Contents lists available at ScienceDirect

Applied Soft Computing

journal homepage: www.elsevier.com/locate/asoc

Review article

Survey of Machine Learning based intrusion detection methods for Internet of Medical Things

Ayoub Si-Ahmed [a,d,*], Mohammed Ali Al-Garadi [b], Narhimene Boustia [c]

[a] Blida 1 University, LRDSI Laboratory, Blida, B.P 270, Algeria
[b] Emory University, School of Medicine, Department of Biomedical Informatics, Atlanta, GA 30322, USA
[c] Blida 1 University, SIIR/LRDSI (Blida1) & RCR/RIIMA (USTHB) Laboratory, Blida, B.P 270, Algeria
[d] PROXYLAN SPA/Subsidiary of CERIST, Algeria, 16028, Algeria

ARTICLE INFO

Article history:
Received 24 September 2022
Received in revised form 9 February 2023
Accepted 13 March 2023
Available online 22 March 2023

Keywords:
Internet of Medical Things
Intrusion Detection System
Machine Learning
Privacy
Security

ABSTRACT

The Internet of Medical Things (IoMT) has revolutionized the healthcare industry by enabling physiological data collection using sensors, which are transmitted to remote servers for continuous analysis by physicians and healthcare professionals. This technology offers numerous benefits, including early disease detection and automatic medication for patients with chronic illnesses. However, IoMT technology also presents significant security risks, such as violating patient privacy or exposing sensitive data to interception attacks due to wireless communication, which could be fatal for the patient. Additionally, traditional security measures, such as cryptography, are challenging to implement in medical equipment due to the heterogeneous communication and their limited computation, storage, and energy capacity. These protection methods are also ineffective against new and zero-day attacks. It is essential to adopt robust security measures to ensure data integrity, confidentiality, and availability during data collection, transmission, storage, and processing. In this context, using Intrusion Detection Systems (IDS) based on Machine Learning (ML) can bring a complementary security solution adapted to the unique characteristics of IoMT systems. Therefore, this paper investigates how IDS based on ML can address security and privacy issues in IoMT systems. First, the generic three-layer architecture of IoMT is provided, and the security requirements of IoMT systems are outlined. Then, the various threats that can affect IoMT security are identified, and the advantages, disadvantages, methods, and datasets used in each solution based on ML at the three layers that make up IoMT are presented. Finally, the paper discusses the challenges and limitations of applying IDS based on ML at each layer of IoMT, which can serve as a future research direction.

Contents

[*] Corresponding author at: Blida 1 University, LRDSI Laboratory, Blida, B.P 270, Algeria.
E-mail addresses: si_ahmed.ayoub@etu.univ-blida.dz, ayoub.siahmed@proxylan.dz (A. Si-Ahmed), m.a.al-garadi@emory.edu (M.A. Al-Garadi), nboustia@univ-blida.dz (N. Boustia).

https://doi.org/10.1016/j.asoc.2023.110227
1568-4946/© 2023 Elsevier B.V. All rights reserved.

List of abbreviations

IoMT	Internet of Medical Things
ML	Machine Learning
IDS	Intrusion Detection System
AI	Artificial Intelligence
EHR	Electronic Health Record
ICD	Implantable Cardioverter-Defibrillator
DL	Deep Learning
WBAN	Wireless Body Area Networks
DBI	Deep Brain Implants
EMR	Electronic Medical Record
DoS	Denial of Service
DDoS	Distributed Denial of Service
IMD	Implementable Medical Device
TPR	True Positive Rate
FPR	False Positive Rate
AUC	Area Under the Curve
MLP	Multi-Layer Perceptron
LPU	Local Processing Unit
MM	Markov Model
NFC	Near Field Communication
BLE	Bluetooth Low Energy
GSM	Global System for Mobile Communications
EEG	Electroencephalogram
PG	Pulse Generator
RMSE	Root Mean Square Error
IHSS	Intelligent Healthcare Security System
MITM	Man-In-The-Middle
OS-ELM	Online Sequential Extreme Learning Machine
EOS-ELM	Ensemble of Online Sequential Extreme Learning Machine
ELM	Extreme Learning Machine
SVM	Support Vector Machine
DT	Decision Tree
RF	Random Forest
NB	Naive Bayes
ANN	Artificial Neural Network
KNN	k-Nearest Neighbor
SOM	Self-Organizing Map
CNN	Convolutional Neural Network
IoT	Internet of Things
ECG	Electrocardiogram
LSTM	Long Short-Term Memory
MLP	Multi-Layer Perceptron
IPG	Implementable Pulse Generation
FAR	False Alarm Rate
RTV	Rest Tremor Velocity
PMD	Personal Medical Device
DNN	Deep Neural Network
PCA	Principal Component Analysis
GWO	Gray Wolf Optimization
SDN	Software-Defined Networking
LR	Logistic Regression
FCM	Fuzzy C-Means Clustering
HTTPS	HyperText Transfer Protocol Secure
EMA	Exponential Moving Average
FPGA	Field Programmable Gate Arrays
Wi-Fi	Wireless Fidelity
CPU	Central Processing Unit
HFL	Hierarchical Federated Learning
RNN	Recurrent Neural Network
GRU	Gated Recurrent Unit
XAI	Explainable AI

1. Introduction

The Internet of Things (IoT) represents the fourth industrial revolution, in which devices and systems are connected to enable communication and data exchange. The first three revolutions focused on agriculture, industry, and information technology. Kevin Ashton, a British technology pioneer, coined the term IoT in 1999 [1] and defined it as a network of physical objects embedded with electronics, software, sensors, and network connectivity, allowing these objects to collect and exchange data, often using the internet [2]. The use of sensors enables machine-to-machine communication, which allows for the exchange of data and information without the need for human intervention. This technology can potentially revolutionize various sectors, including healthcare, transportation, and manufacturing.

IoT is experiencing considerable development and is estimated to reach more than 24.1 billion devices worldwide in 2030, representing about four devices per person [3], which can be explained by the many possible applications that offer IoT. Among these applications is the IoMT. The IoMT uses sensors that are either wearable or implemented in the human body to collect health data. Then these data are sent to a remote server to be analyzed using Artificial Intelligence (AI) assisted by the physicians.

Healthcare has experienced many evolutions in digitalizing health data, as explained in [4] and summarized in this paragraph. The evolution of healthcare began in 1990 with the advent of what is now known as healthcare 1.0. This initial phase involved digitizing medical records, where doctors started entering patient notes into computers. These digital records were then managed and stored by specialized systems such as the Picture Archiving and Communication System and Radiology Information System. The introduction of Healthcare 2.0 saw hospitals adopting systems that integrate and manage the digital data stored on doctors' laptops. Then there was healthcare 3.0, which consists of compiling, and grouping all patient data into an Electronic Health Record (EHR), providing individuals with complete access to their health data and history. Healthcare 4.0 is currently underway, enabled by artificial intelligence, data provided by doctors, imaging centers, equipment, and sensors implemented or worn by patients. This evolution allows doctors and medical staff to make more accurate diagnoses and better treatment decisions and allows hospital managers to control costs.

The IoMT is a rapidly growing field leveraged in various health-related applications. One of its key advantages is its ability to provide real-time and continuous patient health monitoring. This technology has proven particularly effective in managing chronic conditions, such as diabetes, where insulin pumps can automatically inject insulin to regulate glucose levels. Similarly, pacemakers, which send electric shocks to the heart when an abnormality is detected, have been used to manage heart disease. Deep Brain Implants (DBI), another medical device enabled by the IoMT, provide electrical stimulation to the brain to treat neurological disorders like Parkinson's. Beyond treating specific conditions, the IoMT has been used for fall detection in older adults and performance measurement for athletes. In addition, it could improve access to healthcare in rural areas that lack medical infrastructure.

Moreover, the IoMT produces detailed and accurate medical data, increasing treatment efficiency, reducing medical errors, and identifying diseases in their early stages. This can lead to quicker treatment and improved patient outcomes. By transforming healthcare from curative to preventive, the quality of care for patients is significantly improved, and stakeholders like insurance companies and pharmacies benefit as well. Another advantage of IoMT is the remote access to medical data by nurses and patients' families, eliminating the need for regular hospital visits, reducing costs, saving hospital resources, and containing the spread of COVID-19. Additionally, patients can receive care in the comfort of their own home. Overall, the IoMT is a remarkable technological advancement that has the potential to significantly improve healthcare services, benefiting both patients and healthcare providers.

While the IoMT has the potential to revolutionize healthcare through real-time patient monitoring, its adoption faces significant barriers due to security and privacy risks. The use of wireless communication to transmit data from sensors to remote servers creates security vulnerabilities that compromise the data's confidentiality, integrity, and availability, with potentially fatal consequences for patients if incorrect treatments are administered. Several studies [5–7] have demonstrated that even critical medical devices like Implantable Cardioverter-Defibrillators (ICD), DBI, and insulin pumps can be hacked. Furthermore, because IoMT data is highly sensitive and personal, unauthorized access or disclosure could result in severe patient privacy violations. Such incidents have occurred in recent years, for example, the Singapore health service data breach that affected 1.5 million patients [3] and the ransomware attack on a French hospital's system [3]. Given these risks, it is essential to prioritize the security and privacy of IoMT data in order to ensure that patient safety is not compromised.

Securing IoMT presents unique challenges that traditional security methods cannot efficiently address. One such challenge is the low computational and storage capacity of IoMT sensors, which makes it difficult to apply resource-intensive security measures. In addition, designing a secure system for IoMT must consider caregivers' need for quick access during medical emergencies, as prompt response times can mean the difference between life and death. Moreover, the potential for third-party devices to control and upgrade IoMT equipment increases the risk of security breaches, necessitating the implementation of lightweight security solutions. However, since the attack vectors against IoMT systems constantly evolve, these solutions must be regularly revised and updated to ensure their efficacy against zero-day and new attacks.

The following advantages motivated our choice to investigate the use of ML for IoMT intrusion detection:

I ML can give intelligence to the IoMT system and be more suitable to their security requirements. Therefore, these methods can be more effective in emergencies than traditional access control methods.

II IoMT and IoT systems generate a large amount of data that can be considered as big data due to their velocity, variety, and volume. These data are valuable sources for security because they can be used to learn normal behavior and detect abnormal behavior at an early stage, limiting the attack's damage.

III Deep Learning (DL) algorithms can extract the relevant attributes to perform the classification automatically, which eliminates the necessary extraction process required in traditional ML methods and therefore offer an end-to-end security model [8].

IV ML methods can detect zero-day attacks and new vulnerabilities, which threat signature-based methods cannot.

In light of these different advantages that can offer the use of ML in a security application, this study investigates its application for the IoMT by answering the following questions:

A What is the generic architecture of an IoMT system, its security requirements, and the security threats that can affect it?

B What are the different ML-based solutions proposed at the different layers of the IoMT?

C What are the advantages and disadvantages of these different solutions?

D What datasets are used to train and test the ML model at the different layers of IoMT?

The paper is divided into several sections to address the topic of IoMT security comprehensively. In Section Section 3, the different layers of IoMT architecture are described. Section Section 4 discusses the various requirements that are necessary to ensure IoMT security. Section Section 5 presents diverse threats that can undermine IoMT security, detailing the possible attacks that can affect each layer of the system, the types of attacks, attack environments, and the adversary's motivation to conduct an attack. The paper also highlights the significance of IDS in Section Section 6, while Section Section 7 presents an overview of the ML technique. Section Section 8 discusses the state-of-the-art approaches proposed in different layers of the system, highlighting the benefits, drawbacks, and datasets used in each solution. Section Section 9 sheds light on the limitations and challenges in using IDS based on ML for each layer of the IoMT system. Finally, the paper concludes in Section Section 10.

Fig. 1 shows the various components explored in this review paper.

2. Related work

Many review articles address different aspects of security in an IoMT system and include ML to ensure security in these systems. To the best of our knowledge, most of them do not focus on using ML as a method to ensure security in IoMT, and they just mentioned it briefly. Table 1 presents the different review papers that have discussed security in the IoMT, mentioning our main contribution compared with them. *H. Rathore, et al.* explored issues, security risks relating to the privacy and safety of medical equipment, and solutions in [9], including anomaly detection based on ML.

M. Hussain, et al. in [10] reviewed different authentication schemes and classified them according to their type. They give advantages, disadvantages, and the ability to resist different attacks. They also categorized authentication mechanisms based on advanced methodologies, such as game theory and ML.

The work of *M. Wazid, et al.* in [11] covered a variety of malware attacks against IoMT systems, targeting security criteria, namely confidentiality, integrity, authenticity, and availability of data. The current security approach strategy has generally emphasized key management and intrusion detection using different methods such as ML, authentication, and access control.

In the work conducted by *A.I. Newaz, et al.* in [12], they discussed security and privacy in healthcare by presenting a detailed survey of possible attacks, their impact, and solutions proposed in the literature, including solutions based on ML along with their limitations.

B. Narwal and A.K. Mohapatra in [13] presented a systematic survey on security and authentication in Wireless Body Area Networks (WBAN) to cover the main research elements. In particular,

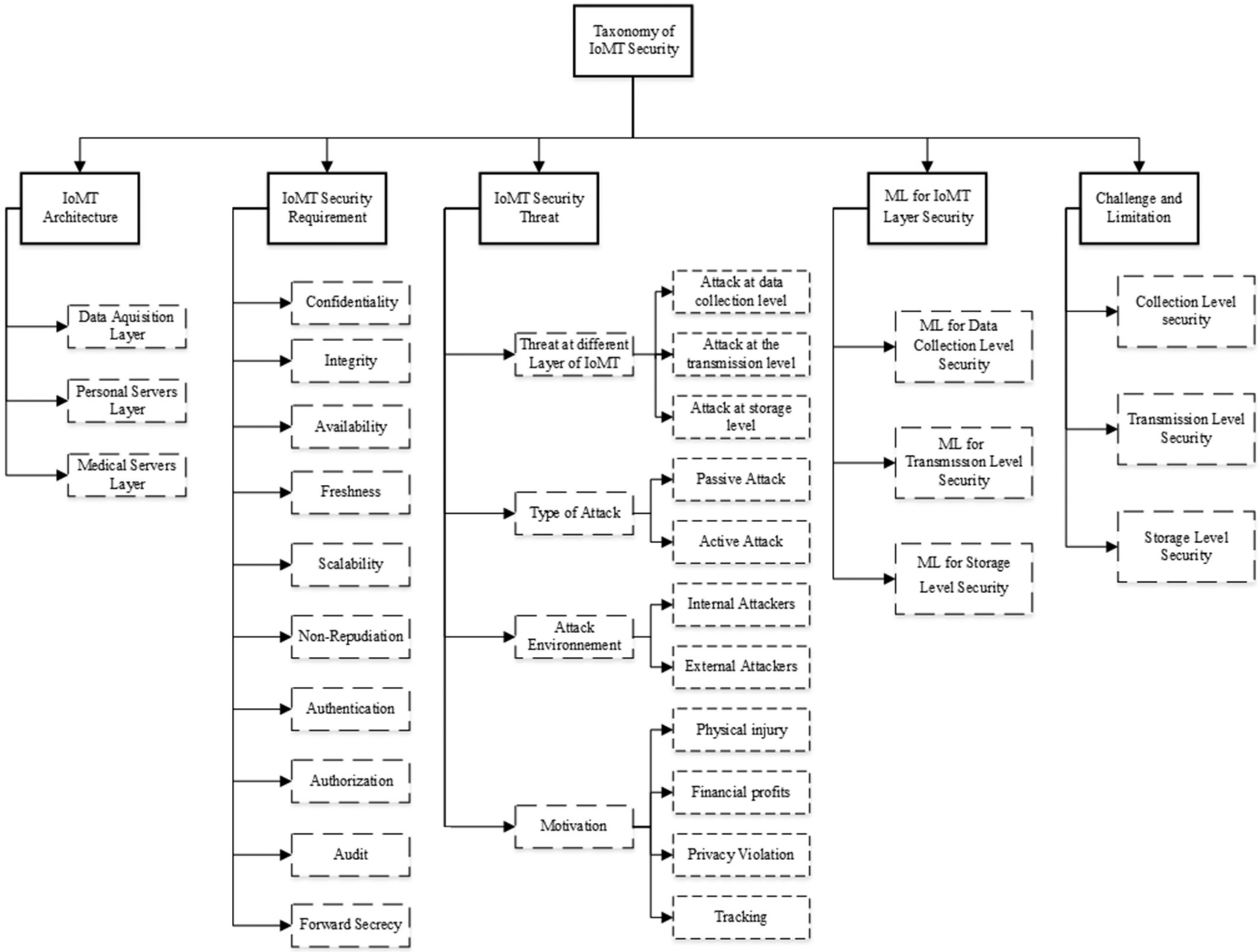

Fig. 1. Thematic taxonomy of ML for IoMT security.

an in-depth classification of protection mechanisms in WBAN is provided along with a thorough analysis of security basics, threats to security, the intruder and their attack strategies, and current mitigation that include ML.

The survey presented by *A. Saxena and S. Mittal* in [14] explained the IoMT ecosystem, reviewed the security requirement and vulnerability of IoMT systems, and presented recent security applications to protect this ecosystem, including blockchain, physically unclonable function and AI/ML.

Among the review papers conducted on security in IoMT, only a few survey papers have reported using ML as a method for security purposes in the literature. They describe it briefly and not in a holistic manner. However, a work similar to the current study conducted by *S.S. Hameed, et al.* in [15] discussed security and privacy in IoMT. They presented the different solutions based on ML proposed in the literature to solve the security challenge of IoMT, giving their advantage, disadvantage, approach, tools, and datasets used. However, the authors focused on network and device-level security and did not discuss the security of electronic medical data when it resides at the medical server level. This paper extends the previous work and discusses the various solutions used for anomaly detection based on ML at the medical device level, at transit, and during the resets by identifying the benefits, drawbacks, and datasets used. Reviewing the solutions at the three levels allow for discussing the ML method used to ensure the security and privacy of the IoMT globally.

3. Architecture of IoMT

Many architectures were presented in the literature. Some research proposes architectures composed of three layers [16,17]. Other research proposes using an architecture with more than three layers [18]. Different technologies are proposed to manage medical data, such as fog/cloud computing [19], Software-Defined Networking (SDN) [20], or Blockchain [21]. This survey paper assumes that a three-layered architecture is suitable for logically dividing IoMT architecture. These layers are data acquisition, personal server, and medical server, and they are explained as follows and illustrated in Fig. 2.

3.1. *Data acquisition layer*

Sensor devices serve as a bridge between the human body and the digital world. There are four types of devices [17,18]:

- The implemented devices: these devices are placed inside the human body, e.g., DBI.

Table 1
Existing surveys.

Year	paper	Discussed topic(s)	Main differences
2017	[9]	Security of wireless medical devices	This survey provides the security and proposed solutions for the three layers composing the IoMT system
2019	[10]	Authentication in the wireless body area network	This survey presents the architecture, attacks on each layer that compose the IoMT, the environment, and the attackers' motivations. Then, the different ML-based solutions proposed for the layers forming the IoMT system are discussed
2019	[11]	Detection and prevention of malware in IoMT	This survey mentioned the attacks that can occur in each layer that composes IoMT, the types and environments of attacks, and the attackers' motivations, not only the malware. The IDS-based ML solutions proposed for the three layers that constitute the IoMT system are discussed in this survey and do not only cover the security of the communications
2020	[12]	Security and privacy in the healthcare system	The IDS-based ML solutions for the three layers of the IoMT system are provided
2021	[13]	Authentication in the wireless body area network	The different attacks occurring at the three layers composing the IoMT system are listed, and the solutions that use an IDS based on ML and proposed for the three layers of the IoMT system are discussed
2022	[14]	Review the use of new technologies to improve IoMT ecosystem security	The security requirement and threats for the three layers that compose the IoMT systems are provided. Then, the IDS solutions based on ML for each layer that forms the IoMT systems are reviewed, which allows identifying the limitations and challenges at each layer of the IoMT systems
2021	[15]	The role of ML in solving the security and privacy issue in IoMT systems	The different attacks that can impact the three layers of the IoMT and the IDS based on ML solutions proposed for layer three of the IoMT system are presented

- The wearable devices: these devices are on the human body e.g., Smartwatch, Pulse Generator (PG), or Electroencephalogram (EEG).
- The ambient devices: these devices allow capturing data from the environment around the patient, e.g., room temperature sensors.
- The stationary devices: these sensors are located in the hospital, e.g., imaging devices.

These devices are equipped with physiological sensors and low-power computing, connectivity, and storage modules, which are used to gather biomedical and context signals [22]. The data collected are used to manage the treatment and diagnosis of patients' health conditions. These medical devices have other constraints at the internal and communication levels. Internally, the medical implants inside the human body can be rejected by the patient's immune system, resulting in inflammation and pain. The battery of these medical devices is limited and must be changed after a number of years. Traditional security methods such as cryptography can quickly shorten the implant's lifespan, which requires surgery to replace the battery and can be dangerous for the patient. Because of medical equipment's limited memory space, it is impossible to keep track of the exchanges made via log files. Regarding communication, medical equipment can only support short-range communication due to energy limitations [9]. Due to scale, computing capacities, and energy constraints, most wearable devices can only preprocess the sensed data. Alternatively, the embedded low-power computing modules compress the sensed data before sending it to personal devices (i.e., smartphones or desktops) through low and ultra-low-power wireless communication like Near Field Communication (NFC) and Bluetooth Low Energy (BLE) [23].

3.2. *Personal server layer*

Medical equipment can send physiological data to personal servers like smartphones and laptops or standard devices like gateways [24]. Personal servers process and save patient data remotely until it is sent to centralized medical servers. The medical data received at the personal server are saved and processed; for example, by adding contextual information such as place and time to detect unusual behavior, these data also can be encrypted or compressed. Then the processed data are sent in a medical standard format like Health Level-7 to the remote medical server using long-range wireless like Wireless Fidelity (Wi-Fi), Global System for Mobile Communications (GSM), or wired communication [10]. This layer is intended to support heterogeneous communication and node mobility and permit the resending of medical data when the network link to the medical servers is interrupted [11,25].

3.3. *Medical server layer*

It consists of a high-performance data center that allows for centralized patient control, complex and long-term behavior analysis, and the correlation of patient data. It also includes a cloud server that makes intelligent decisions. It is used for data aggregation and provides extra patient medical data storage. The doctor, patients, and the pharmacy department (for summary or billing purposes) can access these data. Patients may use an online interface or smartphone to display their past and current health records/bills. Data from various sources are incorporated into EHR, Electronic Medical Records (EMR), or prescription websites. As a result, doctors and patients can access the information whenever needed. It provides a notification service for any patient who uploads or receives health data [26].

4. Security requirements of IoMT

IoMT uses wireless communication and the internet to transmit data collected from the human body to the medical server; therefore, the data in the different layers of the IoMT system, as shown in Fig. 2, are exposed to cyberattacks, which can impact the privacy of the patients and put their lives in danger. Security requirements must be met to prevent, detect and respond to these attacks in real time. This section presents the main security requirements of IoMT (Illustrated in Fig. 3):

4.1. *Confidentiality*

This requirement ensures that the information regarding the patient's health condition or treatment and information that identifies them are not accessible by unauthorized third parties during data storage and data communication; this ensures that the patient's privacy is protected from the disclosure of sensitive information to persons with malicious intent who may cause considerable harm to the patient [11,27]. It is possible to imagine

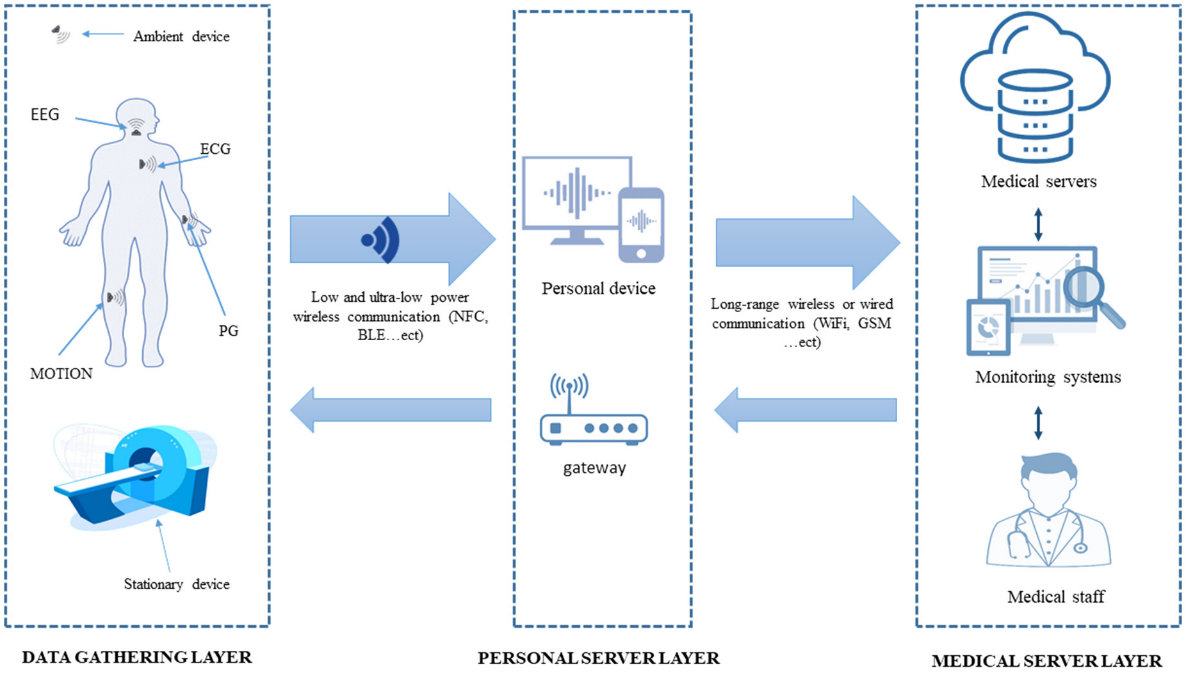

Fig. 2. Internet-of-Medical-Things (IoMT) architecture.

a scenario in which an adversary, who has access to the medical history of a famous person, discloses it in public to impact his/her image.

4.2. Integrity

The data integrity provision for IoMT healthcare systems aims to ensure that the data arriving at the intended destination was not corrupted during wireless transmission. For instance, even a minor change to the medication or patient test results may have catastrophic implications for the patient's life. Preserving the integrity of information ensures that someone other than the person involved (i.e., doctors or nurses) does not change the medical data and, as a result, prohibits giving incorrect treatment [24].

4.3. Availability

Despite the implementation of healthcare, clinical records of patients must be available to the doctor at all times, anywhere, without any interruption. In addition, it is crucial to respond immediately to the emergency so that the doctor can give the patient treatment or precautions. Switching from the attacked node to another node in the network may be an alternative, and this redundancy can be allowed by the network and system design [24,25].

4.4. Freshness

This layer ensures that the health information is recent and that an attacker cannot replay old medical data. Two kinds of freshness are present; weak and strong freshness. Weak freshness gives the partial ordering of the health freshness message, and no delay information is provided. In contrast, strong freshness gives the complete ordering of the medical data and allows the calculation of delay [10,28]. For illustration, a physician must be aware of the present patient's vital signs, such as their oxygen saturation, in order for the physician to make a correct diagnosis of the patient's health condition and provide the appropriate treatment.

4.5. Scalability

Scalability is the ability of the IoMT network to function properly; as the number of devices that compose the IoMT network turn to be larger, insufficient scalability could cause security flaws. Therefore, it is essential to manage overhead computing and storage, especially in an emergency where response time is vital for the patient [29,30].

4.6. Non-repudiation

Non-repudiation ensures that any entity involved in the healthcare application cannot deny the sending and receiving health-related patient information [13].

4.7. Authentication

There are two kinds of authentication in healthcare systems: data and persons. Data authentication is the process by which the initial data source is confirmed. Person authentication in communications between patients and related servers should be checked through accurate identity authentication. Therefore, before they communicate or exchange any details, all parties need to know each other. Before doing some form of sharing, the healthcare system has to recognize each participant to ensure that the user is authorized to receive the stored data. It is, therefore, essential to know the privilege level given to the user to know the kind of data he/she may access [12,24].

4.8. Authorization

Authorization is an access control used to specify permission levels for users (patients, physicians, or nurses) to enter the database of medical data. The healthcare organization must approve the patient and define the type of data that a single user can use [13,27].

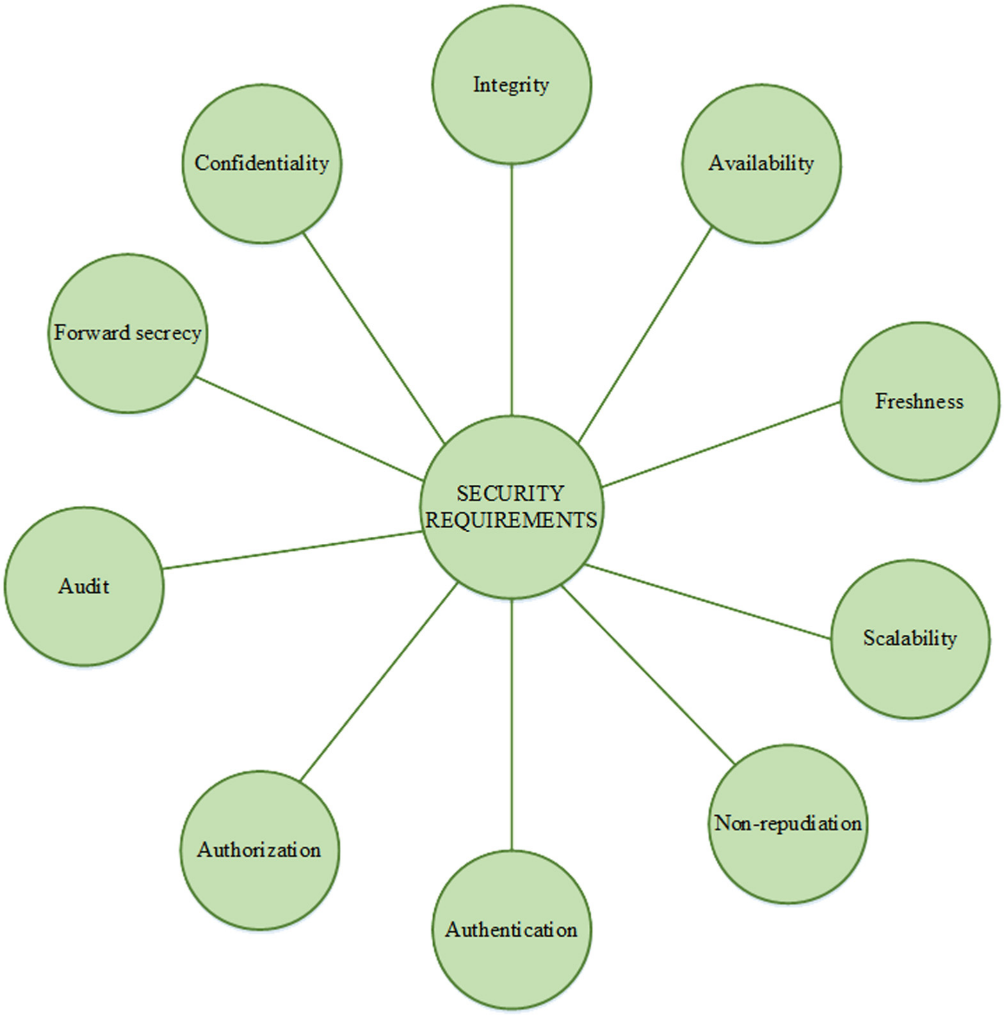

Fig. 3. Security requirements in IoMT.

4.9. Audit

The audit is the inspection of changes in the system and access to the patient's medical data via the verification of log files, which are historical records of the hardware and software operating status. The audit allows the detection of abnormal activities and possible breaches. However, the management and exploitation of this type of information are delicate in practice due to the large quantity and heterogeneity of logs generated by the various medical and network equipment.

4.10. Forward secrecy

- Backward secrecy: Medical sensors who enter a network after a certain amount of time must not decode messages received before entering them [30].
- Forward secrecy: Medical sensors that have left the network are unable to read messages received after their exit [30].

5. IoMT security threat

The integration of wireless communication in the IoMT system and external equipment to control and upgrade sensors makes the IoMT vulnerable to different attacks. Moreover, two types of architecture are proposed in the literature for the IoMT: the single-hope and the multi-hope. For the single-hope, the sensors perform only data collection and transfer; however, this architecture suffers from the vulnerability of a single point of failure, which occurs when one equipment of the personal server layer fails, the whole IoMT system is compromised. The other type of architecture proposed is the multi-hope, here the sensors, in addition to collecting and transmitting data, also provide data routing, which allows node mobility and maintains low energy consumption during data transfer, like Codeblue [31] and MIDiSN [32]. Therefore, relevant vulnerabilities of the wireless sensors network that concern routing may apply to this type of architecture [33].

Attacks can indirectly target devices in the personal server layer to reach patient data. The lack of data storage security in the personal and medical servers and the insecure transmission of data between these different devices can cause various security issues [34].

It is imperative to keep these different attacks in mind when designing a secure architecture for IoMT. The different threats related to each level of IoMT are summarized in Table 2. The most common type of network and systems attacks are listed below:

5.1. Attack at data collection level

During data perception and delivery over a wireless channel and the ability of medical equipment to be remotely configured by external devices led the medical sensors vulnerable to different attacks. Here are the potential security threats that could take place in the following manner:

5.1.1. Data modification

An attacker modifies the medical data of patients [35] to manipulate the medical diagnosis and lead to the administration of inappropriate medication, which can be dangerous for the patients.

5.1.2. Drain the battery

Process that leads to additional battery consumption of a medical device, which leads to battery failure [9].

5.1.3. Modify the software of the device

An attacker can try to modify the software of the medical equipment by introducing a virus that modifies its behavior to conduct malicious actions [36], such as instructing the pacemaker to send an electrical charge to the patient's heart.

5.1.4. Jamming attack

This attack interferes with the radio frequencies that the network's nodes use. A jamming source can interrupt the whole network or part of it. It may be deliberately or unintentionally made [33,35].

5.1.5. Node tampering

In the case where an attacker has physical access to the IoMT nodes, they can gain access to the sensitive information on the node, for example, retrieve the encryption keys and then use them to decrypt the communications in transit. The attacker can even modify the node or replace it with a different node that the attacker controls [25,37].

5.1.6. Data collision attack

When two nodes of IoMT system transmit on the same frequency simultaneously, a collision may occur, which implies a modification of the transmitted data. Therefore, the receiving node of the packet will reject it due to the checksum mismatch [33].

5.1.7. Exhaustion

The collision implies that the packet lost is retransmitted; this retransmission consumes energy at the medical equipment level. The intruder could exploit the repeated collision to create resource exhaustion [28,33].

5.1.8. Unfairness in allocation

Collision and exhaustion attacks can be used by the intruder to create unfairness in the network. Therefore, when incoming patient data packets enter the application's processing device, they are either missed or produce multiple errors [38].

5.2. Attack at the transmission level

There is a high risk of threat at the transmission level because wireless communication allows an attacker to intercept, modify, or block the messages sent and exchange valuable information related to the patient's condition. Some risks include:

Table 2
Threat attack at each level of IoMT.

Data collection level	Data modification Drain the battery Modify the software of the device Jamming attack Node tampering Data collision attack Exhaustion Unfairness in allocation
Transmission level	Eavesdropping Man in the middle attack Scrambling attacks Signaling attacks Message modification attack Data interception attack Wormhole attack Denial of service attack Hello flood attack Sinkhole attack Replaying attack Homing attack Data flooding attack Desynchronization attack Spoofing attack Selective forwarding attack Sybil attacks Path dos attack Overwhelming sensors Reprogramming attacks
Storage level	Patient's data inference Unauthorized access Malware attack Social engineering attacks Location threats Alert attack Extortion/Blackmail

5.2.1. Eavesdropping

Due to the communication over wireless networks, all traffic is vulnerable to detection and eavesdropping by attackers. These threats may result in the loss of personal information such as physiological data and may obtain information about the medical device, such as the type of medical equipment associated with the patient. They can also contribute to other kinds of attacks. There are two types of eavesdropping:

- Passive eavesdropping: By listening to the network's message transmission, a hacker will intercept the content [39,40].
- Active eavesdropping: By pretending to be a friendly entity and sending requests to emitters, a hacker actively obtains information [39,40].

5.2.2. Man in the middle attack

This attack happens when an intruder gets in between a patient and a server's communications and sniffs the data. They can capture all messages received between the two parties and insert new ones [40].

5.2.3. Scrambling attacks

This attack keeps the radio frequency channel for wireless communication occupied for a brief period of time; this causes patients' personal devices to be interrupted to block data transfer, resulting in vulnerabilities of losing the network availability [25,41].

5.2.4. Signaling attacks

In this threat, the attacker will try to disrupt the signaling operation that takes place before the establishment of a communication between two entities and involves key management, authentication, link creation, and registration by sending an additional signal, which will put a heavy load on the base station and thus interrupt its service. As a result, health data cannot be forwarded to their destination [42].

5.2.5. *Message modification attack*

By capturing patients' wireless channels, the attacker can extract health data from patients, which can then be partially or fully altered before being delivered back to the initial recipient [43,44].

5.2.6. *Data interception attack*

An attacker can capture a patient's health data when it is transmitted between two connected healthcare devices over a local area network [41].

5.2.7. *Wormhole attack*

In this attack, a duplicate of a patient's data packet from one location is replayed at a different location with no modifications to the data. This attack usually requires two rogue nodes relaying packets over an out-of-bound channel that is only accessible by the attacker [33,42].

5.2.8. *Denial of Service attack (DoS)*

In this attack, the intruder tries to interrupt, shut down, or stop a service from a system, machine, or a network. A distributed DoS (DDoS) attack, on the other hand, is a kind of DoS attack that originates from several distributed sources [34,40].

5.2.9. *Hello flood attack*

The attacker must persuade all nodes to choose them as the patient's medical data routing node. A malicious node accomplishes this by sending a HELLO packet over a strong radio transmission to the network. When a node receives a message like this, it will presume that the source is within a normal radio range. Such an assumption could be wrong, since the machine of the intruder with high transmission capability could mislead the target into assuming that it is his neighbor [42,45,46].

5.2.10. *Sinkhole attack*

The sinkhole attack occurs when a malicious node attempts to attract all data packets in IoMT system by pretending that it is the most appropriate routing algorithm. This attack is performed to prevent data packets from reaching their destination [45,47].

5.2.11. *Replaying attack*

In a replay attack, an attacker listens to communications received between valid entities in IoMT system, intercepts them, and then sends them again to an initial recipient to alter the overall result [13,48].

5.2.12. *Homing attack*

A scan is performed in the continuous data traffic to find the key manager or the cluster head that can stop the whole network of IoMT system [49].

5.2.13. *Data flooding attack*

This attack occurs when an attacker sends many connection requests to a target node in the IoMT network. As a result, the server exhausts its capabilities and cannot establish any other connections, even legitimate ones [37,50].

5.2.14. *Desynchronization attack*

The intruder repeatedly resends an incomplete message to one or both nodes that participate in communication within IoMT system, which requests the retransmission of the missing data. Consequently, valuable information is prevented from being exchanged between the endpoint [51].

5.2.15. *Spoofing attack*

The attacker manipulates the routing information to compromise the network of IoMT system [52].

5.2.16. *Selective forwarding attack*

In this attack, the attacker will target a node in the IoMT network to compromise it and make it malicious, transmit some messages and block the rest. The number of messages lost will be more important if the compromised node is closer to the base station; therefore, many vital data will be wasted [25,53].

5.2.17. *Sybil attacks*

A Sybil attack occurs when a given node in the IoMT network claims several identities to act (modify) geographical routing protocols [54].

5.2.18. *Path DoS attack*

In this form of attack, the intruder produces a significant volume of traffic to the base station [51].

5.2.19. *Overwhelming sensors*

In this threat, the intruder caused the network capacity dilapidation and node resource exhaustion by overwhelming the network node with sensor stimuli, causing the network to send a large amount of traffic to the base station [28].

5.2.20. *Reprogramming attacks*

TinyOS' Deluge network-programming framework, for example, enables nodes in deployed networks to be remotely reprogrammed. The majority of these systems, like Deluge, are meant for use in a protected environment. A hacker will hijack the reprogramming mechanism and take possession of a vast network area if it is not secure [28].

5.3. *Attack at storage level*

All information related to the patient's health condition, treatment, and identity are stored at this level, which constitutes a valuable target for adversaries to access these data. Some of the possible attacks that can occur are:

5.3.1. *Patient's data inference*

Intruders try to recover medical records such as information about patient's health, maladies, and medications by combining Information that the attacker is authorized to access with other pertinent information [42].

5.3.2. *Unauthorized access*

If the patient data are not protected, the attacker will attempt to access health data to conduct malicious action such as damage it or retrieve it; therefore, it is important to secure the data against unauthorized access [55].

5.3.3. *Malware attack*

Malware (short for "malicious software") is a code or program usually spread over the network. It extracts, infects, or executes other malicious operations directed by the attacker. The types of malware include viruses, spyware, Keylogger, worm, rootkit, ransomware, and Trojan horses [11].

5.3.4. *Social engineering attacks*

Phishing, spear-phishing, baiting, and quid quo pro are examples of techniques to gain sensitive information from victims. These techniques are used to dupe the user into supplying the attacker with sensitive patient information that the user assumes to be supplied to someone or something else [41,56].

5.3.5. Location threats

Most medical devices are equipped with a location component that allows the caregivers to have a quick response in an emergency. If this type of information is not well protected, adversaries can access it and directly invade a person's privacy [43,57,58].

5.3.6. Alert attack

Some medical devices are equipped with an alert system that notifies the medical staff of an abnormality concerning the patient's health or a device's malfunction, such as a necessary battery change. However, this feature can be abused by an attacker to create false alarms; therefore, the wrong treatment can be prescribed, the patient can make unnecessary hospital visits, or genuine alerts can be ignored, and the patient can even disable this notification functionality which has the effect of missing important notifications [34].

5.3.7. Extortion/blackmail

This type of attack consists of blocking access to medical data by an attacker and then asking for a ransom to unlock these data. It can also involve stealing influential people's personal medical history, such as a politician or a star, and then threatening to disclose it publicly if the person concerned does not pay the amount of money requested [59].

5.4. Type of attack

Attack strategies are continually changing. However, they can be divided into passive and active attacks.

5.4.1. Passive attack

In a passive attack, the adversaries will only listen to the traffic and thus will have the possibility to read messages exchanged between the wearable device and the remote system. By simply accessing the content of the messages, a passive attacker will directly affect the confidentiality of communication. They will have access to sensitive information such as the model, the serial number of the medical device, and capture telemetry data. They can also capture the patient's private data such as health record, name, age, and conditions. In all these cases, the result is a severe violation of the patient's privacy [34].

5.4.2. Active attack

The attacker will intercept network messages and give instructions to the wearable device, alter messages transmitted before they reach the remote system, or prevent them from reaching their intended destination. A successful intruder has a wide range of objectives. They might, for example, indiscriminately request information from the medical device to deplete its energy. They may even try to change the device's settings, bypass treatments, or even put the patient in a state of shock [34].

5.5. Attack environment

Threats to the system can be classified according to the adversary's position, i.e., internal attack and external attack.

5.5.1. Internal attackers

Internal attackers require that the attacker is close to the vulnerable device or nearby and has some right to enter the network infrastructure. They may be a legitimate user, like a nurse who accesses a celebrity patient's medical data without justification. The attacker near the medical equipment can then cause physical damage or collect some information and use them to launch remote attacks later [13,60].

5.5.2. External attackers

In this case, the attacker does not need to be close to the medical device and does not have administrative access to the system. Instead, they will try to exploit bugs or vulnerabilities of the system remotely [13,60].

5.6. Attackers motivations

This section discusses various attackers' motivations for targeting IoMT systems [61].

5.6.1. Physical injury

The compromise of medical equipment poses a severe threat, as it could be used to cause harm to patients. Malicious organizations may target patients for political or criminal reasons, and in some cases, even by terrorist groups. Such attacks can be powerful tools for criminal practices, such as extortion or coercion. For example, during his tenure, former US Vice President Dick Cheney had the wireless communication functionality of his pacemaker deactivated as a precautionary measure against potential hacking attempts [62].

5.6.2. Financial profits

Economic and financial profits are important motivators for attackers or rivals of Implementable Medical Device (IMD) vendors to conduct such threats. The ability of an attacker to access to medical data may be used to sell it or blackmail the patient.

5.6.3. Privacy violation

Medical equipment collects vital information about a patient's body based on various criteria. This information may be necessary for the patient's diagnosis, care, and operational or surgical procedures. Medical data divulge information about the patient's behavior. Analysis of the data obtained from a pacemaker, for example, will reveal the patient's physical activity history. Such data can be used to distinguish general and unique patterns in the well-being of individuals/groups if collected in a large enough sample across different device types and marks. This type of information can lead to unauthorized and unethical use of sensitive data.

5.6.4. Tracking

Messages from the Medical equipment are sent wirelessly to the system controller. These exchanges typically provide health data and position information about the patients. Attackers can intercept these communications to track or locate a patient.

6. Intrusion detection system

This section explains the IDS in IoMT systems according to [63]. An intrusion is an attempt to compromise the availability, integrity, confidentiality, or defeat the security mechanisms of an end device or network. The IoMT represents an information system that handles sensitive and private data related to the health data of patients, which constitutes a valuable target for an attacker to perform an intrusion. This intrusion can be performed by a remote attacker using the Internet or by a legitimate internal user who abuses their privileges, such as members of the medical team who are motivated by curiosity to access private data or an error in the handling of medical data, which could have severe repercussions to patients. An IDS is a hardware or software product that automates surveillance and analysis of events that occur in an end device like IMD or network to detect signs of intrusion.

An IDS consists of three parts: information source, analysis, and response. An IDS can use several information sources to perform a pre-configured analysis on them. When an attack is detected, the IDS generates a response that can be passive or active. A passive response implies issuing a notification. An active response does an action such as interrupting communication. The purpose of an IDS is not to find out who conducted the attack. Instead, it is to interrupt it because the attacker's identity may be hidden, making it difficult to identify.

An IDS differs from other security mechanisms, such as a firewall or an antivirus, by monitoring traffic and deciding based on observed events. However, each security mechanism has its advantages and disadvantages, and combining them can provide in-depth security that can protect information systems against various security threats.

Several types of IDS are classified based on their monitoring approach, information source, type of analysis performed, and response time. There are network-based IDS for the monitoring approach and host-based IDS. Network-based IDS monitors network packets by listing network segments. Host-based IDS is designed to monitor events and activities on individual end devices, including the operating system, audit trails, system logs, and other data sources, such as medical records. There is also an application-based IDS, a subdomain of the host-based IDS, which monitors the application transaction log file generated by applications to perform attack detection.

There are two types of analysis methods used by IDS: misuse detection and anomaly detection. Misuse detection identifies attacks by matching the analyzed event to predefined patterns, which ensures high accuracy. However, this method cannot detect new or zero-day attacks, and new attack signatures must be added to the predefined templates continuously. On the other hand, anomaly detection identifies suspicious behavior by learning the normal operating pattern of the system using historical data. Any deviation from this normal behavior is flagged as potentially malicious. This method has the advantage of detecting new vulnerabilities and zero-day attacks. However, it can generate many false positives and requires a large training set to build the normal profile.

The response time of IDS can be real time or interval-based.

There are several possible architectures for IDS: centralized, fully distributed, and partially distributed. In a centralized architecture, monitoring, detection, and reporting are performed in a central node. In a fully distributed architecture, the response to an intrusion is carried out in the part of the network where monitoring is conducted. In a partially distributed architecture, the reporting is executed hierarchically.

The rest of the paper investigates the IDS that uses anomaly detection based on ML since the network that composes the IoMT is heterogeneous and diverse.

7. Machine learning overview

ML is a subfield of AI that gives a machine the ability to learn from data without explicitly programming it [64]. ML has proven efficient for problems requiring a long list of rules and complex problems where traditional approaches are inefficient. Also, ML shows a great capacity for adaptation to new data, especially in a changing and evolving environment such as the IoT system. ML has also shown a great ability to obtain insights from large volumes of data [65].

These ML capacities can be used to enforce security in the IoMT or at least improve it. Some studies demonstrate that using ML in IDS effectively detects zero-day attacks and new vulnerabilities, while IDS that rely on rules and signatures can only detect known attacks.

ML can also be used to learn the behavior of a person or an object by using the data generated to create a so-called normal profile, so any behavior that deviates from the normal profile is considered abnormal and consequently is detected, this is what is done in the field of anomaly detection.

Three types of ML can be used to solve security problems in the IoMT: supervised learning, unsupervised learning, and semi-supervised learning.

For supervised learning, the training data are labeled. The relationship between inputs and their appropriate output is captured. For this, there is a need to train a model with labeled inputs, which are used to predict or classify new data [66]. There are two types of supervised algorithms, which are regression and classification. The regression predicts the next continuous value based on the previous ones. On the other hand, classification predicts discrete variables and separates the data into different categories. Examples of the techniques that can be used for regression and classification are Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), Naive Bayes (NB), and artificial neural network (ANN).

Unsupervised learning involves training ML models on unlabeled data, as manually labeling data can be challenging and time-consuming. Instead, unsupervised learning algorithms analyze the data and identify patterns, relationships, or groupings among the data points. Some popular unsupervised learning techniques for clustering data include K-means, k-Nearest Neighbor (KNN), and Self-Organizing Map (SOM). Unsupervised learning can effectively divide large datasets into meaningful clusters to aid further analysis or decision-making [65].

While obtaining unlabeled data is often straightforward, leveraging its potential can be a significant challenge. Semi-supervised learning presents a solution by incorporating labeled and unlabeled data to build ML models that can classify data with improved accuracy. Compared to traditional supervised learning, semi-supervised learning reduces the need for manual labeling while producing models with greater accuracy. As a result, this approach has a special place in theoretical research and practical applications [67].

DL is a subdomain of ML, and it is inspired by the functioning of the human brain to process the signal. DL enables computational models with several layers of processing to learn data representation with several levels of abstraction [68]. DL differs from classical ML in its ability to capture the relevant feature previously done manually and required human intervention. Another advantage of DL compared to traditional ML is its performance on a large dataset. Therefore, this method is perfectly adapted to IoT systems and their applications, such as IoMT, which generates a huge volume of medical data. There are three types of DL: supervised example Convolutional Neural Network (CNN), unsupervised example the Deep Autoencoder, and finally, the combination of these two types, which is the hybrid DL, example ensemble of learning networks.

8. Review of machine learning applications for IoMT security

Health data are sensitive and can attract the attention of attackers for various reasons mentioned in Section 5.6. It is essential to protect medical data from threats by adopting a solution that ensures the security of this data during collection, transfer, storage, and processing. Protecting patients' privacy from unauthorized access is also necessary to avoid disclosing sensitive information to malicious entities. In addition, security solutions must consider the computational, storage, and energy limitations of medical devices and the heterogeneity, dynamics, and quantity of medical data generated within the IoMT system. In light of these constraints, ML has the potential to provide a solution for intrusion detection.

This section reviews the papers that have proposed a security solution based on ML for the different IoMT layers, specifying

Table 3
Details of published studies that use ML for security purposes in data collection level.

Ref.	Methods	Application	Advantage	Limitations	Dataset
(Kintzlinger et al. 2020) [7]	Rule, statistical and one class SVM	Detection of cyber-attack against ICD	- High TPR - High AUC - Low FPR - Real time - There is no extra consummation of energy and configuration to make in ICD - Anomaly detection can be done even from legitimate equipment - Emergency considered	- The dataset is unbalanced - Learns from only benign data - Layer III–V is not needed - There is no calculation of overhead - The proposed IDS is for a single type of medical equipment - The solution is deployed on external equipment that needs protection	- Self-created clinical data - Not available
(Khan et al. 2017) [69]	Discrete wavelet transform and Simplified Markov model	Detection of abnormality in ECG data	- High detection rate - Real time - High TPR	- Calculation of overhead is not performed - The dataset is imbalanced - They cannot differentiate in their model between emergency and attacks - The Augmentation in the number of attacks decreases the detection rate - High FNR and FPR	- Dataset obtained from MIT-PHYSIOBANK [70]
(Hei et al. 2014) [36]	Supervised learning using the regression method by applying SVM	Detection of an abnormal dosage of insulin in insulin pumps	- Real time - High success rate in detecting single and chronic overdose attacks - The data are real, since they were collected through patients with diabetes	- Need software modification of insulin pumps - Overhead is not calculated well. Possibly saturate the memory of the insulin pumps since they need to collect three months of logs - This solution ensures the safety of a part of the insulin pump system and not the whole system - The model must be adapted for each patient, and a collection of 6 months of log files is necessary to create it, which means the patient is exposed to attacks during this period. - The value of the insulin dose that indicates an emergency is fixed for all patients	- Use of log files generated by the pump system from 4 patients - Not available
(Ahmad et al. 2018) [71]	LSTM and gesture recognition	Prevent lethal insulin administration on patients	- Intuitive solution	- The patient must make a gesture to indicate if the amount of insulin in their body is good based on a symptom. However, what if the patient is young, and what if the patient becomes very sick and cannot perform gestures - The gesture sensor is also equipped with a wireless transmission module, which makes it vulnerable and must be secured - Their solution also requires a modification of the protocol adopted by the insulin pump - Their solution starts to work after three months of log file collection, which makes the system vulnerable during this period - The authors do not present details of their model, the results obtained, deployment of the IDS, and the analysis of their solutions - The solution proposed allows the protection of a single type medical equipment	- Not available

(*continued on next page*)

their objectives, the method employed, the dataset used, and the results obtained. Tables 3, 4, and 5 summarize the papers explored in this review, mentioning the methods, applications, advantages, disadvantages, and dataset.

8.1. ML for data collection level security

Sensors associated with patients allow constant monitoring of their health status and automatic medication for people suffering from chronic diseases. This technology, despite its advantages, must be protected against security threats due to the wireless transmission of medical data to a personal server and the possibility of configuring the medical equipment via a programmer device, which increases the surface of the attack. These security threats can be either intentionally caused by hackers or unintentionally caused by the environment due to interference. Patients need a security solution that detects such threats,

Table 3 (*continued*).

Ref.	Methods	Application	Advantage	Limitations	Dataset
(Rathore et al. 2017) [6]	MLP, a DL approach	Detection of fake glucose measurements and/or command on wireless insulin pump	- High accuracy - High reliability - Real time - Implemented on the chip, so it can be deployed on any device of the system using insulin pumps. These are the reason why the solution is reliable - Better recall compared with linear-SVM	- The authors propose to implement their solution on a chip that can be integrated in the IMD, which requires a modification of the device at the hardware and software level - They do not specify what is the action to take when an erroneous glucose measurement is detected - High space and time complexity compared with SVM - Non comparison is made with the non-linear SVM - The solution proposed allows the protection of a single type medical equipment - The emergency is not considered	- Dataset obtained from the public repository "UCI machine learning repository" [72]
(Shobana, 2022) [73]	Unsupervised learning using the deep autoencoder	Attacks detection using logs generated within insulin pump system	- They use unsupervised learning, which avoids manual labeling of data - High scores (Accuracy, Precision, Recall and F1-measure)	- The attacks are simulated - Overhead and execution time are not calculated - The deployment of the model not mentioned - The emergency is not considered - The solution proposed allows the protection of a single type medical equipment	- Diabetes Data Set [74]
(Rathore et al. 2019) [5]	Supervised learning using LSTM	Prevention of stimulation strategies attacks on DBS	- Real time - The loss value is low	- The authors did not specify where the solution is deployed - Accuracy not mentioned - Overhead not calculated - The attacks are simulated and are not real - The emergency is not considered - The solution proposed allows the protection of a single type medical equipment	- Data obtained from physionet [75]
(Hei et al. 2010) [76]	Linear and non-linear SVM	Prevent resource dilapidation on IMD	- High accuracy - Real time - Add an extra layer of security to IMD -Solution designed for multiple medical devices	- The solution is implemented on an external device (cell-phone) that can be stolen, lost or simply forgotten by the patient - Need software modification of the medical device - At each authentication request, the IMD forwards this request to the cell-phone, which causes the IMD to consume energy and must be taken into consideration - This scheme is not designed to support emergencies - The protocol used between the cell-phone and the IMD is not secure - Their solution is not holistic since it is tested against only one type of vulnerable device - The patient must make a decision if the classification is not accurate	- Not mentioned - Not available
(Newaz et al. 2019) [77]	ANN, DT, RF and KNN	Detection of malicious activity in the smart healthcare system	- High accuracy and f1-score - Computation and detection time considered - The systems proposed can determine if the alert generated is due to a disease or not - The dataset contains data of a healthy person as well as a diseased patient Solution designed for multiple medical devices	- Overhead is not calculated - The FPR metric is not mentioned - They did not specified where this solution is deployed	- Use different datasets obtained from various repositories

(*continued on next page*)

Table 3 (*continued*).

Ref.	Methods	Application	Advantage	Limitations	Dataset
(Salem et al. 2021) [78]	RMSE, Markov chain	Anomaly detection from the data collected by biosensors in WBAN composed of sensors and LPU	- High TPR. - Low FAR - Solution designed for multiple medical devices - The solution is deployed on LPU, which reduces the transmission cost - Emergency considered	- The attack is simulated - The model cannot differentiate between disease and attack if abnormalities are detected - Overhead is not calculated	Public dataset containing real data obtained from physionet website [79]

differentiates them from emergency cases and avoids lethal doses of medication.

Among the different medical devices that researchers have investigated to provide a security solution, there are cardiac implants that provide electrical impulses to stimulate the cardiac muscles in case of abnormalities in the heart rhythm. A well-placed attacker can cause an electrical impulse that can be fatal for the patient. To avoid this kind of situation, the researchers (Kintzlinger et al. 2020) in [7] proposed a system that detects and prevents cyberattacks against ICD. It is implemented at the level of the programmer's device. The Cardiwell is a decision aid for doctors that, in case of detection of an anomaly, generates an alert with the necessary details that allow the doctors to decide then if they pass the programmer commands. The Cardiwell is a multi-layer Security scheme, and it consists of six layers of security. The first five layers use rules and statistics, while the sixth layer uses the method of one class SVM, which is based on ML. To validate their solution, tests were performed on a dataset collected from volunteer patients from different hospitals and clinics over four years. This dataset consists only of benign programmer commands sent from a programmer device to an ICD and which represent a total of 775 samples, while experts generate malicious programmer commands and represent a total of 28 samples. After performing the different tests, the best results obtained are True Positive Rate (TPR) = 0.914, False Positive Rate (FPR) = 0.101, and Area Under the Curve (AUC) = 0.947. However, layers three to six are inefficient and do not participate in improving the results, which according to the authors, is due to the poor datasets that need to be enriched.

The study made by (Khan et al. 2017), as described in [69], presents a novel approach for detecting abnormalities in Electrocardiogram (ECG) data. The authors proposed a centralized solution and chose a simplified Markov model-based detection mechanism due to the changing nature of ECG data over time. The proposed approach involves extracting attributes from the ECG data, followed by reducing the dimensionality of the dataset using the discrete wavelet transform. The reduced dataset is then partitioned into sequences, and the probability of each sequence is calculated to determine if any changes have occurred. If an abnormality is detected, the system associates an abnormal tag with the corresponding data and forwards it to the hospital server for further evaluation by nursing staff. The evaluation process is designed to determine the normality of the received data. To test the efficacy of their approach, the authors utilized a dataset from MIT-PHYSIOBANK [70] and introduced 5% and 10% of attacks composed of forgery, unauthorized insertion, and ECG data modification. After conducting the experiments, the authors achieved a high detection rate, reduced training time, and a high TPR.

Other researchers have studied the security of the insulin pump system, which allows the automatic administration of insulin according to the amount of glucose in the patient's blood. However, an intruder can cause a lethal insulin administration if the device is compromised. In this perspective, the researchers (Hei et al. 2014) in [36] addressed the security gap between the Carelink and the insulin pump, two components of the insulin pump system where the attacker can carry out two types of attacks; the first one is the bolus dose where the attacker delivers a large amount of insulin in a short period. The second possible attack is the basal dose, where the attacker delivers an insignificant amount of insulin over a long period, which can threaten the patient's life. To address these issues, the authors propose to use a supervised machine-learning algorithm using SVM with a regression method to learn the normal insulin dosage of each patient at different parts of the day. The authors collected insulin pump log files from four patients over six months to generate the dataset. Each log entry is composed of infusion rate, dosage, blood glucose level, patient ID, and time of day for each infusion. After performing different tests, the authors obtained better results with the non-linear SVM than the linear SVM by getting a score of 98% of success rate in detecting a single overdose attack and a high success rate in chronic overdose attack detection. The authors propose deploying the insulin pump model with an update every 90 days. In the case of anomaly detection, an alert message is raised. The authors have also defined a value of insulin that, if exceeded it, indicates that the patient is in an emergency and, therefore, the system is deactivated.

In another study made by (Ahmad et al. 2018) in [71], The authors proposed to secure the insulin pump against attacks that aim to alter the functioning of its system to deliver a lethal dosage of insulin to the patient. To address this issue, the authors propose using Long Short-Term Memory (LSTM), a DL algorithm, to define a threshold value for the insulin dosage delivered to the patient. If the insulin dosage value exceeds the threshold value, the system calls the patient to perform a gesture by raising the thumb or spanking it down, which is captured by a gesture sensor. The authors propose to use a gesture sensor because they assume that the patient can feel and judge the significant change of insulin in their body through symptoms like nervousness, trembling, and weakness. Therefore, depending on these symptoms and the dose of insulin to be administered, the patient can accept the insulin dose by raising the thumb or refusing it by lowering it. To test their solution, the authors used a dataset containing log files generated by the insulin pumps system over the last three months to train and test the LSTM and determine a threshold value.

In a study conducted by (Rathore et al. 2017) in [6], the authors proposed a solution for detecting fake glucose measurements in the entire insulin pump framework, which comprises a continuous glucose monitoring system, a sensor, a transmitter, an insulin pump, a remote control, and a one-touch meter. The authors proposed a solution that uses the Multi-Layer Perceptron (MLP), a DL algorithm, to classify glucose measurements in the blood as genuine or fake. To evaluate the effectiveness of their solution, the authors used the Pima Indians Diabetes dataset [72] and achieved 93.98% of accuracy. Furthermore, the authors employed the NB algorithm to test the reliability of their system and obtained a success rate of 90%. According to the authors, this high success rate is due to the deployment of their model on a chip using Field Programmable Gate Arrays (FPGA), which can be integrated into any equipment used in the insulin pump framework, thereby securing it against erroneous blood glucose measurements.

Table 4
Details of published studies that use ML for security purposes in Transmission Level.

Ref	Methods	Application	Advantage	Limitations	Dataset
(Gao and Thamilarasu, 2017) [80]	Different ML (DT, SVM, K-MEANS)	Intrusion detection system for connected medical devices	- High accuracy for DT - Low number of false positives - Their solution does not require any modification of software or hardware - Real time	- The solution is implemented in external equipment that can be stolen, lost or forgotten - The external equipment where the solution is implemented must also be secured - In case of attack detection, there is no measure to stop the attack - It does not allow the detection of attacks emanating from an internal environment Lightweight solution not considered Synthetic datasets - Black-box model	- The dataset is generated using the Castalia simulator [81] - Not available
(Al-Shaher et al., 2017) [82]	MLP activated by wavelet transform and wavelet neural network	Proposal to protect the private health system from cyberattacks by designing and implementing an IHSS	- High accuracy - Real time detection - The proposed detection engine can be integrated into web filter, intrusion detection, and firewall	- Not all metrics are used - It does not allow the detection of attacks emanat ing from an internal environment - Overhead not considered - Black-box model - No measure to protect privacy	- Not mentioned
(He et al. 2019) [83]	Stacked Autoencoder to extract features and XGBoost to perform classification	Proposal of an IDS based on a stacked Autoencoder for anomaly detection in the connected healthcare system	- High accuracy - Low FPR and FNR - Real time - Lightweight solution	- The deployment of the solution is not mentioned - It does not allow the detection of attacks emanating from an internal environment - Overhead is not calculated - The dataset is imbalanced - Black-box model - No measure to protect privacy	- Self-generated datasets were collected from patients, and attacks were simulated
(Newaz et al. 2020) [84]	n-gram for features extraction and four ML (KNN, SVM, RF, DT)	Detection of cyber-attack on PMDs	- High accuracy - High F1-score - System is tested against the different types of attacks using different types of PMD - Scalable. - Perform passive analysis, which is effective in terms of performance overhead - Real time	- Not all performance metrics are used - Detection time is not considered - The combination of ML methods deteriorates the performance of HEKA - Their solution is only tested against the 'just work' authentication mechanism of the Bluetooth and is not tested against the 2 others which are passkey entry and out of band methods - It does not allow the detection of attacks emanating from an internal environment - The data are collected from healthy persons - Black-box model	- The data are generated from different real devices - The dataset is not publicly available
(RM et al. 2020) [85]	PCA and GWO to reduce the dimensionality of data and DNN to classify data	Intrusion detection system in IoMT system	- Increase in accuracy by 15% and decrease in time complexity by 32% comparing with traditional ML approaches - The reduction in data dimensions, reduce the time complexity and increase the accuracy - The gray wolf optimization allows reducing the drawback of the local minimum	- The dataset used is not designed for IoMT - The implementation of this solution is not mentioned - Overhead is not calculated - Black-box model - No measure to protect privacy	- Kaggle intrusion data samples were collected from Kaggle open-source center
(Lee et al. 2021) [86]	CNN	IDS designed for healthcare IoT in the smart city	- High accuracy - Real time - Low computational overhead - Multi-class classification - Different medical devices used to collect data	-The class major has a low accuracy rate - Black-box model - No measure to protect privacy	- Dataset generated from six medical devices - Not available

(continued on next page)

Table 4 (*continued*).

Ref	Methods	Application	Advantage	Limitations	Dataset
(Salemi et al. 2021) [87]	Lyapunov exponent analysis and echo state network	Prediction of DDoS attacks in multimedia-based healthcare systems	- High accuracy - Real time - Can predict the DDoS attack instead of detecting it	- Overhead is not calculated - Old dataset, and it is not specific for IoMT - Black-box model - No measure to protect privacy	DERPA 98 dataset, publicly available [88]
(Thamilarasu and Odesile, 2017) [89]	Mobile agent-based intrusion detection system using ML and regression algorithms	Securing the network of connected medical devices	- High detection accuracy - Low overhead - Detection intrusions are performed at the network and device level - Systems are scalable, hierarchical, distributed, fault-tolerant, and autonomous	- Consume energy at the sensor agent level - The patient data are sent in some cases to the cluster head, which represents a possible violation of privacy - Black-box model	- Data are generated using OMNeT Castalia simulator [81] - Not available
(Begli et al., 2019) [90]	IDS based on supervised learning using non-linear SVM and misuse detection systems	Detection of common attacks including DoS and user to root in remote healthcare systems	- High detection rate for hybrid and anomaly detection systems - Real time	- Low detection rate for misuse detection systems - The dataset used is not specifically made for the IoMT - Overhead not calculated - Not all metrics are used - Rule number 2: This rule does not allow the detection of new vulnerabilities and zero-day attacks - Black-box model - No measure to protect privacy	NSL-KDD dataset, publicly available [91]
(Alrashdi et al. 2019) [92]	EOS-ELM	Framework for attack detection in the Fog node	- High detection rate - Low latency - Real time - The system is distributed	- Overhead is not calculated - No measure to protect privacy - The dataset used is not specific for IoMT - Not all metrics are used - Black-box model	- NSL-KDD dataset [91]
(Kumar et al. 2021) [19]	NB, DT, RF and XGBoot	Cyber-attack detection in IoMT networks using fog–cloud architecture	- Distributed solution - High detection rate - High accuracy - Low FAR	- Training time for ensemble learning is higher than the different ML used alone - The dataset used is not specific for IoMT - NB present the worst result for different metrics used to evaluate the ML model - Black-box model - No measure to protect privacy	Ton-IoT dataset, publicly available [93]
(Gupta et al., 2022) [94]	Deep hierarchical stacked neural networks	IDS to detect modification in data flow within multi-cloud healthcare systems	- High accuracy - Low execution time	- The model needs to be trained with data at the core cloud, which could impact data privacy - Overhead is not calculated - Black-box model	- UNSW-BOT-IoT and UNSW15 [93] datasets - Generated dataset
(Hameed et al., 2022) [95]	Weighted Hoeffding Tree Ensemble	Fog-based IDS for the industrial IoMT	- Lightweight solution - Their solution can be deployed on edge and fog - High accuracy	- The dataset used is not designed for IoMT - Black-box model - No measure to protect privacy	- NSL-KDD [91] and ToN-IoT [93] datasets
(Khan and Akhunzada, 2021) [20]	CNN to extract feature and LSTM to classify data	Hybrid deep learning-based model for malware detection in the IoMT deployed at the SDN plane application level	- High detection accuracy - Speed efficiency	- This framework is prone to a single point of failure - Black-box model - No measure to protect privacy	Use of publicly available datasets. However, they do not mention it
(Wahab et al. 2022) [96]	hybrid model combining LSTM and GRU	IDS based on ML to secure the IoMT architecture based on SDN against cyber threats	- High accuracy, precision and F1-score - Fast execution	- The dataset used is not specific to IoMT systems - The solution is centralized, which suffers from a single point of failure - Overhead not calculated - No measure to protect privacy - Black-box model	CICDDoS2019 dataset [97]

(*continued on next page*)

So far, the methods used to secure the insulin pump system are based on supervised learning methods. However, the study conducted by (Shobana, 2022) in [73] proposed using an IDS based on unsupervised ML to secure the insulin pump injection against four generated attacks: Long Resume, Single Acute Overdose, Underdose, and Chronic Overdose. For this purpose, the authors proposed using a deep autoencoder and a DL algorithm to classify the logs generated within the medical equipment. To test and evaluate their solution, they applied their method to the Diabetes Data Set [74]. They measured the model's performance

Table 4 (*continued*).

Ref	Methods	Application	Advantage	Limitations	Dataset
(Schneble and Thamilarasu, 2019) [98]	Federated learning	Securing the medical cyber–physical systems	- The system is distributed and scalable - High detection accuracy - Low FPR - Real time - Low communication overhead - Protects patient privacy by transmitting only the model instead of the patient data	- The model of ML is not protected during transmission - The minimum and the maximum number of mobile devices that should be taken into consideration is not determined - They did not specify how the medical staff is notified in case of anomaly detection - Black-box model	- MIMIC Dataset obtained from physionet, publicly available [99]
(Singh et al. 2022) [100]	HFL based on hierarchical long-term memory	IDS for distributed dew servers of the IoMT system	- High accuracy, precision, f-score and recall - Reduced computation cost - Data privacy preserved	- Dataset not made for IoMT applications - No measures to protect models transmission - Black-box model - Execution time not considered	- TON-IoT [93] and NSL-KDD [91] datasets
(Khan et al. 2022) [101]	Simple Recurrent Units with skip connections and Local Interpretable Model-Agnostic Explanations	IDS for IoMT network deployed at gateway and router levels	- High accuracy, Precision, Recall, and F-measure - Low computation cost - Time efficiency - Model explained and interpreted	- Dataset used is not specific for IoMT systems - The solution is centralized, which is prone to a single point of failures - No measure to protect privacy	ToN-IoT [93] dataset
(Hady et al. 2020) [102]	They compare the results of different ML methods	IDS for healthcare using medical and network data	- High accuracy and AUC - Real time - Datasets designed for IoMT application	- The dataset contains only two types of attacks - The dataset is imbalanced - Computation overhead is not considered - The IDS are located between the gateway and server. However, the attack can occur between medical equipment and getaway - Black-box model	Dataset publicly available [103]

in terms of accuracy, precision, F1-measure, and recall. The results obtained exceed other traditional ML methods and previous work.

In a pioneer work carried out by (Rathore et al. 2019) in [5], a solution based on ML was proposed to enhance the security of DBI. A DBI comprises a quadripolar electrode implanted in the human brain, an Implementable Pulse Generation (IPG), and a controller that switches on/off the medical device. Some IPGs are customizable to modify voltage levels. The primary function of the DBI is to regulate the Rest Tremor Velocity (RTV) by maintaining its value at zero through electrical charges. Movement disorders and chronic diseases like Parkinson's arise when the RTV deviates from zero. An attacker with access to the DBI can attempt to modify the RTV's value, thereby seriously endangering the patient's life. To address this issue, the authors modified the RTV value to simulate various attacks. They proposed to use LSTM, a DL algorithm, to predict the RTV value at time T. By detecting and classifying any deviations from the predicted RTV value, the proposed solution can prevent potential attacks on the DBI. To create and test the model, the authors used a dataset obtained from Physionet [75], which contained 173,398 samples with ten features. However, the authors focused primarily on the RTV attribute, considered the most critical attribute since its modification by an adversary could have detrimental effects on the patient. After conducting various tests, the model efficiently classified attack strategies with minimal loss values and training times.

The solutions explored so far have focused on securing a single medical device. This section reviews more general solutions that include multiple medical devices. In this regard, (Hei et al. 2010) in [76] suggested adding a security layer for IMD by using patient IMD access pattern and SVM. This solution prevents authentication requests from illegitimate programmers or readers, saves energy, and counters attacks that drain IMD energy resources. If the IMD's battery power is depleted, surgery is required to replace the battery, which can be life-threatening. The additional security layer implements a ML-based cell phone model using SVM that classifies authentication requests from readers. Depending on the response of the cell phone, three situations are considered: (1) in case the request is classified as benign, then the IMD can perform the authentication with readers, (2) in case the request is classified as malicious, then the IMD put itself on standby to not waste more energy. (3) If the model fails to classify the request, the decision is left to the patient, who can authorize or deny the authentication request. For the emergency, the authors suggest assigning a value to cardiac implants that signify a critical condition for the patient when reached. In this case, they suggest either disabling the classification or using a backdoor accessible via a key shared between the IMD and the authorized persons to guarantee access to the implant. The dataset used to create the model consists of 3000 entries, of which 2500 are used to train the model and 500 to test it. The dataset is composed of five attributes which are the reader action type which determines the type of action that the reader wants to perform on the IMD, a time interval of some reader's action, location (home, hospital, pharmacy), time, and day (weekend, weekday). After performing the different tests, they obtained an average accuracy of 90% for the linear SVM and 97% for the non-linear SVM.

Other researchers (Newaz et al. 2019) in [77] presented a secure framework to detect malicious activities in the Smart Healthcare System (SHS). The proposed framework uses different ML: ANN, DT, RF, and KNN, to detect malicious activity in the SHS. The data used to evaluate their framework are collected from eight different databases. The dataset obtained contains 20,000 samples, of which 17,000 represent data from healthy people and people suffering from diseases, and 3000 represent attacks that simulate three different threats, which are compromised medical devices, DoS, and false data injection. After performing the tests, they obtained 91% accuracy and 90% F1-score.

In another work carried out by (Salem et al. 2021) in [78], they proposed a centralized Markov chain-based solution for the

Table 5
Details of published studies that use ML for security purposes in Storage Level.

Ref.	Methods	Application	Advantage	Limitations	Dataset
(Boxwala et al. 2011) [104]	LR and SVM	Help institutions detect suspicious access to electronic health records	- Good AUC - Good sensitivity	-Their method requires the intervention of privacy agents, who are not always present, nor have the necessary knowledge to differentiate between what may or may not constitute a violation - The solution is not real time - The problem has only been addressed by one institution - The solution is not fully automated since labeling dataset is performed manually - Not all metrics are used - Not real time	Not available
(Menon et al. 2014) [105]	Collaboration filtering using latent and explicit features	Detection of privacy breaches resulting from inappropriate access to EHR	- The proposed model offers a significant improvement over supervised learning methods	-Their approach implies the intervention of privacy officers, who may not be present and do not have the expertise to distinguish between violations and non-violations - The model is not real time - The solution is applied to one institution - They use a small training dataset because privacy officers do the labeling of data manually - Not all metrics are used - The model is not fully automated	- Use two datasets named «hospital» and «amazon» - The dataset «hospital», not available - The dataset «amazon» is available at [106]
(Malin and Bradley, 2014) [107]	Unsupervised learning model using singular value decomposition and KNN	Detection of insider threat in collaboration environment using access logs, named community-based anomaly detection system	- High degree of certainty in differentiating anomalous users from real users - Outperform other states of the art approaches	- Experts are needed to validate the result (not fully automated) - The number of k cluster in KNN change from one system to another - This approach cannot detect attackers that imitate legitimate group behavior or legitimate behavior of another user - Not real time	- The First dataset is a collection of six months of access logs from real electronic health records - The second dataset is the report of the editorial board membership for a set of journals discipline over 5 years - Not available
(Marwan et al. 2018) [108]	combination of SVM and FCM	Securing image data processing in a cloud environment based on machine learning	- Good alternative to data encryption	- Small dataset (only two images)	Use of two images for testing purposes
(Sicuranza and Paragliola, 2020) [109]	Rule, DT, neural network and k-means	Hybrid IDS for the detection of cyber-attack against the EHR system	High accuracy for anomaly detection module	- The time of detection is not calculated - The result of the misuse detection module is not reported - The solution is applied to one institution - Due to the requirement for an expert to resolve any conflicts in the presence or absence of attacks, the solution is not fully automated	Dataset was produced by monitoring the Italian EHR system and simulate three different attacks (not available)
(McGlade and Scott-Hayward, 2019) [59]	SVM and EMA	Framework for confidentiality and availability issue detection in EMR systems	- High detection accuracy - High recall	- Not all metrics are used. - The integrity of the system EMR is not checked through the ML method	- Synthea was used to simulate the representation of patient data in the FHIR Database by generating patient information such as names and addresses [110]

detection of anomalies from the data collected by biosensors in WBAN that is composed of sensors and a Local Processing Unit (LPU). In the proposed system, only the measurements captured at the sensors that deviate from the expected values are communicated to the LPU, reducing energy consumption caused by the transmission of routing data. The proposed method is based on a Markov Model (MM) constructed based on the Root Mean Square Error (RMSE) between the forecasted and measured value for complete attributes. The method intends to work with LPU to detect abnormal deviations in the gathered data and reject erroneous or added measurements. After detecting physiology-related changes and removing erroneous or inserted measures, the system alerts the healthcare staff. To test and evaluate their system, the authors used a public dataset containing real data obtained from Physionet [79]. After performing the different tests, the authors obtained 100% TPR while maintaining a low False Alarm Rate (FAR) of 5.2%. They also compared their approach with other existing methods that use the Markov chain for ECG anomaly detection and other supervised ML algorithms: SVM, KNN, J48, and the distance-based method. The system proposed in this paper exceeds the MM-based ECG abnormality detection system by a small margin and outperforms the ML methods regarding accuracy.

After reviewing the different solutions of security based on ML for data collection level, most of these researches are focused on the security of cardiac implants [7,69] and insulin pump injection systems [6,36,71]. There is just one study based on the security of DBI [5]. However, other medical implants use wireless communication and are not yet investigated, such as the Gastricelectrical stimulator. This medical device stimulates the smooth muscles of the lower stomach equipment to help control chronic nausea and vomiting associated with Gastroparesis. This equipment uses wireless communication that suffers from a lack of encryption, authentication, validation mechanism, and Hardware/Software error [111], making it vulnerable to different attack types, including eavesdropping, information disclosure, tampering, jamming, and resource depletion [9]. Therefore, it must be considered when the researchers conceive an IDS for multiple medical devices.

8.2. ML for transmission level security

The transmission of medical data between devices composing the IoMT and the server enables the remote healthcare system to continuously monitor and treat patients in real time. However, the sensitive nature of the data exchanged represents a high interest for cyber-attackers, who, in case of a successful attack, can cause severe repercussions for the patient, ranging from violation of privacy to death. In addition, the heterogeneous nature of the devices used increases the surface of attack, which requires the design of a secure architecture for the IoMT.

In this context, (Gao and Thamilarasu, 2017) in [80] proposed a solution to detect attacks that target connected medical devices based on ML methods. Learning the normal behavior of the connected medical device allows the detection of any deviation from this behavior and generates a warning notification sent to the patient.

The ML model is deployed on an external device that monitors the network and performs an analysis to detect an anomaly. To test the effectiveness of their solution, the authors used three datasets of different sizes generated by a Castilia simulator [81] and evaluated the performance of DT compared to SVM and k-means. After conducting various tests, the authors found that DTs provided higher accuracy, generated fewer false positives, and had a faster training and prediction time.

In another work performed by (Al-Shaher et al., 2017) in [82], they proposed to protect the private healthcare system from known viruses, worms, spyware, and denial-of-service attacks by designing and implementing an Intelligent Healthcare Security System (IHSS). The IHSS integrates the firewall, network intrusion detection subsystem, and web filter. The IHSS is intended to enhance the capabilities of these network protection systems using artificial intelligence approaches. The authors use MLP activated by wavelet transform to classify network traffic. The intrusion detection subsystem uses a wavelet neural network to determine which type of attacks are occurring by solving the multi-class problem. In web filters, they use Wavelet Neural Network to detect malware. After evaluating their method, they obtained 93% accuracy with two hidden layers and 90% with one hidden layer.

Other research group (He et al. 2019) proposed an IDS based on a stacked Autoencoder for anomaly detection in the Connected Healthcare System, as outlined in their publication [83]. The method involves several stages of data processing, including mapping, discretization, and normalization, before feeding the data to the stacked Autoencoder. The Autoencoder is used to extract the relevant features, which the ML models then use to perform detection and classify the data as either an attack or not. To evaluate the performance of their IDS solution, the authors collected a real dataset from patients and simulated various types of attacks, such as DoS, counterfeit attacks, temper attacks, and replay attacks. They compared the performance of different ML models, including SVM, NB, KNN, and XGBoost, using metrics such as accuracy, FPR, and FNR. After conducting several tests, the authors found that the XGBoost model achieved the best performance with 97.83% accuracy, 2.35% FPR, and 1.65% FNR.

Other researchers (Newaz et al. 2020) in [84] presented HEKA an IDS based on ML for personal medical devices (PMD). The traffic generated between the PMD and the smartphone is analyzed with a sniffer to detect possible attacks using ML. The n-gram extracts feature sent to the IDS composed of four ML (KNN, DT, RF, and SVM). The HEKA is tested against four types of attacks, including a Man-In-The-Middle (MITM), false data injection, Replay, and DoS individually, then combining MITM and false data injection, and finally, MITM and Replay. They use eight devices composed of four PMDs (iHealth Air Wireless Pulse Oximeter, blood pressure monitor, QuardioArm blood pressure monitor, and wireless weight scale). The final dataset is composed of 731 benign instances and 308 malicious instances. After the realization of the different tests, they obtained a score of 98.4% accuracy and 98% F1-score.

In another study conducted by (RM et al. 2020) in [85], a new approach was proposed to develop an IDS based on DL to predict and classify cyberattacks in the IoMT using a unique IP address. The proposed methodology aims to reduce the number of features and instances required for the classification process. This was achieved by transforming the categorical data into numerical data using one-shot coding, then normalizing it to a value between 1 and 0. Then, the normalized data is reduced using principal component analysis (PCA) at the first level and gray wolf optimization (GWO) at the second level, extracting only the most important features. The reduced dataset is then ranked using a DL algorithm using deep neural networks (DNN). To evaluate the effectiveness of their proposed solution, the authors used a dataset obtained from Kaggle containing data collected by a wireless sensor network. They compared the performance of their methodology with other commonly used ML algorithms, including KNN, NB, RF, and SVM, using the measures of accuracy, specificity, and sensitivity. After performing various tests, the study found that the proposed methodology improves IDS accuracy by 15% and reduces learning time by 32%. These improvements would enable timely alerts to be generated in the event of intrusion detection in healthcare system.

In another work carried out by (Lee et al. 2021) in [86], they proposed an IDS using ML and multi-class classification for the healthcare IoT within the smart city. The authors used CNN as an ML method to classify the network events generated by different medical devices into four classes, namely (critical, informal, major, and minor). Before the data are fed to the model, the data are preprocessed by transforming the categorical data into numerical data, then normalizing the data to take values within the same range. To evaluate their model, the authors generated a dataset by collecting data from six medical devices and then used them to compare their model results with other ML models regarding AUC, F1-score, Precision, and Recall. After performing the different tests, the authors found that their CNN model produces better results than other ML methods.

In another work performed by (Salemi et al. 2021), they presented a novel approach for predicting Distributed Denial of Service (DDoS) attacks in healthcare systems, as opposed to merely detecting them [87]. The authors demonstrated that DDoS attacks cause traffic data to become chaotic, which can be analyzed using the Lyapunov Expansions Analysis and the Echo State Network. To implement their approach, the authors first represented network traffic as time-series data and applied a simple exponential smoothing method to predict future traffic. They then calculated the time-series prediction error by subtracting the predicted data from the actual data, which served as the basis for DDoS attack analysis. The authors then utilized a recurrent neural echo state network to predict the time series and used the LEA-MA method to detect the DDoS attack. To evaluate their method's effectiveness, the authors tested it on the DARPA 98 dataset [88] and used metrics such as precision, recall, and F1-score. Their experiments showed that their proposed method could efficiently predict DDoS attacks.

In the following, a distributed IDS within the IoMT systems are presented as a solution. Among these solutions, there is work made by (Thamilarasu and Odesile, 2017) in [89]. They proposed an approach that utilizes mobile agents to conduct penetration testing and secure the medical equipment network. The proposed system is characterized by its hierarchical, autonomous, and distributed nature. Intrusion detection is performed using a regression algorithm at the medical equipment level and ML techniques at the network level. Mobile agents traverse from one node to another or within a cluster, collecting network activities or device data based on their role as network or device intrusion detection agents. At the end of an intrusion test, the mobile agent classifies the collected samples as voluntary, malicious, or suspicious. The mobile agent migrates to another node if the samples are classified as voluntary. However, if the samples are malicious, an alarm is generated, and the data is sent to the cluster head. If the samples are suspicious, a request for intervention is sent to the cluster head. The cluster head deploys a special agent to collect data from the network or medical equipment of the entire cluster. The collected data are then tested to determine whether they are benign or malicious. Additionally, the system incorporates a security mechanism to detect intrusion at the cluster head level, which is achieved by using the cluster head agent that performs anomaly detection while traversing the cluster head network. The authors evaluated their proposed solution using OMNeT Castalia 3.2 simulator [81] and tested five ML algorithms (SVM, DT, NB, KNN, and RF) to detect anomalies at the network level. Based on the accuracy, Cost Ratio, Feedback Reliability, training time, Total Rank Score, and Energy Overhead, DT produced the best results. Moreover, to detect anomalies in devices, the authors employed a cubic model of polynomial regression that balanced accuracy, overfitting, and computational resources. Finally, the proposed system was tested in a simulated hospital network topology and showed high accuracy, low overhead, and scalability.

Furthermore, in another study reported by (Begli et al. in 2019), a framework for securing remote healthcare systems was proposed [90]. Given the distributed nature of such systems, the authors employed multiple agents, each categorized based on their energy consumption and sensitivity to security risks. The resulting framework consists of three agent classes: sensors, smartphones, and databases. The first class, comprising sensors, utilizes a non-linear SVM-based anomaly detection approach, which consumes less energy and is effective for the limited data available from sensors. The second class of agents, composed of equipment with more energy autonomy than the sensors, for example, smartphones, uses a misuse-based intrusion detection system. The third and most critical class, which involves databases storing sensitive patient information, uses a hybrid detection system based on anomaly and misuse detection methods, as it is more prone to attacks and therefore has the highest security requirements. The authors evaluated the framework using the NSL-KDD dataset [91] to detect various attacks, including DoS and user-to-root. The results demonstrated the effectiveness of the proposed framework, with efficient execution time, low energy consumption, high accuracy, and a low number of false positives.

In more recent studies, researchers explore other architectures that can be used in the context of IDS in IoMT systems: fog–cloud, SDN, and federated learning. In this regard, the work carried out by (Alrashdi et al. 2019) in [92] developed a framework for detecting attacks in fog nodes [92]. The authors used Online Sequential Extreme Learning Machine (OS-ELM) due to its learning speed. However, since OS-ELM produced inconsistent results, the authors employed a set of OS-ELM and employed majority voting to determine the presence of an anomaly. Prior to applying the ensemble of Online Sequential Extreme Learning Machine (EOS-ELM), the authors preprocess the data by converting discrete values into numerical values. Subsequently, they utilized the Information Gain algorithm and voting method to select features, then normalized the chosen attributes to values between 0 and 1. To evaluate and test their framework, the authors utilized NSL-KDD [91]. After numerous tests, the authors found that EOS-ELM outperforms extreme learning machine, OS-ELM, and ML regarding accuracy, detection rate, and FPR.

In another study made by (Kumar et al. 2021) in [19] proposed an IDS that utilizes ensemble learning and a fog-cloud architecture to detect cyber-attacks in IoMT networks. The system preprocesses traffic data by converting categorical values into numerical values, replacing missing values with the mean of the corresponding feature values, and selecting the relevant features for intrusion detection using the correlation coefficient method. The numerical values are then normalized using the min-max technique to ensure they fall within a specific range. The system uses a learning set consisting of NB, DT, and RF algorithms, which produce three prediction outputs. These outputs are then fed to XGBoost to produce the final output using majority voting. When an intrusion is detected, the administrator is alerted. The framework is deployed using a fog-cloud architecture, which utilizes Software as a Service at the fog level and Infrastructure as a Service at the cloud level. The authors evaluated their framework using the Ton-IoT dataset [93], representing data collected from heterogeneous and large-scale IoT networks. The evaluation metrics were accuracy, detection rate, precision, FAR, and F1-score. The results show a detection rate of 99.98%, an accuracy of 96.35%, and a reduction of up to 5.59% of the FAR. These results surpassed those of previous studies that used IDS.

In another research made by (Gupta et al. 2022) in [94], they proposed to use of deep hierarchical stacked neural networks to detect attacks that would attempt to modify the data flow, including meta-information that transits between the gateways and the edge cloud and between the edge cloud and the core cloud within multi-cloud healthcare systems called MUSE. This method includes reusing the edge cloud's trained layers to merge them and form a pre-trained model at the core cloud level. The tests were performed on three different datasets: UNSW-BOT-IoT and UNSW15 [93] and one generated by the authors. A comparison was made with the method that does not reuse the trained layers of the edge cloud. The results show that the solution proposed by the authors improves the training efficiency and accuracy with a rate that varies between 95%–100% and reduces the training time by 26.2%.

The proposed IDS solution at the fog level has the advantage of being close to the IoT devices and therefore offers a rapid response, decentralization and preserves data privacy. However, the fog level faces an increase in the amount of data arriving at the fog level, which requires a lightweight solution. For this purpose, (Hameed et al. 2022) in [95] proposed to use an incremental ensemble learning method called Weighted Hoeffding Tree Ensemble system consisting of an incremental learning classifier for the industrial IoMT. Tests on NSL-KDD [91] and ToN-IoT [93] datasets and comparison with single incremental classifiers and Bagging Hoeffding Tree ensemble algorithms show that the proposed solution is lightweight and presents a trad-off between accuracy and overhead (CPU, memory and time) and outperforms the results of previous studies.

Other works have proposed SDN as an architecture for ML-based IDS within IoMT systems. Among them is the work led by (Khan and Akhunzada, 2021) in [20], which proposed a hybrid model based on DL for malware detection in IoMT deployed at the SDN plane application level. The system proposed by the authors consists of feature extraction using CNN, and then LSTM is used to classify the data as malware. The authors used the current state-of-the-art IoT malware publicly available dataset to evaluate their model. In addition, they compared their model with the constructed hybrid DL-driven. After performing various tests, the authors found that the proposed model outperformed the other methods regarding detection accuracy and speed efficiency.

In another study, (Wahab et al. 2022) in [96] proposed to use IDS based on ML to secure the IoMT architecture based on SDN against cyber threats. For this purpose, the authors propose using a hybrid model combining the LSTM and GRU deployed at the SDN control plane. The tests were performed on the CICDDoS2019 dataset [97], which was subjected to a preprocessing consisting of eliminating the NAN value, transforming the non-numeric values into numeric values, applying the one-hot encoding to output label, and then using MinMaxScaler for data normalization. They compared the results with other classifiers: cu-GRU and DNN and cu-BLSTM, as well as other previous studies. The results show their solution's efficiency compared to other models and previous studies in terms of accuracy, precision, F1-score and execution time.

The various IDS solutions proposed to improve the security of the IoMT network do not include measures to protect patient privacy. In this perspective, the research realized by (Schneble and Thamilarasu, 2019) in [98] proposed to use an IDS based on ML and federated learning to secure medical cyber-physical systems composed of sensors, mobile devices, and servers. The distributed and scalable nature of this system makes it more effective in protecting patient data privacy. The proposed IDS system follows a process where mobile devices first register with the server and are assigned to a cluster based on their health history. This cluster is associated with a federated model stored on the server. Each mobile device downloads the federated model, trains it, and updates it using patient data. The server then selects some or all of the mobile devices that compose the cluster and asks them to send their updated model. The server then calculates the average weights and biases of the received models to update its federated model, which mobile devices can download. This process continues until the model converges. Mobile devices can be in two modes: testing and learning. In learning mode, the mobile device can predict and send its updated model to the server. In the testing mode, the mobile device can only predict the new data and does not send the model to the server, saving communication costs. The proposed system allows the detection of anomalies, such as a value of an attribute that exceeds its usual value range or has an unexpected correlation with other attributes. In these cases, an alert is generated on mobile devices, allowing the nursing staff to react. The system was tested using the MIMIC dataset from Physionet [99], with the addition of simulated attacks such as DoS, data modification, and injection. The performance metrics used to evaluate the system were detection accuracy, FPR, recall, F1-score, training time, and communication overhead. The tests produced high detection rates and low false positives, with training times equivalent to or better than using a single ML. Additionally, increasing the number of patients does not affect the training time, which improved the accuracy and decreased the FPR by obtaining more data.

In another study made by (Singh et al. 2022) in [100], the author proposed a solution for intrusion detection at the IoMT networks level using Hierarchical Federated Learning (HFL) based on hierarchical long-term memory. Their solution is deployed on the distributed dew servers of the IoMT framework, with a backend supported by cloud computing at the edge layer. The proposed HFL solution aggregates models from different entities that compose the healthcare institution at the dew-servers level to obtain local models. These local models are then aggregated at the cloud computing level to obtain the global model, which is redistributed to the different dew servers participating in the learning process. This iterative process is repeated until the global model achieves a high accuracy. The authors evaluated their solution on TON-IoT [93] and NSL-KDD [91] datasets. They preprocess the datasets by removing unnecessary features, converting non-numeric values to numeric, and applying one-hot encoding to categorical values before normalizing the data to ensure they are represented in the same range. Finally, they applied PCA for dimensionality reduction. The results showed high accuracy, precision, recall, and f-score compared to Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), LSTM, and the previous study, with minimized computation costs.

The previous ML models lack interpretability and do not explain how they detect attacks, making them black-box models. However, (Khan et al. 2022) presented a solution to this issue in their study [101]. They utilized Simple Recurrent Units with skip connections to avoid the vanishing gradient problem for detecting network attacks in the IoMT, which was deployed at the gateway and router levels. To increase trust in their model, the authors employed Explainable AI (XAI) design using the Local Interpretable Model-Agnostic Explanations model to interpret and explain how the model classifies the data. The evaluation was performed on the ToN-IoT [93] dataset, which underwent preprocessing such as labeling categorical data, normalizing data to the same scale, and applying PCA for dimensionality reduction. The results indicate that the proposed solution by the authors is more efficient than two RNN variants: LSTM and GRU, in terms of Accuracy, Precision, Recall, and F-measure. Additionally, the proposed solution has a reduced computation cost compared to previous studies. Furthermore, XAI revealed that the basic category of IoT device features significantly impacts data classification.

The datasets used to evaluate the ML models in the above solutions consist of either network or medical data. The research performed by (Hady et al. 2020) in [102], proposed an IDS for healthcare that uses medical and network data. For this purpose, the authors developed an architecture that allows the creation of a dataset containing medical and network data and simulated MITM attacks to perform two types of attacks: spoofing and data alteration. The generated dataset [103] is used to test and evaluate different ML methods: SVM, KNN, RF, and ANN, with the following metrics accuracy, AUC, and time of execution for training and testing. After performing the different tests, the authors found that their system, which combines medical and network data increased the effectiveness of ML methods by 7 to 25% for the detection of threats in health monitoring systems in real time.

A literature review reveals that current proposals for using IDS based on ML in the IoMT environment have mainly explored centralized architecture solutions [20,80,82–87,96,101,102]. However, some researchers have also investigated distributed solutions [89,90]. Incorporating IDS and blockchain technology to achieve a decentralized architecture in the IoMT setting presents a promising direction for future research. Since it can bring numerous benefits to the IoMT environment, for example, it can enhance security by removing the risk of a single point of failure, making it difficult for malicious actors to alter data. The immutability of blockchain technology also ensures that data is recorded permanently, providing a trustworthy record of transactions. Decentralization can also improve traceability and reduce dependency on intermediaries, leading to more efficient and transparent processes. However, several challenges are also associated with using blockchain technology in the IoMT environment. Scalability remains a significant concern, as current processing speed and storage capacity limitations may not be suitable for large-scale applications. Additionally, the energy consumption associated with proof-of-work consensus algorithms can negatively impact the environment. Finally, the lack of standardization across different blockchain platforms can limit interoperability between them.

The future solution must prioritize protecting patient privacy, provide interpretable and explainable ML models, and apply appropriate learning and testing processes using a custom-designed dataset in an IoMT environment. Adherence to these requirements will ensure the development of a secure, transparent, and trustworthy IDS solution for the IoMT setting, which is critical in today's increasingly connected healthcare ecosystem.

8.3. ML for storage level security

Medical data received from sensors are centralized in a medical server, which the medical staff can access for analysis. These stored data are of two types: the EMR and the EHR. EMR stores a patient's medical and treatment history in a single place and makes it accessible at a single hospital. While EHR focuses on the patient's general health, it can store and transmit the patient's health data, such as patient history, medication, test results, and demographics [112,113]. It is necessary to secure access to these data to preserve patients' privacy, protect the confidentiality of medical data, and guarantee their availability and integrity to make an accurate diagnosis.

In this perspective, (Boxwala et al. 2011) in [104] proposed to use statistics and ML to identify suspicious access in EHR access logs. The authors used Logistic Regression (LR) and SVM to classify new access as suspicious with ranking. The high-scoring event is investigated first by the privacy officers. To create the model based on LR and SVM, the authors used the privacy agent to label the selected events as suspicious or appropriate using an iterative refinement process. Then they trained the model using 10-fold cross-validation. The authors used sensitivity, AUC and compared their model with the rule-based technique to evaluate their model. After performing several tests, the authors obtained more than 0.90 of AUC and more than 0.75 of sensitivity. They find that using a method based on statistics and ML to detect suspicious access in EHR is possible and is more effective than a rule-based technique. For the same purpose, a different approach is proposed by (Menon et al. 2014) in [105] for detecting privacy violations resulting from inappropriate access to EHR. The authors use an approach inspired by collaborative filtering for inappropriate access detection, where the objective is to predict a label for a pair of entities interactions. Their solution incorporates explicit and latent features for staff and patients, allowing for the generation of a fingerprint customizer for users based on previous access history. To evaluate the model, the authors used two datasets named "hospital" and "amazon" [106] using the following metrics: RMSE, the area under curves, and precision–recall curves, then they compared the results obtained with three ML algorithms: linear regression, LR, and SVM. After performing the different tests, the authors improved the performance considerably over the other approaches and detected inappropriate access.

Furthermore, the work performed by (Malin and Bradley, 2014) in [107] proposed an unsupervised learning model for insider threat detection in a collaborative environment using access logs called a community-based anomaly detection system. The approach proposed by the authors is hybrid; they use singular value decomposition, a special case of PCA, to infer communities from relational networks of users, and then they use KNN to create a set of nearest neighbors. The created model detects anomalous users by identifying users who have diverged from typical communication behaviors. To evaluate their model, the authors used two datasets: a six-month collection of access logs from an actual EMR and another dataset that reports the editorial board composition for a set of journals over five years. After running the different tests, the results showed that their model could detect the simulated user with high accuracy, outperforming other anomaly detection models.

Another work carried out by (Marwan et al., 2018) in [108], presented a new approach to secure image data processing in the cloud environment based on ML. Their method consists of segmenting the image into four distinct parts depending on pixel intensity level using Fuzzy C-Means Clustering (FCM) and SVM. The FCM is utilized for extracting color features at the pixel level. These features are fed to the SVM to be classified into different regions, allowing storage of the image in the cloud in a segmented format. The authors have also proposed a 3-layer architecture instead of the traditional 2-layer architecture by introducing a CloudSec module that allows the encryption of data in transit using the HTTPS/Secure Socket Layer. The CloudSec module also allows for restricting access to the data and detecting the misuse of cloud resources by using an access control mechanism.

In a work performed by (Sicuranza and Paragliola, 2020) in [109], they proposed a hybrid IDS for cyber-attack detection against EHR. The proposed system uses agents deployed within the monitored IT infrastructure. They are responsible for collecting, normalizing, and performing security analysis on the logs collected from the local level. Then these agents generate events that are sent to the IDS for analysis. The IDS comprises a misuse detection module and an anomaly detection module. The misuse detection module is rule-based, effectively detecting the well-known attack signature. The anomaly detection module allows the detection of zero-day attacks. Anomaly detection uses three classifiers: DT, Neural Network, and k-means. The results of these classifiers are sent to the voting system to improve the accuracy of each classifier. In addition, an expert system module is designed to resolve any potential conflict between the presence/absence of attacks as determined by the abuse detection module and the anomaly detection voting system. A dataset was generated by monitoring the Italian EHR system to test the proposed model. Three separate attacks on the EHR systems were used to test the misuse and anomaly detection modules. The results demonstrate the efficiency of the proposed solution.

In addition, in a study reported by (McGlade and Scott-Hayward, 2019) in [59], they proposed a framework for detecting privacy and availability issues in EMR systems. The framework is based on ML and uses the SVM to detect privacy-related incidents and the Exponential Moving Average (EMA) to detect anomalies in message flow that may cause a denial of service. To test the framework, the authors have used synthetic data generated by the Synthea tool [110], a synthetic patient population simulator. They have tested three ML algorithms on the dataset, namely SVM, KNN, and multinomial NB, to detect anomaly-related to the confidentiality of the EMR system and EMA for the detection of anomaly-related to the availability of the EMR system. After performing different tests, the authors found that SVM exhibits the best performance regarding accuracy and recall than the two other methods. They also find that EMA can successfully detect message surges, leading to a denial of services.

EHRs and EMRs are critical systems for storing sensitive patient information. Ensuring this information's confidentiality, integrity, and availability are of utmost importance. The literature review reveals that most studies have concentrated on detecting unauthorized access to EHRs [104,105,107]. Only one study has focused on the confidentiality and availability of EMRs [59]. However, there is a need for further research in ML to ensure the integrity of both EHRs and EMRs. Exploration in this area holds great promise and could be a valuable direction for future investigation.

9. Challenges and limitations

The exploration of the different solutions proposed in the literature using IDS based on ML for IoMT led us to identify the limitations and challenges of this approach at the different layers that compose IoMT as follows:

9.1. Data collection level security

The deployment of ML models in medical equipment presents a challenge due to its various limitations. Three methods of deployment have been proposed, which include deployment of the ML model on medical equipment [7], deployment on a third-party device [76], or deployment on a chip followed by integration into the medical equipment [6].

The deployment of ML models on resource-constrained medical devices can have consequences such as shortened battery life, which may require surgery for battery replacement and pose a risk to the patient. Deployment on third-party devices involves communication between the devices and medical equipment, which requires a modification at the software level of the medical device. However, medical device manufacturers do not permit such changes, and third-party devices must also be protected from potential attacks. Deployment on a chip and integration into the medical device involves software and hardware modifications. Lightweight ML models that satisfy the limitations of sensors may be a promising area of research in addressing the challenge of deploying ML models on resource-limited medical devices. Additionally, the ML model must be secured to prevent data manipulation during the learning or testing phase that can compromise the results [15,114].

Detecting anomalies in medical data can arise from various factors, including poor communication quality due to interference or malfunctioning sensors, medical emergencies that result in severe illness, and security attacks carried out by malicious entities. It is crucial to differentiate between these various sources of anomalies, as prompt identification and treatment are necessary for emergencies.

The limited availability of public datasets generated explicitly for security purposes and containing medical data presents a challenge for researchers. Some have resorted to using existing medical datasets, such as PHYSIONET [99], and modified specific values with the help of healthcare professionals to simulate attacks, leading to questions about the validity of their findings when applied in real-world scenarios. Other studies have used real medical equipment volunteers wear to collect health data. However, these results may need to be more representative as the volunteers may not have any underlying health conditions. Using simulators, such as CASTILIA [81], to generate medical data and attacks can also result in unforeseen difficulties during practical implementation. The acquisition of a high-quality, diverse, and representative dataset containing medical data collected from individuals with and without illnesses, and generated explicitly for security purposes, remains a significant challenge.

Another limitation is that the various IDSs proposed in the literature focus on a restricted number of medical devices to generate a medical dataset. However, when patients utilize multiple medical devices, it becomes imperative to have integrated solutions to detect intrusions from these different medical devices. The challenge lies in designing an IDS solution that can accommodate all connected medical devices, as each has specific data collection and communication methods.

Some solutions rely on the patient's ability to determine the occurrence of an attack. However, this approach needs to consider potential limitations such as age, incapacity, or emergency circumstances where the patient may be unable to make such a decision. Establishing effective protocols for communication and decision-making in the event of anomalous behavior detection poses a challenge.

The study [7] has demonstrated that rule-based solutions for anomaly detection in medical data may achieve better results than ML-based anomaly detection systems because some medical attributes contain a range of values that, if exceeded, can be easily detected by implementing clear and defined rules. On the other hand, ML-based anomaly detection can detect anomalies by analyzing correlations between multiple medical attributes. This highlights the need for a comprehensive evaluation of rule-based and ML-based anomaly detection methods to determine their strengths and limitations in detecting anomalies in medical data. Further research should consider this aspect to improve the accuracy and reliability of anomaly detection in medical data.

The generalizability of a ML model constructed from a specific patient's medical dataset is limited, as what may be considered abnormal medical values for one patient may be considered normal for another patient [78]. Ensuring the accuracy of the ML models when applied to different patient populations with varying medical conditions and characteristics remains a challenge.

9.2. Transmission level security

In developing a Network-based IDS for the IoMT, the unique characteristics of the IoMT system must be considered, such as its distributed, mobile, dynamic nature and heterogeneous communication constraints.

When designing an ML-based Network-based IDS for IoMT security, it is essential to consider the evaluation metrics for the ML model, especially when the dataset is imbalanced. The use of metrics that give higher importance to the minority classes and accurately reflect the ability of the ML model to detect attacks is imperative, as the IDS is responsible for protecting the essential information system against security threats. However, implementing an ML model with an imbalanced dataset presents challenges such as biased results, overfitting, and difficulties in evaluating performance using traditional metrics. When developing the ML model, it is necessary to handle the imbalanced nature of the dataset carefully.

A real-time detection system in the IoMT using ML is crucial for prompt and adequate decision-making in the event of security threats. However, implementing such a system presents several technical challenges, including the efficient and accurate processing of a large volume of data generated by the IoMT system, ensuring a high level of accuracy in the ML model's detection of attacks, and low latency in processing and prediction. The system must also be scalable and have the hardware capabilities to support the ML model and handle large amounts of data in real-time.

The use of black-box models in applications like healthcare is limited due to regulations, such as the General Data Protection Regulation, which prohibits automated decisions in critical sectors. Despite their widespread use in other applications, black-box models present significant challenges, including a lack of transparency, making it difficult to understand how the model arrived at its predictions and identify potential biases. Explaining the model's decisions is also a significant challenge, especially in applications where justifiable decisions are indispensable. Black-box models can also be vulnerable to adversarial attacks and have limited interpretability, making it challenging to debug and fine-tune the model to improve its performance. Explainable artificial intelligence (XAI) has become increasingly popular in addressing these challenges. XAI allows for creation of models that can be interpreted, understood, and transparent, and the reasoning behind their decisions can be easily explained. By using XAI, the limitations of black-box models can be overcome, promoting responsible AI development and deployment, improving trust in the model, and increasing accountability.

Implementing a real-time detection system for the IoMT using ML requires using a dataset that accurately represents the IoMT system. The utilization of datasets not designed explicitly for the IoMT system may result in a limited representation of the system and its potential attack scenarios, hindering the ability of the ML model to detect attacks effectively in real-world situations. Obtaining a comprehensive dataset encompassing the diverse range of attacks and communication protocols within the IoMT system remains challenging.

The IoMT system requires effective IDS to ensure the safety and security of medical data. Various architectures have been proposed to support these requirements, including centralized, distributed, fog–cloud and federated solutions. While centralized solutions, such as SDN, offer a centralized control point, they also pose challenges, such as the risk of a single point of failure, increased latency, and privacy concerns. Distributed solutions present a unique approach, but the practical deployment of these solutions in real-world situations still needs to be improved [89]. The use of a fog–cloud architecture presents a promising approach. However, the challenge of submerged data flow must be addressed in this architecture. On the other hand, federated solutions must consider the risk of adversarial attacks during the model-sharing process.

9.3. Storage level security

The concept of IDS in the medical server encounters several challenges and limitations. The data structure and format utilized for training the ML model within the medical server are distinct from other servers, making it challenging to extend the model's applicability to other medical institutions.

A large amount of unlabeled data for supervised learning processes presents a significant obstacle for machine learning practitioners. The lack of labeled data makes it challenging to train the model effectively. The manual data labeling process, which often requires an interview with the patient to ensure correct labeling, can be both time-consuming and resource-intensive. Notably, this manual labeling process and the need for patient interaction result in intrusion detection at the medical server level is not fully automated. Therefore, unsupervised or semi-supervised ML methods should be further investigated at this level with particular attention to reducing false positives.

The possibility of a malicious actor altering a single feature value within an EHR or EMR for a single patient poses a challenge for ML models trained on a large amount of medical data [59]. These models typically rely on identifying patterns within the data and are designed to detect larger deviations from these patterns, making it difficult for the models to detect a single, subtle change in a feature value. Such an attack could have significant consequences, particularly in a medical context where patient data integrity is vital. Measures must be taken to address this challenge, such as utilizing more sophisticated ML models that can detect single-value changes or augmenting the training data with a diverse range of feature changes to enhance the model's ability to identify such modifications.

The difficulty in obtaining public medical data in the form of EMRs or EHRs results from such data's sensitivity and confidentiality. The privacy and security of patients and medical information are of utmost importance. Therefore, the release of such data is often heavily regulated and subject to strict privacy laws and regulations. This presents a significant challenge for those seeking to use the data for research or analysis purposes, as access to a large and diverse sample of medical data is critical for developing and training ML models.

10. Conclusion

A comprehensive survey on how to use an IDS-based ML to secure the IoMT is conducted. For this purpose, the generic architecture of IoMT, which is divided into three layers (data acquisition layer, personal server layer, and medical server layer) is presented. Then the requirements and possible threats that can affect the security of IoMT are provided. Next, the ML-based solutions for IoMT security are reviewed and categorized into three levels: data collection level, transmission level, and storage level, indicating the advantages, disadvantages, and datasets used. Finally, the challenges and limitations of using ML in these categories are discussed. This survey aims to highlight ML ability to bring security to complex infrastructures such as IoMT and the capacity to comply with the particular constraints of IoMT.

The main limitations of this survey are as follows: (i) The literature survey that is the subject of this study may have unintentionally left out the most current non-scientific developments or academic works that were not yet published at the time of the investigation. (ii) Although every attempt has been made to provide background, this research includes several concepts that may need to be referred to additional sources for complete comprehension. (iii) It is noteworthy that our recommendations are inherently subjective. We intend to encourage additional research and discussion to address these limitations.

CRediT authorship contribution statement

Ayoub Si-Ahmed: Methodology, Investigation, Writing – original draft. **Mohammed Ali Al-Garadi:** Methodology, Writing – review & editing, Supervision, Project administration. **Narhimene Boustia:** Resources, Writing – review & editing, Supervision, Project administration.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgments

This study was financed by the laboratory LRDSI of the university Blida 1, Algeria.

References

[1] P. Suresh, J.V. Daniel, V. Parthasarathy, R. Aswathy, A state of the art review on the Internet of Things (IoT) history, technology and fields of deployment, in: 2014 International Conference on Science Engineering and Management Research, ICSEMR, IEEE, 2014, pp. 1–8.

[2] Internet of things, 2022, URL: https://en.wikipedia.org/wiki/Internet_of_things, (Accessed Feb. 04, 2022).

[3] Global IoT market to grow to 24.1 billion devices in 2030, generating $1.5 trillion annual revenue, 2022, URL: https://transformainsights.com/news/iot-market-24-billion-usd15-trillion-revenue-2030, (Accessed Feb. 04, 2022).

[4] Embracing healthcare 4.0, 2022, URL: https://www.siemens-healthineers.com/insights/news/embracing-healthcare-4-0.html, (Accessed Feb. 04, 2022).

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

[6] H. Rathore, A. Al-Ali, A. Mohamed, X. Du, M. Guizani, DLRT: Deep learning approach for reliable diabetic treatment, in: GLOBECOM 2017-2017 IEEE Global Communications Conference, IEEE, 2017, pp. 1–6.

[7] M. Kintzlinger, A. Cohen, N. Nissim, M. Rav-Acha, V. Khalameizer, Y. Elovici, Y. Shahar, A. Katz, CardiWall: a trusted firewall for the detection of malicious clinical programming of cardiac implantable electronic devices, IEEE Access 8 (2020) 48123–48140.

[8] N. McLaughlin, J. Martinez del Rincon, B. Kang, S. Yerima, P. Miller, S. Sezer, Y. Safaei, E. Trickel, Z. Zhao, A. Doupé, et al., Deep android malware detection, in: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, 2017, pp. 301–308.

[9] H. Rathore, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, A review of security challenges, attacks and resolutions for wireless medical devices, in: 2017 13th International Wireless Communications and Mobile Computing Conference, IWCMC, IEEE, 2017, pp. 1495–1501.

[10] M. Hussain, A. Mehmood, S. Khan, M.A. Khan, Z. Iqbal, Authentication techniques and methodologies used in wireless body area networks, J. Syst. Archit. 101 (2019) 101655.

[11] M. Wazid, A.K. Das, J.J. Rodrigues, S. Shetty, Y. Park, IoMT malware detection approaches: analysis and research challenges, IEEE Access 7 (2019) 182459–182476.

[12] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, A survey on security and privacy issues in modern healthcare systems: Attacks and defenses, ACM Trans. Comput. Healthc. 2 (3) (2021) 1–44.

[13] B. Narwal, A.K. Mohapatra, A survey on security and authentication in wireless body area networks, J. Syst. Archit. 113 (2021) 101883.

[14] A. Saxena, S. Mittal, Internet of Medical Things (IoMT) security and privacy: A survey of recent advances and enabling technologies, in: Proceedings of the 2022 Fourteenth International Conference on Contemporary Computing, 2022, pp. 550–559.

[15] S.S. Hameed, W.H. Hassan, L.A. Latiff, F. Ghabban, A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches, PeerJ Comput. Sci. 7 (2021) e414.

[16] A.M. Rahmani, T.N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang, P. Liljeberg, Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach, Future Gener. Comput. Syst. 78 (2018) 641–658.

[17] M. Irfan, N. Ahmad, Internet of medical things: Architectural model, motivational factors and impediments, in: 2018 15th Learning and Technology Conference (L&T), IEEE, 2018, pp. 6–13.

[18] R. Khan, S.U. Khan, R. Zaheer, S. Khan, Future internet: the internet of things architecture, possible applications and key challenges, in: 2012 10th International Conference on Frontiers of Information Technology, IEEE, 2012, pp. 257–260.

[19] P. Kumar, G.P. Gupta, R. Tripathi, An ensemble learning and fog-cloud architecture-driven cyber-attack detection framework for IoMT networks, Comput. Commun. 166 (2021) 110–124.

[20] S. Khan, A. Akhunzada, A hybrid DL-driven intelligent SDN-enabled malware detection framework for Internet of Medical Things (IoMT), Comput. Commun. 170 (2021) 209–216.

[21] S. Chakraborty, S. Aich, H.-C. Kim, A secure healthcare system design framework using blockchain technology, in: 2019 21st International Conference on Advanced Communication Technology, ICACT, IEEE, 2019, pp. 260–264.

[22] S.R. Moosavi, T.N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen, SEA: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459.

[23] K. Zhang, K. Yang, X. Liang, Z. Su, X. Shen, H.H. Luo, Security and privacy for mobile healthcare networks: from a quality of protection perspective, IEEE Wirel. Commun. 22 (4) (2015) 104–112.

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

[25] K. Arya, R. Gore, Data security for WBAN in e-health IoT applications, in: Intelligent Data Security Solutions for e-Health Applications, Elsevier, 2020, pp. 205–218.

[26] J.J. Hathaliya, S. Tanwar, An exhaustive survey on security and privacy issues in healthcare 4.0, Comput. Commun. 153 (2020) 311–335.

[27] E.A. Alkeem, D. Shehada, C.Y. Yeun, M.J. Zemerly, J. Hu, New secure healthcare system using cloud of things, Cluster Comput. 20 (3) (2017) 2211–2229.

[28] M. Roy, C. Chowdhury, N. Aslam, Security and privacy issues in wireless sensor and body area networks, in: Handbook of Computer Networks and Cyber Security, Springer, 2020, pp. 173–200.

[29] S. Pirbhulal, O.W. Samuel, W. Wu, A.K. Sangaiah, G. Li, A joint resource-aware and medical data security framework for wearable healthcare systems, Future Gener. Comput. Syst. 95 (2019) 382–391.

[30] M. Kompara, M. Hölbl, Survey on security in intra-body area network communication, Ad Hoc Netw. 70 (2018) 23–43.

[31] D.J. Malan, T. Fulford-Jones, M. Welsh, S. Moulton, Codeblue: An ad hoc sensor network infrastructure for emergency medical care, in: International Workshop on Wearable and Implantable Body Sensor Networks, 2004.

[32] J. Ko, J.H. Lim, Y. Chen, R. Musvaloiu-E, A. Terzis, G.M. Masson, T. Gao, W. Destler, L. Selavo, R.P. Dutton, MEDiSN: Medical emergency detection in sensor networks, ACM Trans. Embed. Comput. Syst. (TECS) 10 (1) (2010) 1–29.

[33] M. Segovia, E. Grampín, J. Baliosian, Analysis of the applicability of wireless sensor networks attacks to body area networks, in: Proceedings of the 8th International Conference on Body Area Networks, 2013, pp. 509–512.

[34] M. Kintzlinger, N. Nissim, Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems, J. Biomed. Inform. 95 (2019) 103233.

[35] Y.A. Bangash, Y.E. Al-Salhi, et al., Security issues and challenges in wireless sensor networks: A survey, IAENG Int. J. Comput. Sci. 44 (2) (2017).

[36] X. Hei, X. Du, S. Lin, I. Lee, O. Sokolsky, Patient infusion pattern based access control schemes for wireless insulin pump system, IEEE Trans. Parallel Distrib. Syst. 26 (11) (2014) 3108–3121.

[37] R. Doss, S. Piramuthu, Z. Wei, Future Network Systems and Security: First International Conference, FNSS 2015, Paris, France, June 11-13, 2015, Proceedings, Vol. 523, Springer, 2015.

[38] A. Rani, S. Kumar, A survey of security in wireless sensor networks, in: 2017 3rd International Conference on Computational Intelligence & Communication Technology, CICT, IEEE, 2017, pp. 1–5.

[39] G. Xu, Q. Wu, M. Daneshmand, Y. Liu, M. Wang, A data privacy protective mechanism for wireless body area networks, Wirel. Commun. Mob. Comput. 16 (13) (2016) 1746–1758.

[40] S. Sanei, D. Jarchi, A.G. Constantinides, Quality of Service, Security, and Privacy for Wearable Sensor Data, in: Body Sensor Networking, Design and Algorithms, 2020, pp. 325–343.

[41] K. Habib, A. Torjusen, W. Leister, Security analysis of a patient monitoring system for the Internet of Things in eHealth, in: The Seventh International Conference on EHealth, Telemedicine, and Social Medicine, ETELEMED, vol. 335, 2015.

[42] R. Maheswar, G. Kanagachidambaresan, R. Jayaparvathy, S.M. Thampi, Body Area Network Challenges and Solutions, Springer, 2019.

[43] P. Kumar, H.-J. Lee, Security issues in healthcare applications using wireless medical sensor networks: A survey, Sensors 12 (1) (2012) 55–91.

[44] S. Pathania, N. Bilandi, Security issues in wireless body area network, Int. J. Comput. Sci. Mobile Comput. 3 (4) (2014) 1171–1178.

[45] P. Stavroulakis, M. Stamp, Handbook of Information and Communication Security, Springer Science & Business Media, 2010.

[46] M.A. Hamid, M. Rashid, C.S. Hong, Routing security in sensor network: Hello flood attack and defense, IEEE ICNEWS 2 (2006) 2–4.

[47] C. Tumrongwittayapak, R. Varakulsiripunth, Detecting sinkhole attack and selective forwarding attack in wireless sensor networks, in: 2009 7th International Conference on Information, Communications and Signal Processing, ICICS, IEEE, 2009, pp. 1–5.

[48] M. Mana, M. Feham, B.A. Bensaber, SEKEBAN (Secure and efficient key exchange for wireless body area network), Int. J. Adv. Sci. Technol. (2009) Citeseer.

[49] A.V. Stavros, Advances in Communications and Media Research, Vol. 2, Nova Publishers, 2002.

[50] K. Siva Bharathi, R. Venkateswari, Security challenges and solutions for wireless body area networks, in: Computing, Communication and Signal Processing, Springer, 2019, pp. 275–283.

[51] B.B. Gupta, G.M. Perez, D.P. Agrawal, D. Gupta, Handbook of Computer Networks and Cyber Security, Vol. 10, Springer, 2020, 978–3.

[52] M. Masdari, S. Ahmadzadeh, Comprehensive analysis of the authentication methods in wireless body area networks, Secur. Commun. Netw. 9 (17) (2016) 4777–4803.

[53] P. Niksaz, M. Branch, Wireless body area networks: attacks and countermeasures, Int. J. Sci. Eng. Res. 6 (9) (2015) 556–568.

[54] J. Newsome, E. Shi, D. Song, A. Perrig, The sybil attack in sensor networks: analysis & defenses, in: Third International Symposium on Information Processing in Sensor Networks, 2004. IPSN 2004, IEEE, 2004, pp. 259–268.

[55] R. Ramli, N. Zakaria, P. Sumari, Privacy issues in pervasive healthcare monitoring system: A review, World Acad. Sci. Eng. Technol. 72 (12) (2010) 741–747.

[56] J. Partala, N. Keräneny, M. Särestöniemi, M. Hämäläinen, J. Iinatti, T. Jämsä, J. Reponen, T. Seppänen, Security threats against the transmission chain of a medical health monitoring system, in: 2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013), IEEE, 2013, pp. 243–248.

[57] D.W. Curtis, E.J. Pino, J.M. Bailey, E.I. Shih, J. Waterman, S.A. Vinterbo, T.O. Stair, J.V. Guttag, R.A. Greenes, L. Ohno-Machado, SMART—an integrated wireless system for monitoring unattended patients, J. Am. Med. Inform. Assoc. 15 (1) (2008) 44–53.

[58] A. Redondi, M. Tagliasacchi, M. Cesana, L. Borsani, P. Tarrío, F. Salice, LAURA—LocAlization and ubiquitous monitoring of patients for health care support, in: 2010 IEEE 21st International Symposium on Personal, Indoor and Mobile Radio Communications Workshops, IEEE, 2010, pp. 218–222.

[59] D. McGlade, S. Scott-Hayward, ML-based cyber incident detection for Electronic Medical Record (EMR) systems, Smart Health 12 (2019) 3–23.

[60] F. Alsubaei, A. Abuhussein, 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), IEEE, 2017, pp. 112–120.

[61] V. Hassija, V. Chamola, B.C. Bajpai, S. Zeadally, et al., Security issues in implantable medical devices: Fact or fiction? Sustainable Cities Soc. 66 (2021) 102552.

[62] D. Ford, Docs shielded Cheney defibrillator from hacks - CNN, 2013, URL: https://edition.cnn.com/2013/10/20/us/dick-cheney-gupta-interview/index.html, (Accessed Oct. 07, 2021).

[63] R. Bace, P. Mell, NIST Special Publication on Intrusion Detection Systems, Technical Report, Booz-allen and Hamilton Inc, MCLEAN VA, 2001.

[64] A.L. Samuel, Some studies in machine learning using the game of checkers, IBM J. Res. Dev. 44 (1.2) (2000) 206–226.

[65] A. Géron, Hands-On Machine Learning with Scikit-Learn and TensorFlow: Concepts, Tools, and Techniques to Build Intelligent Systems, 2017.

[66] J. Franklin, The elements of statistical learning: data mining, inference and prediction, Math. Intelligencer 27 (2) (2005) 83–85.

[67] N.N. Pise, P. Kulkarni, A survey of semi-supervised learning methods, in: 2008 International Conference on Computational Intelligence and Security, Vol. 2, IEEE, 2008, pp. 30–34.

[68] Y. LeCun, Y. Bengio, G. Hinton, Deep learning, Nature 521 (7553) (2015) 436–444.

[69] F.A. Khan, N.A.H. Haldar, A. Ali, M. Iftikhar, T.A. Zia, A.Y. Zomaya, A continuous change detection mechanism to identify anomalies in ECG signals for WBAN-based healthcare environments, IEEE Access 5 (2017) 13531–13544.

[70] T.S. Lugovaya, ECG-ID database v1.0.0, 2005, URL: https://www.physionet.org/content/ecgiddb/1.0.0/, (Accessed Oct. 07, 2021).

[71] U. Ahmad, H. Song, A. Bilal, S. Saleem, A. Ullah, Securing insulin pump system using deep learning and gesture recognition, in: 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), IEEE, 2018, pp. 1716–1719.

[72] V. Sigillito, Pima Indians diabetes database, 1990, URL: https://www.openml.org/d/37, (Accessed Oct. 07, 2021).

[73] M. Shobana, et al., Towards securing wireless insulin pump system using unsupervised deep learning technique, Iran J. Comput. Sci. (2022).

[74] Diabetes data set, UCI machine learning repository: Diabetes data set, 2022, URL: https://archive.ics.uci.edu/ml/datasets/diabetes, (Accessed Nov. 27, 2022).

[75] A. Goldberger, A.L. LastName, L. Glass, J. Hausdorff, P. Ivanov, R. Mark, J. Mietus, G. Moody, C. Peng, H. Stanley, Effect of deep brain stimulation on parkinsonian tremor v1.0.0, 2000, URL: https://physionet.org/content/tremordb/1.0.0/, (Accessed Oct. 07, 2021).

[76] X. Hei, X. Du, J. Wu, F. Hu, Defending resource depletion attacks on implantable medical devices, in: 2010 IEEE Global Telecommunications Conference GLOBECOM 2010, IEEE, 2010, pp. 1–5.

[77] A.I. Newaz, A.K. Sikder, M.A. Rahman, A.S. Uluagac, Healthguard: A machine learning-based security framework for smart healthcare systems, in: 2019 Sixth International Conference on Social Networks Analysis, Management and Security, SNAMS, IEEE, 2019, pp. 389–396.

[78] O. Salem, K. Alsubhi, A. Mehaoua, R. Boutaba, Markov models for anomaly detection in wireless body area networks for secure health monitoring, IEEE J. Sel. Areas Commun. 39 (2) (2020) 526–540.

[79] G.B. Moody, R.G. Mark, MIMIC Database v1.0.0, 1996, URL: https://www.physionet.org/content/mimicdb/1.0.0/, (Accessed Oct. 07, 2021).

[80] S. Gao, G. Thamilarasu, Machine-learning classifiers for security in connected medical devices, in: 2017 26th International Conference on Computer Communication and Networks, ICCCN, IEEE, 2017, pp. 1–5.

[81] Castalia: An OMNeT-based simulator for low-power wireless networks such as Wireless Sensor Networks and Body Area Networks, 2021, URL: https://github.com/boulis/Castalia, (Accessed Oct. 07, 2021).

[82] M.A. Al-Shaher, R.T. Hameed, N. Ţăpuş, Protect healthcare system based on intelligent techniques, in: 2017 4th International Conference on Control, Decision and Information Technologies (CoDIT), IEEE, 2017, pp. 0421–0426.

[83] D. He, Q. Qiao, Y. Gao, J. Zheng, S. Chan, J. Li, N. Guizani, Intrusion detection based on stacked autoencoder for connected healthcare systems, IEEE Netw. 33 (6) (2019) 64–69.

[84] A.I. Newaz, A.K. Sikder, L. Babun, A.S. Uluagac, Heka: A novel intrusion detection system for attacks to personal medical devices, in: 2020 IEEE Conference on Communications and Network Security, CNS, IEEE, 2020, pp. 1–9.

[85] S.P. RM, P.K.R. Maddikunta, M. Parimala, S. Koppu, T.R. Gadekallu, C.L. Chowdhary, M. Alazab, An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture, Comput. Commun. 160 (2020) 139–149.

[86] J.D. Lee, H.S. Cha, S. Rathore, J.H. Park, M-IDM: A multi-classification based intrusion detection model in healthcare IoT, Comput. Mater. Contin. 67 (2) (2021) 1537–1553.

[87] H. Salemi, H. Rostami, S. Talatian-Azad, M.R. Khosravi, LEAESN: Predicting DDoS attack in healthcare systems based on Lyapunov exponent analysis and echo state neural networks, Multimedia Tools Appl. (2021) 1–22.

[88] MIT Lincoln Laboratory, 1998 DARPA Intrusion Detection Evaluation Dataset | MIT Lincoln Laboratory, 1998, URL: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset, (Accessed Oct. 07, 2021).

[89] G. Thamilarasu, A. Odesile, A. Hoang, An intrusion detection system for internet of medical things, IEEE Access 8 (2020) 181560–181576.

[90] M. Begli, F. Derakhshan, H. Karimipour, A layered intrusion detection system for critical infrastructure using machine learning, in: 2019 IEEE 7th International Conference on Smart Energy Grid Engineering, SEGE, IEEE, 2019, pp. 120–124.

[91] M. Tavallaee, E. Bagheri, A. Ghorbani, Detailed analysis of the KDD CUP 99 data set, in: Submitted to Second IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA, 2009, URL: https://www.unb.ca/cic/datasets/nsl.html, (Accessed Oct. 07, 2021).

[92] I. Alrashdi, A. Alqazzaz, R. Alharthi, E. Aloufi, M.A. Zohdy, H. Ming, FBAD: Fog-based attack detection for IoT healthcare in smart cities, in: 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference, UEMCON, IEEE, 2019, pp. 0515–0522.

[93] N. Moustafa, TON_IoT Datasets for cybersecurity applications based artificial intelligence, 2019, URL: https://research.unsw.edu.au/projects/toniot-datasets, (Accessed Oct. 07, 2021).

[94] L. Gupta, T. Salman, A. Ghubaish, D. Unal, A.K. Al-Ali, R. Jain, Cybersecurity of multi-cloud healthcare systems: A hierarchical deep learning approach, Appl. Soft Comput. 118 (2022) 108439.

[95] S.S. Hameed, A. Selamat, L.A. Latiff, S.A. Razak, O. Krejcar, WHTE: Weighted hoeffding tree ensemble for network attack detection at Fog-IoMT, in: International Conference on Industrial, Engineering and Other Applications of Applied Intelligent Systems, Springer, 2022, pp. 485–496.

[96] F. Wahab, Y. Zhao, D. Javeed, M.H. Al-Adhaileh, S.A. Almaaytah, W. Khan, M.S. Saeed, R. Kumar Shah, An AI-driven hybrid framework for intrusion detection in IoT-enabled E-health, Comput. Intell. Neurosci. 2022 (2022).

[97] I. Sharafaldin, A.H. Lashkari, S. Hakak, A.A. Ghorbani, Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy, in: 2019 International Carnahan Conference on Security Technology, ICCST, IEEE, 2019, pp. 1–8.

[98] W. Schneble, G. Thamilarasu, Attack detection using federated learning in medical cyber-physical systems, in: Proceedings of the 28th International Conference on Computer Communications and Networks (ICCCN), Valencia, Spain, Vol. 29, 2019.

[99] A.E. Johnson, T.J. Pollard, L. Shen, L.-w.H. Lehman, M. Feng, M. Ghassemi, B. Moody, P. Szolovits, L. Anthony Celi, R.G. Mark, MIMIC-III, a freely accessible critical care database, Sci. Data 3 (1) (2016) 1–9, (Accessed Oct. 07, 2021).

[100] P. Singh, G.S. Gaba, A. Kaur, M. Hedabou, A. Gurtov, Dew-cloud-based hierarchical federated learning for intrusion detection in IoMT, IEEE J. Biomed. Health Inf. (2022).

[101] I.A. Khan, N. Moustafa, I. Razzak, M. Tanveer, D. Pi, Y. Pan, B.S. Ali, XSRU-IoMT: Explainable simple recurrent units for threat detection in Internet of Medical Things networks, Future Gener. Comput. Syst. 127 (2022) 181–193.

[102] A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, Intrusion detection system for healthcare systems using medical and network data: A comparison study, IEEE Access 8 (2020) 106576–106584.

[103] A.A. Hady, A. Ghubaish, T. Salman, D. Unal, R. Jain, WUSTL EHMS 2020 dataset for Internet of Medical Things (IoMT) cybersecurity research, 2019, URL: https://www.cse.wustl.edu/{~}jain/ehms/index.html, (Accessed Oct. 07, 2021).

[104] A.A. Boxwala, J. Kim, J.M. Grillo, L. Ohno-Machado, Using statistical and machine learning to help institutions detect suspicious access to electronic health records, J. Am. Med. Inform. Assoc. 18 (4) (2011) 498–505.

[105] A.K. Menon, X. Jiang, J. Kim, J. Vaidya, L. Ohno-Machado, Detecting inappropriate access to electronic health records using collaborative filtering, Mach. Learn. 95 (1) (2014) 87–101.

[106] Amazon access data competition, 2021, URL: https://sites.google.com/site/amazonaccessdatacompetition/, (Accessed Oct. 07, 2021).

[107] Y.C. Malin, Bradley, Detection of anomalous insiders in collaborative environments via relational analysis of access logs, Bone 23 (1) (2014) 1–7.

[108] M. Marwan, A. Kartit, H. Ouahmane, Security enhancement in healthcare cloud using machine learning, Procedia Comput. Sci. 127 (2018) 388–397.

[109] M. Sicuranza, G. Paragliola, Ensuring electronic health record cyber-security through an hybrid intrusion detection system, 2020.

[110] Synthetichealth, Synthetichealth/synthea: Synthetic patient population simulator, 2021, URL: https://github.com/synthetichealth/synthea, (Accessed Oct. 07, 2021).

[111] T. Yaqoob, H. Abbas, M. Atiquzzaman, Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3723–3768.

[112] P. Garrett, J. Seidman, EMR vs EHR – What is the difference? - Health IT buzz, 2011, URL: https://www.healthit.gov/buzz-blog/electronic-health-and-medical-records/emr-vs-ehr-difference, (Accessed Oct. 07, 2021).

[113] T. Cascio, Thorpe, electronic health record | Description, Implementation, & Issues | Britannica, 2021, URL: https://www.britannica.com/topic/electronic-health-record, (Accessed Oct. 07, 2021).

[114] A.I. Newaz, N.I. Haque, A.K. Sikder, M.A. Rahman, A.S. Uluagac, Adversarial Attacks to Machine Learning-Based Smart Healthcare Systems, in: 2020 IEEE Global Communications Conference, GLOBECOM 2020 - Proceedings, 2020.

Ayoub Si-Ahmed obtained his master's degree in Security of information systems in 2019 at the University of Saad Dahleb Blida, where he finished the major of his promotion. Currently, he is a doctoral student at the same university where he got the post after a competition where he was ranked first. He is part of a research project PRFU (Projets de Recherche Formation-Universitaire) named Security of social networks. He also worked as a consultant in computer security for three years at the PROXYLAN branch of a research center called CERIST. His research interests include ML/DL, IoT systems, and cybersecurity.

Mohammed Ali Al-Garadi achieved his PhD from the University of Malaya, Malaysia, in 2017, where he obtained many national and international awards. He has published in many peer-reviewed journals and conferences. He has served as a reviewer in many journals, including IEEE Communications Magazine, IEEE Transactions on Knowledge and Data Engineering, IEEE Access, Future Generation Computer Systems, Computers & Electrical Engineering, and Journal of Network and Computer Applications. His research focuses on big data analytics, IoT systems, cybersecurity, AI for health care, ML and NLP for medical data.

Narhimene Boustia received the Ph.D. degree in computer science from USTHB Algiers in 2011. She is Professor and searcher at Blida 1 university. Her research focuses on security of information system, access control and knowledge management.