diversifies datasets and enhances detection precision. Simultaneously, the discriminator effectively distinguishes genuine stress signals from synthetic ones and boosts accuracy. The LOA model parameters efficiently alter the GAN's performance. Experimental results show that the proposed model exhibits state-of-the-art accuracy and resilience against challenges. This work not only fortifies stress detection capabilities but also ensures adaptability and efficiency. In future, the GAN model is integrated with a multi-attention mechanism to improve the accuracy.

REFERENCES

1. A. Dupre, S. Vincent and P. A. Iaizzo, "Basic ECG Theory, Recordings, and Interpretation," in: P. A. Iaizzo (Ed.), *Handbook of Cardiac Anatomy, Physiology, and Devices*, 2005, pp. 199–201.
2. P. Hubert, A. R. Pipberg and S. F. Arms, "Automatic screening of normal and abnormal electrocardiograms by means of a digital electronic computer," in *Proceedings of the Society for Experimental Biology and Medicine*, vol. 106, pp. 2–130, 1961.

3. F. Murat, O. Yildirim, M. Talo, U. B. Baloglu, Y. Demir and U. R. Acharya, "Application of deep learning techniques for heartbeats detection using ECG signals-analysis and review," *Computers in Biology and Medicine*, vol. 120, p. 103726, 2020.
4. S. Nurmaini, A. Darmawahyuni, A. Noviar, S. Mukti, M. Rachmatullah, F. Firdaus, et al., "Deep learning-based stacked denoising and autoencoder for ECG heartbeat classification," in *Electronics,* vol. 9, p. 135, 2020.
5. S. L. Oh, E. Y. K. Ng, R. S. Tan and U. R. Acharya, "Automated diagnosis of arrhythmia using combination of CNN and LSTM techniques with variable length heart beats," in *Computers in Biology and Medicine*, vol. 102, pp. 278–287, 2018.
6. S. Jayalakshmy and G. F. Sudha, "Respiratory Signal Classification by cGAN Augmented EMD-Scalograms," in *2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC),* Bhubaneswar, India, pp. 1–5, 2021. doi: 10.1109/AESPC52704.2021.9708484.
7. B. Liu, A. Cao and H. -S. Kim, "Unified Signal Compression Using Generative Adversarial Networks," in *ICASSP 2020 - 2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Barcelona, Spain, 2020, pp. 3177–3181, doi: 10.1109/ICASSP40776.2020.9053233.
8. S. Lee, Y. -I. Yoon and Y. J. Jung, "Generative adversarial network-based signal inpainting for automatic modulation classification," in *IEEE Access*, vol. 11, pp. 50431–50446, 2023, doi: 10.1109/ACCESS.2023.3279022.
9. Z. Tang, M. Tao, J. Su, Y. Gong, Y. Fan and T. Li, "Data Augmentation for Signal Modulation Classification using Generative Adverse Network," in *2021 IEEE 4th International Conference on Electronic Information and Communication Technology (ICEICT)*, Xi'an, China, 2021, pp. 450–453, doi: 10.1109/ICEICT53123.2021.9531296.
10. S. A. Kumar, M. K. Muchahari, S. Poonkuntran, L. S. Kumar, R. K. Dhanaraj, and P. Karthikeyan, "Application of hybrid capsule network model for malaria parasite detection on microscopic blood smear images," *Multimedia Tools and Applications*. 2024 Apr 19, pp. 1–27..
11. E. Adib, F. Afghah and J. J. Prevost, "Arrhythmia Classification Using CGAN-Augmented ECG Signals," in *2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, Las Vegas, NV, USA, 2022, pp. 1865–1872, doi: 10.1109/BIBM55620.2022.9995088.
12. S. Janbhasha, S. N. Bhavanam and K. Harshita, "GAN-Based Data Imbalance Techniques for ECG Synthesis to Enhance Classification Using Deep Learning Techniques and Evaluation," in *2023 Third International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 2023, pp. 1–8, doi: 10.1109/ICAECT57570.2023.10118167.
13. N. H. Trinh and D. O'Brien, "Semi-Supervised Learning with Generative Adversarial Networks for Pathological Speech Classification," in *2020 31st Irish Signals and Systems Conference (ISSC)*, Letterkenny, Ireland, 2020, pp. 1–5, doi: 10.1109/ISSC49989.2020.9180211.
14. S. Jang and Y. Kim, "Dual ResNet-based Environmental Sound Classification using GAN," in *2023 17th International Conference on Ubiquitous Information Management and Communication (IMCOM)*, Seoul, Republic of Korea, 2023, pp. 1–6, doi: 10.1109/IMCOM56909.2023.10035597.
15. T. K. Kuan and T. Huy Dat, "Embedding Physical Augmentation and Wavelet Scattering Transform to Generative Adversarial Networks for Audio Classification with Limited Training Resources," in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Brighton, UK, 2019, pp. 3262–3266, doi: 10.1109/ICASSP.2019.8683199.

16. Q. Zhang, J. Yang, X. Zhang and T. Cao, "Generating Adversarial Examples in Audio Classification with Generative Adversarial Network," in *2022 7th International Conference on Image, Vision and Computing (ICIVC)*, Xi'an, China, 2022, pp. 848–853, doi: 10.1109/ICIVC55077.2022.9886154.
17. X. Wang et al., "An ECG signal denoising method using conditional generative adversarial net," in *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 7, pp. 2929–2940, July 2022, doi: 10.1109/JBHI.2022.3169325.
18. Z. Zhang, J. Han, K. Qian, C. Janott, Y. Guo and B. Schuller, "Snore-GANs: Improving automatic snore sound classification with synthesized data," in *IEEE Journal of Biomedical and Health Informatics*, vol. 24, no. 1, pp. 300–310, Jan. 2020, doi: 10.1109/JBHI.2019.2907286.
19. L. Xia, Y. Feng, Z. Guo, J. Ding, Y. Li, Y. Li, M. Ma, G. Gan, Y. Xu, J. Luo, and Z. Shi, "MuLHiTA: A novel multiclass classification framework with multibranch LSTM and hierarchical temporal attention for early detection of mental stress," in *IEEE Transactions on Neural Networks and Learning Systems*, doi: 10.1109/TNNLS.2022.3159573.
20. M. Amin, K. Ullah, M. Asif, A. Waheed, S. U. Haq, M. Zareei and R. R. Biswa, "ECG-based driver's stress detection using deep transfer learning and fuzzy logic approaches," in *IEEE Access*, vol. 10, pp. 29788–29809, 2022, doi: 10.1109/ACCESS.2022.3158658.
21. S. T. Chandrasekaran, S. P. Bhanushali, I. Banerjee and A. Sanyal, "A bio-inspired reservoir-computer for real-time stress detection from ECG signal," in *IEEE Solid-State Circuits Letters*, vol. 3, pp. 290–293, 2020, doi: 10.1109/LSSC.2020.3016924.
22. S. Zheng, M. Murugappan and S. Yaacob, "FCM Clustering of Emotional Stress Using ECG Features," in *2013 International Conference on Communication and Signal Processing*, Melmaruvathur, India, 2013, pp. 305–309, doi: 10.1109/iccsp.2013.6577064.
23. Manimeghalai P, R. R. Chandran, S. Krishnan and S. Shiny, "ECG Based Stress Detection Using Machine Learning," in *2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 2022, pp. 1–5, doi: 10.1109/ICAECT54875.2022.9807877.
24. L. Vanitha and G. R. Suresh, "Hybrid SVM Classification Technique to Detect Mental Stress in Human Beings Using ECG Signals," in *2013 International Conference on Advanced Computing and Communication Systems*, Coimbatore, India, 2013, pp. 1–6, doi: 10.1109/ICACCS.2013.6938735.
25. M. Yazdani and F. Jolai. "Lion Optimization Algorithm (LOA): A nature-inspired metaheuristic algorithm," in *Journal of Computational Design and Engineering*, vol. 3, no. 1, pp. 24–36, 2016.
26. J. Ying, H. Qi and J. Wu. "Capsule network assisted electrocardiogram classification model for smart healthcare," in *Biocybernetics and Biomedical Engineering*, vol. 42, no. 2, pp. 543–555, 2022, ISSN 0208-5216.
27. S. Liu, H. Liu, C. Yang, S. Yang and M. Wang, "Separable attention capsule network for signal classification," in *IEEE Access*, vol. 8, pp. 181744–181750, 2020, doi: 10.1109/ACCESS.2020.3027855.
28. A. Goldberger, L. Amaral, L. Glass, J. Hausdorff, P.C. Ivanov, R. Mark, and H.E. Stanley. "PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals," *Circulation*, vol. 101, no. 23, pp. e215–e220, 2000.

Index