Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2024.054380

ARTICLE

Deep Learning-Driven Anomaly Detection for IoMT-Based Smart Healthcare Systems

Attiya Khan[1], Muhammad Rizwan[2], Ovidiu Bagdasar[2,3], Abdulatif Alabdulatif[4,*], Sulaiman Alamro[4] and Abdullah Alnajim[5]

[1]Department of Computer Science, Kinnaird College for Women, Lahore, 54000, Pakistan

[2]School of Computing, University of Derby, Derby, DE221GB, UK

[3]Department of Mathematics, Faculty of Exact Sciences, "1 Decembrie 1918" University of Alba Iulia, Alba Iulia, 510009, Romania

[4]Department of Computer Science, College of Computer, Qassim University, Buraydah, 52571, Saudi Arabia

[5]Department of Information Technology, College of Computer, Qassim University, Buraydah, 52571, Saudi Arabia

*Corresponding Author: Abdulatif Alabdulatif. Email: ab.alabdulatif@qu.edu.sa

Received: 27 May 2024 Accepted: 23 September 2024 Published: 31 October 2024

ABSTRACT

The Internet of Medical Things (IoMT) is an emerging technology that combines the Internet of Things (IoT) into the healthcare sector, which brings remarkable benefits to facilitate remote patient monitoring and reduce treatment costs. As IoMT devices become more scalable, Smart Healthcare Systems (SHS) have become increasingly vulnerable to cyberattacks. Intrusion Detection Systems (IDS) play a crucial role in maintaining network security. An IDS monitors systems or networks for suspicious activities or potential threats, safeguarding internal networks. This paper presents the development of an IDS based on deep learning techniques utilizing benchmark datasets. We propose a multilayer perceptron-based framework for intrusion detection within the smart healthcare domain. The primary objective of our work is to protect smart healthcare devices and networks from malicious attacks and security risks. We employ the NSL-KDD and UNSW-NB15 intrusion detection datasets to evaluate our proposed security framework. The proposed framework achieved an accuracy of 95.0674%, surpassing that of comparable deep learning models in smart healthcare while also reducing the false positive rate. Experimental results indicate the feasibility of using a multilayer perceptron, achieving superior performance against cybersecurity threats in the smart healthcare domain.

KEYWORDS

Anomaly detection; deep learning; Internet of Things (IoT); health care

1 Introduction

Over the past few decades, the healthcare industry has undergone a rapid transformation from a traditional hospital-centered approach to a patient-centered approach, particularly evident in smart healthcare systems (SHS) [1]. This rapid shift has been facilitated by various technologies, especially the Internet of Medical Things (IoMT). The IoMT, also known as healthcare IoT, represents the growing use of Internet of Things (IoT) technology in the medical sector. It combines software applications and

healthcare devices that integrate with health information systems (HIS) through wireless connectivity. Fig. 1 illustrates the structure of connected smart healthcare.

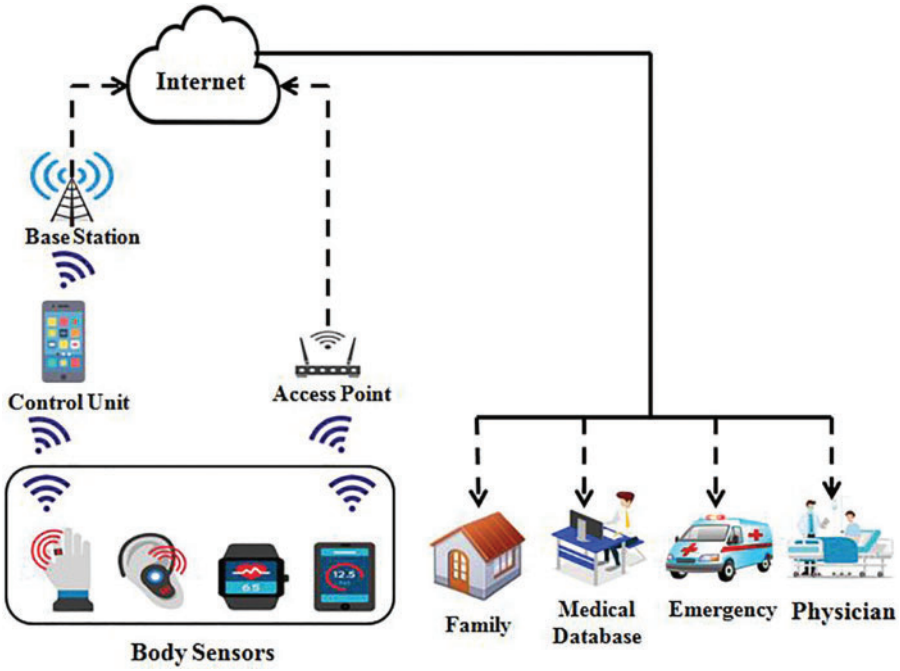

Figure 1: Structure of smart healthcare

Benefiting from numerous IoT devices, various industries, including health tech, are leveraging interconnected sensor technologies, such as standalone devices and wearables, for a more promising future. IoMT encompasses a broad range of IoT applications and devices specifically designed for healthcare settings and needs, including telemedicine consultations, sensors, and remote patient monitoring. The use of remote healthcare monitoring has surged rapidly with the adoption of smartphones and wearable sensors [2].

Currently, there is a growing concern for health among people around the world [3]. The Internet of Medical Things (IoMT) has the potential to enhance patient outcomes through advanced diagnostics, real-time monitoring, and robotic surgery. Traditional healthcare relies on manual methods for managing patients' medication data, case histories, billing information, diagnoses, and demographic data, which increases the risk of human error and can negatively impact patient care. Smart healthcare, powered by IoMT, minimizes human errors and aids medical practitioners in making accurate disease diagnoses through the interconnectivity of vital signs monitoring equipment and decision support systems over a network [4].

This interconnectivity enables the early treatment of health issues before they escalate into serious illnesses [5].

Furthermore, telemedicine services have the potential to decrease the need for hospital visits among the elderly and those with chronic conditions [6], thereby improving the health and well-being of individuals and communities [7]. According to a medical research report, approximately 80% of individuals over the age of 65 suffer from at least one chronic condition, such as diabetes, cancer, or heart disease [8]. The report titled "IoT in Healthcare Market by Component, Application, End User,

and Region—Global Forecast to 2025" predicts that the IoMT sector's value is expected to reach 188 billion by 2025, up from 72.5 billion in 2020."

The main aspect of IoMT-based smart healthcare is to enhance patient well-being by minimizing unpleasant hospital experiences. The IoMT edge network plays a crucial role in this smart healthcare system, comprising many IoMT-enabled devices that enable individuals to monitor their health status and physical well-being digitally [9]. For example, fitness tracking devices, including smartwatches, smart shorts, smart shoes, and wristbands, are capable of collecting, analyzing, and transmitting data on an individual's physical activities to their mobile applications. This data can then be accessed by users through fitness tracking smartphone applications. Fig. 2 illustrates the applications of IoMT in smart healthcare. IoMT-based healthcare devices generate enormous amounts of data each year. It is anticipated that the data generated by the healthcare industry will reach 1656 zettabytes (ZB) by the year 2025 [10]. From this vast data pool, valuable insights can be extracted to aid in effective decision-making. Healthcare institutions and hospitals can integrate this extracted data with their existing Electronic Medical Records (EMR) to enhance health monitoring, enable early disease detection, and ensure timely treatment [11].

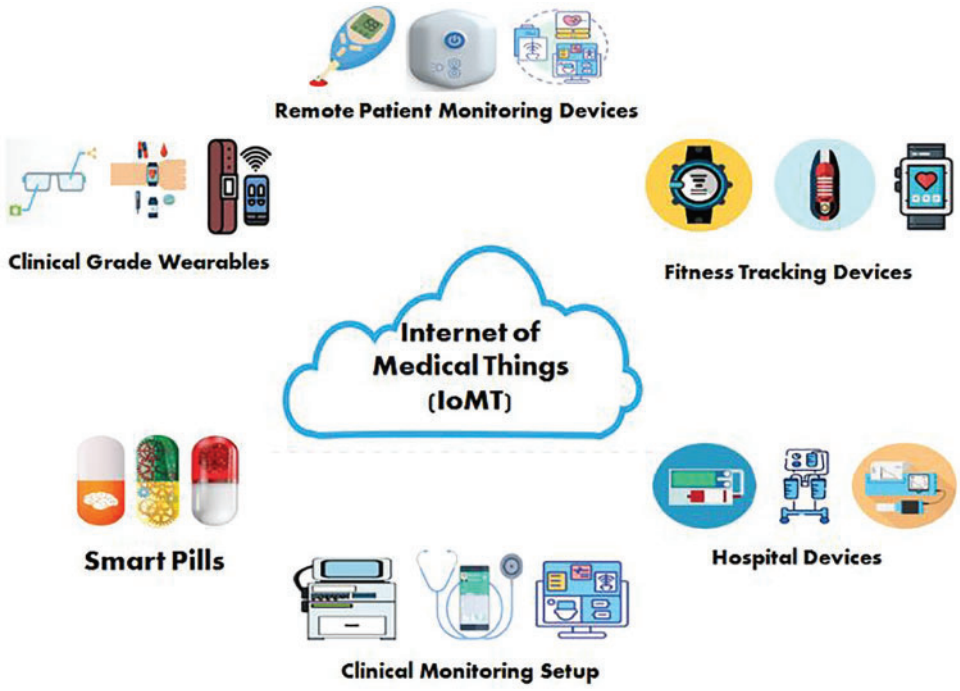

Figure 2: Applications of IoMT in smart healthcare

Despite its numerous benefits, the integration of smart healthcare across various aspects of the healthcare framework introduces several adverse side effects. This transition expands the attack surface, making users' safety, privacy, and security more vulnerable to cyberattacks [12]. Furthermore, the enhanced functionalities of smart healthcare systems introduce a multitude of security risks. Cyber attackers can exploit these systems in various ways: they can manipulate vital signs by injecting false data, disrupt the normal operation of smart healthcare systems, and compromise medical equipment to alter the outcomes of healthcare emergencies. The reliance on wireless connectivity in smart healthcare systems exposes them to additional threats from intruders. These systems face numerous

security threats, including ransomware attacks, distributed denial of service (DDoS) attacks, data breaches, insider threats, router attacks, and replay attacks. Table 1 lists the major cyber incidents in the healthcare industry.

Table 1: Major healthcare industry cyber-incidents

Year	Healthcare industry	Type	People affected	City, Country
2013	Excellus Health Plan, Inc.	Malware	10 million	Rochester, USA
2014	Premera Blue Cross	Phishing	11 million	Mountlake Terrace, USA
2014	Community Health Systems	Malware	4.5 million	Franklin, USA
2015	Anthem, Inc.	Phishing	79 million	Indianapolis, USA
2015	Medical Informatics Engineering	Brute force attack	3.9 million	Fork Wayne, USA
2016	Banner Health	Malware	3.62 million	Phoenix, USA
2020	Trinity Health	Third-party vendor	3.32 million	Livonia, USA
2020	Magellan Health	Ransomware attack	1.7 million	Scottsdale, USA
2020	Inova Health System	Ransomware attack	1 million	Falls Church, USA

The ransomware attack on smart healthcare systems can significantly slow down critical processes or render them completely unavailable. Such attacks may make hospital devices inaccessible, leading to delayed patient care. Distributed Denial of Service (DDoS) attacks can overwhelm the network, rendering smart healthcare systems inoperable and resulting in a loss of communication between hospitals and IoMT devices in the event of a medical emergency [13]. Data breaches are prevalent in the smart healthcare sector, with major causes including credential-stealing malware, insider threats, and backdoors. Protected Health Information (PHI) is more valuable on the illegal market than either Personal Identification Information or credit card information, thereby providing a higher motivation for cyber attackers to target healthcare databases.

In the case of insider attacks, intruders can pose significant threats to the security and privacy of smart healthcare systems. These intruders may sell stolen data for profit or modify medical records out of malice. Phishing attacks involve the sending of authentic-looking emails with attachments or links to hospital staff by attackers. Unwary users who open or click on these attachments or links activate the malicious content, allowing hackers to gain network access. This can lead to the activation of viruses or the theft of information.

Cyberattacks on the smart healthcare sector can have devastating consequences if patients' records are altered or disclosed. Similarly, a loss of connection between IoMT devices and the hospital due to cyberattacks can lead to delayed treatment or even the loss of a patient's life. Beyond compromising patient security, these threats can also damage the brand's reputation, disrupt business continuity, and

reduce revenue [14]. Serious privacy issues persist as data security continues to impact IoMT devices. Given the highly sensitive nature of the data generated and processed by IoMT-based healthcare devices, it is crucial that the interconnection between these devices remains both available and secure at all times. Furthermore, ensuring the confidentiality, availability, and integrity of healthcare data shared within smart healthcare networks is of utmost importance [15].

Numerous studies have explored artificial intelligence-based intrusion detection and classification techniques. However, the majority of security frameworks designed to protect Smart Healthcare Systems (SHS) have suffered from high false alarm rates and an inability to detect unknown network threats, rendering them ineffective at safeguarding SHS from network attacks. Such vulnerabilities can lead to costly damage to smart healthcare networks and devices, loss of critical patient information, and medical identity theft. Therefore, in our framework, we employ deep learning techniques to effectively detect malicious attacks, and network intrusions, and identify abnormal behaviors within smart healthcare networks and devices.

Contributions

The paper has numerous significant contributions:

- We present a comprehensive overview of security issues and cyberattacks targeting smart healthcare systems.
- We develop an artificial neural network that analyzes traffic flow data to detect intrusions in smart healthcare networks, utilizing a multilayer perceptron-based security framework. The primary objective of our work is to protect smart healthcare devices and networks from malicious attacks and security risks. We employ the NSL-KDD and UNSW-NB15 intrusion detection datasets to evaluate our proposed security framework.
- We examine various attacks on smart healthcare systems, including DoS/DDoS attacks, jamming attacks, and man-in-the-middle attacks. The evaluation results indicate that our proposed framework enhances security by effectively detecting intrusions and malicious attacks in Smart Healthcare Systems (SHS).

The rest of the paper is organized as follows: Section 2 presents related work on security solutions for network intrusion and malicious attacks in Smart Healthcare Systems (SHS) and the Internet of Medical Things (IoMT), along with various security frameworks for IoMT and SHS devices. Section 3 discusses the security challenges and attacks faced by smart healthcare devices and networks. Section 4 introduces our proposed framework. Section 5 details the developed model's experimental results and performance analysis. Finally, Section 6 concludes the paper.

2 Related Work

Several research studies have been conducted to analyze security vulnerabilities in smart healthcare systems. In this section, we will discuss some of the existing approaches for addressing security in the following areas: securing smart healthcare devices, securing communication both inside and outside the smart healthcare environment, and protecting data privacy within the smart healthcare context.

Umamaheswaran et al. [16] proposed a deep learning-based IDS approach called "Conditional Generative Adversarial Network-Convolutional Neural Network (CGAN-CNN)" to address the issue of low intrusion detection rate in case of uneven data distribution. To mitigate the functional deterioration caused by unbalanced data, this method uses CGAN paradigm to oversample from

unbalanced data. Moreover, additional constraints are incorporated into the usual CGAN procedure for the generator and critic of the sub-networks to accelerate convergence impacts and reduce leeway in convergence process. Sun et al. [17] proposed an intrusion detection framework that uses the combination of AdaBoost algorithms and particle swarm optimization to detect and classify malicious records in healthcare applications. Alzubi et al. [18] proposed a deep learning-based framework using the combination of Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) to detect intruders and safeguard healthcare data. Alalhareth et al. [19] proposed a Long Short-Term Memory (LSTM) based intrusion detection framework using fuzzy-based self-tuning. Gupta et al. [20] proposed a tree classifier-based intrusion detection system for IoMT networks. Sarosh et al. [21] proposed a security mechanism based on the Hyperchaotic equation, Logistic equation, and Deoxyribonucleic Acid (DNA) encoding. The encrypted secret images are converted into shares using a "Lossless Computational Secret Image Sharing (CSIS)" method for distributed storage on cloud servers. The authors employed DNA and Hyperchaotic encryption to enhance overall system security. Furthermore, Secret Sharing (SS) is applied to improve the security of cloud-based cryptosystems. Zhong et al. [22] introduced an attribute-based encryption (ABE) method that delegates some encryption and decryption processes to edge nodes. Farhin et al. [23] proposed a two-layer security architecture for heterogeneous Internet of Healthcare Things systems using trust management based on Bayesian inference for node trust and digitally signed blockchain for data protection. Wang et al. [24] proposed a computation-transferable authenticated key-agreement (AKA) protocol without an online registration center. This protocol facilitates key negotiation and mutual authentication, enhances authentication efficiency, and reduces dependency on the registration center. In this scheme, a portion of the computation load is transferred to the edge server, resulting in reduced communication and computation overhead on the user side. Quamara et al. [25] proposed an end-to-end technique for secure information storage and transfer in SHS, focusing mainly on secure healthcare data sharing against botnet-based cyberattacks.

Subasi et al. [26] suggested a bagging ensemble classifier-based intrusion detection framework to safeguard smart healthcare systems from intrusions. Haque et al. [27] recommended using blockchain-based smart contracts to protect patient privacy and sensitive information. The proposed system ensures the healthcare data stored is immutable, authentic, and reliable while maintaining data access among healthcare stakeholders. Helen et al. [28] proposed a blockchain-based mechanism to secure healthcare data and prevent data forgery in 5G networks. Anand et al. [29] proposed a compression-then-encryption (CTE) technique based on dual watermarking to protect the Electronic Patient Record (EPR) information in smart healthcare systems. Nguyen et al. [30] introduced an efficient and reliable data offloading scheme that offloads IoT healthcare data to local edge servers for processing while maintaining privacy. Additionally, a data-sharing mechanism using blockchain enables data exchange among healthcare users, and a smart contracts-based trustworthy access control mechanism is created for authorized access to secure EHR sharing.

Khan et al. [31] presented an IoT-based smart healthcare system with efficient and secure monitoring. Initially, a meaningful keyframe is extracted from a summarized video through a regimented keyframe extraction process. Furthermore, it employed a "lightweight cosine-transform encryption technique" over the extracted keyframes to ensure security and prevent any kind of adversarial attacks. Haque et al. [32] proposed SHChecker, a state-of-the-art threat analysis scheme that integrates formal analysis capabilities and machine learning to identify potential attack vectors for IoMT-based Smart Healthcare Systems (SHS). The framework analyzes potential threats to SHS, investigating the relationship between health statuses, sensor readings, and their consistency.

Gope et al. [33] proposed a novel lightweight IoT authentication protocol that provides resistance against machine learning cyberattacks on Physically-Unclonable-Functions (PUFs). Moreover, the proposed strategy ensures the privacy of IoT devices and protection against replay attacks and forgery. Tripathi et al. [34] examined social and technological barriers to the adaptation of Smart Healthcare Systems (SHS) by analyzing users' perceptions and expert views. Furthermore, the authors presented S2HS, a blockchain-based framework for SHS that provides system integrity as well as intrinsic security. Chen et al. [35] presented a protection and security awareness framework for 5G-based smart healthcare platforms that utilize Zero Trust architecture, driven by four important characteristics of 5G-based smart healthcare: subject, behavior, object, and environment. Zhou et al. [36] focused on designing a privacy-preserving scheme aided by human-in-the-loop technology in smart healthcare, obfuscating different health indicators from hospitals and smart wearable devices using a block design method. Kumar et al. [37] proposed a secure cloud-centric IoMT-based SHS with public verifiability. For data transmission security, the system uses an "escrow-free identity-based aggregate signcryption (EF-IDASC)" approach, achieving patients' data confidentiality and reliability of patients' information with public verifiability.

The significant related work in the security of SHS are highlighted in Table 2.

Table 2: Major works in smart healthcare security

Paper	Year	Description
[16]	2024	A "Conditional Generative Adversarial Network-Convolutional Neural Network (CGAN-CNN)" to address the issue of low intrusion detection rate in case of uneven data distribution.
[17]	2024	An intrusion detection framework that uses the combination of AdaBoost algorithms and particle swarm optimization to detect and classify malicious records in healthcare applications.
[18]	2024	A deep learning-based framework using the combination of Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN) to detect intruders and safeguard healthcare data.
[19]	2023	A Long Short-Term Memory (LSTM) based intrusion detection framework using fuzzy-based self-tuning.
[20]	2022	A tree classifier-based intrusion detection system for IoMT networks.
[21]	2021	Advanced security mechanism based on Hyperchaotic equation, Logistic equation, and Deoxyribonucleic Acid encoding.
[22]	2021	An efficient and attribute-based encryption (ABE) scheme that delegates partial encryption-decryption operations to edge nodes.
[23]	2021	A two-layer security architecture for heterogeneous Internet of Healthcare Things systems using trust management based on Bayesian inference with digitally signed blockchain for data protection.
[24]	2021	A "computation-transferable authenticated key-agreement (AKA) protocol" without an online registration centre.
[25]	2021	A comprehensive framework for safe data storage and transmission in smart healthcare systems.

The discussion above indicates that IoMT-based smart healthcare systems contain highly private and confidential information. However, the security mechanisms integrated into existing systems are inadequate to thwart numerous cyberattacks, putting patients' data at risk of theft and forgery. Therefore, there is a pressing need to develop a security mechanism that can efficiently detect cyberattacks and secure patients' data in smart healthcare systems.

3 Security Challenges and Attacks in the Smart Healthcare System (SHS) Environment

By 2025, the expected number of devices connected to the Internet globally is projected to reach 55.9 billion. IoT technology may be deployed in various sectors including industries, factories, companies, airports, hospitals, homes, or public spaces. Given the relentless expansion of IoT, the security of devices utilizing IoT technology becomes paramount. SHS comprises numerous interconnected devices linked to the cloud via a network to transmit data and information. Consequently, a breach in the SHS environment can pose significant risks. Several attacks target SHS devices by exploiting vulnerabilities in the communication protocols these devices use. Below, we discuss some of the prevalent attacks in SHS:

DDoS Attacks: A Distributed Denial of Service (DDoS) attack involves deploying multiple attacking entities to prevent legitimate use of a service. The main objective is to disrupt data flow and overwhelm infrastructures by flooding them with requests, targeting a service provider. Such attacks can be especially damaging when the networks and devices of the SHS are compromised, continually evolving with the changing motivations of attackers and the technologies they employ. Malware, such as zombies or bots, enables hackers to gain control over systems.

Man-in-the-Middle Attack: Attackers intercept and monitor network traffic, inserting manipulated or modified data during transmission before forwarding it to the intended recipient. If successful, the attacker can control the session, steal personal information or login credentials, corrupt data, or sabotage communication.

Brute Force Attacks: Hackers employ a trial-and-error method to gain access to private accounts or systems, often requiring numerous attempts. Brute force attacks can lead to theft of valuable personal data, malware distribution, system hijacking for malicious activities, and damage to a hospital's reputation.

IP Spoofing: This involves creating Internet Protocol (IP) packets with a falsified source address to hide the sender's identity or to impersonate another computer system, often for launching DDoS attacks. In SHS environments, IP spoofing poses a threat to devices, especially if Ethernet/IP is used for communication.

SQL Injection: Attackers use malicious SQL code to manipulate the backend database, gaining access to information that should not be accessible. This can include sensitive patient or hospital data, employee information, or inventory details, with potentially far-reaching impacts in the SHS environment. Successful SQL injection attacks can lead to unauthorized administrative access, deletion of database tables, or exposure of sensitive data.

Malware Threats: Malicious software designed to gain access to or damage a device. SHS devices, being interconnected and often lacking robust security, are susceptible to malware. Detecting malware is challenging as developers continuously innovate to avoid detection. Specific malware attacks targeting SHS devices include:

- **BOTNET:** Networks of hijacked devices controlled by hackers. Botnets can significantly disrupt SHS operations.

- **Mirai Malware:** Self-propagating malware that targets unsecured or poorly configured SHS devices for brute force attacks, facilitating DDoS attacks. The release of Mirai's source code has led to its use in botnet rentals, further exacerbating threats.

Insider Attack: Security threats originating from within the organization, such as a disgruntled former employee misusing access to privileged accounts or sensitive information within the SHS network.

Third-Party Breaches: Occur when individuals with peripheral roles, such as doctors, medics, or vendors, introduce malware into the system or steal data. These breaches can lead to intellectual property theft, network intrusions, credential theft, and fileless malware attacks.

DNS Poisoning: Exploiting DNS server vulnerabilities to redirect traffic to malicious servers, resulting in data theft, malware infections, or censorship within SHS.

Password Spraying: Attackers attempt to access accounts using common passwords across thousands of accounts simultaneously. Even one weak password can compromise the entire SHS. Password spraying is particularly dangerous on cloud-based authentication portals used in SHS.

Replay Attack: Unauthorized users intercept network traffic, steal information, and resend it to trick the receiver into treating it as legitimate, fulfilling the attacker's objectives.

4 Proposed Anomaly Detection Model for Smart Healthcare Systems

In this section, we propose an efficient anomaly detection framework to protect IoMT-based SHS against malicious activities. The architecture of the proposed framework consists of training and testing phases, as shown in Fig. 3.

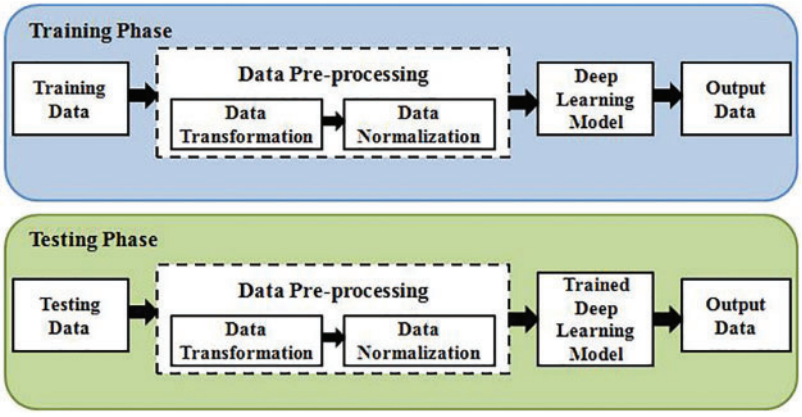

Figure 3: Overview of deep learning process

4.1 Data Pre-Processing

The initial phase of the framework is data pre-processing, which converts raw data into a format that is understandable and suitable for machine learning (ML) and deep learning (DL) algorithms. Data pre-processing involves data transformation and normalization to extract useful information from a large dataset.

4.1.1 Data Transformation

The proposed model operates exclusively with numerical values. Therefore, symbolic feature values present in the dataset are converted into integer values. For example, in the NSL-KDD dataset, feature transformation is applied to convert symbolic feature values such as service types (with nominal values like "private", "HTTP", and "FTP-data") into an integer representation (e.g., 1, 2, and 3, respectively).

4.1.2 Data Normalization

In the proposed model, data normalization is used to improve the optimisability of weights of the neural network model. We use the Z-Score formula for each feature 'a' using:

$$\hat{a} = \frac{a - \mu(a)}{\sigma(a)} \tag{1}$$

where $\sigma(a)$ is standard deviation and $\mu(a)$ is mean value of attribute A.

To enhance the computing resources available for the proposed model, we reduce the dimensionality of the network data. This reduction is achieved through a dimensionality-reduction technique known as Principal Component Analysis (PCA). The PCA technique transforms the original dataset with p dimensions into a subset with k dimensions where $k < p$ while retaining the variation in the original dataset to the full. The new dimensions are called the Principal Components. The algorithm for PCA works as follows:

Input dataset: $x_1, x_2, x_3, \ldots, x_m$

Pre-processing:

$$\mu_j = \sum_{i=1}^{m} x_j(i) \tag{2}$$

Replace each $x_j(i)$ with $x_j - \mu_j$.

Compute the "Covariance Matrix" using:

$$\sum = \frac{1}{m} \sum_{i=1}^{n} (x_i)(x_i)^T \tag{3}$$

Compute the eigenvectors and eigenvalues of the matrix $\sum$.

Sort the eigenvectors by decreasing eigenvalues.

Form Z by selecting k eigenvectors that have the highest eigenvalues.

Transform the samples into a new subset using:

$$y = Z^T \times x \tag{4}$$

where x is $(p \times 1)$ dimensional sample and y is transformed $(k \times 1)$ dimensional sample.

4.2 Network Sniffing Unit

A packet sniffer, designed to capture and inspect network traffic, is embedded in either hardware or software to acquire raw data packets traversing the network. The sniffer stores these raw packets in a buffer, facilitating subsequent data analysis. Additionally, the buffer archives the network's historical profile and attack signatures. A real-time analyzer then processes the network traffic data, forwarding

it for intrusion detection purposes. The packet sniffer implements role-based access control mechanism to limit user access to captured data based on role, ensuring that only authorized users can access patient sensitive information. Moreover, to access the packet sniffer a multi-factor authentication mechanism is used to reduce the threat of unauthorized access.

4.3 Multilayer Perceptron-Based Model

Multilayer Perceptron (MLP) is a feed-forward Artificial Neural Network (ANN). It consists of three layers: input, hidden, and output.

The input data to be processed is fed into the source nodes, which constitute the input layer. The output layer is responsible for performing classification and prediction tasks. Situated between the input and output layers are multiple hidden layers, tasked with performing the computational work essential for the model's function. Each layer forwards the result of its computations to the subsequent layer. This process is consistent across all hidden layers until reaching the output layer. In this architecture, data flows from the input layer to the output layer in a forward direction, while neurons are trained using the backpropagation technique to enhance prediction accuracy. The perceptron generates a linear combination of inputs based on their associated weights, which is then passed through a nonlinear activation function. This function produces a singular output from a set of real-valued inputs. The values at both the output and hidden layers are determined through these processes as:

$$O_x = Hb_2 + W_2hx \tag{5}$$

$$h_x = rb_1 + W_1x \tag{6}$$

where W_1 and W_2 are weight metrices; b_1 and b_2 are bias vectors; and H and r are activation functions.

5 Experimentation and Results

5.1 Dataset Description

The evaluation dataset plays a significant role in testing and evaluating the detection system's performance. A high-quality dataset is essential to produce efficient and effective results in testing as well as a real environment. This paper utilizes UNSW-NB15 and NSL-KDD benchmark datasets which are publicly available.

5.1.1 NSL-KDD

NSL-KDD is a refined form of the KDD Cup '99 dataset that is publicly available. The NSL-KDD training dataset contains 125,973 records, whereas the testing dataset has 22,544 records. The dataset contains 43 features for each record, with 41 indicating traffic input and the final two being score and labels. Within the NSL-KDD dataset exist 4 different categories of attacks. A breakdown of different subcategories of each attack existing in the dataset is shown in Table 3. Some of the advantages of the NSL-KDD dataset are:

- No irrelevant records are included to enable the classifier to produce unbiased results.
- The test dataset has no duplicate records, hence, the learners' performance is not affected by the techniques with improved detection rates on frequently occurring records.
- The proportion of records chosen from each difficulty group is inverse to the percentage of records in the original KDD dataset.

Table 3: Subcategories of attacks in NSL-KDD

Attacks	Subcategories of attacks
Probe	Portsweep, satan, nmap, saint, ipsweep, mscan
DoS	Neptune, back, smurf, pod, land, teardrop, worm, udpstorm, processtable, mailbomb, apache2
R2L	Warezclient, ftpwrite, warezmaster, imap, guesspassword, spy, phf, multihop, httptunnel, sendmail, named, snmpguess, xlock, snmpgetattack, xsnoop
U2R	Butteroverflow, rootkit, perl, loadmodule, ps, xterm, sqlattack

5.1.2 UNSW-NB15

The UNSW-NB15 network intrusion dataset was generated in 2015. There are 257,673 records altogether in the UNSW-NB15 dataset, of which 175,341 are in the train set and 82,332 are in the test set. UNSW-NB15 has 49 features which are classified into six groups: Flow, Basic, Time, Labelled, Additional Generated, and Content Features. The features numbered 36 to 40 are known as General Purpose Features, whereas those numbered 41 to 47 are known as Connection Features. The dataset contains nine modern attack types namely the Fuzzers, Analysis, Reconnaissance, Exploits, DoS, Shellcode, Backdoors, Worms, and Generic. The nine types of attacks and their distribution into train and test datasets are given in Table 4.

5.2 Evaluation Metrics

To improve the performance of our model, we calculate the precision, accuracy, recall, and F1-score. In this section, the following metrics will be used:

- **True Positive (TP):** A state when attack data is accurately predicted as an attack.
- **True Negative (TN):** A state where normal data is accurately predicted as normal.
- **False Positive (FP):** A state where normal data is incorrectly predicted as an attack.
- **False Negative (FN):** A state where attack data is incorrectly predicted as normal.

Next, we discuss the measures to assess our model's performance:

$$Accuracy = \frac{TN + TP}{TN + FP + TP + FN} \tag{7}$$

Accuracy is the ratio of accurately classified data instances to all the data instances.

$$Recall = \frac{TP}{FN + TP} \tag{8}$$

Recall is the ratio of positive data instances that are correctly predicted to all the data instances in actual class 'yes'.

$$Precision = \frac{TP}{FP + TP} \tag{9}$$

Table 4: Distribution of UNSW-NB15 records

Category	Train set	Test set	Description
Analysis	2000	677	It contains various attacks of web penetration, port scan, and spam.
Fuzzers	18,184	6062	Injects randomly generated data into a network/program in an attempt to suspend it.
Backdoors	1746	583	A type of security breach where the hacker can surpass a system's normal security to access a network or its data.
Reconnaissance	10,491	3496	It is the technique used to discover and collect information about a network or system.
Exploits	33,393	11,132	The intruder knows of a vulnerability/security flaw and exploits the vulnerability by leveraging that knowledge.
DoS	12,264	4089	DoS attack is a cyberattack that shuts down a network or machine, making it unavailable to its users by indefinitely or temporarily suspending or interrupting the services of the host connected to the Internet.
Shellcode	1133	378	Shellcode is a small set of instructions used as a payload in the exploitation of software vulnerabilities.
Worms	130	44	A worm is a computer program that self-replicates and spreads to other networks or computers while remaining functional on infected systems.
Generic	40,000	18,871	A technique that works against all the block ciphers without considering the structure of the block cipher.
Normal	56,000	37,000	Normal traffic data.

Precision is the ratio of positive data instances that are accurately predicted to all the predicted positive observations.

$$F - measure = 2 \times \frac{Recall \times Precision}{Recall + Precision} \tag{10}$$

F-measure is the weighted mean of *Recall* and *Precision*. Thus, it considers both false negatives and false positives.

5.3 Experimentation and Results

We utilized the WEKA tool, a comprehensive machine learning suite, to conduct our experiments. For classification purposes, an Artificial Neural Network (ANN) employing a Multilayer Perceptron model was applied to the dataset. To train the model we use the activation function "sigmoid", the learning rate of "0.3", "stochastic gradient descent" optimizer with the momentum of 0.2 and "500" epochs. To optimize the framework based on the dataset, WEKA automatically determines the hidden layers. The seed value of "1" is used to ensure consistency and reproducibility. We performed two-fold cross-validation on the datasets. Using the NSL-KDD dataset, we achieved a classification accuracy of 95.0674% for the data points. A detailed summary of the results obtained from the NSL-KDD dataset is presented in Table 5.

Table 5: Summary of NSL-KDD dataset results

Correctly classified instances	95.0674%
Incorrectly classified instances	4.9326%
Mean absolute error	0.063
Root mean square error	0.2112
Relative absolute error	12.8449%
Root relative square error	42.6528%
Total number of instances	22,544
Time taken to build model	118.54 s

Next, the confusion matrix for all the data instance in NSL-KDD dataset classified as normal traffic or anomalous traffic is shown in Fig. 4.

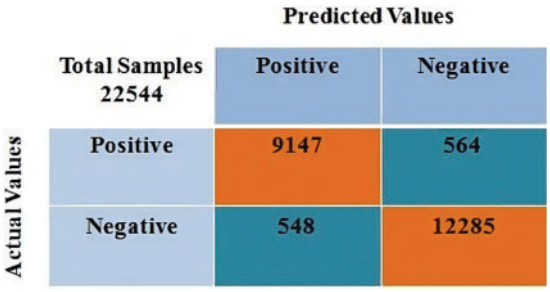

Figure 4: Confusion matrix for NSL-KDD testing data

Using the above discussed evaluation metrics, the proposed model is evaluated and the summary of class wise results is provided in Table 6.

Table 6: Detailed accuracy by class for NSL-KDD test data

Class	TP rate	FP rate	Precision	Recall	F measure
Normal	0.942	0.043	0.943	0.942	0.943
Anomaly	0.957	0.058	0.956	0.957	0.957
Weighted average	0.951	0.051	0.951	0.951	0.951

Fig. 5 represents the detailed accuracy by class for NSL-KDD test data.

Next, we provide MCC value, ROC curve area, and PRC area for NSL-KDD dataset in Table 7.

Fig. 6 represents MCC, ROC area, and PRC area for NSL-KDD test data.

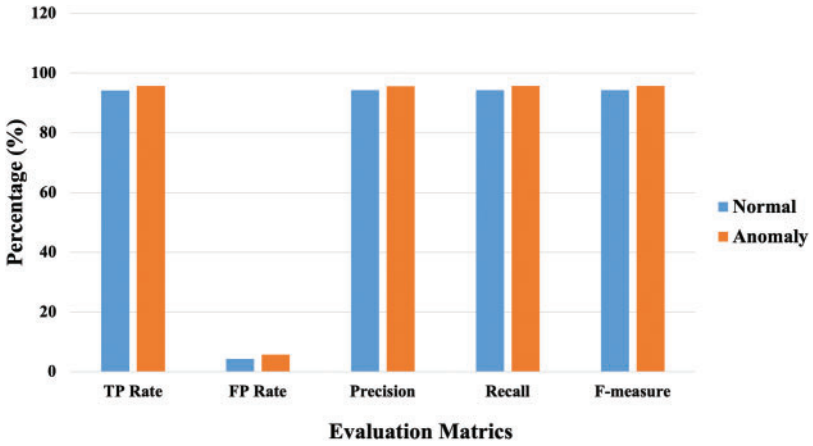

Figure 5: Accuracy by class for NSL-KDD test data

Table 7: MCC, ROC area, and PRC area for NSL-KDD test data

Class	MCC	ROC area	PRC area
Normal	0.899	0.967	0.946
Anomaly	0.899	0.968	0.972
Weighted average	0.899	0.968	0.961

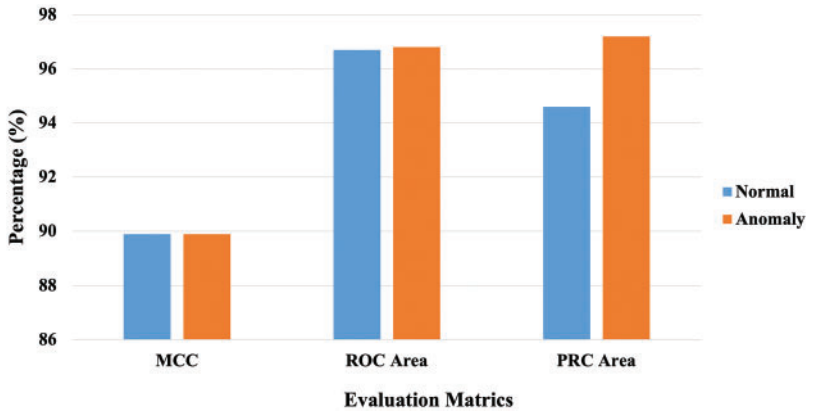

Figure 6: MCC, ROC area, and PRC area for NSL-KDD test data

We classify the UNSW-NB15 dataset artificial neural network (ANN) based on a multilayer perceptron. Two folds cross-validation is performed on the dataset. Using the UNSW-NB15 dataset, 92.0534% of data points are classified correctly. The overall summary of the UNSW-NB15 test dataset is given in Table 8.

Next, the confusion matrix for all the data instances in the UNSW-NB15 dataset classified as various attacks is shown in Fig. 7.

Table 8: Summary of results on UNSW-NB15 dataset

Correctly classified instances	92.0544%
Incorrectly classified instances	7.9456%
Mean absolute error	0.0376
Root mean square error	0.1397
Relative absolute error	21.1786%
Root relative square error	42.1515%
Total number of instances	82,332
Time taken to build model	188.21 s

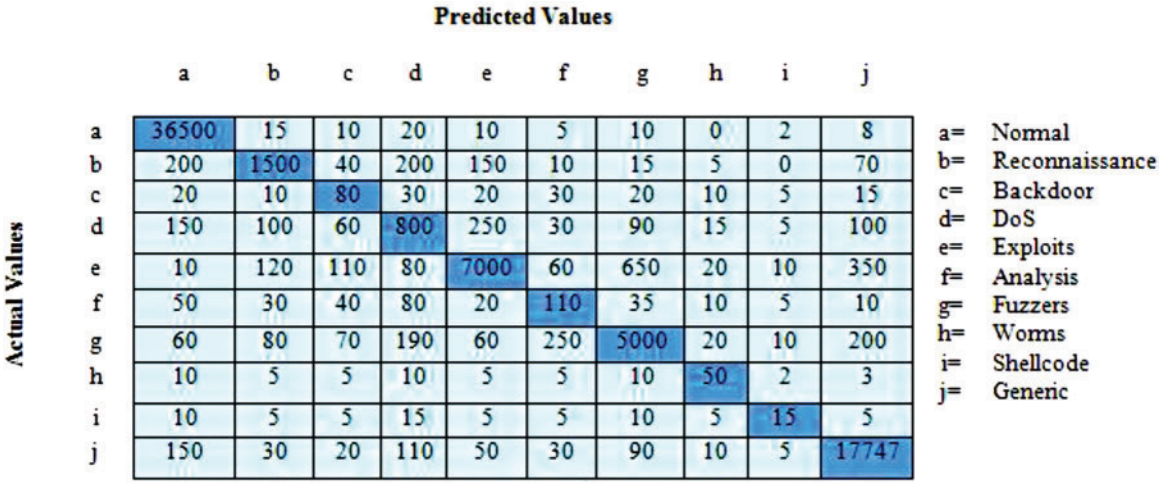

Figure 7: Confusion matrix for UNSW-NB15 dataset

Using the above-discussed evaluation metrics, the proposed model is evaluated and the summary of class-wise results is provided in Table 9. The model performs well against normal class, generic, exploits, and fuzzes. The model performs average against reconnaissance and DoS. Whereas, the model did not perform well against backdoors, analysis, worms, and shellcode. The model performed well for the data represented well in the dataset whereas, the model did not perform well for data not represented very well in the dataset.

Table 9: Detailed accuracy by class for UNSW-NB15 dataset

Class	TP rate	FP rate	Precision	Recall	F measure
Normal	0.981	0.010	0.981	0.981	0.981
Reconnaissance	0.497	0.025	0.475	0.495	0.485
Backdoor	0.051	0.006	0.100	0.051	0.066
DoS	0.256	0.019	0.435	0.256	0.324
Exploits	0.726	0.065	0.638	0.726	0.681

(Continued)

Table 9 (continued)

Class	TP rate	FP rate	Precision	Recall	F measure
Analysis	0.022	0.001	0.500	0.022	0.041
Fuzzers	0.793	0.036	0.628	0.791	0.702
Worms	0.041	0.003	0.081	0.041	0.054
Shellcode	0.021	0.002	0.041	0.021	0.027
Generic	0.950	0.019	0.936	0.941	0.938
Weighted average	0.941	0.021	0.841	0.880	0.861

Fig. 8 represents the detailed accuracy by class for UNSW-NB15 dataset.

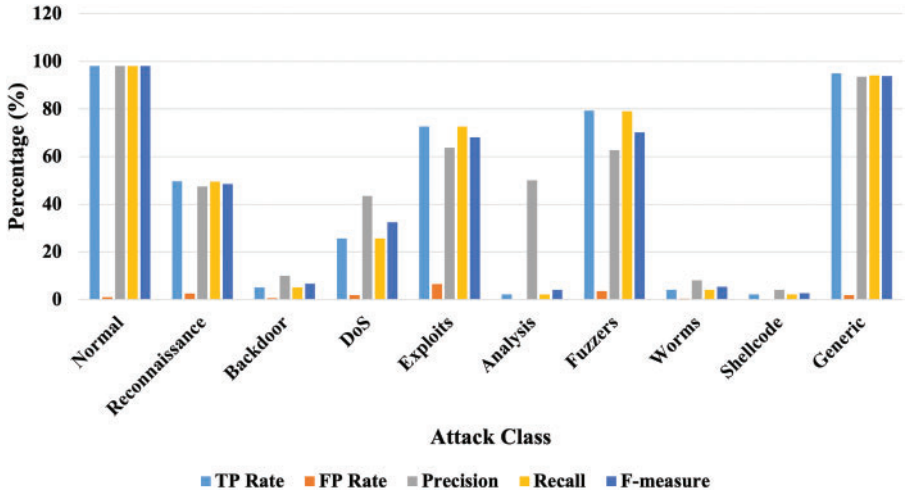

Figure 8: Accuracy by class for UNSW-NB15 dataset

Next, we provide MCC value, ROC curve area, and PRC area for UNSW-NB15 dataset in Table 10.

Table 10: MCC, ROC area, and PRC area for UNSW-NB15 train data

Class	MCC	ROC area	PRC area
Normal	0.981	0.991	0.981
Reconnaissance	0.460	0.956	0.458
Backdoor	0.101	0.926	0.151
DoS	0.307	0.921	0.356
Exploits	0.627	0.955	0.726
Analysis	0.101	0.940	0.135
Fuzzers	0.681	0.958	0.781
Worms	0.051	0.901	0.071
Shellcode	0.041	0.911	0.064

(Continued)

Table 10 (continued)

Class	MCC	ROC area	PRC area
Generic	0.920	0.990	0.980
Weighted average	0.734	0.982	0.869

Fig. 9 represents MCC, ROC area, and PRC area for UNSW-NB15 dataset. The experimentation results show that our proposed model offers high accuracy of 95.0674% using the NSL-KDD dataset. The proposed model also offers a reduced FP rate of 5.1% using the NSL-KDD dataset and 2.1% using the UNSW-NB15 dataset.

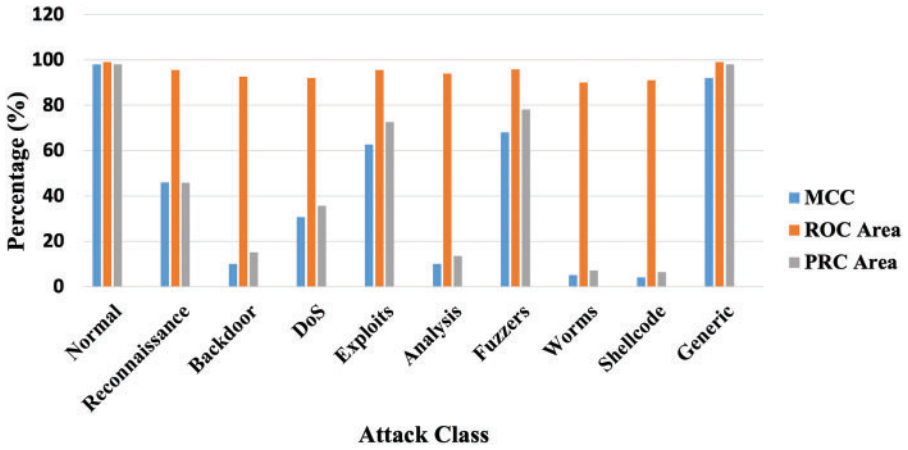

Figure 9: MCC, ROC area, and PRC area for UNSW-NB15 dataset

6 Conclusions and Future Work

The rapid advancement of IoT technologies is transforming existing healthcare systems on technological, social, and economic levels. The Internet of Medical Things (IoMT) merges IoT with healthcare services to enable remote patient monitoring and reduce treatment costs. Wearable and implantable medical devices, integral to IoMT-based Smart Healthcare Systems (SHS), significantly enhance the healthcare domain's value. However, the security of IoMT-based SHS is crucial, as cyberattacks or security breaches can severely impact patient health and, in extreme cases, may lead to fatalities. In this paper, we developed an intrusion detection system utilizing deep learning techniques and benchmark datasets. We propose a Multilayer Perceptron (MLP)-based framework specifically designed for the smart healthcare domain's intrusion detection needs. This framework was implemented in the WEKA tool, and we conducted comprehensive evaluations to assess its effectiveness and efficiency. For these evaluations, we employed the benchmark NSL-KDD and UNSW-NB15 datasets, achieving very promising results. Our evaluation demonstrates that the proposed framework delivers high accuracy, recall, precision, and F-score values, while significantly reducing the false positive rate. In the future, we aim to incorporate semi-supervised and unsupervised learning techniques in our system to further improve the detection of new and modern cyberattacks including zero-day attacks.

Furthermore, we intend to incorporate new data sources including real-time patient data and device telemetry to improve the framework's intrusion detection capabilities.

Acknowledgement: The Researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for financial support (QU-APC-2024-9/1).

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Attiya Khan and Muhammad Rizwan conceptualized the study and led the investigation. Methodology was developed by Attiya Khan and Ovidiu Bagdasar, with implementation and data curation by Attiya Khan and Abdulatif Alabdulatif. Validation was conducted by Muhammad Rizwan, Ovidiu Bagdasar and Sulaiman Alamro. Resources and visualization were provided by Attiya Khan, Ovidiu Bagdasar and Abdullah Alnajim. Attiya Khan and Muhammad Rizwan wrote the original draft, with review and editing by all authors. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The datasets generated during and/or analyzed during the current study are available in the NSL-KDD repository https://www.kaggle.com/datasets/hassan06/nslkdd (accessed on 04 December 2023) and the UNSW-NB15 repository https://www.kaggle.com/datasets/dhoogla/unswnb15 (accessed on 08 December 2023).

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Vaiyapuri T, Binbusayyis A, Varadarajan V. Security, privacy and trust in IoMT enabled smart healthcare system: a systematic review of current and future trends. Int J Adv Comput Sci Appl. 2021;12:731–7. doi:10.14569/IJACSA.2021.0120291.
2. Mohammed BG, Hasan DS. Smart healthcare monitoring system using IoT. Int J Interact Mob Technol. 2023;17(1):141. doi:10.3991/ijim.v17i01.34675.
3. Raj A, Prakash S. Smart contract-based secure decentralized smart healthcare system. Int J Softw Innov. 2023;11(1):1–20. doi:10.4018/ijsi.315742.
4. Vishnu S, Ramson SJ, Jegan R. Internet of medical things (IoMT)–an overview. In: 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), 2020; Nanjing, China: IEEE; p. 101–4.
5. Subhan F, Mirza A, Su'ud MBM, Alam MM, Nisar S, Habib U, et al. AI-enabled wearable medical internet of things in healthcare system: a survey. Appl Sci. 2023;13(3):1394. doi:10.3390/app13031394.
6. Rayan RA, Zafar I, Tsagkaris C. IoT technologies for smart healthcare. Adv Data Sci Anal: Concepts Paradigm. 2023;63:181–202. doi:10.1002/9781119792826.ch8.
7. Chen X, Xie H, Li Z, Cheng G, Leng M, Wang FL. Information fusion and artificial intelligence for smart healthcare: a bibliometric study. Inf Process Manag. 2023;60(1):103113. doi:10.1016/j.ipm.2022.103113.
8. Karthick R, Ramkumar R, Akram M, Kumar MV. Overcome the challenges in bio-medical instruments using IOT–a review. Mater Today: Proc. 2021;45:1614–9. doi:10.1016/j.matpr.2020.08.420.
9. Papaioannou M, Karageorgou M, Mantas G, Sucasas V, Essop I, Rodriguez J, et al. A survey on security threats and countermeasures in internet of medical things (IoMT). Trans Emerg Telecomm Technol. 2020;4:e4049. doi:10.1002/ett.4049.

10. Newaz AI, Haque NI, Sikder AK, Rahman MA, Uluagac AS. Adversarial attacks to machine learning-based smart healthcare systems. In: GLOBECOM 2020-2020 IEEE Global Communications Conference, 2020; Taipei, Taiwan: IEEE; p. 1–6.
11. Tariq N, Qamar A, Asim M, Khan FA. Blockchain and smart healthcare security: a survey. Procedia Comput Sci. 2020;175:615–20. doi:10.1016/j.procs.2020.07.089.
12. Habibzadeh H, Soyata T. Toward uniform smart healthcare ecosystems: a survey on prospects, security, and privacy considerations. In: Connected health in smart cities. Berlin, Germany: Springer; 2020. p. 75–112.
13. Almogren A, Mohiuddin I, Din IU, Almajed H, Guizani N. FTM-IoMT: fuzzy-based trust management for preventing sybil attacks in Internet of Medical Things. IEEE Internet of Things J. 2020;8(6):4485–97. doi:10.1109/JIOT.2020.3027440.
14. Ambarkar SS, Shekokar N. Toward smart and secure IoT based healthcare system. In: Internet of things, smart computing and technology: a roadmap Ahead. Berlin, Germany: Springer; 2020. p. 283–303.
15. Koutras D, Stergiopoulos G, Dasaklis T, Kotzanikolaou P, Glynos D, Douligeris C. Security in IoMT communications: a survey. Sensors. 2020;20(17):4828. doi:10.3390/s20174828.
16. Umamaheswaran S, Mannar Mannan J, Karthick Raghunath K, Dharmarajlu SM, Anuratha M. Smart intrusion detection system with balanced data in IoMT infra. J Intell Fuzzy Syst. 2024;46(2):3191–207. doi:10.3233/JIFS-233649.
17. Sun Z, An G, Yang Y, Liu Y. Optimized machine learning enabled intrusion detection 2 system for internet of medical things. Franklin Open. 2024;6:100056. doi:10.1016/j.fraope.2023.100056.
18. Alzubi JA, Alzubi OA, Qiqieh I, Singh A. A blended deep learning intrusion detection framework for consumable edge-centric IoMT industry. IEEE Trans Consum Electron. 2024;70(1):2049–57. doi:10.1109/TCE.2024.3350231.
19. Alalhareth M, Hong SC. An adaptive intrusion detection system in the internet of medical things using fuzzy-based learning. Sensors. 2023;23(22):9247. doi:10.3390/s23229247.
20. Gupta K, Sharma DK, Gupta KD, Kumar A. A tree classifier based network intrusion detection model for Internet of Medical Things. Comput Electr Eng. 2022;102(5):108158. doi:10.1016/j.compeleceng.2022.108158.
21. Sarosh P, Parah SA, Bhat GM, Muhammad K. A security management framework for big data in smart healthcare. Big Data Res. 2021;25(1):100225. doi:10.1016/j.bdr.2021.100225.
22. Zhong H, Zhou Y, Zhang Q, Xu Y, Cui J. An efficient and outsourcing-supported attribute-based access control scheme for edge-enabled smart healthcare. Future Gener Comput Syst. 2021;115(1):486–96. doi:10.1016/j.future.2020.09.021.
23. Farhin F, Kaiser MS, Mahmud M. Secured smart healthcare system: blockchain and bayesian inference based approach. In: Proceedings of International Conference on Trends in Computational and Cognitive Engineering, 2021; Guangzhou, China: Springer; p. 455–65.
24. Wang W, Huang H, Xiao F, Li Q, Xue L, Jiang J. Computation-transferable authenticated key agreement protocol for smart healthcare. J Syst Archit. 2021;118(25):102215. doi:10.1016/j.sysarc.2021.102215.
25. Quamara M, Gupta BB, Yamaguchi S. 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), 2021; Kyoto, Japan: IEEE; p. 1–4.
26. Subasi A, Algebsani S, Alghamdi W, Kremic E, Almaasrani J, Abdulaziz N. Intrusion detection in smart healthcare using bagging ensemble classifier. In: International Conference on Medical and Biological Engineering, 2021; Valencia, Spain: Springer; p. 164–71.
27. Haque AB, Muniat A, Ullah PR, Mushsharat S. An automated approach towards smart healthcare with blockchain and smart contracts. In: 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), 2021; Shenzhen, China: IEEE; p. 250–5.

28. Helen S, Senthilsingh C. Blockchain based smart healthcare systems in 5G networks for preventing data forgery. 2021. Available from: https://api.semanticscholar.org/CorpusID:233969622. [Accessed 2004].
29. Anand A, Singh AK, Lv Z, Bhatnagar G. Compression-then-encryption-based secure watermarking technique for smart healthcare system. IEEE MultiMedia. 2020;27(4):133–43. doi:10.1109/MMUL.2020.2993269.
30. Nguyen DC, Pathirana PN, Ding M, Seneviratne A. A cooperative architecture of data offloading and sharing for smart healthcare with blockchain. arXiv preprint arXiv: 210310186. 2021.
31. Khan J, Li JP, Haq AU, Khan GA, Ahmad S, Abdullah Alghamdi A et al. Efficient secure surveillance on smart healthcare IoT system through cosine-transform encryption. J Intell Fuzzy Syst. 2021;40(1):1417–42. doi:10.3233/JIFS-201770.
32. Haque NI, Rahman MA, Shahriar MH, Khalil AA, Uluagac S. A novel framework for threat analysis of machine learning-based smart healthcare systems. arXiv preprint arXiv: 210303472. 2021.
33. Gope P, Sikdar B, Millwood O. A scalable protocol level approach to prevent machine learning attacks on puf-based authentication mechanisms for internet-of-medical-things. IEEE Trans Indust Inform. 2021;18(3):1971–80. doi:10.1109/TII.2021.3096048.
34. Tripathi G, Ahad MA, Paiva S. S2HS–a blockchain based approach for smart healthcare system. Healthcare. 2020;8(1):100391. doi:10.1016/j.hjdsi.2019.100391.
35. Chen B, Qiao S, Zhao J, Liu D, Shi X, Lyu M, et al. A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. IEEE Internet Things J. 2020;8(13):10248–63. doi:10.1109/JIOT.2020.3041042.
36. Zhou T, Shen J, He D, Vijayakumar P, Kumar N. Human-in-the-loop-aided privacy-preserving scheme for smart healthcare. IEEE Trans Emerg Top Comput Intell. 2020;6(1):6–15. doi:10.1109/TETCI.2020.2993841.
37. Kumar M, Chand S. A secure and efficient cloud-centric internet-of-medical-things-enabled smart healthcare system with public verifiability. IEEE Internet Things J. 2020;7(10):10650–9. doi:10.1109/JIOT.2020.3006523.