Intrusion Detection in IoMT based Smart Healthcare System (SHS) using Deep Learning techniques

MS Computer Sciences

Attiya Khan

F20MSCS003

Supervisor

Dr. Muhammad Rizwan

Co-Supervisor

Ms. Asma Basharat

Department of Computer Sciences

Kinnaird College for Women

Lahore, Pakistan.

2020-2022

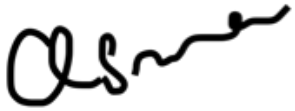
RESEARCH COMPLETION CERTIFICATE

It is certified that Ms. Attiya Khan of MS (session 2020 – 2022), Department of Computer Sciences, has carried out research work entitled **"Intrusion Detection in IoMT based Smart Healthcare System (SHS) using Deep Learning techniques"** under my supervision. All changes suggested by the examiners during defense are incorporated in this final copy.

It is assured that research work is original and has not yet been published anywhere else.

Signature of Supervisor Dated: June 23, 2022.

Designation: Assistant Professor



Signature of Co-supervisor

Designation: Lecturer

Signatures

Head of Department

ANTI-PLAGIARISM DECLARATION

I certify that this is my own research work. The work has not, in whole or in part, been presented elsewhere for assessment. Where material has been used from other sources, it has been properly acknowledged. The similarity index of the research report is 9%. If this statement is untrue and I am found guilty of plagiarism, the punitive actions against me should be taken as per Kinnaird Anti Plagiarism Policy.

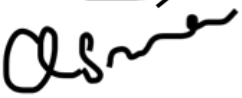
Name of the student: Attiya Khan

Registration No: F20MSCS003

Program: MS (Computer Sciences)

Signature:

Signature of Supervisor: 

Signature of Co-supervisor: 

Signature of HOD:

ACKNOWLEDGEMENT

We are truly grateful to Allah, the Almighty, the Most Generous and Merciful; all gratitude and glory go to Allah, on whom we rely primarily for guidance and support.

I gratefully acknowledge Dr. Muhammad Rizwan, Assistant Professor Kinnaird College for Women, Lahore, for his help and cooperation. Dr. Muhammad Rizwan's effort and cooperation were essential in completing this research. I am grateful to him for his encouragement and guidance in completing the research. I would also like to thank Ms. Asma Basharat, Lecturer Forman Christian University, Lahore, for her guidance and cooperation in completing this research. I would also like to thank my family and friends for their unwavering support, which provided me with the motivation to complete this research.

ABSTRACT

The Internet-of-Things (IoT) has infiltrated nearly every aspect of life. One of the most important areas where IoT solutions and infrastructures are used widely is smart healthcare system (SHS). IoT-based smart healthcare solutions have significantly increased the benefit of the healthcare sector with the use of mobile and wearable devices. Smart healthcare reduces hospitalization costs and provides timely treatment for a number of medical conditions by incorporating IoT sensors into health monitoring equipments. Today, the purpose of healthcare systems is not confined to treating patients only. In SHS, wearables, implantable devices, and sensors monitor the vital parameters of a patient. These parameters are sent for evaluation to the emergency services or healthcare professionals. This results in a significant usage of health data exchange for improved, timely, and more accurate diagnosis. Nevertheless, SHS are extremely prone to a variety of security breaches and malicious attacks, such as tampering, privacy leakage, and forgery. In the smart healthcare domain, it is essential to take a systematic approach to privacy and security measures in communication, data storage, interconnecting things, and data handling. In various studies, several intrusion detection systems (IDS) have been proposed to detect cyber security threats in SHS and to identify malicious attacks and privacy breaches. This study was conducted as a consequence of the limits of IDSs in responding to challenges and attacks and in implementing attacks and privacy access control in the SHSs. In this study, we designed a deep learning-based intrusion detection system to efficiently identify smart healthcare network intrusions by evaluating traffic flow data. We specifically used the “Long Short-Term Memory (LSTM)” technique to detect malicious attacks and other security threats in SHS. In this system, we utilized the CFS algorithm for feature selection. The objective is to select a subset of features having a high feature-class correlation in order to maintain or boost predictive power, and low feature-feature correlation to prevent redundancy. We evaluated the proposed system using Wustl-ehms-2020 IoMT dataset. The proposed system achieves accuracy of 96%, which is greater than existing

approaches. This study demonstrates that our approach outperforms other cutting-edge techniques for intrusion detection.

Contents

CHAPTER NO. 1

INTRODUCTION

1.1. Background Study

With the advancement of modern society, the internet technology is continuously maturing and it has deeply penetrated in the lives of people. Nowadays, as people's lifestyles, medical concepts, and health demands evolve, individuals from all areas of life are becoming more concerned about medical issues [1]. Unfortunately, the increase in chronic sickness and continually aging population is putting immense pressure on modern healthcare systems thus; there is a high demand for resources ranging from equipments to physicians and nurses [2]. The conventional healthcare systems are unable to meet everyone's demands due to massive rise in population. Healthcare services are not affordable or accessible to everyone despite having outstanding infrastructures or state-of-the-art technologies.

Today's age is one of digitization. In conventional healthcare monitoring systems, individuals rely heavily on medical equipments. Most of these equipments are quite heavy and costly, with complicated operation requirements, making them not suitable for everyday use. Therefore, people need more convenient and suitable service platforms in order to monitor and ensure their healthcare monitoring. As a result, smart healthcare monitoring emerges at the historical moment. To improve well-being of humans, universal healthcare is required. Nowadays, healthcare systems have evolved into intelligent systems as a result of remarkable advancements in data analytics, and they have become more widespread as a result of the fast IoT deployment [3].

The advancement of science and technology has begun to informationize the traditional medicine which has biotechnology at its foundation. In essence, healthcare systems and basic medical research are growing smarter [4]. Thus, smart healthcare has emerged, embracing a new wave of information technology.

Smart healthcare is more than just a technological improvement; it is a multi-level transformation. This transformation is incorporated into following areas: changes in medical model, changes in data characteristics, changes in the way of interaction, and changes in treatment concepts. These developments focus on meeting specific requirements of people while increasing healthcare efficiency, considerably improving the healthcare and medical experience, and representing modern medicine's future progress trajectory.

Smart healthcare originated from the IBM's (Armonk, NY, USA) notion of "Smart Planet" presented in 2009 [5]. Smart Planet is a sensor-based infrastructure that detects information using sensors, transmits it over internet of things (IoT), and uses cloud-computing to process it. It has the ability to coordinate and integrate social processes in order to achieve the dynamic human society management. Smart healthcare is a healthcare system that leverages technology such as sensor devices, IoT, and internet to obtain information, link people, materials, and healthcare institutions, and then intelligently manage and respond to medical environments' demands. The smart healthcare systems educate the users about their medical condition and keep them aware about their health. Smart healthcare allows people to handle various emergency circumstances on their own.

In addition, the adoption of ever-expanding IoT technology will reduce several inefficiencies present in healthcare systems [6]. In 1999, Kevin Ashton originally used the term "Internet of Things (IoT)", during his work for supply chain optimization [7]. The IoT links smart things to Internet. It can speed up data communication and deliver processed data to users in a more secure and reliable manner [8]. IoT transforms healthcare by substantially enhancing quality, and IoT will provide individuals with a smart healthcare system [9]. It focuses on increasing the user's quality of life and experience. Smart healthcare enables the most efficient use of available resources. It allows for remote patient monitoring and reduces the cost of treatment for the patient. It also enables medical professionals to expand their services across geographical boundaries. With the

trend toward smart cities on the rise, an effective and efficient smart healthcare system ensures a healthy lifestyle for its residents.

In general, smart healthcare involves any digital health solution that can function remotely, and it incorporates subclasses such as mobile health and telehealth, but with the addition of continuous health monitoring, detection of emergency situation, and automatic notification to appropriate person. Smart healthcare enables self-care and complements it with remote-care, hence improves the quality and effectiveness of healthcare. Smart healthcare can encourage interaction among all stakeholders in the healthcare industry, ensuring that participants receive the services they require, assisting parties in informed decision-making, and facilitating resource allocation. In a nutshell, smart healthcare represents a greater level of information building in the medical industry. Furthermore, these systems are capable enough to be directed by instructions such as commands and queries. The devices implanted on patient can collect the data needed on the instruction of physician [10].

"United Nations International Standard Industry Classification" classified healthcare as an industry which consists of medical and dental activities supervised by physicians, nurses, physiotherapists, and other health professionals [11]. Smart healthcare is built on the foundation of information technologies such as the IoT, edge computing, big data, 5G, artificial intelligence, machine learning, and biotechnology. These technologies are frequently employed in smart healthcare systems. Individual users can benefit from smart healthcare since it allows them to better control their own health. When needed, timely and suitable medical treatments can be accessible, and their content will be more customized. For research institutes, smart healthcare can decrease research time, reduce research cost, and enhance overall research efficiency. For hospitals and healthcare institutes, smart healthcare can lower costs, decrease staff pressure, establish a centralized management of healthcare data, and improve the medical experience of patient.

1.2. IoMT based Smart Healthcare System (SHS)

The healthcare business has rapidly evolved from a traditional hospital centered strategy to a patient centered one in recent decades, specifically in smart healthcare systems [12]. A large number of technologies, including the Internet-of-Medical-Things (IoMT), have enabled this rapid transition. IoMT, sometimes referred to as healthcare IoT, refers to the growing use of the Internet-of-Things (IoT) in the medical industry. The IoMT can be useful in developing a completely integrated healthcare environment [13]. It is a combination of healthcare equipments and software applications that link wirelessly to Health Information Systems (HIS). IoMT's services include remote patient monitoring for people with prolonged or chronic illnesses. Figure 1.1 depicts the framework of smart healthcare. As countless IoT devices serve multiple sectors, interconnected sensing technologies, such as wearable and standalone devices, are paving the way for a more hopeful future in health technology. IoMT refers to a wide range of IoT based applications and devices that are specifically built for healthcare environments and demands, such as tele-medicine consultation, remote patient monitoring, and wearable sensors.

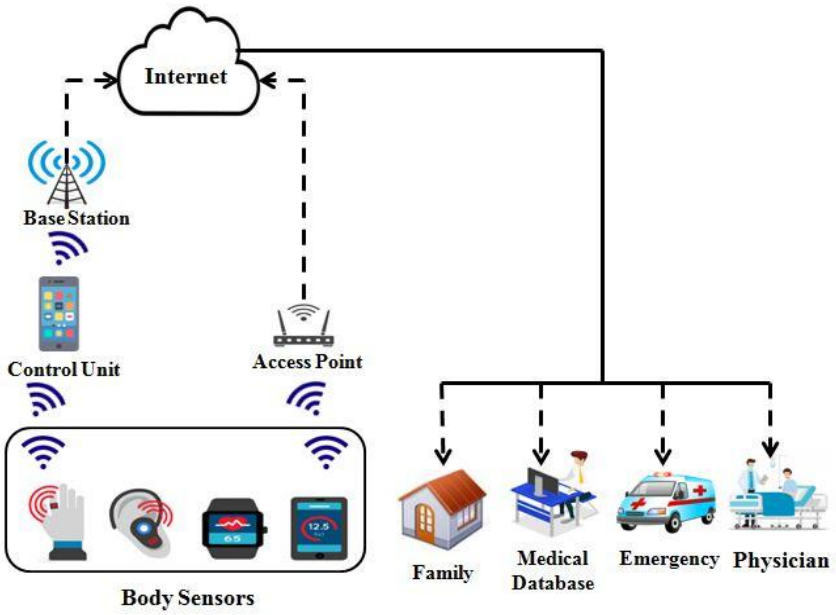


Figure 1.1: Structure of Smart Healthcare

IoMT can enhance patients' outcomes through real-time monitoring of patients' health, robot-assisted surgeries, and advanced diagnostics. IoMT services monitor patient's medicine prescriptions and the wearable healthcare devices, which may transmit each patient's medical information to their designated caregiver. These devices connect to open supply networks and interact with real world. This not only connects them universally, but also strengthens and comforts them. They can also keep track of patients' location admitted to different hospitals. Medical devices and equipments that can be implemented as IoMT technology include infusion pumps and hospital beds embedded with sensors that track vital signs of patients. These sensors then transmit the information to remote sites through M2M (machinery to machine), which includes computers, portable devices, and smartphones [14].

Smart healthcare enables individuals from various backgrounds such as physicians, nurses, and patients to gain access to right information and solutions, primarily to increase efficiency, reduce medical errors, and lower the cost in healthcare field [15]. Traditional healthcare employs manual ways of maintaining and managing patients' medicine data, anamnesis of patient, billing data, demographical data, and diagnosis information which increases the likelihood of human error and, as a result, negatively impacts patients. IoMT based smart healthcare systems eliminate human error and assists healthcare professionals in the accurate disease diagnosis through the interconnection of patient vital signs monitors with decision support systems through a network [16]. Moreover, big data analytics in healthcare domain along with cloud computing technology has enabled processing, storing, and managing of healthcare related data for complex decision-making [17]. Furthermore, the diagnosis can be automated, reducing or eliminating the need to see a doctor for basic ailments such as the flu and other more prevalent disorders [18].

According to a healthcare study report, around 80% of people over the age of 65 have at least one chronic ailment such as diabetes, arthritis, cancer, stroke, or heart disease [19]. According to the research report "IoT in Healthcare Market by

Component, Application, End User, and Region-Global Forecast to 2025", the IoMT sector is expected to be worth 188 billion dollars by 2025, up from 72.5 billion dollars in 2020. IoMT achieves its complete potential by employing "Smart" objects, which use various actuators and sensors to measure ready-to-understand information in their environment and interact with every possible alternative via integral network.

1.3. Applications of IoMT-based SHS

The main goal of IoMT-based SHS is to improve patients' well-being by reducing unpleasant hospital visits. The key component of an IoMT-based SHS is the IoMT edge network. It incorporates several IoMT-enabled devices that allow people to monitor their physical fitness and health status digitally [20]. For instance, fitness tracking gadgets such as smartwatches, fitness shoes, smart jackets, smart shorts, wearable health bands, and smart earbuds can collect, analyze, and transmit physical activity data of an individual to the smartphone application and this data can be seen by users via fitness tracking applications. Moreover, Smartphone applications make it easier to keep a medical case history with frequent warnings and emergency assistance. The applications of IoMT in smart healthcare are shown in Figure 1.2.

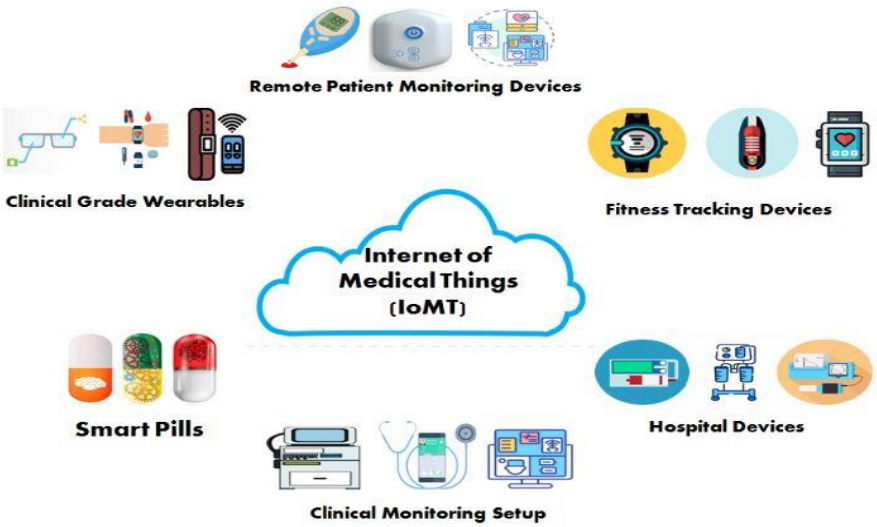


Figure 1.2: IoMT applications in Smart Healthcare

There are several types of IoMT devices that are used in the healthcare industry. Some of these categories include:

- Wearable devices such as biosensors and portable insulin syringes.
- Internal devices such as remotoscope, wireless capsule endoscope, and GLUCO-WISE.
- Smart wristbands such as Misfit, Fitbit Charge, Withings, Nabu Razer X, Jawbone UP3, and Healbe [21].
- Stationary devices such as heart rate monitors, pulse oximeters, and stroboscope.

One of the significant and vital application of IoMT based SHS is to monitor cardiac patients, which is accomplished via sensor devices. Data from ECG is used to monitor patients and it is sent to specialists for analysis [22]. Holter monitors take 24 hours to record continuous ECG data, and hence power comsumption is a constraint. IoMT based SHS provides minimal local processing and transmits data to cloud servers that help in resolving the drawback of holter monitors [23].

Each year, IoMT-based medical devices generate massive volumes of data. By 2025, the healthcare business is expected to generate 1,656 zettabytes (ZB) of data [24]. Useful and valuable insights can be obtained from this data to aid in efficient and effective decision-making. The retrieved data can be used by medical institutions and hospitals to integrate with their current Electronic Medical Records (EMR) for better healthcare monitoring, early illness identification, and timely treatment [25]. Aside from its numerous advantages, incorporating smart healthcare into different elements of the healthcare system has a number of negative consequences. This change broadens the attack surface, putting users' safety, privacy, and security at risk of cyberattacks [26]. Furthermore, the growing functionality of the SHS raises several security risks and the cyber attackers can exploit SHS in numerous ways: they can tamper vital signs by inserting fake data, obstruct the regular operation of the SHS, and tamper medical equipment in order

to change the outcome of a medical emergency. The consequences of vulnerabilities exploited in SHS can be life-threatening [27].

1.4. Security Attacks on IoMT-based SHS

Smart healthcare systems are vulnerable to attackers due of their wireless connection. There are several threats from cyberattackers that can be damaging to these systems [28]. These security risks include SQL injection, Ransomeware, Data Breaches, Router Attacks, Insider Threats, and Replay attacks. Some of the most significant cyber-incidents in healthcare domain are listed in Table 1.1.

Table 1.1: Major Cyber-Incidents in Healthcare Domain

Year	Healthcare Industry	Type	People Affected
2020	Trinity Health	Third-party vendor	3.32 million
2020	Inova Health System	Ransomware Attack	1 million
2020	Magellan Health	Ransomware Attack	1.7 million
2016	Banner Health	Malware	3.62 million
2015	Medical Informatics Engineering	Brute Force Attack	3.9 million
2015	Anthem, Inc	Phishing	79 million
2014	Community Health Systems	Malware	4.5 million
2014	Premera Blue Cross	Phishing	11 million

2013	Excellus Health Plan, Inc	Malware	10 million

Cyberattacks against healthcare devices have been extensively studied. Attacks against healthcare devices can be categorized as system attacks, which include Denial-of-service (DoS) attack and other attacks that corrupt the system's operation, or information attacks, which attempt to access or change confidential healthcare data [29]. "The International Criminal Police Organization (INTERPOL)" issued a report in April 2020 warning of a global rise in cyberattacks related to the COVID-19 pandemic [30]. On 13 March 2020, the Czech hospital, which housed one of the country's largest COVID-19 testing laboratories, was hit by a cyberattack, causing an immediate IT network shut down. As a result, major diagnostic delays occurred across the area that negatively impacted the patients. On 22 March 2020, Paris Hospital Authority APHP, France was hit by a cyberattack, in an attempt to disrupt hospital services in Paris by overwhelming their computers. According to the ANSSI, the APHP countered the attack successfully [31].

On 14 March 2021, the health department of Ireland was hit by Conti Ransomeware attack. As a result, several systems were severely disabled and majority of the department's other systems were forced to shut down. To limit the effect of attack, the healthcare department decided to shut down its IT system as a precaution. In 2020, the French press reported 27 serious cyberattacks on healthcare institutions. Most of these attacks were reported to be ransomeware attacks, with nearly one such attack occurring every week. The cyberattackers specifically target healthcare institutions because a successful ransomware poses a threat to public healthcare and the cyberattackers feel this will increase the likelihood of receiving a ransom amount to release healthcare data and systems. In January 2021, Spain's health industry suffered an average of 626 cyberattacks per week per organization, in comparison to 430 in last months of year 2020 [32]. According to the report of "The European Union Agency for Cybersecurity (ENISA)", the cyberattacks on healthcare industry of European Union increased

by approximately 50% in 2020 compared to the previous year, posing major threats to patients' safety as well as whole healthcare supply chain [33].

The ransomware attacks on the SHS slow down or entirely disable critical processes. This type of attack may leave medical devices inoperable, causing patient treatment to be delayed. DDoS attacks have the potential to overwhelm the system and network, rendering SHS inoperable, causing breakdown in communication between the hospital and the IoMT devices in a medical emergency situation [34]. In healthcare sector, a DDoS attack may prevent access to crucial services such as scheduling appointments, sharing information and bed capacity. In 2014, a hacktivist group convicted of conducting a major DDoS attack on "Boston Children's Hospital", which caused the hospital's network to be down for at least one week. The attack was conducted as retaliation because the hospital was involved in a controversial child custody dispute.

A man-in-the-middle (MitM) attack is a form of eavesdropping attack in which an attacker intercepts a conversation or data transmission in progress. The attackers place themselves in the middle of transfer, and pretend to be legitimate parties on both sides. In this way, the attacker intercepts the data and information from either side while also providing malicious links to both legitimate parties in a manner that may go undetected until very late. The flow of man-in-the-middle attack is shown in figure 1.3.

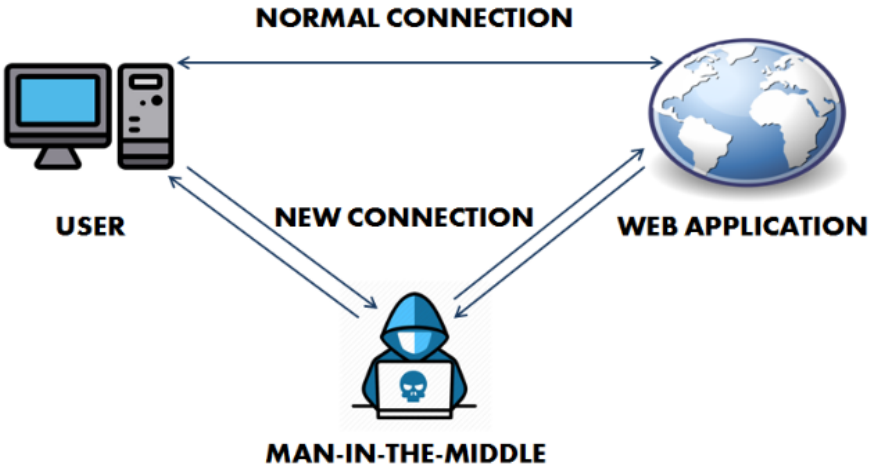


Figure 1.3: Man-in-the-middle Attack

According to the report of Swedish IT firm Specops Software, Man-in-the-Middle cyberattacks are the most common cybersecurity threat faced by the healthcare organizations. In man-in-the-middle attack on healthcare system, hackers put themselves between two communicating parties such as two healthcare professionals or a healthcare professional and patient. Similarly, the attackers can also accomplish this by interrupting communication between healthcare devices in same hospital. Once a cyberattacker has accomplished this, they can acquire, copy, or manipulate patient data, such as laboratory test results. Patient data is particularly sensitive as compared to other types of personal information, making it more beneficial to cybercriminals.

Data breaches are common in the smart healthcare domain. The most common causes of data breach in smart healthcare are credential-stealing malware, back doors, and insider threat. Over the last few years, there has been an increase in the number of data breaches in healthcare sector. Since 2009, there have been over 2100 reports of medical data breaches in the United States. According to "US healthcare data breaches statistics", 599 data breaches were recorded in 2020. Over 26 million medical records were impacted by these data breaches, with 92% of them being compromised [35]. On illegal market, Protected Health Information (PHI) is more valuable than Personal-Identification Information (PII)

or the credit card information. As a result, cyberattackers are strongly motivated to target healthcare systems' databases.

In an insider threat or attack, the intruder may pose a threat to privacy and security of SHS. The attacker may sell data for a profit or alter medical records as a form of retaliation. Insider threats account for nearly 48% of all breaches in the healthcare sector. In phishing attacks, the attackers send the hospital employees a fraudulent message or an authentic-looking email with an attachment or a link. The content is activated when an unaware user opens or clicks on this link or attachment. As a result, the hacker gains network access and can use it to spread a virus or obtain information. Lateral phishing attack can be used by cyberattackers to steal intellectual property (IP) on research and pharmaceuticals valued billions of dollars. Various security threats to IoMT based SHS are shown in figure 1.4.

In terms of cybersecurity, the healthcare industry is among the most vulnerable sectors. Cyberattacks on the smart healthcare industry can be disastrous if patient health records are manipulated or leaked. The healthcare sector, particularly nursing homes, has long been a prime target for cyberattackers [36]. Similarly, a loss of connectivity between healthcare centre and the IoMT devices as a consequence of cyberattack can result in patient treatment delays or the patient's death. Aside from compromising patient safety, these threats can obstruct brand reputation, income generation, and business continuity [37].The data being created and processed by the IoMT enabled medical devices is of extremely sensitive nature thus, the connectivity between medical devices must be secure and available at all times. Furthermore, data availability, integrity, and confidentiality are crucial for the sharing of medical data in smart healthcare systems and networks [38].

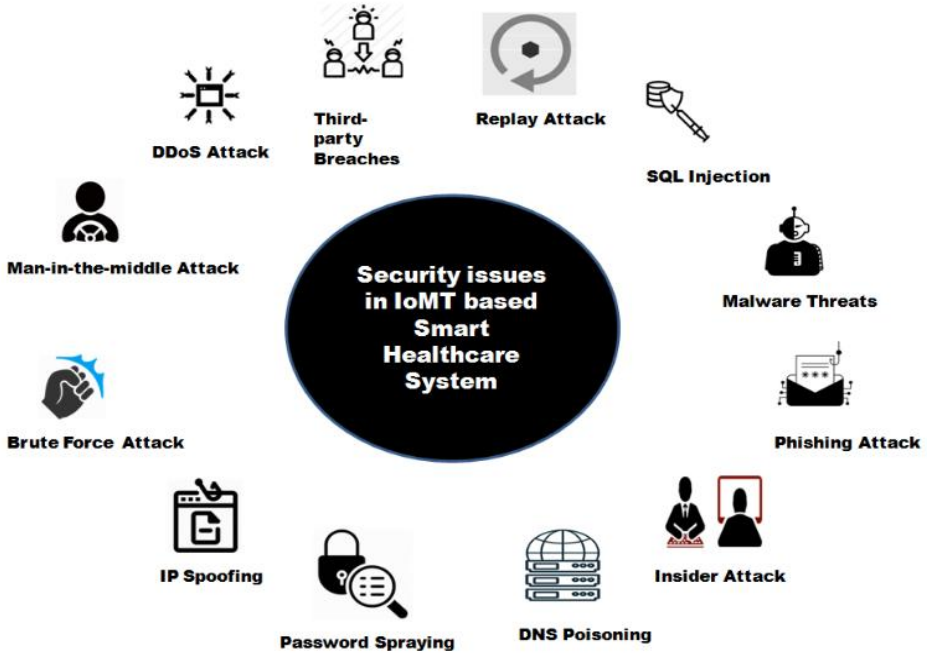


Figure 1.4: Security issues in IoMT based SHS

1.5. Deep Learning

Artificial intelligence (AI) and machine learning (ML) are the foundations of the next computer revolution. These technologies have the potential to recognize patterns and forecast future outcomes on the basis of data gathered in the past. Although AI-based machines are commonly referred to as "Smart", the majority of these machines do not learn all alone; human interaction is required. Data scientists pick the factors to be utilised in predictive analytics and prepare the inputs. On the contrary, deep learning is capable of performing this task automatically. Deep learning automatically identifies useful features in images, and that's the reason computer vision is much better now compared to five years ago [39]. Deep learning is allowing revolution and innovation in all facets of modern life [40].

Deep learning (DL) is considered as a subclass of machine learning. This particular field is built on self-learning and improvement through the examination of computer algorithms. Deep learning employs artificial neural networks (ANN),

to imitate the thinking and learning processes of humans, as opposed to machine learning, which uses simpler principles and concepts. Until recently, the complexity of neural networks was constrained by computing power. However, advances in Big Data analytics techniques have enabled larger, more powerful neural networks, enabling computers to monitor, understand, and respond to complicated situations quicker than people. Deep learning helps in language translations, image processing, and speech recognition. It is capable of solving pattern recognition problems without the need for human interaction.

Deep learning is driven by artificial neural networks with several layers. Deep Neural Networks (DNN) are networks with several layers that can execute complicated operations like abstraction and representation to make sense of audio, text, video, and images. Deep learning, often regarded as the fastest-growing subject in machine learning, is a really innovative digital technology that is being employed by an increasing number of businesses to develop new business models.

Deep learning models are often called “deep neural networks” because the majority of the deep learning approaches employ neural network architecture. Deep neural networks are based on trial and error, so they require a large quantity of data to train on. Nodes within particular layers are linked to nodes in adjacent layers. The deep neural network is made up of three different types of layers i.e. input layer, hidden layers, and output layer. Deep neural networks can have up to 150 hidden layers, whereas traditional neural networks have only 2 or 3 hidden layers. The schematic representation of deep neural network with two hidden layers is depicted in figure 1.5.

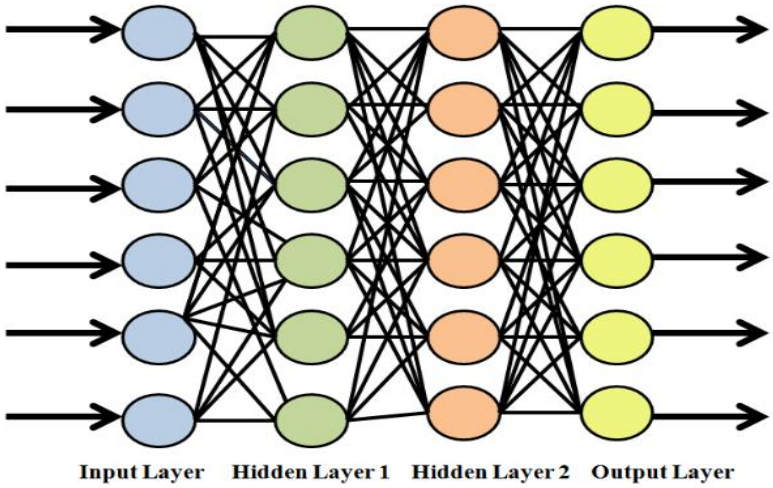


Figure 1.5: Deep Neural Network with two hidden layers

In deep neural network, the input layer accepts input signal. The input signals pass between hidden layers and weights are assigned. The hidden layers execute mathematical calculations on the inputs. A node with a higher weight has a greater impact on the next layer nodes. The weighted inputs are compiled in the last layer to generate an output. The output layer is responsible for performing tasks like classification and prediction. Iterations are repeated until the result is accurate enough to be useful. Deep learning systems need strong hardware since they handle a large quantity of data and include multiple complex mathematical computations.

Various artificial intelligence-based classification techniques and intrusion detection frameworks have been researched in the literature. The majority of the security frameworks designed to protect SHS have a high false positive rate. They are also unable to identify unknown network attacks. Hence, they are ineffective in protecting SHS from network attacks and other security threats, which result in damage to smart healthcare devices, medical identity theft, and loss of sensitive patient information. Thus, we employ deep learning algorithms in our framework to effectively identify malicious attacks, abnormal behaviour, and network intrusion in the smart healthcare systems.

The coming sections will give further details and more information about this study. Chapter 2 presents the problem statement and objectives of our study. Chapter 3 presents the literature review for the smart healthcare system in which the work of different authors to secure SHS is discussed in detail. Chapter 4 presents the main idea and proposed methodology for research work in detail. In chapter 5, the analysis and discussion on results of the proposed model is given. Chapter 6 concludes the entire work.

CHAPTER NO. 2

PROBLEM STATEMENT AND OBJECTIVES

2.1. Problem Statement

Most of the data privacy issues and security breaches are reported in healthcare industry [41]. There are numerous machine learning algorithms embedded in smart healthcare devices, but the majority of them are heavy-weighted [42]. The majority of the security frameworks designed to protect SHS have a high false positive rate. They are also unable to identify unknown network attacks. Hence, they are ineffective in protecting SHS from network attacks and other security threats, which result in damage to smart healthcare devices, medical identity theft, and loss of sensitive patient information.

Modern healthcare systems necessitate collaboration among hospitals, research institutes, and federal agencies. Moreover, improved cooperation among healthcare professionals increase the likelihood that patients will be able to access improved specialized treatment in their home country. Deep learning enables this collaboration since it protects privacy. Furthermore, the SHS employ IoMT technology, which executes operations in real time, resulting in a high volume of data production. These systems are now exposed to network and other malicious attacks because of internet connectivity [43]. As a result, the authenticity and legitimacy of data cannot be guaranteed. Furthermore, existing intrusion detection systems (IDS) have a very low accuracy rate [44]. As a result, maintaining the security and privacy in smart healthcare networks and devices with a better accuracy rate is a critical problem that must be addressed if SHS security is to be improved. Hence, we apply deep learning algorithms in our framework to efficiently detect network intrusion, cybersecurity threats, and identify anomalous behaviour in SHS. In order to increase the security of SHS, this manuscript provides an intrusion detection system based on deep learning techniques.

2.2. Research Objectives

Artificial Intelligence (AI) and Machine Learning (ML) are two extraordinary breakthroughs in computer sciences but, they still contain issues and challenges today. In healthcare domain, the majority of hospitals employ AI and ML techniques to function efficiently. Various AI and ML based classification techniques and intrusion detection frameworks have been researched in the literature. Existing AI and ML based healthcare systems face issues like prescription mistakes, data classification errors, data availability, sensitive data breaches, professional realignment, term and conditions, privacy regulations and many more. Therefore, adequate security measures must be implemented to secure healthcare systems and infrastructure, as well as to preserve the privacy of confidential healthcare data.

The following research questions are the basis for the proposed study:

- What are the security issues and challenges that smart healthcare systems face in terms of performance?
- What information must be secured to ensure the integrity and confidentiality of smart healthcare system?
- What classification approaches are needed to efficiently classify patient health record or big data?
- What security mechanisms and algorithms are necessary to protect medical data servers in IoMT environment?

The primary goal of this study is to secure smart healthcare networks and devices from cybersecurity threats and malicious attacks. For this purpose, an intrusion detection framework based on deep learning algorithms is developed to efficiently identify intrusion in smart healthcare systems by traffic flow analysis. In this framework, the data is classified using the most up-to-date DL-based classification approach, which must be feasible to use in the real time scenarios.

On the basis of the problem statement, the aim of current research is to provide such techniques that can improve the accuracy rate of data classification as well as increase security by implementing a DL-based framework. The deep learning paradigm has a significant influence on healthcare systems. Deep learning's application in medicine is new and hasn't been thoroughly investigated. Deep learning enables the healthcare sector to analyze medical data at exceptionally high speed while maintaining accuracy. Healthcare is a complicated, high-risk, and sensitive process. A better deep learning technique is employed to secure Patient-Health Record (PHR) and sensitive healthcare data. The research provides classification of SHS network data with the goal of avoiding security threats by putting deep learning algorithms and classification tools into practise. The DL-based SHS helps to improve the quality of healthcare by avoiding cybersecurity risks and preserving data privacy. This study will make a significant contribution to smart healthcare security and performance. The following are the goals that must be met as a result of this research:

- In this research, we propose an intrusion detection framework based on long short-term memory (LSTM) deep learning algorithm to detect malicious traffic data in smart healthcare environment. We use CFS algorithm for efficiently selecting the most relevant features for our framework.
- The main goal of this study is to secure smart healthcare networks and devices from cyberattacks and other cybersecurity threats. To achieve this, we analyze several cyberattacks including man-in-the-middle attacks, like spoofing attack, data injection etc.
- The proposed framework helps to maintain the confidentiality, integrity, and availability of smart healthcare environments.
- The framework is evaluated using state-of-the-art Wustl-ehms-2020 IoMT-based dataset which contains real-time IoMT traffic data.

These goals are to be achieved with the proposed study. After completing the training process, the system will become smarter, allowing for more efficient

decision-making. Moreover, patients, physicians, pharmacists, researchers, and laboratories will have easier access to healthcare systems. It will also improve data privacy and security, which is the most important aspect. It enables the training model to work on different datasets, after which the model sends the dataset to the trained data servers with a single final model output. This process will continue to iterate in order to get a greater accuracy rate. It will also improve data privacy and security, which is the most important aspect. Deep learning helps in more accurate traffic analysis, fewer false alarms, and assists security teams in distinguishing between malicious and normal network activity. This process will continue to iterate in order to get a greater accuracy rate. Moreover, DL-based algorithms can detect abnormal activity that may signal the existence of malicious actor or malware. This is extremely effective in dealing with many cybersecurity threats, such as DoS/DDoS attacks and SQL injections.

CHAPTER NO. 3

LITERATURE REVIEW

In this section, a literature study is conducted to shed light on various researchers' attempts to improve the security of IoMT-based SHS. Several researches have been carried out to investigate security threats and vulnerabilities in SHS. Here, we will present some of the currently existing schemes to address security in areas such as healthcare device security, patient data security, secure communication among healthcare devices, and healthcare network security. Figure 3.1 depicts the taxonomy of IoMT-based SHS security solutions.

3.1. Threat and Network Intrusion Detection Models

Iwendi et al. [45] proposed an intrusion detection system based on machine learning using a genetic algorithm (GA) and Random Forest (RF) to achieve an improved detection rate and lower false positive rate. An RF-based fitness function is proposed which selects the subset of optimal features. Initially, the datasets i.e. CSE-CIC-IDS2018 and NSL-KDD are preprocessed and all of their features are passed into the GA fitness function. The RF entropy function is used in the GA fitness algorithm to compute the fitness values. The selected optimal features are passed into RF algorithm to predict network intrusion. The newly developed approach has the ability to employ Random Forest within a genetic algorithm.

Gupta et al. [46] proposed anomaly detection (AD) model based on federated learning (FL) that uses edge cloudlets to locally run anomaly detection model without the need to share patient data in smart healthcare environment. The authors also identified certain potential risks in centralized AD models. In this research, a hierarchical FL is introduced for aggregation at various levels, allowing for multi-party collaboration. Furthermore, a new disease-based grouping technique is introduced in which distinct AD models are categorized based on certain types of diseases. A privacy-preserving AD scheme is developed

using “Federated Time Distributed (FEDTIMEDIS) Long Short-Term Memory (LSTM)” approach to mitigate security threats in smart healthcare field.

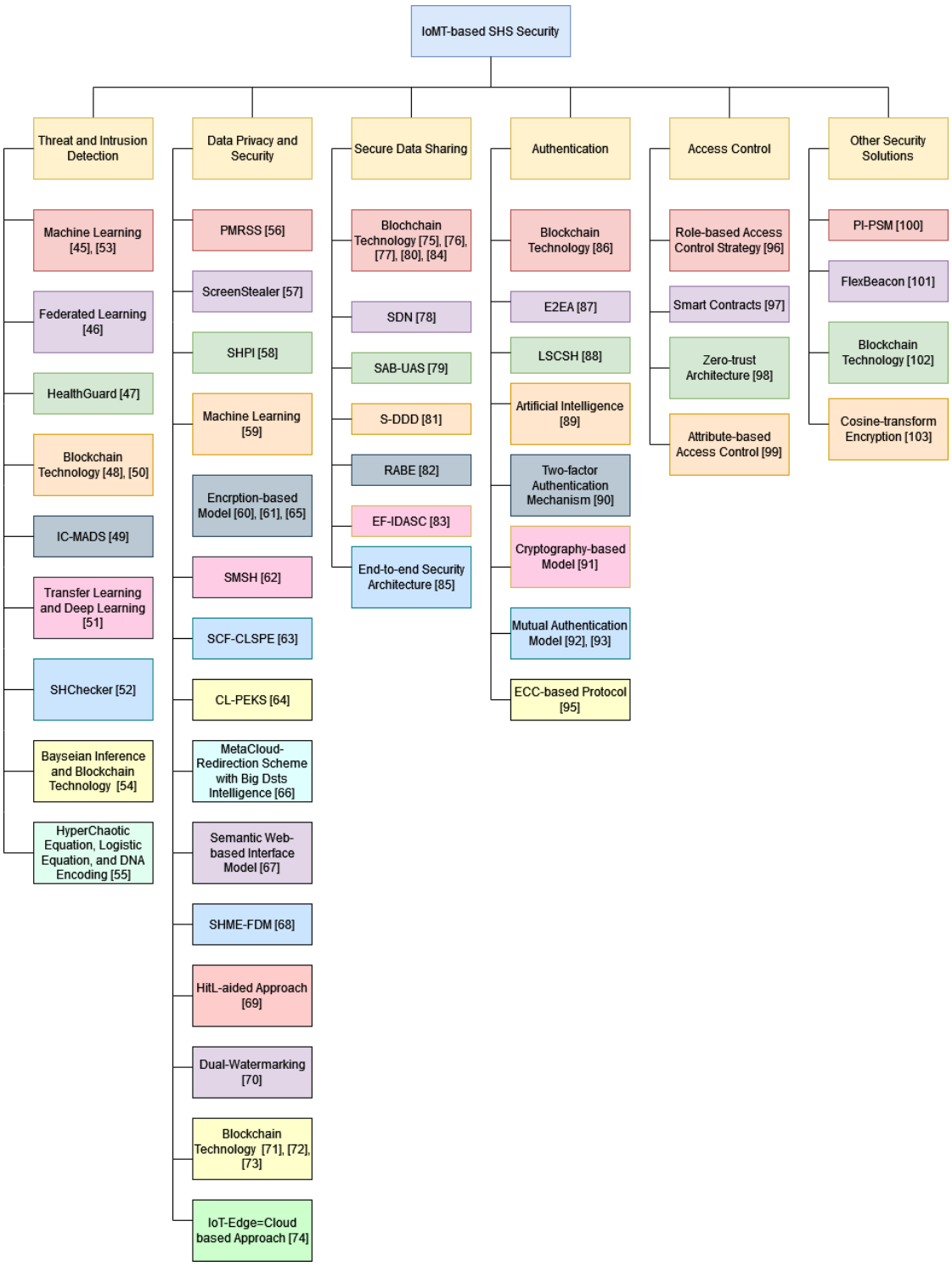


Figure 3.1: Taxonomy of IoMT-based SHS Security Solutions.

Newaz et al. [47] proposed “HealthGuard,” a security framework based on machine learning techniques to identify malicious activity in smart healthcare systems. HealthGuard performs vital signs monitoring of different healthcare devices and finds correlation between the vital signs to comprehend the patient’s biological functions to distinguish malicious and normal activities. To identify malicious activity in a SHS, HealthGuard employs four distinct machine learning-based detection approaches i.e. Decision Trees, Artificial Neural Network, k-Nearest Neighbor, and Random Forest. The proposed model is trained using data from eight distinct smart healthcare devices for twelve benign activities, comprising five disease-infected and seven normal user events.

Yang et al. [48] proposed a privacy-preserving framework for data transmission that supports malicious users detection and safe ciphertext conversion. The proposed framework is based on blockchain technology and oblivious transfer for secure transmission of medical data. In this study, a new protocol is specifically designed to ensure the two-way privacy protection of communication participants. Moreover, the authors used proxy re-encryption technique to provide safe ciphertext conversion and maintain data confidentiality in a many-to-many communication process. If the data is distributed across numerous servers and a doctor wants data, he must use a large number of server private keys to decrypt the ciphertexts. As a result, the privacy of data-storage servers will be compromised. Using this new protocol, a doctor may decipher all ciphertexts using only his own key. This protocol swiftly queries data and protects servers' and doctors' privacy. Furthermore, a protocol is presented that uses the blockchain technology to avoid data tampering and efficiently detect malicious users.

Kore and Patil [49] proposed an innovative and lightweight security system namely IC-MADS based on cross-layer trust computing technique for effectively detecting the man-in-the-middle attack with lesser communication cost as compared to previous approaches. The proposed IC-MADS architecture is described in two phases, including clustering and cross-layer attacks detection with a comprehensive range of parameters. The clustering technique presented for

selection of optimum Cluster-Head (CH) employs a probability calculation and evaluation technique. The probability of each sensor node is calculated using parameters such as residual energy, node degree, and distance from the base station. The node with the highest probability value is designated as the CH. This resolves the issues of load balancing and energy imbalance problems. To detect man-in-the-middle attacks in the network, the cross-layer trust computing technique included node evaluation. Each node's trust evaluation is carried out by utilizing the sensor node's parameters across various layers such as MAC, network, and physical layers. Lastly, each sensor node's aggregate trust value is compared to the threshold value in order to determine if it is an attacker.

Al-Shammari et al. [50] proposed a scheme and prototype to provide secured blockchain-based smart healthcare application processing. The proposed approach was discussed in terms of different highlights and issues about the design and development of an IoMT framework and its corresponding intrusion detection. The paper also focused on the numerous algorithmic techniques utilized in optimising IoT and IoMT-based devices in the cloud environment. The current study also describes how the IoMT protocol may be improved in terms of the validating methodologies of intrusion detection system automation. Moreover, the authors presented a standard protocol for reflecting and maintaining the IoMT operational standards, as well as its major functionalities when dealing with intrusion detection utilizing a blockchain method. For data extraction tampering and intrusion detection in an IoT context, the proposed approach employs an improved Crow search algorithm. Various types of attacks and intrusion detection were found, detected, calibrated, investigated, and reported. Deep CNNs are used to process the technique for data security element coordination and comparative analysis.

Selvakkumar et al. [51] discussed the several types of adversarial attacks in this research, as well as their impact on the SHS. The authors proposed a method for detecting adversarial attacks in order to identify security vulnerabilities in SHS. The method takes into account the attacks throughout the training phase and

testing phase and demonstrates how it can possibly misdirect the system. The medical imaging dataset is used to test the proposed model. The model showed a high level of accuracy in classifying images. The model is then attacked using a white-box attack, i.e., the FGSM attack, to cause it to predict the medical images and classify them incorrectly. Transfer learning is used to train a VGG-19 model to accurately classify the medical images using the dataset. Furthermore, the FGSM is implemented to the CNN to investigate the major influence it has on the machine learning model's accuracy and performance. The authors evaluated the proposed attack on the system using a confusion matrix and a classification report of the test data.

Haque et al. [52] proposed SHChecker, an innovative threat analysis scheme that combines formal analytic skills and machine learning to identify possible attacks and their consequences on an IoMT-enabled SHS. The tool can evaluate possible threats that meet the attacker's objectives. Machine learning is employed to comprehend how sensor data, health status, and consistency are related. This information is used to conduct formal analysis in order to synthesize possible attacks for a specific attack model, in which the attacker can alter the actual health status to a wrong state. Using different ML techniques, a real-time SHS is simulated by utilizing disease classification model and a corresponding anomaly detection model. The proposed system provides all possible attack vectors, where each vector represents a group of sensor readings to be adjusted, for a SHS given a certain set of attack characteristics, enabling the realization of the system's resilience and hence the insight to improve the model's robustness. The authors implemented SHChecker on both a real and a synthetic dataset, proving that the system can detect possible threat vectors in an IoMT-enabled SHS.

Hussain et al. [53] proposed a platform for designing context-aware IoT security solution to identify malicious activity in IoT scenarios, particularly in the IoT healthcare setting. The proposed scheme is comprised of IoT-Flock, a newly developed open-source IoT data generating tool. According to the authors, IoT-Flock is the first open-source IoT traffic generation tool. The IoT-Flock tool

enables researchers to create an IoT use-case composed of both malicious and normal IoT devices, as well as generate traffic. Previously, no IoT traffic generation tool has been able to generate malicious IoT traffic. In addition, the proposed system includes an open-source application for turning IoT-Flock recorded traffic into a dataset. Using this approach, the authors first created an IoT healthcare dataset that includes both IoT attack and normal traffic. Following that, six machine learning algorithms, i.e., Random Forest, Naïve Bayes, Adaboost, K-Nearest Neighbors, Decision Tree, and Logistic Regression, are applied to the obtained dataset in order to detect cyberattacks and safeguard the healthcare system against cyberattacks.

Farhin et al. [54] proposed a heterogeneous multi-layered IoHT structure and also discusses potential vulnerabilities. The study provides a one-of-a-kind security approach to protect the healthcare network's end-to-end safety and confidentiality from various types of threats and attacks. A two-layer security system is provided to assure overall security, which combines bayesian inference-based trust management and blockchain technology that protects individual nodes and data. The proposed system is comprised of three modules: first, the IoHT module, which covers the five-layer framework; second, vulnerabilities and attacks in the relevant layers; and third, distributed security module examining the inner-workings of recommended safety measures. In the proposed system, data generated by different devices and sensors in healthcare must go across the underlying layer before being stored or analyzed. Furthermore, behavioral profiling is used to determine the physical device's trustworthiness, and the data packets are then saved in blocks if the node is reliable. The evaluation results demonstrate the feasibility and usefulness of the proposed technique for detecting malicious nodes.

Sarosh et al. [55] proposed enhanced security architecture based on the hyperchaotic equation, logistic equation, and DNA encoding. The medical images of COVID-19 patients, such as CT-Scans and X-Rays, are encrypted using a chaos-based encryption algorithm. The image bits are globally shuffled using the

hyperchaotic system, and the resultant sequence is encrypted using the logistic equation and DNA encryption. After that, the encrypted image is converted into shares using the CSIS approach for storage in cloud servers. The system creates entirely noise-like images while retaining the CSIS scheme's threshold property. According to the authors, both medical and natural images can be secured against differential and statistical attacks using the proposed system. Moreover, it is ideally suited for an IoT-enabled SHS since it decreases the need for resources such as transmission bandwidth and storage space. This security system guarantees that the IoT-based SHS offers timely access to high-quality care through the secure and reliable transfer of healthcare data.

3.2. Data Privacy and Security

SUN et al. [56] developed a "Privacy-Preserving Medical Record Searching Scheme (PMRSS)" based on the ELGamal bling signatures. In this model, by blinding the patient's healthy data and iDoctor's database, the patient can reach a secure self-aided clinical diagnosis by accessing a previous case database and safely comparing blindfolded current data abstracts with past records. Furthermore, the patient can intelligently acquire target searching information simultaneously as he learns whether or not the abstracts match, rather than acquiring it after matching. Moreover, bilateral security is attainable in proposed scheme. Regardless of whether or not the abstracts match, the confidentiality of both the iDoctor database and current patients' information is ensured. In addition, it resists various levels of brutal ergodic attacks by altering the amount of zeros in bit-string to meet various security needs.

In [57], the authors investigate threats and risks to sensitive user data on smartphones, as well as how malicious applications like screenshot attacks can impact user privacy and system resources. The study also investigates the capabilities of Android Debug Bridge and how ADB and internet access work together to allow applications to reveal sensitive data on an Android-based smartphone. Furthermore, the authors also developed a malicious application

called “ScreenStealer” and evaluated its affects on Android smartphone. This application has been created to comprehend the threats and risks of an application that monitors smartphone screen and records front-end user activity, then secretly captures screenshots and sends them to the opponent. Moreover, the study also includes the analysis of outcomes after the application has been successfully uploaded to the “Google Play Store”.

Egala et al. [58] proposed a state-of-the-art architecture called “Smart Healthcare System for Patients in ICU (SHPI)” that uses blockchain technology to improve IoT privacy and security for healthcare applications. The proposed architecture combines edge computing, IoT, cloud computing, and blockchain to provide transparency, privacy, security, and decentralization of patient health data in the healthcare sector. To decrease communication latency, sensitive patient data is handled through edge computing situated within the hospital. SHPI employs blockchain and cryptographic techniques to guarantee data confidentiality and tamper-proof health records. In addition, a system using access tokens is implemented to provide confidentiality and privacy.

Ghoneim et al. [59] proposed a novel scheme to detect image forgery for smart healthcare framework to ensure that medical-related images are not altered or modified. In the proposed scheme, a Wiener-filter is used to extract a noise pattern from the color or monochrome image. The image's estimated noise pattern is obtained by subtracting the noise-free image from the actual image. The multiresolution regression filter is used on the noise pattern to discover a correlation between pixels. The filter's output is passed into two classifiers i.e. ELM classifier and SVM classifier. The authors examined several SVM kernels: RBF, linear, and polynomial. The BSR is used to fuse the ELM and SVM scores, and the BSR score is used to determine image forgery.

Choi et al. [60] developed security model for IoT-based smart healthcare system services. A local healthcare provider updates the user's medical information and sends it to the certification manager through a healthcare institution. The proposed

model is separated into two blocks: a smart healthcare “information manager” and a smart healthcare “certification manager,” and guarantees access control, encryption of patients’ health information, as well as the confidentiality of each center's medical data. The proposed model provides privacy protection, integrity, authentication, confidentiality, access control, key management, network security, system security, and encryption for efficient and secure medical-institution-focused smart healthcare services.

Alabdulatif et al. [61] proposed a novel and secure Edge-of-Things (EoT) computing system to provide smart healthcare surveillance. Data privacy is preserved by Fully Homomorphic Encryption, which has the potential to ensure end-to-end privacy for patients' data and data owners can obtain and decrypt encrypted analysis outcomes on a safe side. FHE both secures stored data and conducts analytic operations in an encrypted environment. Furthermore, distributed clustering-based techniques are used to analyze biosignals data such as electrocardiogram (ECG) data that is gathered from IoT-enabled sensors for patients in smart communities. In addition, the 5G network is used to overcome the issues associated with the transfer of huge volumes of encrypted data in an EoT environment.

Khan et al. [62] proposed probabilistic image encryption-based framework called “Secure Surveillance Mechanism on Smart Healthcare (SMSH)” for IoT-based smart healthcare systems. The research work is divided into two parts. In the first part, a keyframe extraction technique is used to extract meaningful keyframes (detected normal activity/abnormal activity) from recorded video by employing YOLOv3 algorithm. The effectively and successfully generated keyframes are moved to keyframe encryption module to perform further operations. Secondly, the authors proposed a lightweight and probabilistic encryption model to keep the extracted keyframes safe from any potential adversary. The proposed study guarantees some of the essential properties like patients’ privacy from any adversary by data encryption.

Ma et al. [63] proposed a "secure-channel free certificateless searchable public key encryption (SCF-CLSPE)" technique for SHS that does not need a random oracle model to resolve the security issues, including keyword guessing attacks to ensure patients' data confidentiality. The authors analyzed the proposed scheme and showed that it is secure against keyword guessing attacks and can resist chosen keyword attacks under the standard model. In SCF-CLSPE, the private-key of data owner is included in ciphertext. As a result, it is not possible to acquire a valid ciphertext for an adversary by guessing certain candidate keywords and encryption those keywords. In SCF-CLSPE, the designed server can perform the test algorithm. Even if the adversary successfully captures a trapdoor, it is unable to perform the test algorithm accurately. As a result, the SCF-CLSPE is able to resist keyword guessing attacks.

In [64], proposed an efficient "certificateless public key encryption with keyword search (CLPEKS)" to protect data privacy and security in mobile healthcare system. The CLPEKS can resist keyword guessing and chosen keyword attacks under two categories of adversaries. In the first category, the public key of any user can be replaced by an adversary, whereas in the second category, the master key can be accessed by an adversary. The user can check the accuracy of the private key, so CLPEKS can resist keyword guessing attacks and chosen keyword attacks.

Khan et al. [65] addressed security and privacy challenges in smart healthcare systems. The authors implemented image encryption methods to protect medical images. In order to get an encrypted image, the suggested approach combines two processes: high-speed scrambling and pixel adaptive diffusion. Three rounds of these processes are implemented in the proposed framework. The high-speed scrambling approach rapidly scrambles each pixel position in medical images. This efficiently reduces the strong correlation among nearby pixels by shifting pixel row and column positions at the same time. Adaptive pixel diffusion disperses the cipher-image pixels with minimum plain-image change. The overall pixel is changed by executing this process using a randomized value and the

previous pixel. The arithmetic modulo is employed as a software environment adaptation to carry out pixel adaptation diffusion throughout the complete plain images. To secure medical imaging data, the proposed approach demonstrates a high and strong level of security.

Manogaran et al. [66] proposed a secure industrial IoT architecture for storing and processing big data for healthcare applications. A Meta Cloud-Redirection scheme with a big data intelligence system is proposed, which collects and stores big data generated by various sensor devices. When the heart rate, respiratory rate, blood pressure, blood sugar, and body temperature levels exceed the normal range, the devices send a clinically significant alert message to the doctor over a wireless network. The data created by Meta cloud is divided into three categories: sensitive, normal, and critical. Depending on the privacy level, each category of data is stored in a distinct data centre. An interface is used in the proposed architecture to redirect user requests to the appropriate cloud datacenter. In this framework, the log files are processed using AWS CloudTrail. In cloud computing, the proposed scheme secures and processes big data. This interaction provides high-value business insights and boost overall performance. Medical sensor devices are attached to the human body in order to collect clinical data from the patient. To provide big data security in healthcare industry, a key management mechanism is used.

Alraja et al. [67] proposed an integrated approach to help normal IoT application users in efficiently protecting their privacy and data by themselves. The proposed system enables users to make meaningful decisions about data sharing and control their data release. The authors proposed a semantic web-based inference model that allows the user to identify the privacy risks that allows the user to assess the privacy risks associated with sharing certain personal data pieces with a recipient of data. In this system, when a user is asked to grant access to his personal data to a data recipient concealed behind an IoT environment smart service, the system assesses the privacy concerns associated with sharing, weighs them against the potential advantages to be gained, and enables the user to make an informed

decision about which data items may be revealed and with what precision. The proposed system also enables users to benefit from their personal data by making practical data sharing agreements with data consumer or smart services in the IoT environment. The authors applied their solution to a case study from the healthcare industry and actual patients to show the feasibility and usability of their approach.

Quasim et al. [68] proposed a "Smart Healthcare Management Evaluation using Fuzzy Decision Making (SHME-FDM)" approach to evaluate the efficiency of technology integration. Therefore, using the Fuzzy AHP combined with the smart healthcare system's fuzzy TOPSIS, the research evaluates the security of patient's medical data privacy in the smart healthcare environment. The fuzzy logic-based neural network is employed in this research to predict healthcare outcomes. The proposed technique was aided by a basic, easy-to-use and implement fuzzy logic framework for decision-making. The proposed system's structure is designed using fuzzy decisions and sensor data. The study examined various data protection aspects that impact the information security of online applications in healthcare. The evaluation findings suggested that the proposed model can be used in real-time while creating the smart healthcare management applications or systems. Furthermore, the study evaluated the neuro-fuzzy system developed for prediction of health status and found the optimum performance.

Zhou et al. [69] presented a practical approach for preserving privacy in smart healthcare. The authors designed a human-in-the-loop-aided (HitL-aided) approach to protect patient privacy in the smart healthcare. The proposed strategy differs from prior studies in terms of efficiency and feasibility. A block design strategy is used to conceal numerous health indications obtained from hospitals and wearable devices. Then, using representative vectors as a foundation, HitL is presented to facilitate random selection, preserving the privacy of prediction outcomes from various machine learning models. Moreover, Human-in-the-loop (HitL) technology is used to provide private access to health records from smart healthcare platforms. The privacy of health indicators, i.e., machine learning

inputs and physical conditions, i.e., machine learning outputs, is properly safeguarded by using the block design approach and the HitL. Furthermore, the results of the performance evaluation and case study show that the HitL-assisted approach is beneficial in protecting privacy in smart healthcare.

Anand et al. [70] developed a dual watermarking technique based on compression-then-encryption for protecting EPR data in healthcare systems, which yields various major benefits. This approach employs generated watermarking, in which turbo coding is used to encode EPR data before being incorporated into the watermark image's wavelet coefficient. This EPR watermark is generated and incorporated into the cover image's RDWT-RSVD coefficient. To assure the security and robustness of EPR, an integration of SPIHT-STE and RDWT-RSVD is employed. The innovation of this method is the employment of a compression-then-encryption approach on watermarked images, which allows for efficient and safe transmission across public networks. The results reveal that the system performs well in terms of robustness, security and privacy. In addition, the proposed approach provides better BER and NC values as compared to related existing approaches. The experimental results and improved performance demonstrate that the proposed approach provides a captivating tool for data security in smart healthcare.

Tripathi et al. [71] investigated the social and technological constraints to SHS adoption by examining cutting-edge expert perspectives and user perception. Furthermore, a blockchain-based SHS architecture called S2HS is proposed to ensure the system's inherent integrity and security. The sensitive and personal information and data of patients, electronic medical record, and clinical trial data captured by various sensors are encrypted with blockchain technology and kept in decentralized way rather than centralized cloud storage. With the patients' approval, this data can be accessible by any authorized person, such as insurance firms, healthcare providers, and pharmaceutical companies. When a physician or clinician wishes to access a patient's data, a real-time notification is issued to the patients, and the data may only be accessible by the physicians or clinicians if the

patients consent to share it. All entities in S2HS architecture are linked together via a WSN. In S2HS, two-level blockchain technique is used. Internal healthcare ecosystem entities such as healthcare providers, physicians, inventories, and other internal entities use a private blockchain. External entities including patients, insurance firms, and pharmacists interact using a public blockchain. The adoption of a two-level blockchain ensures that separate entities are isolated, resulting in a transparent and consistent process that is both privacy-preserving and secure.

Senthilsingh [72] proposed a system to safeguard data in SHS through the use of blockchain technology in 5G networks and the ECC algorithm in order to avoid data forgery. In this system, the patient is remotely monitored using medical IoT devices. These IoT devices detect the patient's medical conditions such as respiration, blood pressure, pulse, glucose level, and temperature. The doctor monitors this data and stores it in the cloud via blockchain. Smart Contract are deployed is used to safeguard transactions stored on the blockchain. Moreover, the privacy is provided by keeping the patient records in encrypted form. Hospitals that want to access the patient's health information should approach them with their identification. The patient produces the key with an algorithm and securely exchanges the key and the record with a third party. Furthermore, the key escrow mechanism will be utilized to overcome the difficulty of accessing the record when the user or patient is unresponsive. The proposed approach is compared to currently existing algorithms like Diffie-Hellman and RSA. In comparison to existing algorithms, the proposed technique is more secure.

Haque et al. [73] presented an approach using Blockchain and smart contracts in order to safeguard sensitive patient information while maintaining privacy. In the proposed system, a private blockchain with Ethereum as the implementation platform is used to ensure data confidentiality and integrity. In a healthcare environment, there are several stakeholders, such as patients, physicians, and hospitals, and many processes are involved in the whole workflow of the system. Smart contracts establish an environment where several processes can be performed without human intervention. As a result, the system relies less on

physical labor, making it more resource-friendly. Smart contracts are be used in the proposed system for appointment scheduling, patient registration, consultation, exchanging lab results between doctors and patients, invoicing, and patient monitoring. Furthermore, the saved information is demonstrated to be reliable and immutable, and it requires the consent of appropriate authorities in all situations. As a result, healthcare becomes more safe, automated, accessible to all, and decentralized.

Singh and Chatterjee [74] presented a system that combines IoT-Edge-Cloud for SHS. For real-time applications, an intermediate edge computing layer lowers network latency and enhances data processing. In real-time applications, edge computing minimizes response time and requires low bandwidth. The proposed system uses Privacy-Preserving Searchable Encryption to protect sensitive patients' data confidentiality and privacy. Furthermore, the proposed system includes a module for access control that prevents unauthorized access to remotely stored patient health information. The authors analyzed and demonstrated the proposed system in terms of efficiency and performance using different performance metrics such as transfer time, latency, energy and power consumption, throughput, and encryption time. The proposed system's access control mechanism enables controlled access to patient data. In addition, the privacy of patient data is protected, service latency is minimized, and the access control approach protects against illegal access.

3.3. Secure Data Sharing

In [75], a blockchain-based model i.e. "Blockchain-based Zero-Knowledge Proof (BZKP)" has been proposed for sharing patient health records in Bahrain's smart cities that use IoT technologies. The proposed model is an IoT-based patient centered paradigm that combines zero-knowledge proof to be designed for preserving patient privacy and ensuring patients' prior consent on access to their personal data such as their health condition and account balance. Moreover, the immutability feature of blockchain can help to provide unchangeable and reliable

stored data to different stakeholders in the healthcare sector. BZKP model is based on pre-authorized blockchain access tokens; hence, it enables a secure and trustworthy access paradigm for data sharing in the healthcare sector.

In [76], the authors investigated the usage of distributed ledger technology to address security challenges such as data integrity, confidentiality, access control, and authentication in health data transfer. In this work, a scheme is designed using the masked authenticated messaging for the secure transfer of healthcare and medical data from IoT sensors and devices to the distributed ledger. A novel paradigm with zero-miner, zero-fee, and zero-block is designed for sharing and storing of health information safely and smoothly. The cryptographic functionality of MAM protocol provides an additional level of security for ensuring the authenticity, confidentiality, and integrity of medical data. Moreover, the study also provides a proof-of-concept of using the proposed model for securing medical data in IIoT environment.

Wang et al. [77] proposed a blockchain-based system namely GuardHealth for secure data sharing and privacy-preserving. Smart contracts are used on blockchain to ensure efficient and secure healthcare data sharing and storage. GuardHealth ensures integrity, data preservation, data sharing, and confidentiality when dealing with sensitive information. GuardHealth isolates raw data storage from the index of data storage while data is encrypted and stored in a CSP. Using proxy re-encryption scheme, the user can grant requestors data access and simply remove permissions at any moment. A trust model is used to accurately manage user trust, with the development of a novel Graph Convolutional Network-based model for anomaly detection.

Meng et al. [78] proposed a security enforcement scheme based on SDN for smart healthcare data-sharing systems. In this scheme, a virtual machine (VM) is allocated to each patient in data-sharing system, and each VM provides data services which could be delivered to authorized service consumer or system IoT devices. Furthermore, SDN-based gateway is proposed to protect the virtual

machine from unauthorized access. This gateway offers a firewall mechanism and ensures that only authorized and legal entities can access patients' virtual machine. Since IoT devices have unique MAC addresses, thus the proposed scheme is capable of authenticating resource-constrained IoT devices and handling the security challenges posed by identity theft.

Deebak et al. [79] proposed" Secure and Anonymous Biometric Based User Authentication Scheme (SAB-UAS)" to obtain secure communication and improved security efficiency in healthcare applications. To demonstrate the storage, performance, and security efficiencies, the SAB-UAS approach includes a formal security model, as well as performance and resource efficiency analysis. The SAB-UAS can protect a user's sensitive information from an adversary in order to attain perfect forward secrecy. Furthermore, the thorough formal and informal security analysis employing the random-oracle model and BAN logic demonstrates that the SAB-UAS provides stronger security for the prevention of different possible attacks for IoM-based applications.

Hu et al. [80] proposed a blockchain-based security data sharing method to achieve secure health data sharing among patients and healthcare providers. The edge cloud is comprised of four types of nodes namely storage nodes, security broker nodes, edge gateway nodes, and processing nodes. The wearable sensors connect to the edge cloud using 5G networks, and the edge cloud gathers context information and physiological signals. The gathered data is stored in storage nodes and shared with different healthcare providers. The security broker node acts as the gateway to blockchain, ensuring the integrity of health data exchanges between patients and healthcare providers. The Ethereum platform's smart blockchain and smart contracts are responsible for secure data exchange mechanism.

Ullah et al. [81] proposed a novel "Secure De-duplicated Data Dissemination (S-DDD)" scheme for the healthcare IoT context employing FoG server at the network's edge. In this scheme, the authors presented adaptive chunking approach

to decrease the redundancy and symmetric key-based encryption approach for secure healthcare data sharing from smart healthcare devices to a collector node, which transmits the data to the FoG server through the sink node for the purpose of processing and storage. It achieves a trustworthy and reliable security system for assuring secure data distribution. Hence, patient privacy and security vulnerabilities are handled in a trustworthy manner.

Fang et al. [82] proposed an efficient and innovative "Revocable attribute-based encryption (RABE)" scheme for privacy protection in smart healthcare data sharing. The authors presented data-sharing system and an access control model for the smart healthcare environment. The authors developed a revocation mechanism based on a doctor's identity and time, making it impossible for physicians to regain access to past medical information following revocation. Furthermore, a digital watermarking mechanism in the data encryption process is proposed to allow tracing of leaked healthcare records. In addition, a novel access control mechanism is used for secure healthcare record sharing between medical practitioners and researchers. The source of Electronic Medical Records determines the physician's authorization for the EMRs. Doctors have the option of sharing EMRs written by them. However, if the doctor wishes to share EMRs provided by patients, the doctor must request the patient to modify the access structure.

Kumar and Chand [83] proposed an innovative efficient and secure cloud-centric IoMT-based SHS which is publicly verifiable. The authors proposed an "escrow-free identity-based aggregated signcryption (EF-IDASC)" scheme to solve the problem of key escrow. The proposed system collects health data from several sensors implanted on a patient's body, performs signcryption and aggregates it using the EF- IDASC method, and then sends it to a health cloud server through a smartphone. This approach does not expose any information regarding the patient's identify or medical information. The EF-IDASC scheme is secure against EUF-CMA and IND-CCA in the ROM and well-known BDHP. The comparison of EF-IDASC with other relevant signcryption techniques showed that the

proposed strategy uses the least amount of energy when compared to other schemes. Furthermore, the authors proposed a secure communication protocol for D2D data aggregation in the context of cloud-centric IoMT for SHS, with security based on the EF-IDASC scheme. The proposed secure system ensures patient anonymity, public auditing of cloud data integrity, and mutual authenticity of patient data with public integrity.

Nguyen et al. [84] presented an innovative and hybrid strategy of data sharing and data offloading for healthcare by using Ethereum blockchain and edge-cloud. Firstly, a data offloading technique is proposed that allows IoT medical data to be offloaded to an edge server for processing while maintaining privacy. Secondly, a novel data sharing scheme that incorporates blockchain technology is offered to allow data exchange among users of healthcare. In addition, an access control technique based on smart contracts is designed for access authentication in order to ensure reliable and safe EHR sharing. The experimental results show the considerable benefits of the proposed offloading strategy over previous baseline approaches in terms of lowered time delay, energy consumption, and improved memory management. Furthermore, the data sharing technique can accomplish effective user authentication considerably improve data retrieval speed while protecting the healthcare system from malicious access. System analysis reveals that the operating cost of smart contracts is minimal and guarantees the system's security.

Quamara et al. [85] proposed an end-to-end architecture for safe information storage and exchange in the SHS to provide protection against botnet-based cyberattacks. The authors mainly focused on several layers of protection affecting the storage and transfer of healthcare data. The proposed architecture consists of two types of entities: Patient and Smart healthcare infrastructure, which includes authorization servers, hospital authorities, information storage servers, and suppliers. There are two levels of interaction between the entities i.e. Patient-HA and HA-Supplier interaction. Furthermore, the proposed scheme offers three levels of security against botnet i.e. client-side security, network security, and

server-side security. In client-side security, the patient's wearable device can be incorporated with botnet protection methods to detect malicious behavior. In network security, the anti-botnet method can be implemented on transmission channels. In server-side security, the information storage server which is responsible for maintaining patient-specific medical data can be secured from botnet.

3.4. Authentication Mechanisms

Alzubi et al. [86] proposed a blockchain-based secure authentication technique using "Lamport Merkle Digital Signature (LMDS)" for transmission of sensitive data between medical practitioner and patient. Initially, IoT devices are authenticated using the "Lamport Merkle Digital Signature Generation (LMDSG)" model by creating a tree whose leaves represent the hash function of sensitive patient data. Further, the root of LMDSG is determined by centralized healthcare controller to detect malicious user behaviour by using "Lamport Merkle Digital Signature Verification (LMDSV)" technique. When the public key equals hash of leaf, the signature is considered valid.

Nashwan [87] proposed an end-to-end authentication mechanism called E2EA using WMSNs for IoT-enabled healthcare systems. The proposed scheme is based on symmetric cryptography and one-way hash functions. The proposed approach incorporates security features such as a flexible and robust authentication mechanism, forward secrecy services, and physician and patient confidentiality. Furthermore, BAN logic is used to validate mutual authentication services for security verification. The security analysis reveals that the proposed strategy can resist a variety of security attacks including impersonation attack, man-in-the-middle attack, desynchronization attacks, replay attacks, smart-card-loss-attack, and insider attacks.

Chaudhary et al. [88] proposed "lattice-based secure cryptosystem for smart healthcare (LSCSH)" for smart cities. A mutual authentication mechanism based on lattice is developed to authenticate requests between cloud

server and end users like physicians, patients, and healthcare workers. For data sharing between cloud server and different users a data encryption strategy is designed. For encryption and decryption of data, this strategy uses a third-party based key exchange protocol between the cloud and users. Furthermore, a mechanism for verification of access rights is designed to provide permissions to users. This mechanism limits patients' access to their own information, while physicians can only access information about their own patients.

El Zouka and Hosni [89] presented a secure and lightweight authentication technique that ensures secure communication while protecting patients' health information. The authors proposed secure health monitoring system that integrates artificial intelligence such as fuzzy systems and neural networks in order for the system to function as a decision support model that determines priority based on the health parameters acquired from sensor nodes. The proposed system has been created using the FBIS approach that can reveal the patient's health condition and forward it to the health advisory as a precautionary measure. As a result, the proposed model enables reliable, secure, accurate, and real-time monitoring of patient.

Wu et al. [90] proposed an innovative two-factor authentication mechanism for global mobility network to protect smart healthcare system against attacks and other security threats. To establish a session, the user is required to have a smart card and a password, and the user must be authenticated by both a foreign agent and a home agent. Moreover, a mobile user can also directly or indirectly validate home and foreign agent using information saved on the smart card. Lastly, a session key will be created between foreign agent and the user after the interconnection.

Garg et al. [91] presented a robust, trusted, lightweight, and secure protocol for key agreement and mutual authentication between remote patients and a remote medical server in the smart healthcare sector. The proposed protocol takes advantage of Elliptic-Curve Cryptography's (ECC) increased security and smaller

key size properties to build mutual trust between patients and medical servers, followed by agreement on a shared session key for future communication. In addition, the proposed protocol takes advantage of one of the key aspects of blockchain technology, namely the ability to retain the preceding transaction hash. This feature provides increased security and significantly reduces the risk of impersonation attacks in smart healthcare domain. The security analysis of the designed protocol ensures that the proposed protocol allows for mutual authentication and is resilient against a variety of attack vectors, including impersonation, forward secrecy, and DoS.

Gope et al. [92] proposed a novel mutual authentication mechanism for IoT devices that protects PUFs from modeling and machine learning attacks. Moreover, the proposed system can provide increased scalability, as well as protection against forgery, man-in-the-middle attacks, IoT device privacy, and replay attacks. According to the authors, the proposed system is the first ever PUF-based authentication system that can protect IoT device security and privacy against modeling or ML attacks. Furthermore, the findings from high-level OPUF simulations are provided that demonstrate the forward and backward unpredictable behaviour of the PUF employed in the protocol to give resistance against modeling or ML attacks. The detailed security evaluation of the proposed system demonstrates that it is resistant to several imperative security threats to IoT devices.

Wang et al. [93] designed a novel authenticated key agreement technique for safe mutual authentication in SHS between the user and the edge server. The proposed technique does not necessitate the use of an online registration centre to aid with authentication, nor does it make use of complicated bilinear operations. In particular, the proposed technique can implement key agreement and mutual authentication without requiring an online registration centre while still meeting privacy and security protection criteria. The proposed technique reduces the user's computational and communication cost by moving some computational workloads to the server. This technique can also be used for other IoT applications.

Furthermore, the proposed approach uses CL-PKC to overcome key escrow and certificate management issues. Security evaluation reveals that the proposed approach can meet security criteria and withstand a variety of common attacks and security threats. Performance evaluation demonstrates that the proposed approach is more efficient than other existing approaches, which indicates that it is appropriate for IoT applications such as SHS.

Yuanbing et al. [94] examined the work proposed in [95] for protecting information security and privacy from unauthorized users, as well as highlights current vulnerabilities like insider attack, password guessing attack, smart card attack, and user anonymity issues. To address these security issues, the authors presented an enhanced ECC-based protocol for anonymous user authentication in smart healthcare systems utilizing WMSN. The security evaluation utilizing Burrows-Abadi-Needham (BAN) logic guaranteed that the protocol can offer safe mutual authentication as well as the potential to withstand different security attacks. Furthermore, AVISPA simulation results demonstrated that the scheme is safe to protect against intruders. The comparison of protocol's security features and efficiency with currently existing schemes proved that the upgraded protocol provides more powerful security features and lower communication costs while raising computing cost. As a result, the protocol is appropriate for usage in the context of smart healthcare.

3.5. Access Control Mechanisms

Pal et al. [96] proposed a new access control strategy for IoT-based smart healthcare that integrates roles, attributes, and capabilities to generate a flexible and fine-grained approach while lowering the required number of policies necessary to be developed and maintained. Attributes are used in the assignment of roles-membership and the evaluation of permissions. Capabilities are granted by role-membership. The capabilities that are granted can be parameterized depending on additional user attributes. Furthermore, they can be used to access the specific services offered by IoT things.

Saini et al. [97] proposed a dynamic and distributed access control technique based on smart contracts that allow patients to own and safely share their sensitive EMRs across various entities included in smart healthcare. Furthermore, the proposed technique incorporates the complete healthcare system scenario, which primarily consists of three types of entities: hospitals, patients, and computationally limited IoT-based smart healthcare devices. For this purpose four types of smart contracts are proposed: access authorization, user verification, access revocation, and misbehavior detection. In this system, the cloud storage is used to prevent congestion and lower overhead on the blockchain network. When the EMRs are created, they are saved in the cloud storage after being encrypted, with the corresponding EMRs' hash and index number kept in the blockchain. For the purpose of encryption, "Elliptic Curve Cryptography (ECC)" and "Edwards-Curve Digital Signature Algorithm (EdDSA)" cryptographic functions are used.

Chen et al. [98] proposed a security and protection framework based on zero-trust architecture for 5G-enabled smart healthcare platform. The security challenges that 5G networks and smart healthcare face are discussed, and the needs for 5G-enabled smart healthcare system privacy and security are highlighted. The authors then observed that the zero-trust idea, which assumes that all organizations involved are untrustworthy until authorized or verified to be safe, is a possible option, but it must be expanded for context of 5G-enabled smart healthcare. In the proposed work, a four-dimensional security system for 5G-enabled smart healthcare systems based on zero-trust architecture has been developed. The four basic dimensions of access, i.e., subject, object, behaviour, and environment, are collectively employed by the risk judgment process, access control model, and trust evaluation model to continually analyze possible threats at all levels and execute fine-grained access control. The authors tested the proposed system at the industrial level and demonstrated that the system provides improved security for 5G-enabled smart medical applications.

Zhong et al. [99] proposed an efficient attribute-based access control strategy for edge-based smart healthcare with outsourced encryption and decryption

functionality. In this strategy, some encryption and decryption processes are outsourced to the edge, rather than the typical attribute encryption technique, to minimize the processing load on resource-restricted devices like sensors while protecting the security and privacy of healthcare data. This improves the suitability of proposed system for smart healthcare. Simultaneously, the system offers attribute update, which increases the system's efficiency and improves the security of healthcare data. The proposed system is comprised of five participants: cloud server, key authority, edge node, data user, and data owner. The cloud layer includes remote cloud servers, while the edge layer comprises key authority and edge nodes, and the IoT layer contains data users and data owners. The authors proved that the proposed system is secure under the DBDH assumption. Moreover, the system's performance is assessed at various levels of security, and the results demonstrate that the proposed system is more effective for resource-limited devices than the conventional ABE for smart healthcare.

3.6. Other Security Solutions

He et al. [100] presented an overview of healthcare IoT security challenges. This article also investigates the security risks associated with password building and provides a technique for evaluating password strength that takes user personal information into consideration. In this study, a password strength meter named PI-PSM is proposed to address the drawbacks of existing approaches and to evaluate password strength based on the personally identifiable information. In this technique, the context-free grammars are used for personal information classification as well as tag processing, which can correctly discover personal information included in passwords and other hidden variations. In this way, the mechanism offers strong resistance against targeted password attacks. Moreover, this scheme can be incorporated with existing heuristic-based and rule-based PSMs to help the user choose a strong password.

Salahuddin et al. [101] proposed a novel software-enabled IoT infrastructure to provide flexibility, privacy-preserving, cost-effectiveness, and security in smart

healthcare environment. The proposed architecture incorporates edge-cutting technologies like blockchain, message brokers, fog and cloud services, IoT, and Tor enabling secure, flexible, and cost-effective IoT deployment of smart healthcare domain. Moreover, the authors also proposed a state-of-the-art platform called flexBeacon for seamless data integration and management using rule-based beacon and machine-to-machine communication. Furthermore, the role of decision and data fusion in the fog and the cloud for smart healthcare systems is discussed.

Abugabah et al. [102] proposed a blockchain-based architecture that would open the future of healthcare industry and enhance healthcare services. The study provides a smart contracts-based telemedicine system solution that ensures safe transaction and the rights of physicians, patients, healthcare providers, and health insurers. The study offers a solution that uses smart contracts enabled by the Ethereum blockchain platform to monitor, control, and execute telemedicine transactions. When the Ethereum smart contracts are executed, events are triggered, allowing all authorized entities in the network, including patients, to monitor healthcare transactions. The proposed architecture eliminates the requirement for a trusted central administration or database by recording healthcare transactions with reliability, security, and integrity, and it also increases transparency among all participants in telemedicine interactions. The Interplanetary file system is used to store healthcare records, and the proof-of-existence is achieved by saving the hash in a smart contract. This setup provides the better possibility for achieving interoperability, data integrity, and transparency.

Khan et al. [103] proposed secure and efficient surveillance on IoT smart healthcare systems using cosine-transform encryption. The authors focused on safe monitoring using intelligently recorded summary keyframe extraction and two rounds of cosine-transform encryption. Firstly, a structured procedure of keyframe extraction that is used to collect meaningful and significant frames of an image using a visual sensor with an alert to authorities is applied. Secondly, a

regulated cosine-transform encryption mechanism has been plotted over the retrieved keyframes to provide security and protection against any future adversary attacks. In addition, this integrating mechanism can effectively lower crucial communication costs, data transmission costs, storage, and bandwidth problems, ensure protection from adversaries or attackers by employing effective encryption methods, and maintain patients' privacy and confidentiality in the SHS. The proposed scheme is also capable of taking timely, effective, and rational decisions regarding suspicious activity in the event of any emergency among patients in SHS. Table 3.1 highlights some of the key efforts in SHS security.

Table 3.1: Significant Contributions to Smart Healthcare Security

Paper	**Year**	**Description**
[45]	2021	An intrusion detection system based on machine learning using a genetic algorithm (GA) and Random Forest (RF)
[47]	2019	Proposed "HealthGuard," a security framework based on machine learning techniques to identify malicious activity in SHS.
[48]	2021	A privacy-preserving framework for data transmission that supports malicious users' detection and safe ciphertext conversion.
[49]	2020	An innovative and lightweight security system namely IC-MADS based on cross-layer trust computing technique for effectively detecting the man-in-the-middle attack.
[61]	2019	A novel and secure Edge-of-Things (EoT) computing system to provide smart healthcare surveillance.
[70]	2020	A dual watermarking technique based on compression-then-encryption

		for protecting EPR data in healthcare systems.
[73]	2020	A dynamic and distributed access control technique based on smart contracts that allow patients to own and safely share their sensitive EMRs across various entities included in smart healthcare.
[77]	2020	A blockchain-based system namely GuardHealth for secure data sharing and privacy-preserving.
[78]	2019	A security enforcement scheme based on SDN for smart healthcare data-sharing systems.
[80]	2021	A blockchain-based security data sharing method to achieve secure health data sharing among patients and healthcare providers.
[83]	2020	An innovative efficient and secure cloud-centric IoMT-based SHS which is publicly verifiable.
[87]	2021	An end-to-end authentication mechanism called E2EA using WMSNs for IoT-enabled healthcare systems.
[89]	2021	A secure and lightweight authentication technique that ensures secure communication while protecting patients' health information.
[92]	2021	A novel mutual authentication mechanism for IoT devices that protects PUFs from modeling and machine learning attacks.
[94]	2021	An enhanced ECC-based protocol for anonymous user authentication in smart healthcare systems utilizing WMSN.

[97]	2020	A robust, trusted, lightweight, and secure protocol for key agreement and mutual authentication between remote patients and a remote medical server in the smart healthcare sector.
[98]	2020	A security and protection framework based on zero-trust architecture for 5G-enabled smart healthcare platform.

According to the discussion above, an IoMT-based smart healthcare system transmits extremely sensitive and personal data. The shared resources in SHS provide several benefits, but there is still a lack of integrity and privacy protection for medical data. Furthermore, the security mechanisms built into currently existing systems are insufficient to prevent numerous cyberattacks, putting patients' data at danger of theft and forgeries. As a result, a security system that rapidly identifies cyberattacks and safeguards patient data in smart healthcare systems is required. In this research, we propose an intrusion detection framework based on long short-term memory (LSTM) deep learning algorithm to detect malicious traffic data in smart healthcare environment. The deep learning paradigm has a significant influence on healthcare systems. Deep learning algorithms are applied to efficiently detect network intrusion, cybersecurity threats, and identify anomalous behaviour in SHS. In order to increase the security of SHS, this manuscript provides an intrusion detection system based on deep learning techniques.

CHAPTER NO. 4

METHODOLOGY AND MATERIALS

4.1. Research Idea

In this section, the primary concept of the research is described in detail. Incorporating smart healthcare into the healthcare framework has several advantages, but it also has significant disadvantages. This change broadens the attack surface, exposing patients' confidentiality, security, and privacy to attacks. In addition, the wireless connectivity employed in SHS leaves it open to cyberattackers and network intruders. If not identified early enough, these attacks can compromise protected health information, resulting in data theft, loss, or disclosure of confidential medical data. Building security systems to detect different types of threats and attacks is one of the ways for securing computers. Intrusion detection systems (IDSs) are available to identify and prevent different types of attacks. A crucial gap that IDS face is the potential of detecting any new kind of attack that is not already recognised.

Furthermore, the fast advancement of communication and information technology applications has introduced a new issue. With the emergence of the new technological era, passing vast amounts of data from various sources on a network created in a short span is another issue because it is difficult to detect intrusive behavior in these huge amounts of data and increased network speed. AI and ML are two ways used to identify suspicious attacks. In this research, we intend to use and examine the deep learning approach in conjunction with technological advancement rather than typical machine learning approaches.

The primary goal of this research is to safeguard smart healthcare applications and devices from malicious threats and other security concerns. For this purpose, we designed a deep learning-based intrusion detection system to efficiently identify smart healthcare network intrusions by evaluating traffic flow data. Deep learning (DL) is considered as a subclass of machine learning (ML), and the

results of deep learning techniques are clearly better to those of classic machine learning approaches or shallow models in the majority of application cases. While both methods use data to learn features, the capacity of deep learning to scale with the data is a key difference between the two. After training with big datasets, ML algorithms' performance tends to plateau, and then declining returns take effect. On the contrary, deep learning algorithms outperform as the volume of training datasets grows. The figure 4.1 shown below, created by Andrew Ng, an American technology entrepreneur and co-founder of Google Brain, accurately depicts the distinction between classic ML models and DL.

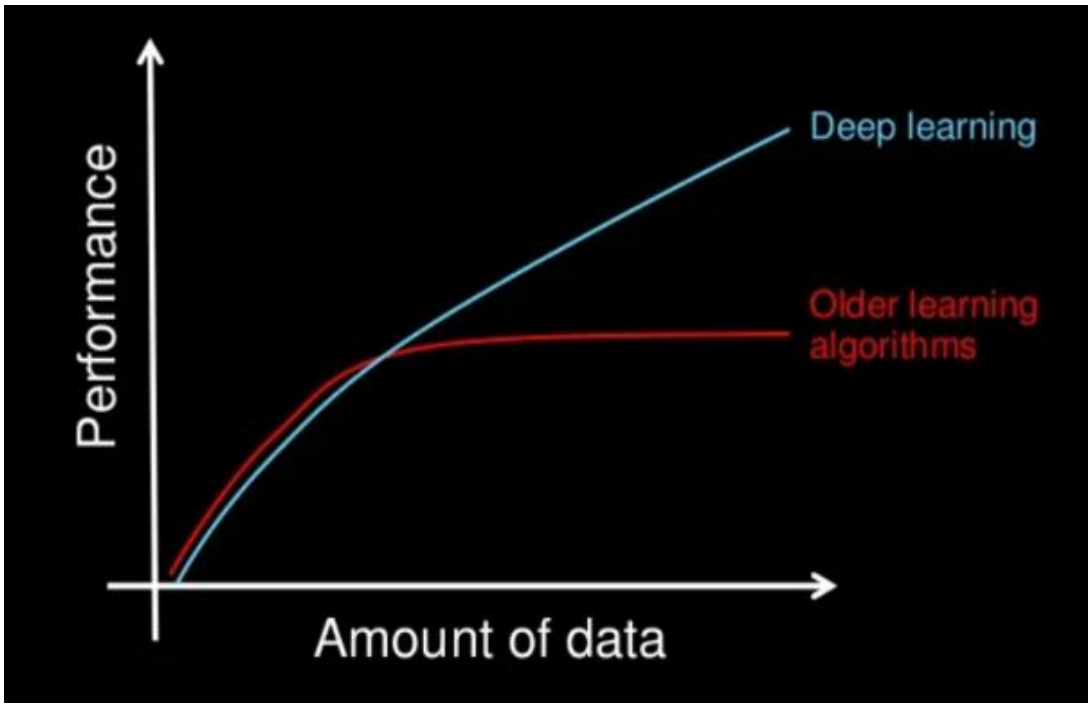


Figure 4.1: Illustration of how can data science methodologies scale as the amount of data increases [107]

Deep learning algorithms learn feature representation directly from source data such as texts and images, eliminating the need for human feature engineering. As a result, deep learning algorithms can be used from beginning to end. Deep learning algorithms outperform shallow models when dealing with large datasets. The primary focuses of deep learning research are hyperparameter selection, network design, and optimization technique.

4.2. Proposed Work

The proposed framework's architecture is divided into two phases: training and testing. The training and testing phase is the most important aspect influencing the success of deep learning model. In deep learning, we simply strive to build a model that can predict test data. As a result, we fit the model with training data and test it with testing data. The models created aim to predict the unknown results, which are referred to as the testing set. An efficient training process raises the developed model’s quality. Deep learning algorithms are fed training data in order to make them learn how to execute a desired activity or make predictions. They are required to train the algorithm to create correct predictions in order to achieve the AI project's objectives.

Machines must begin isolating patterns in the data in the same way that humans do. Computers, unlike humans, require a lot more instances because they are unable to reason in the same manner that humans do. The neural network is continually given similar training data in each epoch, and the system continues to train on the data's features. The training set includes a diverse range of inputs to ensure that the model learns in all circumstances and can forecast any previously unknown data instance that may arise in the future. The model assesses the data several times in order to learn more about the data's behaviour and then adapts itself to fit its intended goal. During the training phase, the normal and anomalous traffic data is given to the deep learning-based model to help it learn.

Once the model is trained, it is evaluated using unique test data. Once the model is developed, testing data confirms the model's ability to make correct predictions. Testing data, as its name implies, aids in validating the algorithm's training progress and adjusting or optimizing it for better outcomes. Moreover, it provides an unbiased assessment of a model's performance and guarantees that it generalizes well to new, previously unknown data. When testing data is passed through the model, it performs the function of a black box. Test data offers a final, real-world verification of an unknown dataset to ensure that the DL model was

properly trained. During the testing phase, the test data is loaded into the deep learning-based model, which predicts whether the data is normal or abnormal based on the training data. Moreover, the model also categorizes the data into several attack types. Figure 4.2 shows training and testing process in deep learning.

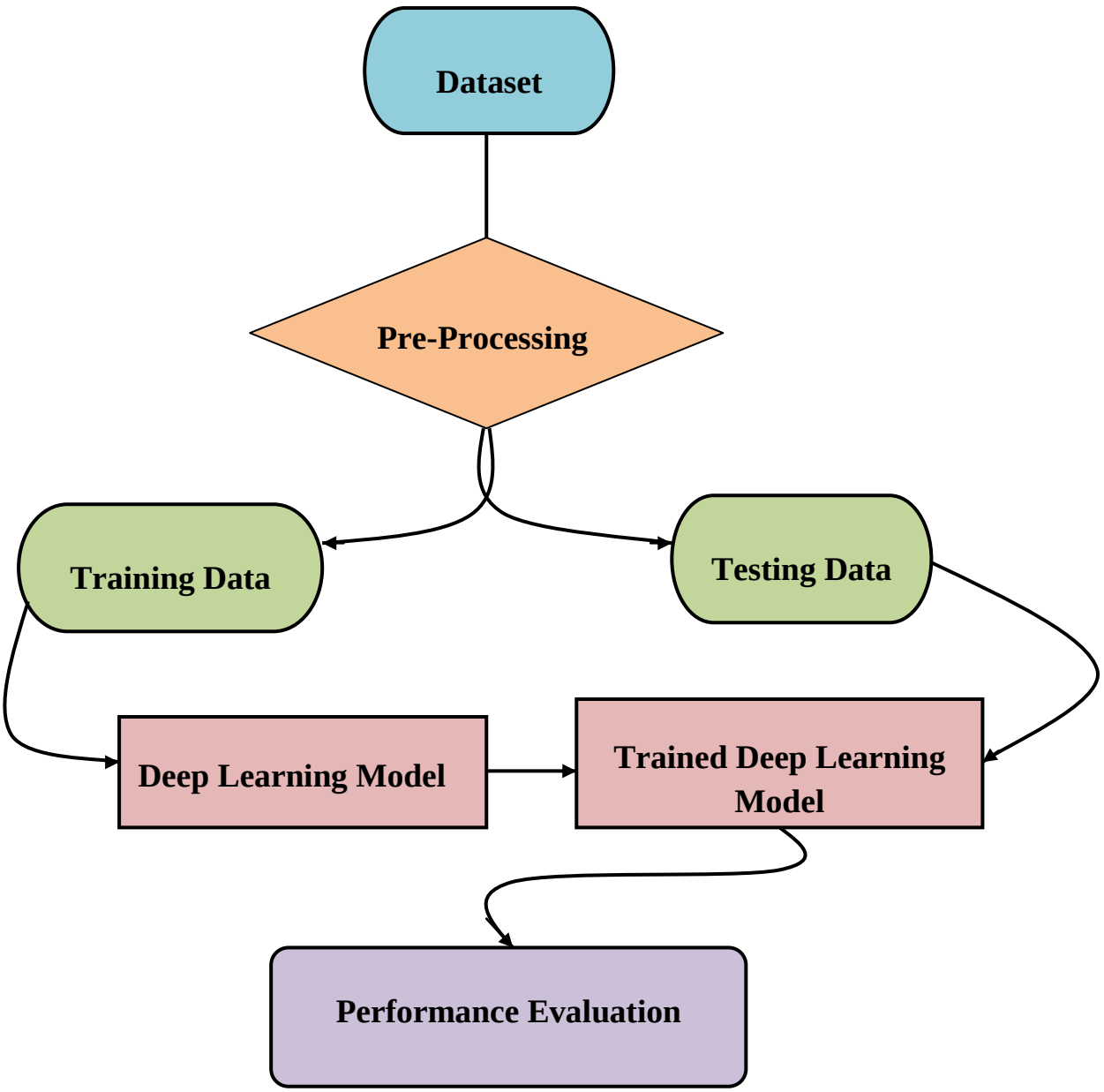


Figure 4.2: Training and testing process in deep learning.

This manuscript describes an automated approach for detecting intrusions in an IoMT-based smart healthcare system. Soft computing approaches play a critical role in improving network security by detecting intrusions. Deep learning approaches for classifying and detecting intrusion are used in this thought-provoking work. In this study, we attempted to use deep learning approaches to handle network intrusion issues. Every year, IoMT-based smart healthcare devices create massive volumes of data. The data created by SHS is continuously at danger of theft because to its sensitive nature. First, normal and abnormal traffic data is acquired and pre-processed to turn it into a comprehensible format, making it suitable for deep learning models. Data pre-processing includes transforming, normalizing, and reducing big datasets to extract relevant information. The pre-processed data is separated into two datasets: training and testing. The deep learning model is fed the training dataset. The source nodes that make up the input layer receive the data to be processed. Classification and prediction are done in the output layer.

The computational work is performed by the hidden layer that is positioned between the input layer and the output layer. Memory cells and gate units are found in the hidden layer. The proposed model can accept both current and previously obtained input data. In addition, it can remember past inputs due to its internal memory. In this model, there are loops or cycles that are used to connect hidden layers in order to get information. This holds true for all hidden layers up to and including the output layer. The testing dataset is fed into the model once it has been trained. The model predicts test data results based on training data. The output data is divided into two categories: normal traffic and abnormal traffic. Furthermore, the model categorizes the data into several attack categories. Finally, several evaluation matrices such as accuracy, precision, recall, true positive rate, false positive rate, and F-measure are utilized to evaluate the proposed model's performance. The results of the proposed model are also compared with existing models in order to test the accuracy of the proposed model against the existing models. The flow diagram of proposed work is presented in Figure 4.3.

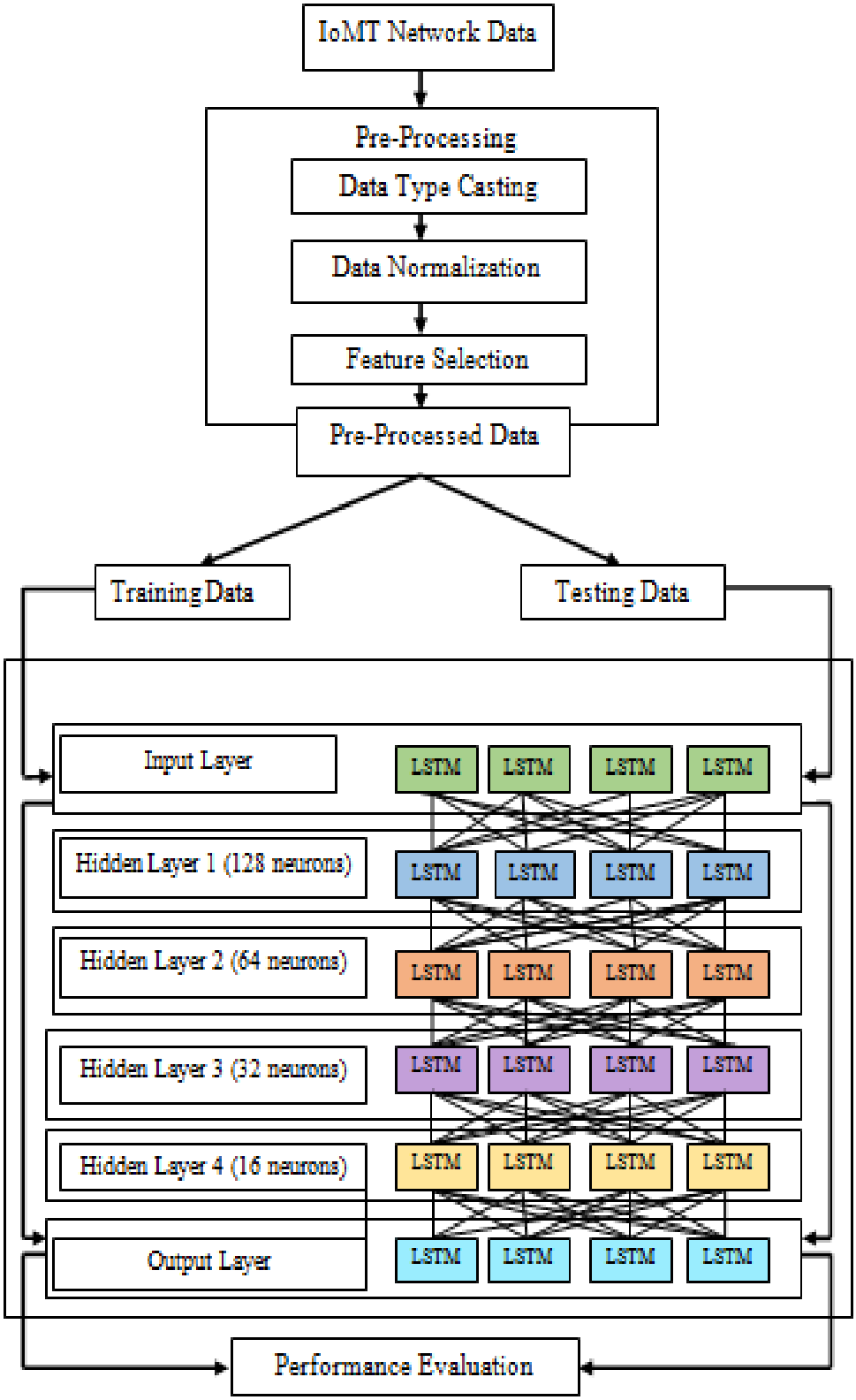


Figure 4.3: Proposed intrusion detection model.

Pseudocode

1: Conversion of nominal attribute values to numeric values.

2: Drop null values from the dataset.

3: Normalize data using z-score normalize: $Z = \frac{x-\mu}{\sigma}$.

4: Calculate correlation matrix through CFS algorithm using Pearson's correlation formula: $r = \frac{\sum(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum(x_i-\bar{x})^2 \sum(y_i-\bar{y})^2}}$.

5: Drop strongly correlated attributes from the dataset.

6: Split the dataset into train and test subsets with ratio of 60/40.

7: Split the test subset into test and validation subsets with ratio of 20/20.

8: Build LSTM model using 4 hidden layers with 128, 64, 32, and 16 neurons respectively.

9: Fit the LSTM model.

10: Evaluate the model using test and validation subsets.

11: Evaluate the results using classification metrics: accuracy, recall, precision, and F-Score.

12: Compare results with existing models.

4.2.1. Dataset Description

Over the last decade, intrusion detection analysis has grown in importance, with researchers focusing on diverse datasets to increase system accuracy and minimize false positive rates. The performance of the detection system is tested and evaluated using the evaluation dataset. A high quality dataset is required to generate efficient and productive outcomes in both testing and in real-world scenarios. This research makes use of publicly accessible IoMT dataset: WUSTL-EHMS-2020 for testing and evaluating our model. The characteristics of the dataset are discussed next.

4.2.1.1. WUSTL-EHMS-2020 Dataset

The WUSTL-EHMS-2020 is an IoMT cybersecurity dataset that was generated in 2020. This dataset was developed using a real-time "Enhanced Healthcare Monitoring System (EHMS)" testbed [111]. This testbed gathers both patients' biometrics and network traffic metrics. Previously, there was unavailability of such a dataset that incorporates both these biometrics. The testbed is composed of four parts: medical sensors, network, gateway, and control and visualization. The data flow begins with sensors embedded to the body of the patient and continues to the gateway. The gateway then sends this data from the sensors to the server through the router and switch for visualization. These data can be intercepted by an attacker before they reach the server. The IDS is in charge of recording real-time network flow, as well as biometric data from patients and detecting anomalies.

This dataset contains man-in-the-middle attacks like data injection and spoofing.

- **Data Injection:** The data injection is used to change packets on the fly, hence compromising the integrity of data.
- **Spoofing Attack:** The spoofing attack only sniffs packets between the server and the gateway, which compromises the patient data confidentiality.

The dataset contains 44 features, 35 of which are network traffic metrics, eight biometric features from patients, and one label feature. In this dataset, the records with MAC addresses of the attacker machine are labeled as ‘”1”, and the remainder as “0”. Table 5.1 displays statistical data from the WUSTL-EHMS-2020 dataset.

Table 4.1: Statistical data from the WUSTL-EHMS-2020 dataset.

Measurements	**Values**
Number of attack records	2,046
Number of normal records	14,272
Total number of records	16,318

4.2.2. Data Pre-Processing

In this stage, we will prepare the data for feeding to the deep learning model. Data pre-processing is the procedure for preparing raw data for use in a deep learning model. It is the primary and most important stage in the process of developing a deep learning model. The data pre-processing stage consumes the most time on a deep learning project, but it is well worth the effort [104]. When working on a deep learning project, we don't always have access to clean and prepared data. And, before doing any data-related activity, it is necessary to clean the data and format it. The data must be formatted properly in order to achieve better outcomes from the used model in deep learning applications. For instance, if the algorithm only accepts numerical data, a class named "malignant" or "benign" must be substituted with "0" or "1” [105]. In order to reduce the model's dimensionality, only variables that provide unique and relevant information are selected. Another consideration is that the dataset should be organized in such a manner that it can

run many deep learning algorithms in the same dataset and select the best of them. As a result, we utilize a data pre-processing activity for this.

Real-world data sometimes contains noise, missing values, and is in an unsuitable format that cannot be utilized directly in deep learning models. Furthermore, it is inconsistent, incomplete, inaccurate, and lacking in particular attribute values. This is where pre-processing comes into play: it cleans, formats, and organizes raw data, making it ready for deep learning models to use. Data preprocessing is a necessary step for cleaning data and making it acceptable for a deep learning model, which improves the model's efficiency and accuracy. The pre-processing is necessary to deal with missing data and address discrepancies. Outliers are removed during preprocessing, and the features are scaled to a comparable range [106]. Data cleaning and data transformation are techniques for removing outliers and standardizing data so that it can be utilized to build a model. The training set is the result of data preparation. Data pre-processing includes data transformation, data normalization, and data reduction to extract relevant information from the dataset.

4.2.2.1 Data Transformation

The process of turning raw or unprocessed data into a structure or format that is more suited for model development and data discovery is known as data transformation. It is a crucial stage in feature extraction that aids in the discovery of new information. Moreover, it assures data quality and improves prediction accuracy. Data transformations can be used to make comparisons and interpretations easier. Transforming data can provide the highest level of data quality that is necessary for accurate analysis and the generation of important insights that will support data-driven choices. The Deep learning model is only as capable as the data used to train it. If the model contains too few attributes, it won't be able to learn much.

If the model contains too many attributes, we might be providing the model with too much unnecessary information. In addition, each attribute's values must also

be taken into account. Though developing and training data-processing models is a complex topic, many businesses have implemented or intend to implement technology capable of handling more realistic applications. It is not possible to acquire an accurate result from deep learning projects if dataset quality is not evaluated correctly. In order for the model to learn from the data and produce useful predictions, the data must first be organized in such a way that the analysis can give useful results. Moreover, models must consume clean datasets while maintaining fresh incoming data while processing and analyzing data insights.

4.2.2.2. Data Cleaning

The dimensionality and sheer volume of the data necessitate effective data pre-processing to format and clean the data before training. The deep learning model does not accept string data type. The original WUSTL-EHMS-2020 dataset contains one feature with string data type which is “Sport”. We simply remove this attribute from the dataset in order to provide appropriate input for deep learning model.

Next, we convert nominal data type attributes into numeric data type. In WUSTL-EHMS-2020 dataset, there are six attributes with nominal data type which are “Dir”, “Flgs”, “SrcAddr”, “DstAddr”, “SrcMac”, “DstMac”. We use factorization to convert these nominal data type attributes into numeric data type. The value count of attribute “Flgs” before and after conversion from nominal to numeric data type is shown in Figure 4.2.

Name: Flgs	**dtype: int64**
e	15237
M	924

Name: Flgs	**dtype: int64**
0	15237
1	924

eR	138
e s	8
M *	7
M d	3
MR	1

(a) Nominal data type before conversion

2	138
4	8
3	7
5	3
6	1

(b) Numeric data type after conversion

Figure 4.2: Value Count of attribute "Flgs".

Next, we check the data if there is a possibility that part of the data is corrupt or missing. Missing data can introduce significant bias, making data management and analysis more complex while also decreasing accuracy. The WUSTL-EHMS-2020 dataset does not contain any null values.

4.2.2.3. Data Normalization

Data normalization is notably useful for systems where measurements are typically represented on a wide range of levels. Normalization approaches can significantly reduce the training time of model. It normalizes every feature such that the contribution of each feature is maintained, despite the fact that some features have larger numerical values than others. As a result of this, the model will remain unbiased [108]. In this model, we use Z-Score normalization. Z-Score normalization also known as zero-mean normalization is an approach of data normalization that avoids the outlier problem. In this strategy, values are normalized using the mean (μ) and standard deviation (σ) of the data. In this

technique, the data is transformed through value conversion to a common scale with an average mean of "0" and a standard deviation of "1". Technically, it calculates the standard deviations above or below the mean.

Equation 4.1 shows the Z-Score normalization formula:

$$z = \frac{x - \mu}{\sigma}$$

- **z**: new value
- **x**: original value
- **μ**: mean
- σ: standard deviation

A data point with a positive z-score value means it is above average. A data point with a negative z-score value means it is below average. A data point with z-score value close to "0" indicates that it is close to the average. If the z-score value of a data point is more than "3" or less than "-3", it is considered unusual. Figure 4.3 shows a part of normalized dataset.

	Dir	Flgs	SrcAddr	DstAddr	Dport	SrcBytes	DstBytes	SrcLoad	DstLoad	SrcGap	...	DstMac	Packet_num	Temp	SpO2	Pulse_Rat
3649	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.598828	0.277197	0.0	...	0.0	-0.969152	0.099862	0.167928	2.68925
6631	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.793409	0.371366	0.0	...	0.0	-0.334185	-0.662737	-0.812403	-0.91607
11293	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.264085	0.115223	0.0	...	0.0	0.658843	1.407176	0.167928	-0.50007
11135	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.398000	0.180024	0.0	...	0.0	0.625188	1.734004	0.167928	-0.50007
14350	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.348435	0.156039	0.0	...	0.0	1.309999	-1.970051	0.167928	-0.50007
14912	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.608328	0.281806	0.0	...	0.0	1.429707	-0.118023	0.167928	-0.50007
15143	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.542392	0.249894	0.0	...	0.0	1.478911	-0.009080	0.167928	-0.50007
4272	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.371395	0.167156	0.0	...	0.0	-0.836450	-0.553794	0.167928	-0.08407
7123	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	0.417100	0.189260	0.0	...	0.0	-0.229387	-0.335909	0.167928	0.88658
52	0.0	-0.238173	0.0	0.0	0.0	-0.017063	-0.055604	-0.082253	-0.052375	0.0	...	0.0	-1.734691	2.060833	-4.733730	0.60925

Figure 4.3: A part of normalized dataset.

4.2.2.4. Feature Selection and Extraction

The dataset size can be too enormous for data analysis techniques to manage. One possible option is to develop a simplified representation of the data that is substantially less in bulk but delivers comparable analytical findings. In this framework, dimensionality reduction is used in order to perform feature selection. Feature selection is a fundamental topic in DL that has a significant impact on prediction accuracy. Our outcomes are heavily influenced by the data attributes used to train DL models. Feature selection is the process of picking a subset of relevant attributes based on particular assessment criteria. By using feature selection, we can reduce training time, improve accuracy, and reduce over-fitting.

Before implementing any model, it is critical to eliminate noisy data, identify valuable characteristics that aid in achieving accurate findings, and minimize the dimensionality and complexity of the dataset. As a result, feature selection is a key step in improving data clarity and reducing training time for deep learning models. In general, the process of feature selection is divided into three stages. It begins with the selection of a subset of initial features and the assessment of each feature's value within the subset. Second, certain subset features may be enumerated or eliminated from the already existing subset using this evaluation. Finally, it uses a set of evaluation criteria to see if the resulting subset is acceptable enough. This method eliminates irrelevant or redundant features or information from the dataset, resulting in improved classification accuracy and reduced computational costs.

In this framework, we utilize the CFS algorithm for feature selection. The correlation-based feature selection technique is a filter strategy; hence it is not affected by the classification model. CFS assesses feature subsets only on data intrinsic qualities, as the name implies: correlations. The objective is to select a subset of features having a high feature-class correlation in order to maintain or boost predictive power, and low feature-feature correlation to prevent redundancy.

In addition to eliminating irrelevant features from the dataset, redundant features should also be removed. CFS ranks features based on correlations-based heuristic assessment function. The heuristic for determining the value or quality of a feature in a subset is important to the CFS algorithm. This heuristic considers the efficacy of individual features in predicting class label as well as the degree of inter-correlation among these features. This technique implies that irrelevant attributes have low correlations with the class; therefore they should be discarded by the algorithm. Excessive attributes, on the contrary, should be investigated since they are frequently highly correlated with other features.

The feature selection approach provided in this study is based on the following hypothesis:

"A good feature subset is one that contains features highly correlated with the class, yet uncorrelated with each other."

The heuristic is formalized in equation 4.1:

$$M_s = \frac{k\overline{r_{zJ}}}{\sqrt{k + k(k-1)\overline{r_{JJ}}}}$$

- **M_s:** the evaluation of the merit of subset "s"
- **k:** number of subset features
- **$\overline{r_{zJ}}$:** the average of feature and the external variable correlation
- **$\overline{r_{JJ}}$:** the average between features inter-correlation

Equation 4.1 is the Pearson's correlation coefficient with standardized variables. It is evident that we want the subset with the highest merit. It can be obtained with a high feature and the external variable correlation in the numerator and with a low inter-correlation between features. We use the best first search strategy using merit as a heuristic. The search begins with a subset that is completely empty and examines each feature's merit of being included in the empty set. The feature

inter-correlation can be ignored for this step since the above equation's denominator simplifies to 1 because of k=1.

$$M_s = \frac{k\overline{r_{zJ}}}{\sqrt{k + k(k-1)\overline{r_{JJ}}}}$$

$$= \frac{1\overline{r_{zJ}}}{\sqrt{1 + 1(1-1)\overline{r_{JJ}}}}$$

$$= \frac{\overline{r_{zJ}}}{\sqrt{1}}$$

$$= \overline{r_{zJ}}$$

As a result, the first iteration's evaluation is purely dependent on feature and the external variable correlation. The attribute with the highest feature and the external variable correlation is added to the subset that has so far been empty. In the next stage, all features are evaluated again, except the one that has already been added, and the feature that forms the finest subset with the already added one is preserved. This is an iterative process, and if expanding features does not result in an improvement, the algorithm returns to the best unexpanded subset. This method searches the entire feature subset space without limitation. As a result, there must be a limit on the total number of backtracks. When the algorithm reaches this limit, it returns the subset with the highest merit thus far.

In this framework, the algorithm returns the correlation matrix as shown in Figure 4.4 and a subset of 16 highly correlated features having a strong correlation coefficient value larger than 0.7. The correlated features are "DIA", "DIntPkt", "DstJitter", "DstLoad", "Dur", "Load", "Loss", "Rate", "SrcJitter", "TotBytes", "TotPkts", "pDstLoss", "pLoss", "pSrcLoss", "sMaxPktSz", "sMinPktSz". We drop these 16 features from the dataset in order to avoid data redundancy as well as data inconsistency.

	Dir	Flgs	SrcAddr	DstAddr	Dport	SrcBytes	DstBytes	SrcLoad	DstLoad	SrcGap	...	DstMac	Packet_num	Temp	SpO2
Dir	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
Flgs	NaN	1.000000	NaN	NaN	NaN	0.136860	0.222226	-0.443757	-0.179726	NaN	...	NaN	-0.012033	-0.040027	-0.089022
SrcAddr	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
DstAddr	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
Dport	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
SrcBytes	NaN	0.136860	NaN	NaN	NaN	1.000000	0.296669	-0.043144	-0.145572	NaN	...	NaN	-0.019253	0.005280	0.003388
DstBytes	NaN	0.222226	NaN	NaN	NaN	0.296669	1.000000	-0.149197	-0.118823	NaN	...	NaN	-0.005228	-0.005696	-0.017269
SrcLoad	NaN	-0.443757	NaN	NaN	NaN	-0.043144	-0.149197	1.000000	0.449880	NaN	...	NaN	-0.065340	0.041392	0.055028
DstLoad	NaN	-0.179726	NaN	NaN	NaN	-0.145572	-0.118823	0.449880	1.000000	NaN	...	NaN	-0.044381	0.011415	0.016399
SrcGap	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
DstGap	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
SIntPkt	NaN	0.164895	NaN	NaN	NaN	-0.115615	0.025619	-0.145135	0.599052	NaN	...	NaN	-0.015693	-0.014432	-0.018095
DIntPkt	NaN	0.329223	NaN	NaN	NaN	-0.117098	0.496770	-0.260439	0.378481	NaN	...	NaN	-0.015039	-0.016938	-0.036166
SIntPktAct	NaN	0.178623	NaN	NaN	NaN	0.070648	0.246458	-0.054305	-0.026431	NaN	...	NaN	-0.027801	0.002571	0.003395
DIntPktAct	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	NaN	...	NaN	NaN	NaN	NaN
SrcJitter	NaN	0.182383	NaN	NaN	NaN	0.077244	0.250207	-0.059341	-0.028971	NaN	...	NaN	-0.026926	0.002635	0.003498
DstJitter	NaN	0.367276	NaN	NaN	NaN	-0.068799	0.628322	-0.287013	0.313841	NaN	...	NaN	-0.009676	-0.021331	-0.039601
sMaxPktSz	NaN	0.028161	NaN	NaN	NaN	0.802138	0.393258	-0.026869	-0.013075	NaN	...	NaN	-0.011462	0.004313	0.001697

Figure 4.4: A part of correlation matrix for the dataset.

4.2.2.5. Train-Test Split

In this step, we divide the dataset into two subsets: train subset and test subset. Train dataset is used to train or fit the deep learning model whereas; test dataset is used to evaluate the performance of the deep learning model. In this framework, we split the dataset into 60/40 ratio. 60% of the dataset is used for training the model whereas; 40% of the dataset is used for evaluating the model. Further, the test dataset is divided into test and validation datasets with a ratio of 20/20 which means 20% of data subset is used for testing whereas; 20% of data subset is used for validation.

4.2.3. Methodology

On a high level, LSTM functions similarly to an RNN cell. LSTMs are a kind of RNN that can learn long-term dependencies. Long-term memory is basically their default behavior; it is not something they have to work hard to learn. The training

of LSTM-IDS is clearly divided into two parts: forward and backward propagation. Forward Propagation is in charge of computing the output values, whereas Backward Propagation is in charge of transmitting the collected residuals to adjust or update the weights. This is not substantially different from standard neural network training. Long Short-Term Memory is an enhanced RNN, or sequential network, that permits information to be stored. All RNNs are made up of a chain of repeated neural network modules. This repeating module in ordinary RNNs will have a relatively basic structure, with a single layer of tanh. LSTMs have a chain-like structure as well, but the structure of repeating module is different. There are four neural network layers instead of a single layer, and they interact in a unique way. The LSTM network's internal workings are shown here. As seen in the Figure 4.3 below, the LSTM is composed of three parts, each of which serves a distinct function.

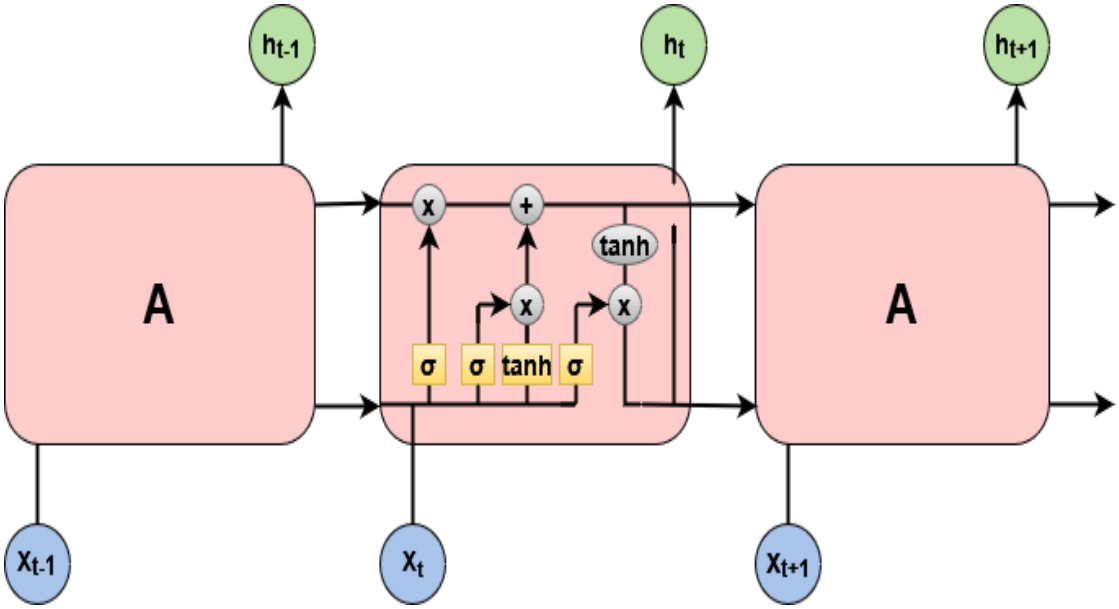


Figure 4.4: Internal functioning of LSTM network. Diagram adapted from [110].

4.2.3.1. Architecture of the Proposed Model

LSTM, like any other neural network, includes layers that enable it to learn and detect patterns for improved performance. The fundamental operation of an

LSTM can be thought of as holding the necessary information and discarding the information that is not essential or beneficial for further prediction. An LSTM network is made up of several memory blocks known as cells. The cell can remember values across arbitrary time periods. Two states are passed to the succeeding cell; the hidden state and the cell state. It is made up of four interacting layers to produce the cell's output as well as the cell state. The succeeding hidden layer receives these two things. There are four neural network layers, three sigmoid gates, and a tanh layer, instead of a single layer, and they interact in a unique way. Memory blocks are in charge of remembering things, and modifications of this memory are carried out by three primary processes known as gates. Gates have been added to limit the amount of information that may flow through the cell. These gates decide which information the next cell needs and which will be discarded. The result is often in the 0-1 range, where “0” means “reject all” and “1” means “include all”. Each of these is discussed in detail below.

4.2.3.1.1. The Forget Gate

The first step in an LSTM network cell is to select whether to retain or discard the information from the preceding timestamp. One of the primary aspects of the LSTM is its ability to memorize and identify information flowing into the network, as well as reject information that is not necessary for the network to learn data and make predictions. This aspect of the LSTM is controlled by this gate. A sigmoid layer known as the "forget gate layer" makes this decision. It helps in determining whether or not information can flow through the network layers. In order to optimize the performance, the information that is not needed by the LSTM to comprehend things or information that is of lesser value is eliminated by multiplying a filter. The internal working of the Forget Gate is shown in Figure 4.4.

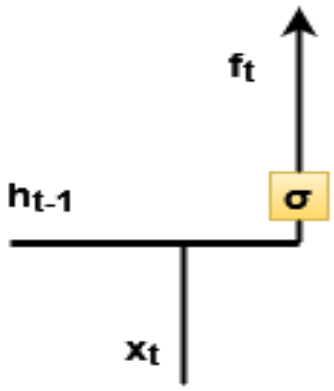


Figure 4.5: Internal functioning of Forget Gate.

The forget gate equation is as follows:

$$\mathbf{f_t = \sigma(W_f . [h_{t-1}, x_t] + b_f)}$$

h_{t-1} and x_t are the two inputs to this gate. h_{t-1} is the preceding cell's hidden state or its output, whereas x_t represents the input at that timestamp. The inputs given are multiplied by weight matrices, and then bias is added. The sigmoid function is then applied to this resulting value. The sigmoid function returns a vector containing values in the 0-1 range, one for each cell state number. The sigmoid function determines which values to preserve and which to reject. If the forget gate outputs a "0" for a specific cell state value, it signifies that the forget gate desires that the cell state fully forget that information. A "1" indicates that the forget gate needs to remember the complete piece of information. The cell state is multiplied by the vector output of the sigmoid function.

4.2.3.1.2. The Input Gate

The next stage is to determine what new information will be stored in the cell state. The input gate is in charge of updating the cell state with new information. It determines the significance of the information. The input gate aids the forget function in eliminating unimportant information while helping other layers learn

the essential information for making predictions. This information addition is a three-step procedure, as seen in the Figure 4.5 below.

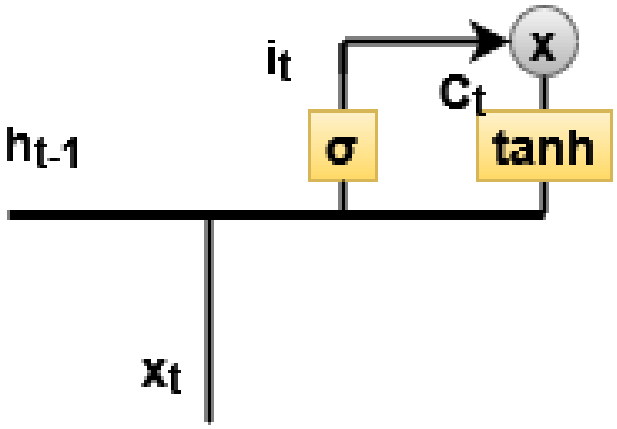


Figure 4.6: Internal functioning of Input Gate.

1. A sigmoid function is used to control which values must enter into the cell. This works similarly to the forget gate in that it filters all of the information from x_t and h_{t-1}.
2. Creating a vector that contains all potential values that may be added to the cell state (as determined by h_{t-1} and x_t). This is accomplished with the "tanh" function, which returns values in the -1 to +1 range.
3. The regulatory filter value i.e. the sigmoid gate is multiplied by the produced vector i.e. the tanh function. This beneficial information is subsequently added to the cell state using the addition operation.

After we've completed this three-step procedure, we make sure that the cell state is updated using only the most significant and non-redundant information.

The input gate equations are as follows:

$$\mathbf{i_t = \sigma(W_i . [h_{t-1}, x_t] + b_i)}$$

$$\widetilde{C}_t = \tanh(W_C . [h_{t-1}, x_t] + b_C)$$

4.2.3.1.3. The Output Gate

Finally, we must determine what we will output. The cell state will be the basis for this output, but it will be filtered. It is the circuit's last gate, and it aids in determining the network's next hidden state, in which information passes via the sigmoid function. The cell state's updated cell is sent to the "tanh" function, which is then multiplied by the output state's sigmoid function. This aids the hidden state in carrying the information. The internal working of output gate is shown in Figure 4.6.

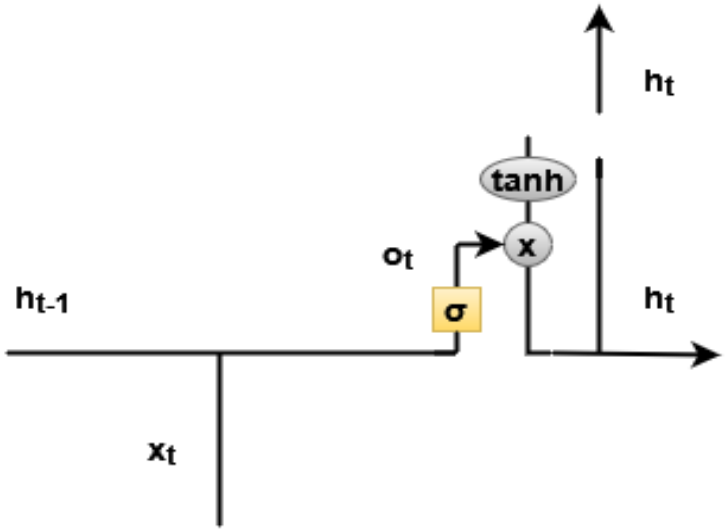


Figure 4.7: Internal functioning of Output Gate.

The operation of the output gate can be broken down into three steps:

1. After applying the tanh function on the cell state, the values are scaled to the -1 to +1 range, resulting in the creation of a vector.
2. Making a filter with the values of x_t and h_{t-1} so that it may control the values that must be output from the previously created vector. A sigmoid function is used once again in this filter.

3. Multiplying the regulatory filter value by the vector formed in step 1 and forwarding it as an output as well as to the next cell's hidden state.

A typical LSTM unit's final outputs are the current state and the current hidden state.

The output gate equations are as follows:

$$\mathbf{o_t = \sigma(W_o . [h_{t-1}, x_t] + b_o)}$$

$$\mathbf{h_t = o_t * \tanh(C_t)}$$

CHAPTER NO. 5

RESULTS AND DISCUSSIONS

In this section, we discuss the results of our proposed framework and evaluate the results based on evaluation metrics provided below. We also compare our results with existing state-of-the-art intrusion detection models in order to evaluate the performance of our framework.

5.1. Evaluation Metrics

To increase our model's performance, we discuss confusion matrix and compute the accuracy, recall, precision, true positive (TP) rate, false positive (FP) rate, and F-measure. A model is optimized using performance metrics. The metrics described below are utilized to evaluate the performance of our model.

5.1.1. Confusion Matrix

A confusion matrix summarizes the predicted outcomes of classification problems. It compares the actual outcomes to the predicted outcomes of the deep learning model. This provides us with a comprehensive picture of how well the classification model is working and the types of errors it makes. The rows in the confusion matrix represent actual classes, whereas the columns represent predicted classes. The matrix is used to derive additional information regarding model performance. The confusion matrix allows us to see whether the classification model is "confused" when it comes to distinguishing between the actual and predicted classes. To summarize, when the prediction is incorrect, the word used is “false”. It is “true” otherwise. The aim is to increase the metrics that contain the term “true” while minimizing the metrics that contain the term “false”. A confusion matrix is depicted in Figure 5.1.

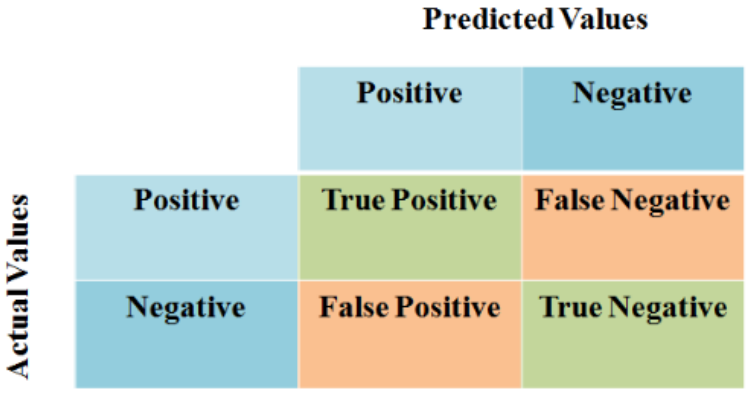


Figure 5.1: A Confusion Matrix

The four metrics of the matrix are as follows:

- **True Positive (TP):** True positives are outputs in which the positive class is predicted correctly by the model.
- **True Negative (TN):** True negatives are outputs in which the negative class is predicted correctly by the model.
- **False Positive (FP):** False Positives are outputs in which the positive class is predicted incorrectly by the model.
- **False Negative (FN):** False Negatives are outputs in which the negative class is predicted incorrectly by the model.

The three basic measures which we used to evaluate our model are described next:

5.1.2. Accuracy

Accuracy is the ratio of the total number of correctly predicted instances to the total predictions. It is calculated as:

$$\boldsymbol{Accuracy} = \frac{\boldsymbol{TP} + \boldsymbol{TN}}{\boldsymbol{TP} + \boldsymbol{TN} + \boldsymbol{FP} + \boldsymbol{FN}}$$

5.1.3. Precision

Precision is the ratio of correct positive outcomes to the total number of positively classified samples.

$$\boldsymbol{Precision = \frac{TP}{TP + FP}}$$

5.1.4. Recall

Recall is the ratio of correct positive outcomes to the total number of relevant samples.

$$\boldsymbol{Recall = \frac{TP}{TP + FN}}$$

5.1.5. False Positive Rate

It is the ratio of negative data instances that is incorrectly considered positive when compared to all the negative data instances.

$$\boldsymbol{FPR = \frac{FP}{FP + TN}}$$

5.1.6. F1-Score

The harmonic mean between recall and precision values is F1-Score. The value of F1-Score ranges between 0 and 1.

$$\boldsymbol{F1 - Score = 2 * \frac{Precision * Recall}{Precision + Recall}}$$

5.2. Experimental Results

This section describes our framework's evaluation process and demonstrates that the method provides high confidence in securing IoMT-based SHS from malicious traffic.

To train the model we use the activation function "tanh", learning rate of "0.0001", batch size of "256", "Adam" optimizer, and "100" epochs. We train the

model using 4 hidden layers of with 128, 64, 32, 16 neurons respectively. Table 5.2 summarizes the selection of various hyper-parameters.

Table 5.1: The values of the various hyper-parameters

Hyper-parameters	**Values**
Hidden layers	4
Number of neurons in hidden layers respectively	128, 64, 32, 16
Number of epochs	100
Batch size	256
Activation function	tanh
Optimizer	Adam
Learning rate	0.0001
Loss function	Binary Cross Entropy

Figure 5.2 presents the summary of the LSTM model.

```
_________________________________________________________________
 Layer (type)                 Output Shape              Param #
=================================================================
 lstm_49 (LSTM)               (None, 26, 128)           66560

 lstm_50 (LSTM)               (None, 26, 64)            49408

 lstm_51 (LSTM)               (None, 26, 32)            12416

 lstm_52 (LSTM)               (None, 26, 16)            3136

 dense_24 (Dense)             (None, 26, 1)             17

=================================================================
Total params: 131,537
Trainable params: 131,537
Non-trainable params: 0
_________________________________________________________________
```

Figure 5.2: Summary of LSTM model

Table 5.3 summarizes the epoch-by-epoch trend of train and validation loss and accuracy. The loss trend for train subset continues to decrease in the beginning and then it increases and decreases at small irregular intervals. The loss trend for validation dataset increases and decreases till epoch 40 and then it becomes stable. The accuracy trend for train subset continues to decrease in the beginning and then it increases and decreases at small irregular intervals till the last epoch. The accuracy trend for validation dataset increases and decreases till epoch 40 and then it becomes stable till the last epoch.

Table 5.2: Summary of the epoch-by-epoch trend of loss and accuracy.

Epoch	Loss	Accuracy	Val_loss	Val_accuracy
0	0.060443	0.932645	0.052642	0.938584
1	0.044623	0.950011	0.045200	0.950450

2	0.038885	0.958676	0.041062	0.956413
3	0.036965	0.960922	0.040256	0.956778
4	0.040720	0.956690	0.062603	0.933022
5	0.044974	0.950858	0.040199	0.956036
95	0.033337	0.963923	0.037958	0.958616
96	0.034746	0.962258	0.038026	0.958604
97	0.034425	0.962689	0.037957	0.958616
98	0.033860	0.963314	0.037938	0.958604
99	0.035480	0.961408	0.038050	0.958604

Figure 5.3 depicts the epoch-by-epoch trend of train and validation loss. The loss trend for train and validation sets is similar and after a few epochs it converges. The graph shows that the train loss decreases to a point and then continues to show an increasing and decreasing trend at small irregular intervals. The graph of validation loss decreases with each epoch and continues to decrease till the last epoch.

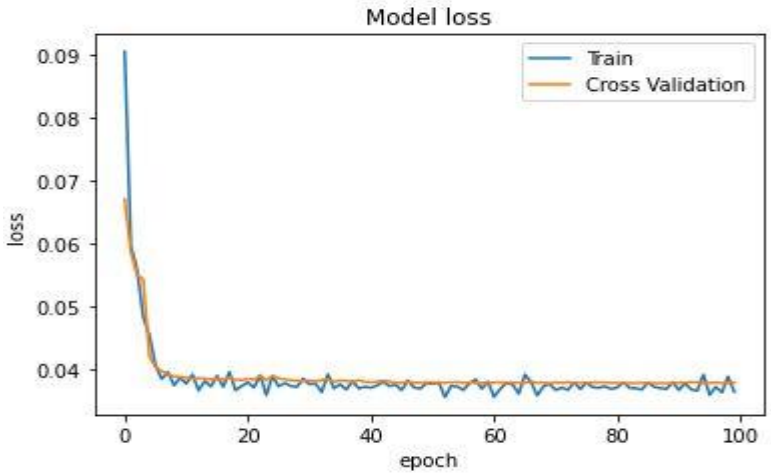


Figure 5.3: The epoch-by-epoch trend of train and validation loss.

Figure 5.4 depicts the epoch-by-epoch trend of train and validation accuracy. The values of accuracy trend for train and validation sets have very small difference. The graph shows that the train accuracy initially shows increasing and decreasing trend to a few epochs and then it becomes nearly stable with very little change till the last epoch. The graph of validation accuracy initially increases to a point and then shows an increasing and decreasing trend at irregular intervals with each epoch and continues to show this trend till the last epoch.

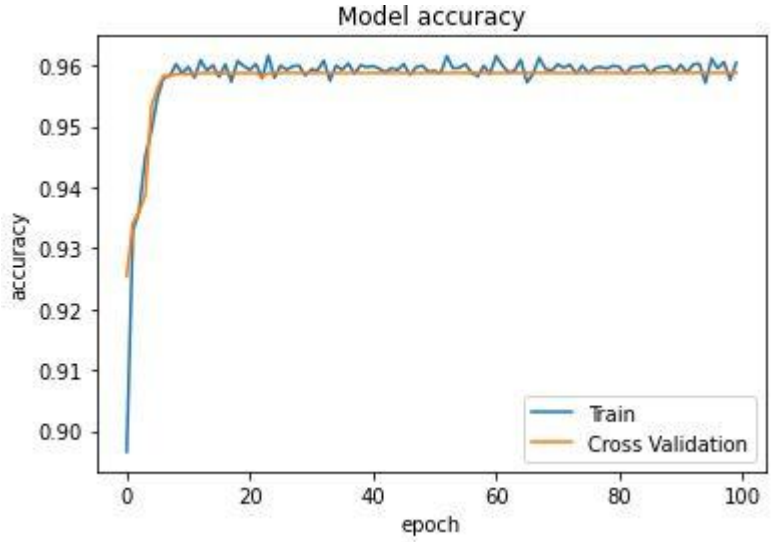


Figure 5.4: The epoch-by-epoch trend of train and validation accuracy.

We also evaluate our proposed model's efficiency in terms of computation time. The computation time is critical when evaluating the performance of a classifier, especially in the age of big data, because massive amounts of data are required for real-time classification. We evaluate our model using train, validation, and test datasets. Table 5.3 shows the train and test evaluation time for the proposed approach. Furthermore, shows the evaluation loss and accuracy for train, validation, and test datasets.

Table 5.3: Summary of evaluation results of train, validation, and test datasets.

Dataset	**Accuracy**	**Loss**	**Time (s)**	**Time per Epoch (ms/step)**
Train Set	0.9570	0.0395	17	43
Validation Set	0.9615	0.0360	4	37
Test Set	0.9613	0.0362	4	39

Furthermore, we evaluate our proposed model's efficiency in terms of confusion metrics defined above. We evaluate our model using TP, FP, TN, and FN. The confusion matrix shows the values as: TP=2094, FP=78, TN=1044, and FN=48. Figure 5.5 shows the confusion matrix for the binary classifier.

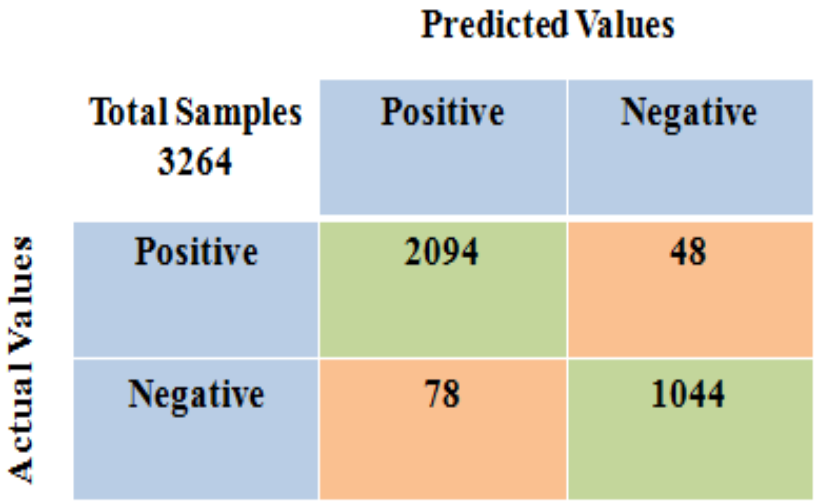


Figure 5.5: Confusion matrix for WUSTL-EHMS-2020 test dataset.

In this research, we focus on binary classification in which each observation is classified as either normal or anomalous data. For our deep learning model, we analyze the F-score, recall, precision, and accuracy values. Table 5.3 summarizes the results.

Table 5.4: Summary of evaluation metrics by class of WUSTL-EHMS-2020 test dataset.

Class	TP Rate	FP Rate	Precision	Recall	F-measure
Normal	0.977	0.069	0.964	0.977	0.969
Anomaly	0.930	0.022	0.956	0.930	0.942
Weighted Average	0.961	0.053	0.961	0.961	0.959

The experimentation results depict that the proposed model shows a very high accuracy rate of 96% and True Positive Rate of 96.1% which is higher than its counterpart intrusion detection frameworks. The proposed model also shows a low False Positive Rate of 5.3% which is lower than its counterpart intrusion detection frameworks.

5.3. Discussion

In this subsection, we provide a comparison of results by visualization using column charts, bar charts, and area charts. The column chart in Figure 5.6 depicts accuracy and loss of train, test, and validation datasets converted into percentages.

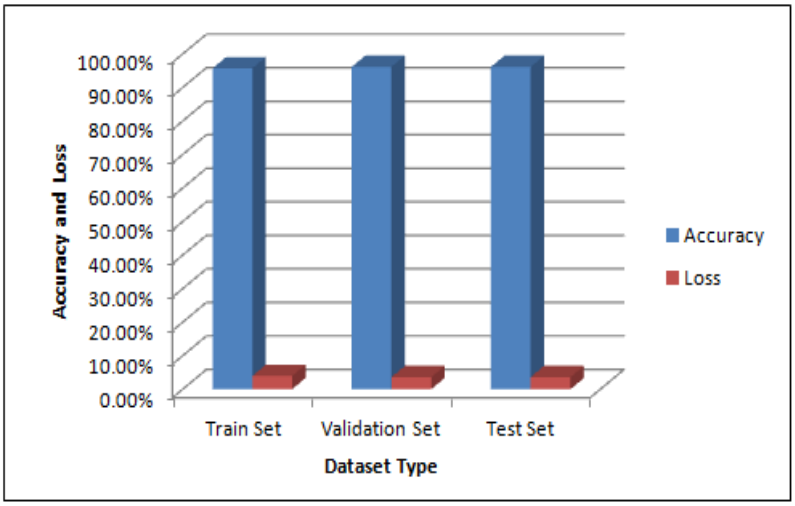


Figure 5.6: Column chart showing accuracy and loss percentages.

The bar chart in Figure 5.7 depicts the accuracy and loss values of train, test, and validation datasets on the scale of 0 to 1.

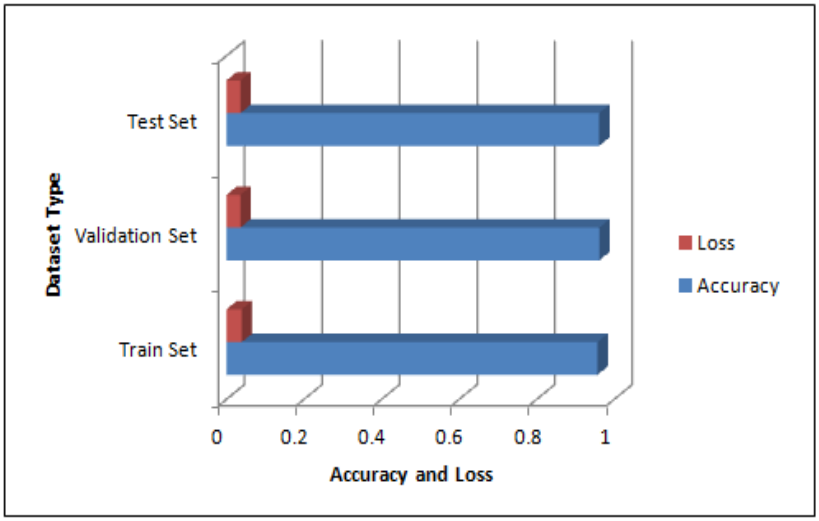


Figure 5.7: Bar chart showing accuracy and loss values.

In Figure 5.8, the area chart depicts the area covered by loss and accuracy values on the scale of 0 to 1.

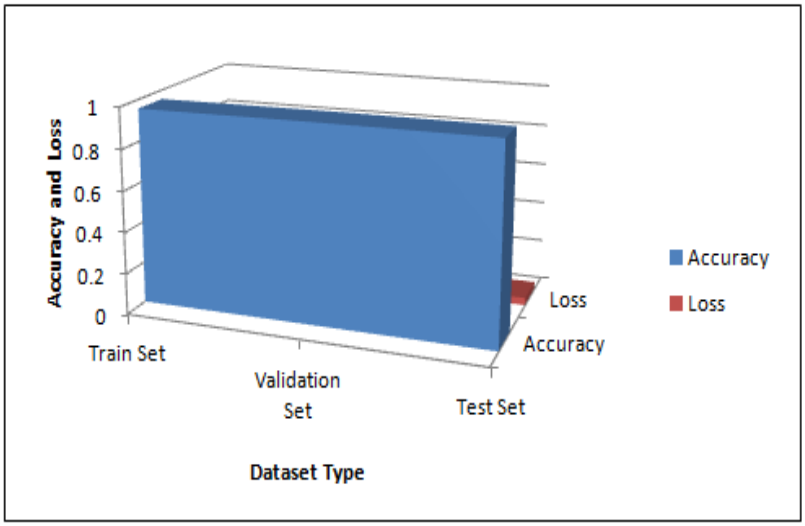


Figure 5.8: Area chart showing accuracy and loss values.

The column chart in Figure 5.9 shows the time taken by train, validation, and test datasets for evaluation. The chart depicts the total time taken by each of the datasets for evaluation as well as the time taken by each epoch to complete. The total time is represented in seconds(s) whereas; time per epoch is represented in millisecond per epoch (ms/step).

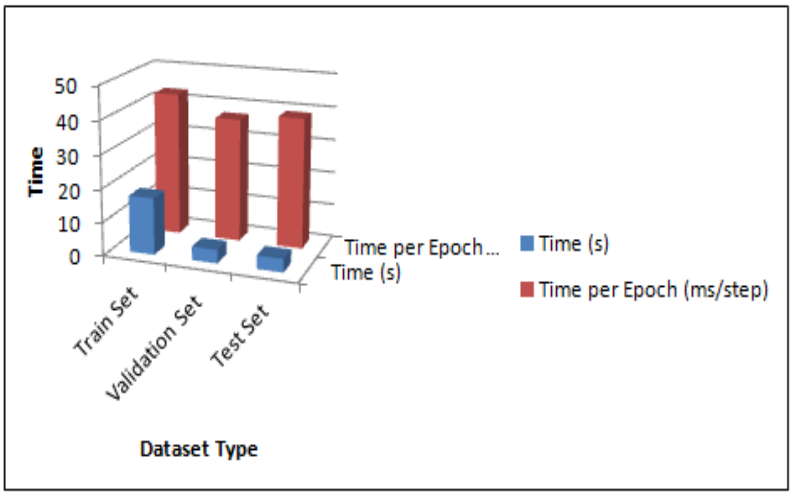


Figure 5.9: Column chart showing computational time.

The column chart in Figure 5.10 shows the time taken by train, validation, and test datasets for evaluation. The chart depicts the total time taken by each of the datasets for evaluation as well as the time taken by each epoch to complete. Here, the time per epoch is converted into seconds. Thus, the total time and time per epoch are represented in seconds(s).

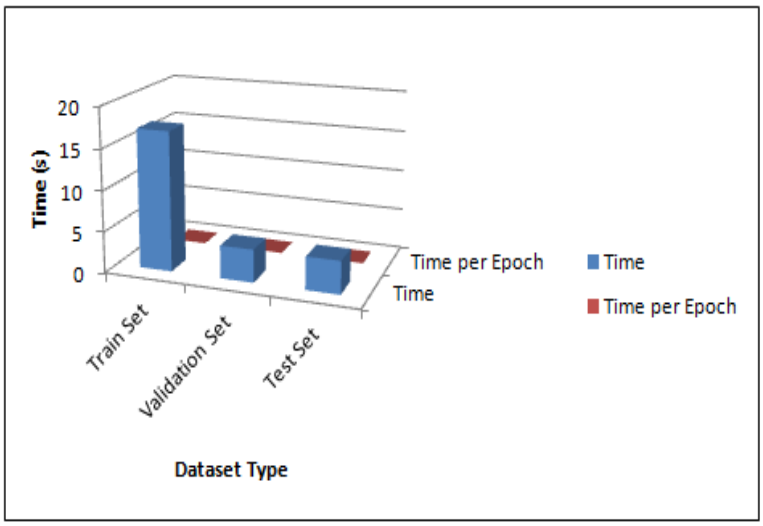


Figure 5.10: Column chart showing computational time in seconds.

The line graph in Figure 5.11 shows the five evaluation metrics used to evaluate our model and their corresponding values. The graph shows the evaluation metrics values for the normal and anomalous classification.

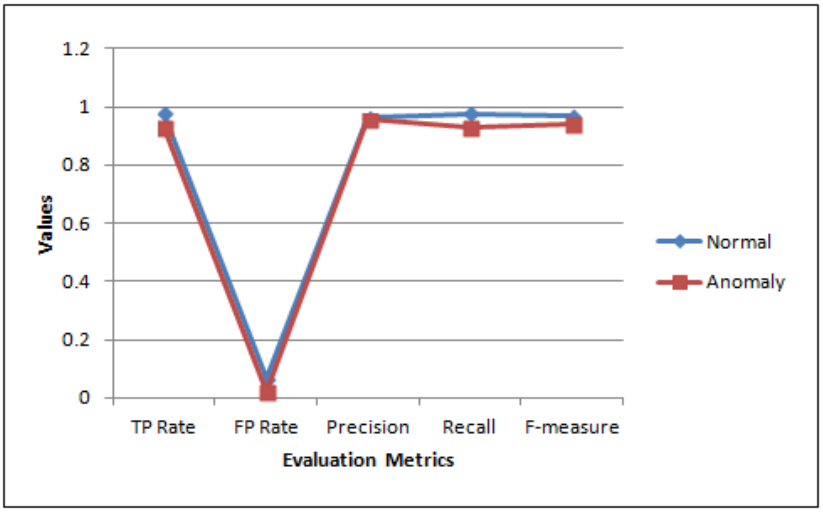


Figure 5.11: Line graph showing evaluation metrics and their corresponding values.

The line graph in Figure 5.12 shows the five evaluation metrics used to evaluate our model and their corresponding values converted into percentages. The graph shows the evaluation metrics values for the normal and anomalous classification.

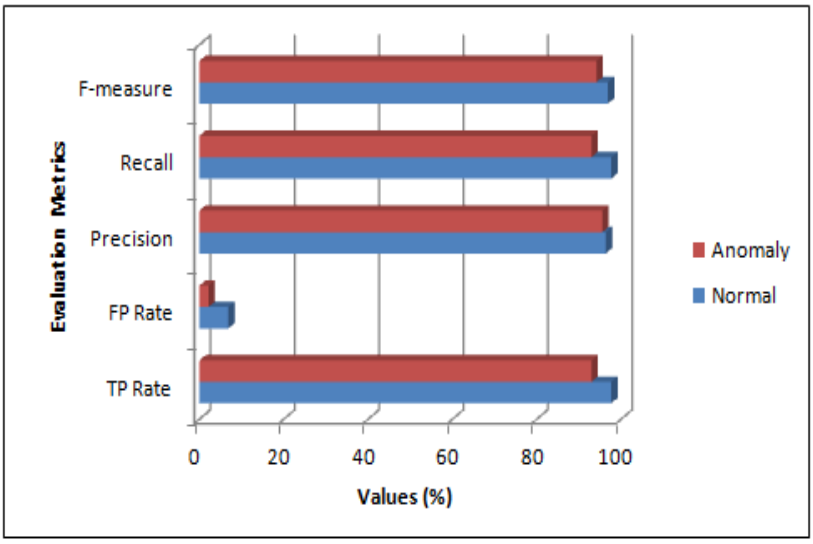


Figure 5.12: Bar Chart showing evaluation metrics and their corresponding values in percentages.

The evaluation results depict that the proposed model shows a very high accuracy rate of 96% and True Positive Rate of 96.1% which is higher than its counterpart intrusion detection frameworks. The proposed model also shows a low False Positive Rate of 5.3% which is lower than its counterpart intrusion detection frameworks.

5.4. Comparison with existing models:

In this subsection, we compare the performance accuracy of our proposed model with other existing models for intrusion detection. The intrusion detection model proposed in [112] using Siamese-CNN shows an accuracy of 93%. The PSO-LightGBM model proposed in [113] shows an accuracy rate of 86.68%. The SMOTE-ENSEMBEL-CNN-IDS proposed in [114] shows an accuracy rate of 92.45%. The intrusion detection model based on Deep Active Learning proposed in [115] gives an accuracy rate of 94%. The AE-CNN based intrusion detection framework proposed in [116] gives an accuracy rate of 93.99%. The intrusion detection model called GTO-BSA proposed in [117] shows an accuracy of 95.5% using NSL-KDD dataset. The comparison of accuracy of different intrusion detection models is given in Table 5.5.

Table 5.5: Comparison of accuracy of different intrusion detection models.

Model	Accuracy
Proposed IDS	96%
Siamese-CNN Model [112]	93%
PSO-LightGBM[113]	86.68%
SMOTE-ENSEMBEL-CNN-IDS [114]	92.72%
Active Learning-based IDS [115]	94%
AE-CNN [116]	93.99%
GTO-BSA using NSL-KDD [117]	95.5%

Figure 5.13 depicts the comparison of accuracy of different intrusion detection models which clearly shows that the proposed IDS has higher accuracy as compared to its counterpart intrusion detection models.

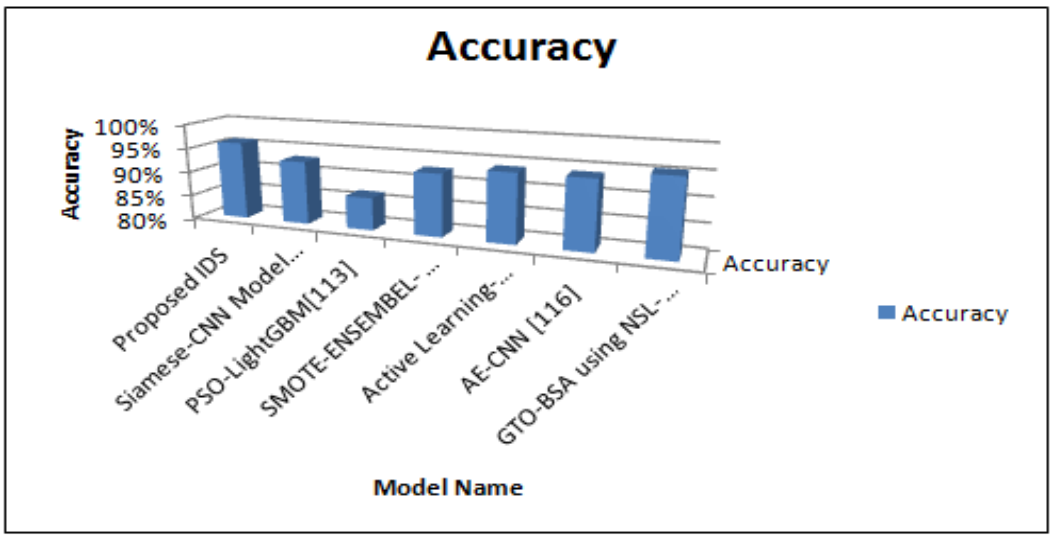


Figure 5.13: Comparison of accuracy of different intrusion detection models.

CONCLUSION

In recent years, smart healthcare has become increasingly popular. A smart healthcare system allows doctors and patients to connect with one another as well as remotely share information monitored, gathered, and analyzed from the everyday activities of patients via IoT. As a result, there is a substantial use of health data exchange for better, timely, and more accurate diagnosis. For smart healthcare systems, security and privacy protections are critical for patient safety, patient information privacy, and effective treatment. On the contrary, the healthcare sector accounts for the majority of data privacy issues and security breaches. Human and malware involvement for financial gain and theft of sensitive healthcare data for third-party use, pose a serious threat to healthcare data. Surprisingly, many existing smart healthcare systems do not place sufficient emphasis or effort on implementing security and privacy frameworks. This leads to major security flaws and privacy problems with sensitive personal data.

In this study, we designed a deep learning-based intrusion detection system to efficiently identify smart healthcare network intrusions by evaluating traffic flow data. We used the “Long Short-Term Memory (LSTM)” deep learning approach to identify malicious attacks and other security concerns in SHS. The basic operation of an LSTM can be regarded as storing the necessary information and discarding the information that is not needed or advantageous for further prediction. For feature selection, the CFS algorithm is used in which a subset of features is selected with a high feature-class correlation to retain or improve predictive power and a low feature-feature correlation to avoid redundancy. We evaluated the performance of the proposed system using Wustl-ehms-2020 IoMT dataset. The proposed system achieved the accuracy of 96%, which is greater than existing approaches. This study shows that our approach outperforms other cutting-edge intrusion detection systems.

LIMITATIONS

Deep learning-based models are becoming increasingly important and have emerged as an outstanding field of research. Deep learning techniques include various deep networks that can be utilized to enhance the performance of IDS. Deep learning models outperform machine learning models in terms of generalization and fitting. Furthermore, deep learning techniques are not dependent on domain expertise or feature engineering, giving them a significant advantage over machine learning techniques. However, the deep learning models take too long to execute in order to fulfill the real-time requirements of IDS, which is its limitation.

Furthermore, as the architecture grows larger, the deep learning-based model becomes more data hungry in order to deliver valid results. In such cases, data reuse may not be the best option, and data augmentation may be beneficial to some level, but having massive amount of data is always preferable. Furthermore, because of the complexity of the data models, training a deep learning model is an extremely expensive affair. They can require hundreds of computers and expensive GPUs, which raises the cost for users.

FUTURE WORK AND CHALLENGES

In future, we want to use deep learning to construct a real-time IDS for actual networks. Furthermore, feature learning using raw network traffic data headers rather than derived features might also be a high-impact research topic in this field. Moreover, interpretability is crucial for practical IDSs. Interpretability is described as "the ability to explain or communicate to a person in understandable words." The more interpretable a model is, the more easily it can be understood and trusted. Interpretable models are persuasive and can help people make decisions. That’s why model interpretability may become a major research focus for IDSs. In the future, we plan to develop an IDS based on interpretability so that it can make human-interpretable decisions and predictions.

Furthermore, blockchain should be viewed as a major possibility for providing reliable and secure SHS. Because blockchain is open and safe, it can be used in the healthcare sector to improve the security of healthcare records and patient privacy. The sensitivity of healthcare data is extremely high, which implies that protecting the integrity and accessibility of healthcare data by authorized users necessitates the development of intelligent security solutions. That’s why, we plan to develop and integrate blockchain-based security scheme into SHS for a more secured and reliable healthcare experience.

REFERENCES

1. Jiang, N., Wang, L. and Xu, X., 2021. Research on Smart Healthcare Services: Based on the Design of APP Health Service Platform. *Journal of Healthcare Engineering*, *2021*.

2. Baker, S.B., Xiang, W. and Atkinson, I., 2017. Internet of things for smart healthcare: Technologies, challenges, and opportunities. *Ieee Access*, *5*, pp.26521-26544.

3. Yin, H., Akmandor, A.O., Mosenia, A. and Jha, N.K., 2018. Smart healthcare.

4. Zhao, W., Luo, X. and Qiu, T., 2017. Smart healthcare. *Applied Sciences*, *7*(11), p.1176.

5. Pattnaik, P.K., Vaidya, A., Mohanty, S., Mohanty, S. and Hol, A. eds., 2022. *Smart Healthcare Analytics: State of the Art*. Springer.

6. Gupta, P., Agrawal, D., Chhabra, J. and Dhir, P.K., 2016, March. IoT based smart healthcare kit. In *2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT)* (pp. 237-242). IEEE.

7. Li, W., Chai, Y., Khan, F., Jan, S.R.U., Verma, S., Menon, V.G. and Li, X., 2021. A comprehensive survey on machine learning-based big data analytics for IoT-enabled smart healthcare system. *Mobile Networks and Applications*, *26*(1), pp.234-252.

8. Budida, D.A.M. and Mangrulkar, R.S., 2017, March. Design and implementation of smart HealthCare system using IoT. In *2017 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1-7). IEEE.

9. Jeong, J.S., Han, O. and You, Y.Y., 2016. A design characteristics of smart healthcare system as the IoT application. *Indian Journal of Science and Technology*, *9*(37), p.52.

10. Yang, G., Jan, M.A., Menon, V.G., Shynu, P.G., Aimal, M.M. and Alshehri, M.D., 2020. A centralized cluster-based hierarchical approach for green communication in a smart healthcare system. *IEEE Access*, *8*, pp.101464-101475.

11. Shukla, R.G., Agarwal, A. and Shukla, S., 2020. Blockchain-powered smart healthcare system. In *Handbook of research on blockchain technology* (pp.

245-270). Academic Press.

12. Vaiyapuri, T., Binbusayyis, A. and Varadarajan, V., 2021. Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. *International Journal of Advanced Computer Science and Applications*, *12*(2), pp.731-737.

13. Alshehri, F. and Muhammad, G., 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access*, *9*, pp.3660-3678.

14. Islam, M. and Rahaman, A., 2020. Development of smart healthcare monitoring system in IoT environment. *SN computer science*, *1*(3), pp.1-11.

15. Ahad, A., Tahir, M. and Yau, K.L.A., 2019. 5G-based smart healthcare network: architecture, taxonomy, challenges and future research directions. *IEEE access*, *7*, pp.100747-100762.

16. Vishnu, S., Ramson, S.J. and Jegan, R., 2020, March. Internet of medical things (IoMT)-An overview. In *2020 5th international conference on devices, circuits and systems (ICDCS)* (pp. 101-104). IEEE.

17. Hossain, M.S., Muhammad, G. and Alamri, A., 2019. Smart healthcare monitoring: a voice pathology detection paradigm for smart cities. *Multimedia Systems*, *25*(5), pp.565-575.

18. Sakr, S. and Elgammal, A., 2016. Towards a comprehensive data analytics framework for smart healthcare services. *Big Data Research*, *4*, pp.44-58.

19. Karthick, R., Ramkumar, R., Akram, M. and Kumar, M.V., 2021. Overcome the challenges in bio-medical instruments using IOT–A review. *Materials Today: Proceedings*, *45*, pp.1614-1619.

20. Papaioannou, M., Karageorgou, M., Mantas, G., Sucasas, V., Essop, I., Rodriguez, J. and Lymberopoulos, D., 2020. A survey on security threats and countermeasures in internet of medical things (IoMT). *Transactions on Emerging Telecommunications Technologies*, p.e4049.

21. Muhammad, G., Rahman, S.M.M., Alelaiwi, A. and Alamri, A., 2017. Smart health solution integrating IoT and cloud: A case study of voice pathology monitoring. *IEEE Communications Magazine*, *55*(1), pp.69-73.

22. Selvaraj, S. and Sundaravaradhan, S., 2020. Challenges and opportunities in IoT healthcare systems: a systematic review. *SN Applied Sciences*, *2*(1), pp.1-8.

23. Tekeste, T., Saleh, H., Mohammad, B. and Ismail, M., 2018. Ultra-low power QRS detection and ECG compression architecture for IoT healthcare devices. *IEEE Transactions on Circuits and Systems I: Regular Papers*, *66*(2), pp.669-679.

24. Newaz, A.I., Haque, N.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S., 2020, December. Adversarial attacks to machine learning-based smart healthcare systems. In *GLOBECOM 2020-2020 IEEE Global Communications Conference* (pp. 1-6). IEEE.

25. Tariq, N., Qamar, A., Asim, M. and Khan, F.A., 2020. Blockchain and smart healthcare security: a survey. *Procedia Computer Science*, *175*, pp.615-620.

26. Habibzadeh, H. and Soyata, T., 2020. Toward uniform smart healthcare ecosystems: A survey on prospects, security, and privacy considerations. In *Connected Health in Smart Cities* (pp. 75-112). Springer, Cham.

27. Marshal, R., Gobinath, K. and Rao, V.V., 2021, April. Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks. In *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)* (pp. 1-4). IEEE.

28. Butt, S.A., Diaz-Martinez, J.L., Jamal, T., Ali, A., De-La-Hoz-Franco, E. and Shoaib, M., 2019, July. IoT smart health security threats. In *2019 19th International Conference on computational science and its applications (ICCSA)* (pp. 26-31). IEEE.

29. Sethuraman, S.C., Vijayakumar, V. and Walczak, S., 2020. Cyber attacks on healthcare devices using unmanned aerial vehicles. *Journal of medical systems*, *44*(1), pp.1-10.

30. Muthuppalaniappan, M. and Stevenson, K., 2021. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. *International Journal for Quality in Health Care*, *33*(1), p.mzaa117.

31. Muthuppalaniappan, M., & Stevenson, K. 2021, *Cyber-attacks on healthcare indicate criminals never let go of opportunity*, International journal for quality in health care : journal of the International Society for Quality in Health Care, viewed 12 Feb 2022, < https://pubmed.ncbi.nlm.nih.gov/33351134/>

32. Dorian, R. 2021, *Cyber attacks in healthcare: the position across Europe*, Pinsent Masons LLP, viewed 12 Feb 2022, <https://www.pinsentmasons.com/out law/analysis/cyber-attacks-healthcare-europe>

33. Marianne. M 2021, *EU Report Calls for More Health-Specific Incident Response*, Information Security Media Group, Corp, viewed 12 Feb 2022, < https://www.govinfosecurity.com/eu-report-calls-for-more-health-specific-incident-response-a-17923 >

34. Almogren, A., Mohiuddin, I., Din, I.U., Almajed, H. and Guizani, N., 2020. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet of Things Journal*, *8*(6), pp.4485-4497.

35. Deyan, G. 2022, *25+ Alarming Healthcare Data Breaches Statistics 2022 [& The Largest Healthcare Data Breaches]*, TechJury.net, viewed 14 Feb 2022, < https://techjury.net/blog/healthcare-data-breaches-statistics/#gref >

36. Alam, A. J., Veilleux, C. B., 2021, 'Smart Health and Cybersecurity in the Era of Artificial Intelligence', in I. Dey (ed.), Computer-Mediated Communication, IntechOpen, London. 10.5772/intechopen.97196.

37. Ambarkar, S.S. and Shekokar, N., 2020. Toward smart and secure IoT based healthcare system. In *Internet of Things, Smart Computing and Technology: A Roadmap Ahead* (pp. 283-303). Springer, Cham.

38. Koutras, D., Stergiopoulos, G., Dasaklis, T., Kotzanikolaou, P., Glynos, D. and Douligeris, C., 2020. Security in IoMT communications: A survey. *Sensors*, *20*(17), p.4828.

39. Sejnowski, T.J., 2018. *The deep learning revolution*. MIT press.

40. Kelleher, J.D., 2019. *Deep learning*. MIT press.

41. Karunarathne, S.M., Saxena, N. and Khan, M.K., 2021. Security and privacy in IoT smart healthcare. *IEEE Internet Computing*, *25*(4), pp.37-48.

42. Bhattacharya, S., Somayaji, S.R.K., Gadekallu, T.R., Alazab, M. and Maddikunta, P.K.R., 2022. A review on deep learning for future smart cities. *Internet Technology Letters*, *5*(1), p.e187.

43. Vaiyapuri, T., Binbusayyis, A. and Varadarajan, V., 2021. Security, privacy and trust in iomt enabled smart healthcare system: A systematic review of current and future trends. *International Journal of Advanced Computer*

Science and Applications, *12*(2), pp.731-737.

44. Alshehri, F. and Muhammad, G., 2020. A comprehensive survey of the Internet of Things (IoT) and AI-based smart healthcare. *IEEE Access*, *9*, pp.3660-3678.

45. Iwendi, C., Anajemba, J.H., Biamba, C. and Ngabo, D., 2021. Security of things intrusion detection system for smart healthcare. *Electronics*, *10*(12), p.1375.

46. Gupta, D., Kayode, O., Bhatt, S., Gupta, M. and Tosun, A.S., 2021. Hierarchical Federated Learning based Anomaly Detection using Digital Twins for Smart Healthcare. *arXiv preprint arXiv:2111.12241*.

47. Newaz, A.I., Sikder, A.K., Rahman, M.A. and Uluagac, A.S., 2019, October. Healthguard: A machine learning-based security framework for smart healthcare systems. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)* (pp. 389-396). IEEE.

48. Yang, H., Shen, J., Lu, J., Zhou, T., Xia, X. and Ji, S., 2021. A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in the Smart Healthcare. *Security and Communication Networks*, *2021*.

49. Kore, A. and Patil, S., 2020. IC-MADS: IoT enabled cross layer man-in-middle attack detection system for smart healthcare application. *Wireless Personal Communications*, *113*(2), pp.727-746.

50. Al-Shammari, N.K., Syed, T.H. and Syed, M.B., 2021. An Edge–IoT framework and prototype based on blockchain for smart healthcare applications. *Engineering, Technology & Applied Science Research*, *11*(4), pp.7326-7331.

51. Selvakkumar, A., Pal, S. and Jadidi, Z., 2021. Addressing Adversarial Machine Learning Attacks in Smart Healthcare Perspectives. *arXiv preprint arXiv:2112.08862*.

52. Haque, N.I., Rahman, M.A., Shahriar, M.H., Khalil, A.A. and Uluagac, S., 2021. A novel framework for threat analysis of machine learning-based smart healthcare systems. *arXiv preprint arXiv:2103.03472*.

53. Hussain, F., Abbas, S.G., Shah, G.A., Pires, I.M., Fayyaz, U.U., Shahzad, F., Garcia, N.M. and Zdravevski, E., 2021. A framework for malicious traffic

detection in IoT healthcare environment. *Sensors*, *21*(9), p.3025.

54. Farhin, F., Kaiser, M.S. and Mahmud, M., 2021. Secured smart healthcare system: blockchain and bayesian inference based approach. In *Proceedings of international conference on trends in computational and cognitive engineering* (pp. 455-465). Springer, Singapore.

55. Sarosh, P., Parah, S.A., Bhat, G.M. and Muhammad, K., 2021. A security management framework for big data in smart healthcare. *Big Data Research*, *25*, p.100225.

56. Sun, Y., Liu, J., Yu, K., Alazab, M. and Lin, K., 2021. PMRSS: privacy-preserving medical record searching scheme for intelligent diagnosis in IoT healthcare. *IEEE Transactions on Industrial Informatics*, *18*(3), pp.1981-1990.

57. Muzammal, S.M., Shah, M.A., Khattak, H.A., Jabbar, S., Ahmed, G., Khalid, S., Hussain, S. and Han, K., 2018. Counter measuring conceivable security threats on smart healthcare devices. *IEEE Access*, *6*, pp.20722-20733.

58. Egala, B.S., Priyanka, S. and Pradhan, A.K., 2019, December. SHPI: Smart healthcare system for patients in ICU using IoT. In *2019 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1-6). IEEE.

59. Ghoneim, A., Muhammad, G., Amin, S.U. and Gupta, B., 2018. Medical image forgery detection for smart healthcare. *IEEE Communications Magazine*, *56*(4), pp.33-37.

60. Choi, J., Choi, C., Kim, S. and Ko, H., 2019, June. Medical information protection frameworks for smart healthcare based on IoT. In *Proceedings of the 9th International Conference on Web Intelligence, Mining and Semantics* (pp. 1-5).

61. Alabdulatif, A., Khalil, I., Yi, X. and Guizani, M., 2019. Secure edge of things for smart healthcare surveillance framework. *IEEE Access*, *7*, pp.31010-31021.

62. Khan, J., Li, J.P., Ahamad, B., Parveen, S., Haq, A.U., Khan, G.A. and Sangaiah, A.K., 2020. SMSH: Secure surveillance mechanism on smart healthcare IoT system with probabilistic image encryption. *IEEE Access*, *8*, pp.15747-15767.

63. Ma, M., He, D., Fan, S. and Feng, D., 2020. Certificateless searchable public key encryption scheme secure against keyword guessing attacks for smart healthcare. *Journal of Information Security and Applications*, *50*, p.102429.

64. Ma, M., He, D., Khan, M.K. and Chen, J., 2018. Certificateless searchable public key encryption scheme for mobile healthcare system. *Computers & Electrical Engineering*, *65*, pp.413-424.

65. Khan, J., Li, J., Haq, A.U., Parveen, S., Khan, G.A., Shahid, M., Ullah, S. and Ruinan, S., 2019, December. Medical Image Encryption Into Smart Healthcare IOT System. In *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing* (pp. 378-382). IEEE.

66. Manogaran, G., Thota, C., Lopez, D. and Sundarasekar, R., 2017. Big data security intelligence for healthcare industry 4.0. In *Cybersecurity for industry 4.0* (pp. 103-126). Springer, Cham.

67. Alraja, M.N., Barhamgi, H., Rattrout, A. and Barhamgi, M., 2021. An integrated framework for privacy protection in IoT—Applied to smart healthcare. *Computers & Electrical Engineering*, *91*, p.107060.

68. Quasim, M.T., Shaikh, A., Shuaib, M., Sulaiman, A., Alam, S. and Asiri, Y., 2021. Smart Healthcare Management Evaluation using Fuzzy Decision Making Method.

69. Zhou, T., Shen, J., He, D., Vijayakumar, P. and Kumar, N., 2020. Human-in-the-loop-aided privacy-preserving scheme for smart healthcare. *IEEE Transactions on Emerging Topics in Computational Intelligence*.

70. Anand, A., Singh, A.K., Lv, Z. and Bhatnagar, G., 2020. Compression-then-encryption-based secure watermarking technique for smart healthcare system. *IEEE MultiMedia*, *27*(4), pp.133-143.

71. Tripathi, G., Ahad, M.A. and Paiva, S., 2020, March. S2HS-A blockchain based approach for smart healthcare system. In *Healthcare* (Vol. 8, No. 1, p. 100391). Elsevier.

72. Senthilsingh, C., 2021. Blockchain Based Smart Healthcare Systems in 5G Networks For Preventing Data Forgery.

73. Haque, A.B., Muniat, A., Ullah, P.R. and Mushsharat, S., 2021, February. An automated approach towards smart healthcare with blockchain and smart contracts. In *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)* (pp. 250-255). IEEE.

74. Singh, A. and Chatterjee, K., 2021. Securing smart healthcare system with edge computing. *Computers & Security*, *108*, p.102353.

75. Al-Aswad, H., El-Medany, W.M., Balakrishna, C., Ababneh, N. and Curran, K., 2021. BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), pp.154-171.

76. Abdullah, S., Arshad, J., Khan, M.M., Alazab, M. and Salah, K., 2022. PRISED tangle: a privacy-aware framework for smart healthcare data sharing using IOTA tangle. *Complex & Intelligent Systems*, pp.1-19.

77. Wang, Z., Luo, N. and Zhou, P., 2020. GuardHealth: Blockchain empowered secure data management and Graph Convolutional Network enabled anomaly detection in smart healthcare. *Journal of Parallel and Distributed Computing*, *142*, pp.1-12.

78. Meng, Y., Huang, Z., Shen, G. and Ke, C., 2019. SDN-based security enforcement framework for data sharing systems of smart healthcare. *IEEE Transactions on Network and Service Management*, *17*(1), pp.308-318.

79. Deebak, B.D., Al-Turjman, F., Aloqaily, M. and Alfandi, O., 2019. An authentic-based privacy preservation protocol for smart e-healthcare systems in IoT. *IEEE Access*, *7*, pp.135632-135649.

80. Hu, J., Liang, W., Hosam, O., Hsieh, M.Y. and Su, X., 2021. 5GSS: a framework for 5G-secure-smart healthcare monitoring. *Connection Science*, pp.1-23.

81. Ullah, A., Sehr, I., Akbar, M. and Ning, H., 2018, August. FoG assisted secure De-duplicated data dissemination in smart healthcare IoT. In *2018 IEEE international conference on smart internet of things (SmartIOT)* (pp. 166-171). IEEE.

82. Fang, L., Yin, C., Zhu, J., Ge, C., Tanveer, M., Jolfaei, A. and Cao, Z., 2020. Privacy protection for medical data sharing in smart healthcare. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, *16*(3s), pp.1-18.

83. Kumar, M. and Chand, S., 2020. A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. *IEEE Internet of Things Journal*, *7*(10), pp.10650-10659.

84. Nguyen, D.C., Pathirana, P.N., Ding, M. and Seneviratne, A., 2021, May. A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. In *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 1-8). IEEE.

85. Quamara, M., Gupta, B.B. and Yamaguchi, S., 2021, January. An End-to-End Security Framework for Smart Healthcare Information Sharing against Botnet-based Cyber-Attacks. In *2021 IEEE International Conference on Consumer Electronics (ICCE)* (pp. 1-4). IEEE.

86. Alzubi, J.A., 2021. Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare. *Computer Communications*, *170*, pp.200-208.

87. Nashwan, S., 2021. An end-to-end authentication scheme for healthcare IoT systems using WMSN. *Comput. Mater. Contin*, *68*, pp.607-642.

88. Chaudhary, R., Jindal, A., Aujla, G.S., Kumar, N., Das, A.K. and Saxena, N., 2018. Lscsh: Lattice-based secure cryptosystem for smart healthcare in smart cities environment. *IEEE Communications Magazine*, *56*(4), pp.24-32.

89. El Zouka, H.A. and Hosni, M.M., 2021. Secure IoT communications for smart healthcare monitoring system. *Internet of Things*, *13*, p.100036.

90. Wu, F., Li, X., Xu, L., Kumari, S. and Sangaiah, A.K., 2018. A novel mutual authentication scheme with formal proof for smart healthcare systems under global mobility networks notion. *Computers & Electrical Engineering*, *68*, pp.107-118.

91. Garg, S., Kaur, K. and Kaddoum, G., 2020, June. ECC-based secure and provable authentication mechanism for smart healthcare ecosystem. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)* (pp. 1-6). IEEE.

92. Gope, P., Millwood, O. and Sikdar, B., 2021. A Scalable Protocol Level Approach to Prevent Machine Learning Attacks on Physically Unclonable Function Based Authentication Mechanisms for Internet of Medical Things. *IEEE Transactions on Industrial Informatics*, *18*(3), pp.1971-1980.

93. Wang, W., Huang, H., Xiao, F., Li, Q., Xue, L. and Jiang, J., 2021. Computation-transferable authenticated key agreement protocol for smart healthcare. *Journal of Systems Architecture*, *118*, p.102215.

94. Yuanbing, W., Wanrong, L. and Bin, L., 2021. An Improved Authentication Protocol for Smart Healthcare System using Wireless Medical Sensor

Network. *IEEE Access*.

95. Farash, M.S., Turkanović, M., Kumari, S. and Hölbl, M., 2016. An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment. *Ad Hoc Networks*, *36*, pp.152-176.

96. Pal, S., Hitchens, M., Varadharajan, V. and Rabehaja, T., 2017, November. On design of a fine-grained access control architecture for securing iot-enabled smart healthcare systems. In *Proceedings of the 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp. 432-441).

97. Saini, A., Zhu, Q., Singh, N., Xiang, Y., Gao, L. and Zhang, Y., 2020. A smart-contract-based access control framework for cloud smart healthcare system. *IEEE Internet of Things Journal*, *8*(7), pp.5914-5925.

98. Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H. and Zhai, Y., 2020. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), pp.10248-10263.

99. Zhong, H., Zhou, Y., Zhang, Q., Xu, Y. and Cui, J., 2021. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. *Future Generation Computer Systems*, *115*, pp.486-496.

100. He, D., Ye, R., Chan, S., Guizani, M. and Xu, Y., 2018. Privacy in the internet of things for smart healthcare. *IEEE Communications Magazine*, *56*(4), pp.38-44.

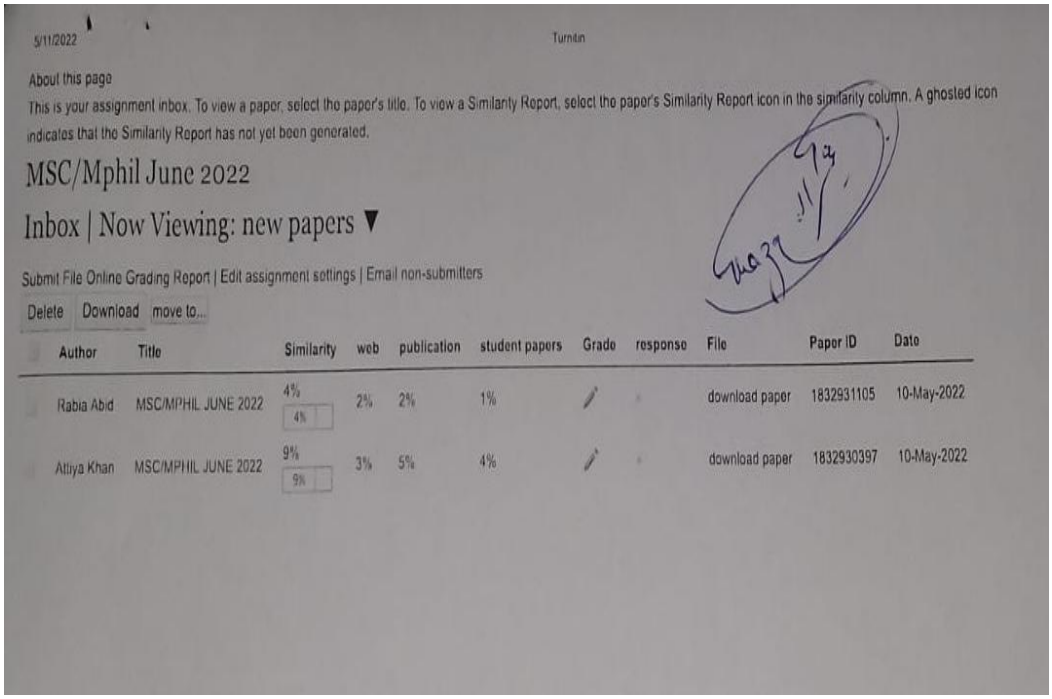
101. Salahuddin, M.A., Al-Fuqaha, A., Guizani, M., Shuaib, K. and Sallabi, F., 2018. Softwarization of internet of things infrastructure for secure and smart healthcare. *arXiv preprint arXiv:1805.11011*.

102. Abugabah, A., Nizamuddin, N. and Alzubi, A.A., 2020. Decentralized telemedicine framework for a smart healthcare ecosystem. *IEEE Access*, *8*, pp.166575-166588.

103. Khan, J., Li, J.P., Haq, A.U., Khan, G.A., Ahmad, S., Abdullah Alghamdi, A. and Golilarz, N.A., 2021. Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption. *Journal of Intelligent & Fuzzy Systems*, *40*(1), pp.1417-1442.

104. Acheme, I.D. and Vincent, O.R., 2021. Machine-learning models for predicting survivability in COVID-19 patients. In *Data Science for COVID-19* (pp. 317-336). Academic Press.
105. Singh, P., Singh, N., Singh, K.K. and Singh, A., 2021. Diagnosing of disease using machine learning. In *Machine Learning and the Internet of Medical Things in Healthcare* (pp. 89-111). Academic Press.
106. Misra, S., Li, H. and He, J., 2020. Robust geomechanical characterization by analyzing the performance of shallow-learning regression methods using unsupervised clustering methods. *Machine Learning for Subsurface Characterization*, pp.129-155.
107. Andrew, N. 2022, *Learning to Caption,* SlideShare from Scribd, viewed 6 March 2022, < https://www.slideshare.net/ExtractConf>
108 AAkash, B. 2019, Normalization Techniques in Deep Neural Networks, Techspace, viewed 8 March 2022, < https://medium.com/techspace-usict/normalization-techniques-in-deep-neural-networks-9121bf100d8>
109. Aleesa, A.M., Younis, M.O.H.A.M.M.E.D., Mohammed, A.A. and Sahar, N., 2021. Deep-intrusion detection system with enhanced UNSW-NB15 dataset based on deep learning techniques. *Journal of Engineering Science and Technology*, *16*(1), pp.711-727.
110. Christopher, O. 2015, *Understanding LSTM Networks,* Oinkina with Hakyll, viewed 10 March 2022, < http://colah.github.io/posts/2015-08-Understanding-LSTMs/ >
111. Hady, A.A., Ghubaish, A., Salman, T., Unal, D. and Jain, R., 2020. Intrusion detection system for healthcare systems using medical and network data: A comparison study. *IEEE Access*, *8*, pp.106576-106584.
112. Park, D., Kim, S., Kwon, H., Shin, D. and Shin, D., 2021. Host-Based Intrusion Detection Model Using Siamese Network. *IEEE Access*, *9*, pp.76614-76623.
113. Liu, J., Yang, D., Lian, M. and Li, M., 2021. Research on intrusion detection based on particle swarm optimization in IoT. *IEEE Access*, *9*, pp.38254-38268.
114. Tian, L. and Lu, Y., 2021, February. An intrusion detection model based on SMOTE and convolutional neural network ensemble. In *Journal of Physics: Conference Series* (Vol. 1828, No. 1, p. 012024). IOP Publishing.
115. Ahmed, U., Lin, J.C.W. and Srivastava, G., 2021, July. Network-Aware SDN Load Balancer with Deep Active Learning based Intrusion Detection Model. In *2021 International Joint Conference on Neural Networks (IJCNN)* (pp. 1-6). IEEE.
116. Xiao, Y., Xing, C., Zhang, T. and Zhao, Z., 2019. An intrusion detection model based on feature reduction and convolutional neural networks. *IEEE Access*, *7*, pp.42210-42219.
117. Kareem, S.S., Mostafa, R.R., Hashim, F.A. and El-Bakry, H.M., 2022. An Effective Feature Selection Model Using Hybrid Metaheuristic Algorithms

for IoT Intrusion Detection. *Sensors*, *22*(4), p.1396.



5/11/2022 Turnitin

About this page

This is your assignment inbox. To view a paper, select the paper's title. To view a Similarity Report, select the paper's Similarity Report icon in the similarity column. A ghosted icon indicates that the Similarity Report has not yet been generated.

MSC/Mphil June 2022

Inbox | Now Viewing: new papers ▼

Submit File Online Grading Report | Edit assignment settings | Email non-submitters

Delete Download move to...

Author	Title	Similarity	web	publication	student papers	Grade	response	File	Paper ID	Date
Rabia Abid	MSC/MPHIL JUNE 2022	4% 4%	2%	2%	1%			download paper	1832931105	10-May-2022
Atiiya Khan	MSC/MPHIL JUNE 2022	9% 9%	3%	5%	4%			download paper	1832930397	10-May-2022