AI FOR IOMT SECURITY: A SURVEY OF INTRUSION DETECTION SYSTEMS, ARCHITECTURES, ATTACKS AND CHALLENGES

Ghaida Balhareth, Mohammad Ilyas, and Basmh Alkanjar

Department of Electrical Engineering & Computer Science, Florida Atlantic University, 777 Glades Road, Boca Raton, FL 33431, USA.

ABSTRACT

The Internet of Medical Things (IoMT) has transformed healthcare by allowing real-time patient monitoring, remote diagnoses, and effective data interchange. The increasing reliance on interconnected medical equipment has increased cybersecurity risks for healthcare organizations. This survey offers an extensive examination of Intrusion Detection Systems (IDSs) targeted for IoMT contexts. This surveyemphasizes the proposed methods that used to build IDS,classifying them into machine learning (ML), deep learning (DL), fuzzy logic (FL), and hybrid approaches for safeguarding healthcare networks. This paper investigates the IoMT architecture, identifies security concerns across multiple tiers, and analyzes potential vulnerabilities including denial-of-service attacks, ransomware, and man-in-the-middle attacks. The research highlights the significance of IDSs in alleviating cyber threats and protecting sensitive medical information through a comparison of cutting-edge methodologies. We outline significant issues that persist and emphasize domains requiring additional research to enhance the security and resilience of IoMT systems.

KEYWORDS

Machine learning, Deep learning, Fuzzy logic, Intrusion Detection Systems (IDS), Internet of Medical Things (IoMT).

1. INTRODUCTION

The exponential growth of networked devices within the Internet of Things (IoT) has dramatically improved the effectiveness and simplicity of providing services in various sectors, including healthcare [1] [2]. The Internet of Medical Things (IoMT) has provided unprecedented prospects in the medical sector to enhance care delivery by improving the collection, transfer, and analysis of patient data for healthcare providers [3]. IoMT devices, including wearables, remote monitoring systems, and diagnostic equipment specifically developed for home use, enable a direct connection between patients and physicians [4]. Moreover, IoMT technologies enable direct communication between patients and healthcare providers, decrease the strain on healthcare systems, and reduce the number of unnecessary hospital visits. In addition, they assist in the earliest possible diagnosis, safeguarding the health and well-being of patients [5]. IoMT also holds the potential to improve diagnosis accuracy, lower healthcare costs, and reduce medical errors by allowing real-time data transmission [1]. Nevertheless, the expanded interconnectivity of IoMT devices raises considerable security and privacy issues, as they are susceptible to various kinds of cyber-attacks [6]. IoMT networks are vulnerable to cyber-attacks such as ransomware, denial-of-service (DoS) attacks, and man-in-the-middle (MitM) attacks, which can compromise sensitive medical data and even endanger patient lives. These devices collect and transmit highly sensitive information on medical health problems, including essential

biological signs, patient monitoring, and other health-related data [7]. For example, during the worldwide COVID-19 pandemic, there was a recognition of the need for robust digital technology solutions to provide remote medical interventions, which also increased the opportunities for cyber-attacks on healthcare institutions, including hospitals, patient and clinical data repositories, and laboratories [8].Over the years, various security measures have been devised to safeguard IoMT systems, including encryption, authentication, and intrusion detection [7]. However, the interconnectivity of these systems also presents notable security barriers, hence requiring the implementation of resilient. IDSs specifically designed for IoMT environments. IDSs play a critical role in identifying and mitigating security threats in IoMT networks by employing techniques such as signature-based detection, anomaly detection, and policy enforcement [9]. On the other hand, existing IDS solutions usually fail due to scalability and the continuous creation of new attacks and utilization of advanced hacking techniques by attackers [10]. To address this, researchers are exploring new artificial intelligence (AI) methods, particularly ML, DL, FL and hybrid approaches, all of which offer promising new avenues for enhancing IDS performance in these complex environments.

This survey addresses a notable gap in the literature by providing a focused overview of IDS approaches tailored for IoMT contexts. Current studies often emphasize general IoT security or underscore traditional IDS approaches, overlookingthe distinct challenges and requirements of IoMT systems. Table 1 presents a comprehensive comparison of recently published surveys, illustrating the methodologies addressed, and focused areas, and how this study expands upon these works. Although each survey provides significant insights regarding IoMT security, they vary in scope and depth.

Table 1. A Comparison of our Survey with Related State-of-the-Art Surveys.

Study	**Year**	**Field**	**Method Covered**				**Classification IDS**	**Architecture of IoMT**	**Security Requirements**	**Attacks on IoMT**
			ML	**DL**	**Hybrid**	**Fuzzy Logic**				
[11]	2022	IoMT	√	X	X	X	X	√	√	√
[1]	2022	IoMT	√	√	X	X	X	X	X	X
[12]	2023	IoT	√	√	√	X	X	X	X	√
[13]	2022	IoMT	√	√	X	X	X	√	√	√
[14]	2023	IoT	√	√	√	X	√	X	X	√
[15]	2024	IoMT	√	√	X	X	X	√	X	√
[16]	2022	IoT	√	√	X	X	√	X	X	X
[17]	2022	IoT	√	√	X	X	√	X	X	X
[10]	2023	IoMT	√	X	X	X	X	√	√	√
[18]	2023	IoMT	√	√	√	X	√	√	√	√
[19]	2024	IoT	√	√	√	√	X	X	X	X
Our Survey	2024	IoMT	√	√	√	√	√	√	√	√

The key contributions of this study include:

- We illustrate the IDS background and a clear framework for evaluating the performance of IDS systems using commonly accepted metrics such as accuracy, recall, f1-score, and precision.

- We propose a classification of the techniques that have been used for the IDS into ML, DL, hybrid, and FL approaches.
- We explain a four-layer IoMT architecture and the potential security threats targeting each layer.
- We illustrate numerous challenges in the advancement and implementation of IDSs within the IoMT systems.

The remaining sections of this research are organized as follows: Section 2 provides fundamental insights into Intrusion Detection System within the IoMT, including an evaluation of IDS performance and the role of AI in IDS. Section 3 presents an overview of related works. Section 4 describes the IoMT architecture and examines the security threats associated with each layer. Section 5 outlines the security requirements for protecting IoMT environments. Section 6 explores the different categories of attacks targeting IoMT systems. Section 7 details the challenges associated with the security of IoMT. Finally, Section 8 concludes our paper.

2. INTRUSION DETECTION SYSTEM

2.1. Background on IDSs in the IoMT

An Intrusion Detection System is a component of hardware or software that monitors networks and computer systems for suspicious activity. In the context of the IoMT, an IDS is critical in protecting medical data and guaranteeing the efficient functioning of interconnected medical equipment. According to Attou (2023), it entails a methodical approach to the monitoring, detection, and identification of detrimental behaviors that occur within the network environment. The IDS framework consists of three primary components. The monitoring component analyzes traffic flow behaviors. The detection component recognizes potentially suspicious actions and rapidly notifies the reaction component of any detected occurrences [20]. lastly, the reaction component activates an alarm or alerts network management.

2.2. IDSs in IoMT Security

IDSs are a key component of IoMT security, addressing growing concerns about cyber threats and vulnerabilities by protecting sensitive medical data and ensuring reliable operation of interconnected devices. Unlike conventional firewalls, IDSs identify and classify various forms of suspicious network traffic and cyber activities, effectively detecting and monitoring potential security breaches [21].

Among their many benefits, IDSs offer the ability to promptly identify and neutralize cyber threats through real-time detection mechanisms. Their dynamic nature, leveraging anomaly detection and machine learning, enables them to address emerging and previously unknown threats, such as zero-day attacks. By mitigating the impact of cyber incidents, IDSs help ensure the seamless operation of healthcare systems, preserving both patient safety and the efficiency of IoMT environments.

IDSs use two main detection methods: signature-based detection (SIDS) and anomaly-based detection (AIDS). SIDS, or knowledge-based detection, matches data patterns against a database of known attack signatures. However, it cannot detect new attacks and is resource-intensive due to maintaining a large signature database [22]. AIDS, or AI-based IDS, assumes malicious behaviors differ from normal activity, using AI algorithms to model standard behaviors and flag deviations as potential attacks [23]. AIDS can detect new and unknown attacks and is effective for zero-day threats, offering adaptability to specific networks and applications [24].

2.3. Evaluating IDS Performance

Understanding the performance metrics frequently employed in IDS research is essential to evaluating an IDS effectively. These metrics are crucial for evaluating the accuracy and reliability of intrusion detection algorithms[25]. The confusion matrix is an essential tool for this assessment, categorizing detection results into the following: True Negative (TN), True Positive (TP), False Negative (FN), and False Positive (FP) rates. The definitions of these metrics are as follows:

- *TN* refers to the quantity of benign data included in the IoMT network traffic, which is considered harmless.
- *TP* is the quantity of malicious data within network traffic on IoMT that is classified as suspicious.
- *FN* refers to the malicious samples in the IoMT network traffic that are incorrectly considered normal.
- *FP* represents the benign or regular samples in the IoMT network traffic incorrectly identified as harmful samples or assaults. From the confusion matrix, key performance metrics such as accuracy, recall, f1-score, precision.

Key performance metrics such as accuracy, recall, f1-score, precision, TPR, and FPR can be derived from these categories. The following formulas define the metrics commonly used to assess IDS performance:

- **Accuracy**is a measure that quantifies the ratio of accurately predicted samples to the total number of instances.

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

- **Recall:** is computed as the percentage of the total count of true positives divided by the sum of all true positives.

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

- **F1-score** is calculated as the harmonic average of the recall and precision measures, with their weights considered. The harmonic average is employed as an alternative to the basic arithmetic mean to assign greater importance to smaller values, effectively penalizing any disparities in precision and memory.

$$F1\text{-}score = 2 \cdot \frac{Precision.Recall}{Precision+Recall} \quad (3)$$

- **Precision** is a measure that quantifies the ratio of accurately detected positive results among all the observations that are predicted as positive.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

- **TPR** is the ratio of the number of correctly identified positive samples to the total number of actual positive samples.

$$TPR = \frac{TP}{TP+FN} \quad (5)$$

- **FPR** represents the proportion of negative events incorrectly forecasted as positive out of the total negative events.

$$FPR = \frac{FP}{FP+TN} \quad (6)$$

An additional crucial component in assessing classification efficacy is the receiver operating characteristic (ROC) curve, along with the area under the curve (AuC) score. The ROC curve illustrates the TPRvs the FPR, while the AuC score, which ranges from 0.5 to 1.0, indicates the

classification performance of an IDS. In evaluating an IDS, both FPR and accuracy are critical, as high accuracy and low FPR are needed to detect threats while minimizing interruptions. For example, a study [26] using the UNSW-NB15 dataset assessed IDS models with these metrics, noting that high accuracy can obscure a high FPR, especially in imbalanced datasets. A low FPR reduces false alarms, enhancing system usability, highlighting the need to balance accuracy and FPR for effective IDS development.

2.4. AI in IDS for the IoMT

The integration of AI methods, such as ML, DL, and FL has significantly enhanced IDSs in addressingdiverse cyber threats while safeguarding sensitive medical information. These AI-driven systems monitor network traffic, detect irregularities, and implement responses to minimize risks [7]. Unlike conventional IDSs, IoMT systems require advanced methods to manage the large-scale, fast-paced data that generated by medical devices,which often utilize complex communication protocols and data formats. Table 2 below summarizes the advantages and disadvantages of three AI methods frequently employed in IDSs for IoMT security.

Table 1. Advantages and disadvantages of AI methods in IDS for IoMT security

Method	Advantages	Disadvantages
Machine Learning (ML)	Widely used for recognizing malicious patterns and adapting to new threats[27]. Excels at identifying known attacks (supervised learning) and discovering unknown patterns (unsupervised learning).	Relies on labelled datasets and is susceptible to false positives in imbalanced data.
Deep Learning (DL)	Efficiently processes high-dimensional data and automates feature extraction. Enables accurate detection of complex threats, including zero-day attacks.	High computational requirements and ‘black-box’ nature may limit its use in resource-constrained IoMT environments.
Fuzzy Logic (FL)	Effectively handles uncertainty in medical data, reducing false positives and enhancing reliability in sensitive contexts [28].	Rule-based systems can be hard to scale and may struggle with complex attack patterns without integration with other techniques.

By combining these methods, IDSs in IoMT security can address evolving threats, leveraging the strengths of each approach to enhance adaptability, accuracy, and reliability.

3. RELATED WORKS

Several surveys discuss various facets of cybersecurity in IoMT contexts. However, only a few studies specifically address using AI approaches in IDSs to enable the security of smart healthcare organizations. We present a complete taxonomy to clarify the various IDS methodologies utilized in the IoMT. Our taxonomy classifies IDS systems according to advanced detection methods, covering ML, DL, hybrid approaches, and fuzzy logic techniques, as illustrated in Figure 3.

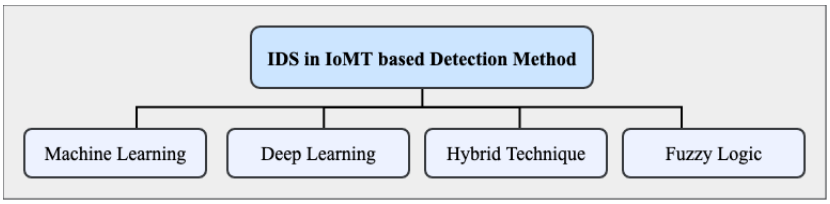

Figure. 3. IDS Classification Taxonomy in IoMT based on Detection Methods.

3.1. IDS-Based ML

The work presented by [29], the authors adeptly combined the Random Forest (RF) algorithm with a complex feature scaling method to manage extensive and intricate categorical data in IoMT networks. This method is especially valuable for e-healthcare systems, where processing large datasets efficiently is crucial. By reducing both the feature size and the number of instances, the framework significantly improved classification speed while maintaining high accuracy, achieving an average accuracy of 94.23%.

This research emphasizes the most recent scholarly works on attack types and employs an ML-based framework for network assistance in the IoT and intrusion detection [30]. Hence, the present study encompasses a comprehensive examination of various intelligence techniques and their implemented frameworks for network IDSs, with a specific emphasis on IoT threats and intrusion detection strategies based on ML.

The authors in [31] propose a decision-making system utilizing the IoMT to identify breast cancer detection. The system utilizes a region expanding algorithm to identify concerning areas in the breast, subsequently applying texture and shape-based feature extraction approaches, such as center-symmetric local binary pattern (CS-LBP), histogram of oriented gradients (HOG), and statistical techniques. A combination of ML algorithms, such as K-Nearest Neighbor (KNN), Support Vector Machine (SVM), and Linear Discriminant Analysis (LDA), are then used to classify these features. The model shows promise for precise early breast cancer detection with 96.3% accuracy, 94.1% sensitivity, and 98.2% specificity when tested on the MIAS database.

The research introduces a novel form of insider attack known as a loophole attack, which capitalizes on the weaknesses inherent in the routing over low power and lossy networks (RPL) routing protocol, which is extensively employed in IoT devices [32]. The suggested attack was executed utilizing a Contiki IoT operating system that operates on the Cooja simulator, and an analysis was conducted to assess the consequences of the assault. The analysis of the gathered online traffic data reveals that the utilization of ML techniques, in conjunction with the suggested characteristics, effectively facilitates the precise identification of insider attacks within network traffic data.

The study utilizes an ML-supervised algorithm-based IDS for the IoT [33]. The initial phase of this study approach involved applying feature scaling to the UNSW-NB15 dataset using the minimum-maximum (min-max) normalization concept. This was done to prevent any loss of information on the test data. The data set consists of a blend of contemporary attacks and routine network traffic activities. Principal component analysis (PCA) was used to conduct dimensionality reduction in the subsequent stage. The results were compared to previous studies, and the findings demonstrated competitiveness, with an accuracy rate of 99.9% and a mean squared error (MCC) of 99.97%.

3.2. IDS-Based DL

The study presents an improved anomaly-based DL approach for IDSs [34]. The CICIDS2017 dataset has a multi-class classification model (EIDM) capable of accurately classifying 15 traffic behaviors encompassing 14 different attack types, with a classification accuracy of 95%. A comprehensive comparison analysis is undertaken to evaluate the classification accuracy and efficiency metrics of EIDM with other advanced DL-based IDSs.

Another research introduces a novel methodology for network-based ID in the context of IoMT systems [35]. The proposed strategy leverages DL techniques to analyse network traffic and patient biometrics. The model under consideration demonstrated a 10-fold cross-validation accuracy of 95% when applied to network features, 89\% when applied to patient biometrics, and 99% when applied to combination features. The proposed model's resilience and generalization ability is demonstrated by tests conducted on several network-based intrusion datasets in addition to the IoMT environment.

The literature study proposed a methodology for identifying unauthorized individuals during the transmission of data, enabling the effective and precise examination of medical data at the periphery of the network [36]. A real-time NF-ToN-IoT dataset was utilized to evaluate the system's performance in the context of IoT applications. This dataset encompassed operating systems and healthcare data. The experimental findings demonstrate that the suggested model achieves an accuracy rate of 89.0% when applied to the ToN-IoT dataset.

In the study [37], the authors utilized particle swarm optimization (PSO) to choose features and subsequently employed ML/DL models to identify cyber assaults in the IoMT. An evaluation of the performance of the suggested approach was conducted using the NSL-KDD datasets. The PSO and RF-based solution achieved the maximum accuracy of 99.76%. Nevertheless, the evaluation of threat detection in IoMT networks should not be done using the NSL-KDD dataset since it was not designed with the IoT network environment in perspective.

Cybersecurity threats, such as man-in-the-middle assaults on the IoMT communication network, are highlighted in the study [38]. PCA is utilized to optimize the features, while a multi-layer perceptron is employed to categorize unforeseen cyber-attacks on healthcare equipment, with a specific focus on those originating from the IoT. The technique's efficacy is evaluated using real-time data from the WUSTL-EHMS, which stands for the St. Louis Enhanced Healthcare Monitoring System. According to the results, the multi-layer perceptron outperformed the other classifiers tested with a 96.39% accuracy rate.

3.3. IDS-Based Hybrid

The authors in [39] proposed a novel hybrid method that combines ML and DL to enhance detection rates while ensuring dependability. A comparative analysis is conducted between the created technique and many ML, and DL approaches to determine the most efficient algorithm for integration into the pipeline. The optimal network intrusion model is chosen by evaluating a stringent set of evaluated performance analysis criteria. The suggested method demonstrates exceptional efficacy on two distinct datasets, namely KDDCUP’99 and CIC-MalMem-2022, achieving accuracy rates of 99.99% and 100\%, respectively. Notably, there are no cases of overfitting or Type-1 for either dataset.

An intrusion detection model for the industrial IoT was created by [40] using a two-phase hybrid approach. In the first step, we combine SVM and NB into an ensemble. I utilized the RF approach to predict the labels for the classes. To improve the accuracy of the predictions even

further, an ANN classifier based on Adam's optimization was employed. While taking into consideration the maximum accuracy value, the second phase is fed the outputs of the ANN and RF.

In another study [41], a novel hybrid IDS model for the IoMT network was introduced. The model involves the analysis of patients' health data collected from various wearable sensors and utilizes a genetic algorithm to forecast unexpected intrusions at the network's edge. The aim is to address and avoid security and privacy issues. The research results showed more accurate and precise identification of attacks taking place during data transmission in the network compared to the ToN-IoT data set.

The research introduces a hybrid intelligent IDS that combines ML and metaheuristic methods [42]. The HHIIDS is designed for IoT applications, specifically in the healthcare sector. The performance evaluation of the proposed HIIDS was conducted using the widely used NSL-KDD dataset, which consists of 41 characteristics and 125,973 samples. The implementation of six variations of suggested hybrid algorithms, which combine GA, PSO, and DE with KNN and DT, is carried out using MATLAB 2019b. The accuracy achieved by the GA-DT version is 99.88%. A healthcare architecture based on the IoT is developed, employing a hybrid GA-DT version-based HIIDS to effectively identify and mitigate harmful network traffic.

The study [43] introduces SafetyMed, a specialized IDS designed to enhance the security of the IoMT. The author improved the reliability of IDSs and decreased the number of false alarms by combining convolutional neural networks (CNNs) with long short-term memory (LSTM) models to examine data that are structured in a grid or a sequence. This study successfully implemented network monitoring to ensure that only authorized devices were allowed to connect. Through the implementation of these security measures, confidential patient data was safeguarded against unauthorized access.

Another research presents a novel hybrid architecture called "Immune-Net" that utilizes DL to identify and protect healthcare data from the most recent intrusion assaults [44]. To achieve high accuracy and performance, the given model employs several procedures under biomedical engineering, oversampling approaches to enhance hyper-parameter optimization, and class balancing strategies. Immune-Net demonstrated superior performance on the CIC Bell DNS 2021 dataset, achieving an accuracy of approximately 99.19%, precision of 99.22%, recall of 99.19%, and ROC-AUC scores of 99.2%.

3.4. IDS-Based Fuzzy Logic

The research presents the design of a failure detection framework for the Internet of Nano Things architecture in the medical field using fuzzy logic [45]. The design of the fuzzy defect detection system was informed by two established methodologies, namely the Takagi-Sugeno-Kang (TSK) and Mamdani fuzzy systems. The computer simulation and comparison analysis conducted on 37 individuals with atherosclerosis provide evidence that the suggested technique effectively identifies the underlying cause and extent of defects in the nanonetwork.

The research study examines the issue of achieving precise and comprehensible intrusion detection in IoT systems through the knowledge-discovery ML methodology designed for threat detection [46]. The study utilizes a fuzzy rule-based classifier to optimize the accuracy-interpretability trade-off of IoT IDSs. The proposed technique is based on an extension of the widely recognized multi-objective evolutionary optimization algorithm. The primary contribution of the study is the development of precise and comprehensible IoT IDSs using the latest data sets, known as the MQTT-IOT-IDS2020 data sets.

Literature research offers a meticulous examination of the latest and most pertinent cutting-edge techniques for ensuring security in the IoT. The study presents a novel security mechanism, referred to as GLSF2IoT, which aims to identify malevolent behaviors in undetermined IoT settings by using a fog-based and fuzzy logic-based method [47]. The concept is founded around the premise of "zero trust," which entails placing no faith in anything and perceiving everything as hostile. Upon the detection of malicious behaviors, GLSF2IoT promptly restricts network access to the IoT device responsible for initiating the activity, therefore preventing it from affecting other devices.

The IoMT sensors transmit data to a server for rapid diagnosis in the medical field. The biometric input employed in the literature is frequency domain-based bio-acoustics. The study presents a novel user authentication scheme for IoMT applications by utilizing a secure lightweight bioacoustics approach and including a fuzzy embedder [48]. To safeguard the network from attacks by previous sensor nodes, the suggested strategy utilizes the remainder technique to produce a group secret key. The security of the proposed system is assessed using the formal verification tool AVISPA.

Literature research presents the Duo-Secure IoMT framework, which utilizes data from multi-modal sensory signals to distinguish between attack patterns and normal data from IoMT devices [49]. The suggested model employs a hybrid approach, integrating dynamic Fuzzy C-Means clustering with a customized Bi-LSTM algorithm. The study utilizes a dataset of 36 variables and 18940 cases to assess heart disease. The proposed model effectively analyses two aspects: a) the prediction of cardiac difficulties and b) the detection of network malware. The individual accuracy achieved by the model is 92.95%, while the multi-modal joint precision is 89.67% in the distributed network environment based on the IoMT.

Literature work introduces a novel clustering approach for IoMT applications, referred to as the FC-IoMT technique, which utilizes fuzzy logic [50]. The FC-IoMT approach employs five input factors: Energy, Distance, Delay, Capacity, and Queue to determine the cluster heads (CHs). The use of the FC-IoMT technology has the potential to yield a substantial reduction in energy usage inside the IoMT system. The suggested model has been subjected to thorough validation, and the outcomes have consistently demonstrated higher performance across several metrics.

4. IOMT ARCHITECTURE

Utilizing the architecture of the IoMT is vital for this work, and the following section investigates security attacks that target these environments. Several studies suggest different IoMT architectures. Some recommend a three-layer architecture [11][51][10]. Other researchers recommend using more than three layers [18][52][53]. Researchers have not reached a consensus on a single IoMT architecture. The various structures of the IoMT are formed by important aspects such as the development of the IoMT, the functional requirements of applications, and significant concerns about security and privacy in the IoMT. This survey represents a four-layer architecture as the most logical division for the IoMT framework. The four layers are the perception layer, network layer, middleware layer, and application layer, as illustrated in Figure 4. Each layer serves a particular purpose in the IoMT process, encompassing data collection via sensors and wearable devices from patients, as well as the storage, processing, and presentation of this data to both patients and healthcare providers. The IoMT architecture facilitates the effective transmission of substantial data amounts, enabling the remote monitoring of diverse health metrics in patients.

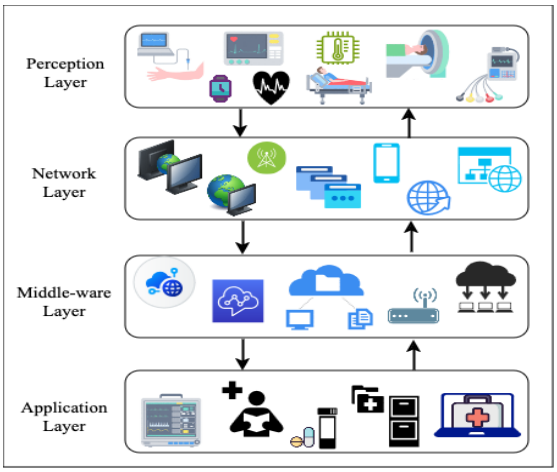

Figure 3: The Four-Layers Architecture of The IoMT

4.1. Perception Layer

The perception layer is the initial layer of the IoMT architecture, comprising medical devices that collect, analyze, and organize sensor data, such as temperature, heart rate, and pressure. These devices facilitate further analysis and decision-making and are categorized based on their placement in the human body [54]:

- Implantable devices: are inserted into the body through surgery to assist with or replace physiological activities; examples include insulin pumps, artificial joints, and heart pacemakers.
- Wearable devices: provide ongoing monitoring and customized health services that can be worn on the human body; examples include pulse generators (PG), pain relief devices, fitness devices, and smartwatches.
- Ambient devices: These blend seamlessly into the patient's environment, constantly monitoring health metrics without necessitating direct user engagement; examples include bed sensors, room temperature, and humidity.
- Stationary devices: Primarily found in clinical settings, these are utilized for diagnosis, treatment, and monitoring, including x-ray machines and computed tomography (CT) scanners.

The FDA categorizes IoMT devices by patient risk. High-risk devices like EEGs and defibrillators undergo strict regulation, while low-risk devices such as fitness monitors and smartwatches face less scrutiny. Medical equipment and sensors transmit raw biological data (e.g., brain signals, heart rate) in real-time through communication protocols to the network layer for further processing [55].

4.2. Network Layer

The network layer facilitates connectivity in the IoMT environment by enabling interaction and data transfer between medical devices, healthcare applications, and sensors. It forms the foundation of healthcare platform architecture but faces significant security challenges due to sensitive data transmission. Protocols in this layer often adhere to the IEEE 802.15 standard [56] and operate on short-range (e.g., Bluetooth, NFC, WSNs, RFID, UWB, Zigbee) or long-range (e.g., blockchain, LoRaWAN) communication frequencies [53]. Wi-Fi and ZigBee are the most widely used protocols in IoMT for their adaptability, while Bluetooth sees limited use due to its

shorter range [11]. UWB is another cost-effective option for short-distance data transmission using infrared light.

4.3. Middle-Ware Layer

Introducing this layer into the IoMT structure is crucial for effectively managing the diversity of interconnected medical devices and objects within the network. The primary role of the middle-ware layer is to provide seamless end-to-end communication, transmitting gathered physiological data to central medical servers or cloud storage for analysis and retention [18]. This analysis may involve processing the data to detect alterations in the patient's health, which can then be presented to medical professionals or patients to make intelligent decisions for subsequent action [2]. In addition, the middle-ware layer includes a data processing unit and a local database to store the patient's initial data. This layer acts as an alarm generator, notifying patients and healthcare providers of any detected abnormalities. By using a wireless transmission module, it establishes secure connections between patients, healthcare providers, and medical servers, ensuring real-time access to health data and facilitating prompt medical interventions when necessary.

4.4. Application Layer

The application layer is the highest tier of the IoMT architecture, acting as the interface between patients, doctors, and healthcare applications. Its primary goal is to connect the middleware layer with end users, providing personalized interfaces and control panels tailored to specific roles [11]. This layer facilitates efficient diagnostics by integrating data into electronic medical records (EMRs) accessible to both patients and healthcare professionals. Patients can review their medical history and invoices through apps, while physicians monitor health and adjust treatments. It encompasses systems for monitoring, tracking, fitness, smart health records, remote diagnosis, and telemedicine. Ensuring data security is critical, as the growing number of connected devices increases the risk of cyberattacks [57]. Encrypted and untraceable communication is essential to protect sensitive information and prevent breaches that threaten patient privacy and healthcare security [58].

5. IOMT SECURITY

5.1. Security Requirements of the IoMT

The four mentioned layers represent the fundamental elements of the IoMT that must be secured to safeguard patient data at every level. Establishing a comprehensive set of security requirements is crucial for preventing, detecting, and responding to attacks in real time [10]. The CIA triad, which is comprised of Confidentiality, Integrity, and Availability, are the primary security requirements of the IoMT. These principles, as highlighted in numerous studies [59][60][13] form the fundamental basis for secure healthcare systems.

5.1.1. Confidentiality

This requirement guarantees that unauthorized third parties cannot access personal or sensitive information about the patient’s health status or treatment, which could endanger patient privacy and safety. Thus, protecting such information during storage and exchange across IoMT devices is vital. Although the standards provide general guidelines, ensuring confidentiality in IoMT systems requires certain measures, including robust network access controls and strong encryption protocols to prevent unauthorized data access [2].

5.1.2. Integrity

Data integrity is essential for the healthcare sector as it guarantees that the data remain unaltered during transmission to ensure that the data are received exactly as they were sent. This means that patients' health data are received exactly as transmitted and have not been tampered with during transmission. It is crucial to provide this safeguard to preserve the accuracy and reliability of medical data, which directly influences diagnoses, treatments, and patient results. Healthcare providers are becoming more aware of the need to maintain data integrity to preserve the confidence and effectiveness of healthcare systems [61].

5.1.3. Availability

Availability refers to an IoMT system's ability to function continuously and reliably to ensure that users can always access vital data and services. This is a critical element of healthcare systems, particularly when continuous patient health monitoring is necessary. To ensure availability, IoMT systems must be updated regularly, and redundant measures should be in place to enable additional paths for data access in the case of an attack, such as a distributed denial of service (DDoS) incident [62]. Additionally, the system infrastructure should be strengthened to improve its durability and ability to fix problems quickly [63].

5.2. Security Threats in the IoMT

While the rapid growth of IoMT has enhanced healthcare, it has also made these networks attractive targets for attackers. Vulnerabilities arise due to limited device resources, data heterogeneity, and evolving systems, along with cybercriminals targeting medical devices and sensitive data for financial gain, such as extortion or data sale on dark websites [64]. IoMT devices relying on wireless communication are especially prone to breaches in wireless sensor networks (WSNs) [65]. These threats jeopardize patient safety and the healthcare system’s confidentiality, integrity, and availability (CIA) [66]. Securing IoMT is critical, as weak security measures risk patient confidentiality and lives. Healthcare providers recognize these risks, slowing IoMT adoption. Cybercriminals increasingly exploit wearable devices through remote malware planting or programmable interfaces to steal data, control devices, or cause harm. Attacks on IoMT are categorized into four types: on sensors, communication mediums, medical professionals, and patients [67]. These occur due to design flaws or weak authentication, allowing hackers to monitor data, inject malicious code, or gain elevated privileges undetected [5][23]. High computational demands further limit robust security measures, exposing IoMT devices to compromise [24]. This survey primarily focuses on the cyber risks faced by IoMT environments and examines how AI methods are integrated into IDS solutions to enhance the security of these systems. The following section is a list of the various attacks associated with each level of the IoMT.

6. ATTACKS ON THE IOMT

The purpose of this section is to explain the various types of attacks that target the IoMT ecosystem. These assaults can result in irreparable financial and reputational harm in addition to compromising patient privacy [63]. Unsecured data in IoMT systems are vulnerable to destruction, alteration, theft, and other types of attacks. According to a recent report by Comparitech, the healthcare industry has incurred a loss of over $160 million due to these cyber-attacks since 2016 [68]. To guarantee maximum medical data security throughout collecting and processing, it is imperative to adopt precautionary measures by being aware of the potential risks

and vulnerabilities in IoMT contexts. The following section, we have categorized these assaults into four sections following the IoMT layered architecture based on the current state of the art.

6.1. Attacks on the Perception Layer

The initial phase of an IoMT system involves gathering patient data in the perception layer. Attacks on this layer of devices can jeopardize the integrity and confidentiality of the data, potentially leading to severe and even fatal consequences. The following are some of the most common assaults that target this layer, along with strategies to address them:

- **Tampering of Devices:** A tampering attack refers to the deliberate modification, insertion, or removal of data on IoMT devices [65]. These attacks occur when vulnerabilities in device firmware allow intruders to implant malware and gain control over the device. The goal is to capture, alter, or replicate sensitive information transmitted or stored within the device. It has been widely recognized that IoT devices are susceptible to such attacks.
- **Side-Channel Attacks**: This attack take advantage of data leakage within electromagnetic emissions, power consumption, or timing information, present a substantial risk to this layer. By analyzing this spilled information, attackers can gain access to sensitive data, such as encryption keys or medical information [65]. Medical devices are particularly susceptible to this type of attack due to their limited computational capabilities, leading to robust encryption and the protection of critical defences [69]. If a side-channel assault is successful, confidential data might be revealed [52].
- **Sensor Tracking:** Unsecured devices may enable attackers to access patients' location information or falsify GPS data, which can expose patient location information, violating privacy [65]. If there is a vulnerability in a device, the attacker may fake GPS data and find out the patient’s location. For example, devices that are used in fall prevention systems can be used to reveal private patient information or interfere with patient safety protocols [70].
- **Tag Cloning:** It refers to the replication of fake RFID tags by an attacker using information obtained from side-channel attacks [69]. In such a cyber-attack, the attacker can access unauthorized information, potentially compromising patient data [65]. This type of attack disrupts the perception layer of the IoMT network, which could result in varying degrees of system failure. Adopting a challenge-response authentication system is an effective strategy for preventing this danger by verifying RFID tags' authenticity and preventing unauthorized access [71].

6.2. Attacks on the Network Layer

The primary objective of this layer is to ensure dependable communication between the middleware layer and the perception layer; however, this layer poses a significant concern due to the vulnerability of using wireless communication, which makes it susceptible to various types of attacks. The following are the most common kinds of attacks that target the network layer, along with an explanation of how and what damage they cause:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)**: DoS attacks overwhelm healthcare devices with excessive demands, rendering them unavailable to users [72]. IoMT devices, with limited capacity, are particularly susceptible, leading to disruptions in medical operations and patient care [73]. For example, the SweynTooth vulnerability affects Bluetooth low energy (BLE)-enabled devices, allowing attackers to exploit buffer overflows, causing system crashes and shutdowns. DDoS Attacks: A more

aggressive form of DoS, DDoS floods systems with botnets, complicating source identification and attack prevention [18]. For instance, the hacktivist group "Kill-Net" recently launched DDoS assaults on US hospital websites, highlighting the severe damage such attacks can cause to IoMT devices [74].

- **Eavesdropping**: Because IoMT devices transmit data through wireless networks, all traffic is susceptible to detection, attackers can capture sensitive information, including biological data, and can even gather information on the specific medical device linked to the patient [75]. While encryption can potentially resolve this issue, many low-powered IoMT devices have limited processing power and memory for robust encryption [65].
- **Man-in-the-Middle Attack (MitM)**: The IoMT and wireless sensor networks (WSNs) are particularly susceptible to security vulnerabilities, including MitM attacks. In this type of attack, an attacker intercepts communications between two devices, enabling them to monitor, change, or replay data without the victims' awareness. In an MitM attack, the attacker takes advantage of a security vulnerability, which can lead to severe consequences, such as the manipulation or disclosure of sensitive patient information [76]. These data can subsequently be traded in, exploited for other kinds of cybercrime, or even used as blackmail. For instance, modifying the data while being transmitted by medical devices could result in mistreatment, such as medicine overdosing [73].
- **Replay Attack**: A replay attack refers to an attacker's act of reusing a recently exchanged message among authorized users for authentication [77]. In such a scenario, an intruder can intercept a signed message and retransmit it to the target numerous times. Devices such as One Touch Ping insulin and blood glucose meters do not employ sequence numbers or timestamps. Consequently, attackers can capture transmissions and replay them later to administer an insulin bolus without specialized knowledge [78].
- **Sybil Attack**: This prevalent type of assault specifically targets WSNs within the IoMT system. By granting the victim node several identities, a malicious node can execute a single operation repeatedly. Due to the attacker's ability to assume various identities within the WSN, the target node unknowingly routes its data across hacked nodes, thereby leaking important information [79].

6.3. Attacks on the Middleware Layer

At this level, the patient's health state, identity, and treatment are all stored, making it an attractive target for attackers seeking to acquire this data. Several potential attacks that may occur include:

- **Malicious Insider**: A malicious insider could be an employee, medical staff member, or business partner who misuses their access to intentionally harm the medical organization. Furthermore, they can engage in malicious behaviors such as modifying, eliminating, or altering the original dataset. Such occurrences frequently arise when someone has authorized access and can be challenging to identify and prevent, yet their impact on patient privacy and system integrity is substantial [80].
- **Unauthorized Access to the Tags**: RFID tags employ frequency bands to facilitate identifying, tracking, and data interchange with IoMT equipment. Robust access controls are necessary for these tags to guarantee that only individuals with the proper authorization can communicate with them. If an attacker gains access to these tags, the entire system's security is compromised. To prevent this, systems must use advanced user authentication mechanisms.

6.4. Attacks on the Application Layer

This uppermost layer of the IoMT architecture is responsible for providing end-user services. This layer is responsible for allowing communication between patients, medical professionals, and IoMT equipment; however, software and hardware flaws make it highly vulnerable to attacks. These attacks usually exploit coding flaws such as code injections or buffer overflows. In addition to these assaults, applications and services are frequently threatened by various types of malware, including viruses, worms, and trojans [79]. Below are some of the most prevalent threats:

- **Ransomware:** is a distinctive subset of malware that restricts or prevents users' access by encrypting data or locking users out of systems until a ransom is paid. If an infected device is connected to the network, the ransomware can spread throughout the entire network, potentially crippling entire systems. Healthcare facilities are increasingly concerned about this type of attack due to the financial burden and service disruptions it can cause [81]. This threat, which has even prompted a notice from Interpol, specifically targets sensitive information such as patients' private health records stored in healthcare systems [76]. A notable example is the 2020 ransomware attack that completely shut down systems and data at Germany's University Hospital of Düsseldorf, rendering the hospital's emergency room inaccessible [82].
- **Brute Force Attacks**: A basic brute force attack can quickly breach a device's access control. Due to the weaker computational capacity of most IoMT devices in a medical network, attackers can further compromise the network by installing malware [65]. One form of a brute force attack is known as a dictionary attack and is particularly risky for devices with weak security [83].
- **Phishing attack**: In a typical phishing assault, the attacker pretends to be a trusted source, such as a healthcare organization or individual, to attempt to get sensitive information, such as credit card details or user login credentials [65]. To secretly obtain valuable data from approved users, attackers create malicious links or attempt to get users to download harmful attachments. When executed, these acts damage the user's device, giving attackers access to confidential data [79].
- **Location threats**: The majority of medical devices are designed with a location component to aid in emergency response or continuous monitoring; however, if it is not properly protected, attackers can breach this feature to track patients' locations. This type of attack poses a direct threat to patients' privacy [84].

It is vital to secure the entire system, not just certain technologies within a single layer, because assaults can happen at any level of the IoMT ecosystem. A comprehensive strategy that protects all layers of the IoMT ecosystem is required to guarantee the maximum degree of security, preserve patient data, and keep healthcare systems operating.

7. CHALLENGES IN THE IOMT

- **Data Privacy and Security**: Ensuring patient privacy and protecting sensitive data is a paramount concern in the IoMT ecosystem. Healthcare businesses are often targeted by cyberattacks due to their management of enormous amounts of sensitive medical information. The potential for malicious individuals to attack hospital servers and exploit private information presents significant threats to patient data. Traditional security protocols or encryption methods are sometimes unsuitable for direct implementation because of the limited computational power and memory of IoMT sensors.

- **Power Efficiency:** Since medical equipment, machinery, and applications depend on electrical or solar energy, controlling power efficiency is among the most significant issues in IoMT systems. Sensors are necessary for continuous patient monitoring, and to continue to remain connected and send data effectively, they need constant power sources.
- **System Compatibility:** In healthcare, system compatibility indicates the seamless, secure, and efficient transfer of data among interconnected devices to guarantee optimal performance. The incompatibility of equipment, software, machinery, and applications can cause ineffective communication and data sharing, resulting in elevated costs and reduced operational efficiency.
- **AI Model Training and Performance Concerns:** Training is an essential component of AI models, particularly within the context of the IoMT. AI models must be retrained and reparametrized when environmental conditions or device features are altered. For DL and ML algorithms, a lack of training data may result in overfitting, which decreases model performance. Medical experts are concerned about AI performance in IoMT devices, especially when invalid information leads to incorrect diagnoses or high FPRs, resulting in unneeded alerts. The accuracy and precision of AI models ensure these devices' credibility, particularly in clinical decision-making platforms where it is critical to minimize false positives and identify real positives.

8. CONCLUSION

Due to the growing number of cyber threats, a robust and reliable IDS is essential in the healthcare industry. This survey provided a comprehensive analysis of an IDS tailored for IoMT, a critical component in safeguarding healthcare systems against emerging cyber threats. We proposed a new classification to classify the proposed techniques used to build IDS for detecting and mitigating cyber threats in IoMT environments into ML, DL, fuzzy logic, and hybrid approaches. These AI-driven approaches are vital in addressing the limitations of traditional security methods, enhancing the accuracy and adaptability of IDSs in a rapidly evolving cyber threat landscape.While ML, DL, and FL methods offer distinct advantages, such as adaptability and managing uncertainty, they also face challenges like resource demands and scalability, highlighting the need for optimized hybrid approaches.Our survey highlighted the critical role of robust IDS mechanisms in enhancing the security of the IoMT architecture at multiple layers along with their potential vulnerabilities, ensuring the confidentiality, integrity, and availability of sensitive medical data. This paper also identified several unresolved challenges in IoMT security, including the importance of ensuring data privacy and security, addressing power efficiency constraints, enabling system compatibility across diverse devices, and overcoming AI model training and performance concerns. Despite the significant progress in the development of AI-based IDSs for the IoMT, further research is needed to address the particle challenges of real-world deployment, scalability, and the handling of highly dynamic and heterogeneous IoMT environments. Future studies should focus on developing lightweight, scalable, and adaptive IDS models that can effectively balance the resource constraints of IoMT devices with the increasing complexity of cyber threats. Additionally, ongoing research is needed to improve AI models accuracy, minimize false positive, and enhance system compatibility within IoMT ecosystems.

REFERENCES

[1] Y. Rbah, M. Mahfoudi, Y. Balboul, M. Fattah, S. Mazer, M. Elbekkali, and B. Bernoussi, “Machine learning and deep learning methods for intrusion detection systems in iomt: A survey,” in 2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), pp. 1–9, IEEE, 2022.

[2] A. Ghubaish, T. Salman, M. Zolanvari, D. Unal, A. Al-Ali, and R. Jain, "Recent advances in the internet-of-medical-things (iomt) systems security," IEEE Internet of Things Journal, vol. 8, no. 11, pp. 8707–8718, 2020.

[3] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," Wireless Networks, vol. 27, no. 8, pp. 5503–5509, 2021.

[4] S. Razdan and S. Sharma, "Internet of medical things (iomt): Overview, emerging technologies, and case studies," IETE technical review, vol. 39, no. 4, pp. 775–788, 2022.

[5] G. Thamilarasu, A. Odesile, and A. Hoang, "An intrusion detection system for internet of medical things," IEEE Access, vol. 8, pp. 181560–181576, 2020.

[6] A. Ali, B. A. S. Al-Rimy, F. S. Alsubaei, A. A. Almazroi, and A. A. Almazroi, "Healthlock: Blockchain-based privacy preservation using homomorphic encryption in internet of things healthcare applications," Sensors, vol. 23, no. 15, p. 6762, 2023.

[7] B. Bhushan, A. Kumar, A. K. Agarwal, A. Kumar, P. Bhattacharya, and A. Kumar, "Towards a secure and sustainable internet of medical things (iomt): Requirements, design challenges, security techniques, and future trends," Sustainability, vol. 15, no. 7, p. 6177, 2023.

[8] I. F. Kilincer, F. Ertam, A. Sengur, R.-S. Tan, and U. R. Acharya, "Automated detection of cybersecurity attacks in healthcare systems with recursive feature elimination and multilayer perceptron optimization," Biocybernetics and Biomedical Engineering, vol. 43, no. 1, pp. 30–41, 2023.

[9] I. A. Khan and D. Pi, "Explainable learning machines for securing the iomt networks," in The Internet of Medical Things (IoMT) and Telemedicine Frameworks and Applications, pp. 135–154, IGI Global, 2023.

[10] A. Si-Ahmed, M. A. Al-Garadi, and N. Boustia, "Survey of machine learning based intrusion detection methods for internet of medical things," Applied Soft Computing, p. 110227, 2023.

[11] R. Hireche, H. Mansouri, and A.-S. K. Pathan, "Security and privacy management in internet of medical things (iomt): A synthesis," Journal of cybersecurity and privacy, vol. 2, no. 3, pp. 640–661, 2022.

[12] A. Aldhaheri, F. Alwahedi, M. A. Ferrag, and A. Battah, "Deep learning for cyber threat detection in iot networks: A review," Internet of Things and Cyber-Physical Systems, 2023.

[13] R. U. Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, and J. Qadir, "Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial ml," Journal of Network and Computer Applications, vol. 201, p. 103332, 2022.

[14] Z. Azam, M. M. Islam, and M. N. Huda, "Comparative analysis of intrusion detection systems and machine learning based model analysis through decision tree," IEEE Access, 2023.

[15] S. Messinis, N. Temenos, N. E. Protonotarios, I. Rallis, D. Kalogeras, and N. Doulamis, "Enhancing internet of medical things security with artificial intelligence: A comprehensive review," Computers in Biology and Medicine, p. 108036, 2024.

[16] A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions," Artificial Intelligence Review, vol. 55, no. 1, pp. 453–563, 2022.

[17] P. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T.-H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in iots: A survey," IEEE Access, vol. 10, pp. 121173–121192, 2022.

[18] M. L. Hernandez-Jaimes, A. Martinez-Cruz, K. A. Ram´ırez-Guti´errez, and C. Feregrino-Uribe,"Artificial intelligence for iomt security: A review of intrusion detection systems, attacks, datasets andcloud-fog-edge architectures," Internet of Things, p. 100887, 2023.

[19] M. Saied, S. Guirguis, and M. Madbouly, "Review of artificial intelligence for enhancing intrusion detection in the internet of things," Engineering Applications of Artificial Intelligence, vol. 127, p. 107231, 2024.

[20] J. M. Kizza, "System intrusion detection and prevention," in Guide to computer network security, pp. 295–323, Springer, 2024.

[21] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for internet of things," Arabian Journal for Science and Engineering, pp. 1–15, 2022.

[22] M. Uddin, A. A. Rahman, N. Uddin, J. Memon, R. A. Alsaqour, and S. Kazi, "Signature-based multilayer distributed intrusion detection system using mobile agents.," Int. J. Netw. Secur., vol. 15, no. 2, pp. 97–105, 2013.

[23] P. Kumar, G. P. Gupta, and R. Tripathi, "An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for iomt networks," Computer Communications, vol. 166, pp. 110–124, 2021.

[24] J.-P. A. Yaacoub, M. Noura, H. N. Noura, O. Salman, E. Yaacoub, R. Couturier, and A. Chehab, "Securing internet of medical things systems: Limitations, issues and recommendations," Future Generation Computer Systems, vol. 105, pp. 581–606, 2020.

[25] G. Balhareth and M. Ilyas, "Optimized intrusion detection for iomtnetworks with tree-based machine learning and filter-based featureselection," Sensors, vol. 24, no. 17, p. 5712, 2024

[26] J. L. Leevy and T. M. Khoshgoftaar, "A survey and analysis of intrusion detection models based on cse-cic-ids2018 big data," Journal of Big Data, vol. 7, pp. 1–19, 2020.

[27] F. Bouchama and M. Kamal, "Enhancing cyber threat detection through machine learning-based behavioralmodeling of network traffic patterns," International Journal of Business Intelligence and Big Data Analytics, vol. 4, no. 9, pp. 1–9, 2021.

[28] A. S. Mashaleh, N. F. B. Ibrahim, M. Alauthman, M. Almseidin, and A. Gawanmeh, "Iot smart devices risk assessment model using fuzzy logic and pso.," Computers, Materials & Continua, vol. 78, no. 2, 2024.

[29] K. Gupta, D. K. Sharma, K. D. Gupta, and A. Kumar, "A tree classifier based network intrusion detection model for internet of medical things," Computers and Electrical Engineering, vol. 102, p. 108158, 2022.

[30] E. Rehman, M. Haseeb-ud Din, A. J. Malik, T. K. Khan, A. A. Abbasi, S. Kadry, M. A. Khan, and S. Rho, "Intrusion detection based on machine learning in the internet of things, attacks and counter measures," The Journal of Supercomputing, pp. 1–35, 2022.

[31] A. R. Khan, T. Saba, T. Sadad, H. Nobanee, and S. A. Bahaj, "Identification of anomalies in mammograms through internet of medical things (iomt) diagnosis system," Computational Intelligence and Neuroscience, vol. 2022, no. 1, p. 1100775, 2022.

[32] M. Chowdhury, B. Ray, S. Chowdhury, and S. Rajasegarar, "A novel insider attack and machine learning based detection for the internet of things," ACM Transactions on Internet of Things, vol. 2, no. 4, pp. 1–23, 2021.

[33] Y. K. Saheed, A. I. Abiodun, S. Misra, M. K. Holone, and R. Colomo-Palacios, "A machine learning-based intrusion detection for detecting internet of things network attacks," Alexandria Engineering Journal, vol. 61, no. 12, pp. 9395–9409, 2022.

[34] O. Elnakib, E. Shaaban, M. Mahmoud, and K. Emara, "Eidm: deep learning model for iot intrusion detection systems," The Journal of Supercomputing, vol. 79, no. 12, pp. 13241–13261, 2023.

[35] V. Ravi, T. D. Pham, and M. Alazab, "Deep learning-based network intrusion detection system for internet of medical things," IEEE Internet of Things Magazine, vol. 6, no. 2, pp. 50–54, 2023.

[36] J. B. Awotunde, K. M. Abiodun, E. A. Adeniyi, S. O. Folorunso, and R. G. Jimoh, "A deep learning-based intrusion detection technique for a secured iomt system," in International Conference on Informatics and Intelligent Applications, pp. 50–62, Springer, 2021.

[37] Y. K. Saheed and M. O. Arowolo, "Efficient cyber attack detection on the internet of medical things-smart environment based on deep recurrent neural network and machine learning algorithms," IEEE Access, vol. 9, pp. 161546–161554, 2021.

[38] A. Judith, G. J. W. Kathrine, and S. Silas, "Efficient deep learning-based cyber-attack detection for internet of medical things devices," Engineering Proceedings, vol. 59, no. 1, p. 139, 2023.

[39] M. A. Talukder, K. F. Hasan, M. M. Islam, M. A. Uddin, A. Akhter, M. A. Yousuf, F. Alharbi, and M. A. Moni, "A dependable hybrid machine learning model for network intrusion detection," Journal of Information Security and Applications, vol. 72, p. 103405, 2023.

[40] V. Priya, I. S. Thaseen, T. R. Gadekallu, M. K. Aboudaif, and E. A. Nasr, "Robust attack detection approach for iiot using ensemble classifier," arXiv preprint arXiv:2102.01515, 2021.

[41] S. Nandy, M. Adhikari, M. A. Khan, V. G. Menon, and S. Verma, "An intrusion detection mechanism for secured iomt framework based on swarm-neural network," IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 5, pp. 1969–1976, 2021.

[42] S. Saif, P. Das, S. Biswas, M. Khari, and V. Shanmuganathan, "Hiids: Hybrid intelligent intrusion detection system empowered with machine learning and metaheuristic algorithms for application in iot based healthcare," Microprocessors and Microsystems, p. 104622, 2022.

[43] N. Faruqui, M. A. Yousuf, M. Whaiduzzaman, A. Azad, S. A. Alyami, P. Li`o, M. A. Kabir, and M. A. Moni, "Safetymed: a novel iomt intrusion detection system using cnn-lstm hybridization," Electronics, vol. 12, no. 17, p. 3541, 2023.

[44] M. Akshay Kumaar, D. Samiayya, P. D. R. Vincent, K. Srinivasan, C.-Y. Chang, and H. Ganesh, "A hybrid framework for intrusion detection in healthcare systems using deep learning," Frontiers in Public Health, vol. 9, p. 824898, 2022.

[45] S. Sharif, S. A. H. Seno, and A. Rowhanimanesh, "A fuzzy-logic-based fault detection system for medical internet of nano things," Nano Communication Networks, vol. 30, p. 100366, 2021.

[46] M. B. Gorzalczany and F. Rudzi´nski, "Intrusion detection in internet of things with mqtt protocol—an accurate and interpretable genetic-fuzzy rule-based solution," IEEE Internet of Things Journal, vol. 9, no. 24, pp. 24843–24855, 2022.

[47] S. R. Zahra and M. A. Chishti, "A generic and lightweight security mechanism for detecting malicious behavior in the uncertain internet of things using fuzzy logic-and fog-based approach," Neural Computing and Applications, vol. 34, no. 9, pp. 6927–6952, 2022.

[48] R. Praveen and P. Pabitha, "A secure lightweight fuzzy embedder based user authentication scheme for internet of medical things applications," Journal of Intelligent & Fuzzy Systems, vol. 44, no. 5 pp. 7523–7542, 2023.

[49] S. A. Wagan, J. Koo, I. F. Siddiqui, N. M. F. Qureshi, M. Attique, and D. R. Shin, "A fuzzy-based duo-secure multi-modal framework for iomt anomaly detection," Journal of King Saud University Computer and Information Sciences, vol. 35, no. 1, pp. 131–144, 2023.

[50] V. Sellam, N. Kannan, and H. A. Basha, "An effective fuzzy logic-based clustering scheme for edge-computing based internet of medical things systems," Cognitive Internet of Medical Things for Smart Healthcare: Services and Applications, pp. 105–116, 2021.

[51] H. K. Bharadwaj, A. Agarwal, V. Chamola, N. R. Lakkaniga, V. Hassija, M. Guizani, and B. Sikdar, "A review on the role of machine learning in enabling iot based healthcare applications," IEEE Access, vol. 9, pp. 38859–38890, 2021.

[52] A. I. Newaz, A. K. Sikder, M. A. Rahman, and A. S. Uluagac, "A survey on security and privacy issues in modern healthcare systems: Attacks and defenses," ACM Transactions on Computing for Healthcare, vol. 2, no. 3, pp. 1–44, 2021.

[53] R. Dwivedi, D. Mehrotra, and S. Chandra, "Potential of internet of medical things (iomt) applications in building a smart healthcare system: A systematic review," Journal of oral biology and craniofacial research, vol. 12, no. 2, pp. 302–318, 2022.

[54] N. Nanayakkara, M. Halgamuge, and A. Syed, "Security and privacy of internet of medical things (iomt) based healthcare applications: A review," in 2019 IIER 750th International Conference on Advances in Business Management and Information Technology (ICABMIT), pp. 1–18, Institute for Technology and Research, 2019.

[55] L. M. Dang, M. J. Piran, D. Han, K. Min, and H. Moon, "A survey on internet of things and cloud computing for healthcare," Electronics, vol. 8, no. 7, p. 768, 2019.

[56] T. Poongodi, A. Rathee, R. Indrakumari, and P. Suresh, "Iot sensing capabilities: sensor deployment and node discovery, wearable sensors, wireless body area network (wban), data acquisition," Principles of internet of things (IoT) ecosystem: Insight paradigm, pp. 127–151, 2020.

[57] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the internet of things," Sensors, vol. 19, no. 9, p. 1977, 2019.

[58] S. Gupta, V. Venugopal, V. Mahajan, S. Gaur, M. Barnwal, and H. Mahajan, "Hipaa, gdpr and best practice guidelines for preserving data security and privacy-what radiologists should know.," European Congress of Radiology-ECR 2020, 2020.

[59] V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou, and C. Douligeris, "Risk assessment methodologies for the internet of medical things: A survey and comparative appraisal," IEEE Access, vol. 9, pp. 40049–40075, 2021.

[60] M. Elhoseny, N. N. Thilakarathne, M. I. Alghamdi, R. K. Mahendran, A. A. Gardezi, H. Weerasinghe, and A. Welhenge, "Security and privacy issues in medical internet of things: overview, countermeasures, challenges and future directions," Sustainability, vol. 13, no. 21, p. 11645, 2021.

[61] G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou, and C. Tsatsoulis, "Review of security and privacy for the internet of medical things (iomt)," in 2019 15th international conference on distributed computing in sensor systems (DCOSS), pp. 457–464, IEEE, 2019.

[62] M. Papaioannou, M. Karageorgou, G. Mantas, V. Sucasas, I. Essop, J. Rodriguez, and D. Lymberopoulos, "A survey on security threats and countermeasures in internet of medical things (iomt)," Transactions on Emerging Telecommunications Technologies, vol. 33, no. 6, p. e4049, 2022.

[63] Y. Sun, F. P.-W. Lo, and B. Lo, "Security and privacy for the internet of medical things enabled healthcare systems: A survey," IEEE Access, vol. 7, pp. 183339–183355, 2019.

[64] S. Pirbhulal, O. W. Samuel, W. Wu, A. K. Sangaiah, and G. Li, "A joint resource-aware and medical data security framework for wearable healthcare systems," Future Generation Computer Systems, vol. 95, pp. 382–391, 2019.

[65] N. N. Thilakarathne, M. K. Kagita, and T. R. Gadekallu, "The role of the internet of things in healthcare: a systematic and comprehensive study," Available at SSRN 3690815, 2020.

[66] I. A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, and B. S. Ali, "Xsru-iomt: Explainable simple recurrent units for threat detection in internet of medical things networks," Future generation computer systems, vol. 127, pp. 181–193, 2022.

[67] R. Priyadarshini, M. R. Panda, and B. K. Mishra, "Security in healthcare applications based on fog and cloud computing," Cyber security in parallel and distributed computing: Concepts, techniques, applications and case studies, pp. 231–243, 2019.

[68] H. Rathore, A. K. Al-Ali, A. Mohamed, X. Du, and M. Guizani, "A novel deep learning strategy for classifying different attack patterns for deep brain implants," IEEE Access, vol. 7, pp. 24154–24164, 2019.

[69] I. Yasser, A. Khalil, M. Mohamed, and F. Khalifa, "A new chaos-based approach for robust image encryption," J. Cybersecur. Inf. Manag, vol. 7, pp. 51–64, 2021.

[70] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "Gps vulnerability to spoofing threats and a review of antispoofing techniques," International Journal of Navigation and Observation, vol. 2012, no. 1, p. 127072, 2012.

[71] B. A. Tama, K.-H. Rhee, et al., "Attack classification analysis of iot network via deep learning approach," Research Briefs on Information and Communication Technology Evolution, vol. 3, pp. 150–158, 2017.

[72] R. Khader and D. Eleyan, "Survey of dos/ddos attacks in iot," Sustainable Engineering and Innovation, vol. 3, no. 1, pp. 23–28, 2021.

[73] N. N. Thilakarathne, "Security and privacy issues in iot environment," International Journal of Engineering and Management Research, vol. 10, 2020.

[74] F. Alsubaei, A. Abuhussein, and S. Shiva, "Security and privacy in the internet of medical things: taxonomy and risk assessment," in 2017 IEEE 42nd conference on local computer networks workshops (LCN workshops), pp. 112–120, IEEE, 2017.

[75] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, "Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications," Sensors, vol. 21, no. 11, p. 3654, 2021.

[76] M. Ahmed, S. Byreddy, A. Nutakki, L. F. Sikos, and P. Haskell-Dowland, "Ecu-ioht: A dataset for analyzing cyberattacks in internet of health things," Ad Hoc Networks, vol. 122, p., 2021.

[77] B. Narwal and A. K. Mohapatra, "A survey on security and authentication in wireless body area networks," Journal of Systems Architecture, vol. 113, p. 101883, 2021.

[78] T. Beardsley, "Multiple vulnerabilities in animas onetouch ping insulin pump." https://blog.rapid7.com/2016/10/04/17-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump, 2016. Accessed: 2024-07-28.

[79] K. Chen, S. Zhang, Z. Li, Y. Zhang, Q. Deng, S. Ray, and Y. Jin, "Internet-of-things security and vulnerabilities: Taxonomy, challenges, and practice," Journal of Hardware and Systems Security, vol. 2, pp. 97–110, 2018.

[80] M. Wazid, A. K. Das, J. J. Rodrigues, S. Shetty, and Y. Park, "Iomt malware detection approaches: analysis and research challenges," IEEE access, vol. 7, pp. 182459–182476, 2019.

[81] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A. K. Al-Ali, and R. Jain, "Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach," Applied Soft Computing, vol. 118, p. 108439, 2022.

[82] A. Ghourabi, "A security model based on lightgbm and transformer to protect healthcare systems from cyberattacks," IEEE Access, vol. 10, pp. 48890–48903, 2022.

[83] M. J. Mar´ın-Jim´enez, F. M. Castro, N. Guil, F. De la Torre, and R. Medina-Carnicer, "Deep multitask learning for gait-based biometrics," in 2017 IEEE international conference on image processing (ICIP), pp. 106–110, IEEE, 2017.

[84] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," Sensors, vol. 12, no. 1, pp. 55–91, 2012.