International Journal of Sustainable Applied Science and Engineering (IJSASE)

Contents lists available at IJISASE
International Journal of Sustainable Applied Science and Engineering
journal homepage: IJISASE
Volume 1, No. 1, 2024

Internet of Medical Things with Considering of Artificial Intelligence

Talayeh Ghodsizad [a,b]

[a] *Department of Biomedical Engineering, Science and Research Branch, Islamic Azad University, Tehran, Iran*
[b] *Member of the board and head of the medical equipment department of Gorouh-E-Chahar Consulting Engineers.*

ARTICLE INFO

Received: 2024/09/15

Revised: 2024/10/09

Accept: 2024/10/19

Keywords:

Artificial Intelligence, Internet of Things, Medical, Deep Learning, Machine Learning.

ABSTRACT

The growth of Internet of Things (IoT) devices in the healthcare sector has enabled the new era of the Internet of Medical Things (IoMT). However, IoT devices are vulnerable to various cybersecurity attacks and threats, leading to negative consequences. Cyberattacks can harm IoMT devices in use and risk human lives. Given the promising potential of Artificial Intelligence (AI)-related technologies to enhance specific cybersecurity measures, this article provides a comprehensive review of this emerging field to introduce modern cybersecurity technologies that leverage AI techniques to improve performance and address security and privacy vulnerabilities. Our findings indicate that integrating Machine Learning (ML) and Deep Learning (DL) techniques enhances cybersecurity measures' performance, speed, reliability, and efficiency. This issue could be useful in improving the security and privacy of IoMT devices. This article outlines the numerous advantages of AI technologies compared to traditional cybersecurity technologies, such as blockchain, anomaly detection, homomorphic encryption, differential privacy, and federated learning. We conclude with considerations for future research, emphasizing the promising Potential of AI-based cybersecurity in the IoMT landscape, particularly in protecting patient data and data-driven healthcare.

1. Introduction

The term "Internet of Things" (IoT) was introduced by British entrepreneur Kevin Ashton [1]. He described a world where all inanimate objects have a digital identity and can be managed and controlled through computers. All people are connected through the Internet, but according to the title, things are connected in the Internet of Things. IoT, a concept of interconnected sensors

[a] Corresponding author email address: talayeh.ghodsizad@gmail.com (Talayeh Ghodsizad).
Available online 20/10/2024.

3060-6349/BGSA Ltd.

called "things," originates from the Internet Protocol (IP). The Internet of Things refers to the integration of physical objects equipped with sensors and actuators that can communicate with computer systems through wired or wireless networks [2]. The rapid advancement in IoT technology plays a crucial role in the healthcare sector, making the Internet of Medical Things (IoMT) increasingly common. Additionally, developing high-speed network systems and the growing use of portable monitors, smartphones, wearable devices, and electronic health records in healthcare contribute to the significant growth of IoT devices in the healthcare sector [3].

Integrating IoT devices into healthcare systems enhances connectivity and system interoperability, enabling collaboration between isolated systems in the healthcare domain [4-6]. However, IoT devices are vulnerable to various security threats and attacks, as they lack self-protection capabilities.

Recent research has shown that over 90% of IoT devices transmit data insecurely, with 57% vulnerable to attacks that could leak sensitive data. Cyberattacks not only target IoMT devices but also pose a threat to human lives [7].

IoMT, regarded as a collection of medical devices and related software applications, has emerged as a specific aspect of IoT, focusing on the integration and interoperability of medical devices. This makes it a powerful tool in the healthcare sector. Additionally, it provides unparalleled opportunities for collecting, analyzing, and exchanging biomedical data, revolutionizing the delivery of healthcare services [8].

One of the most critical debates in the IoMT field involves a trade-off between patient privacy, device usability, and data accessibility. Maintaining patient confidentiality while using patient data for therapeutic and research purposes remains a major challenge [9]. Additionally, security levels may vary depending on the manufacturer of the IoMT device, which often leads to vulnerabilities within the healthcare ecosystem.

Despite the numerous benefits IoMT offers in daily healthcare, such as effective patient monitoring and improved decision-making, it has also raised several security concerns. Notably, cybersecurity breaches have significantly impacted the global healthcare industry. In 2023, at least 2,620 organizations were affected, leading to the theft of 77.2 million records, with 78.1% of the affected entities based in the United States [10]. These breaches, primarily attributed to hacking and ransomware attacks, accounted for 88.52% of incidents and 99.94% of the compromised records [11]. According to IBM's 2023 Cost of a Data Breach Report, the

healthcare sector consistently incurs the highest costs related to data breaches compared to other industries, rising from $10.1 million in 2022 to $10.9 million in 2023 [12].

The structure of this review article is as follows. In Section 2, we present some previous studies in the field of cybersecurity. Section 3 introduces networked medical devices. In Section 4, we discuss the security and privacy of IoMT devices. Section 5 highlights the role of artificial intelligence technologies in enhancing IoMT security. Before concluding in Section 7, we address future research challenges in Section 6.

2. Literature review

Recent scientific reviews on this topic have highlighted the security and privacy features, threat models, requirements, and major challenges affecting the security of IoMT devices [8, 9, 13, 14]. Specifically, in [15], the authors present recent contributions focusing on implementing formal methods to improve the security of IoMT ecosystems. A recent review on security threats and associated countermeasures in IoMT also focuses on developing advanced security countermeasures, considering the primary security objectives [16]. Recently, the authors of [17] proposed an innovative classification for intrusion detection schemes tailored to IoMT. In contrast to the reviews above, some cybersecurity technologies, especially in the context of Networked Medical Devices (NMDs), seem to benefit from the increasing potential of Artificial Intelligence (AI) [18].

AI, through its ability to analyze large amounts of data and detect abnormal patterns, enhances patient data's integrity, confidentiality, and availability. Additionally, AI-based threat detection can be useful in identifying emerging threats and vulnerabilities, thereby improving the security of modern healthcare systems [17]. In this context, specific reviews discuss several privacy and security challenges in healthcare systems and present various privacy-preserving techniques in DL and ML for secure data mining and processing [19, 20].

Explainable Artificial Intelligence (XAI) refers to a set of methods and techniques to increase the transparency and interpretability of decisions made by AI models. Understanding how the model operates and makes decisions in traditional AI systems can be challenging, especially in complex models like deep neural networks. XAI seeks to transform this "black box" into a more interpretable system, enabling users to understand and trust AI decisions. XAI methods include the following:

1. **Model-Specific Methods**: These methods are designed for specific models and include inherently transparent and interpretable algorithms. For example:
    - **Decision Trees**: These models create a hierarchy of decisions that can easily explain how each decision was made.
    - **Linear Models**: Because these models use specific weights for each feature, it is straightforward to understand the impact of each feature on the decisions.
2. **Model-Agnostic Methods**: These methods can be applied to any AI model and typically assist in explaining complex models such as deep neural networks. Some of these methods include:
    - **LIME (Local Interpretable Model-agnostic Explanations)**: This method examines the decisions of a model in small, local areas of the data space and provides simple explanations for those decisions.
    - **SHAP (Shapley Additive Explanations)**: This method is based on game theory and explains how much each input feature contributes to the model's output.
    - **Saliency Maps**: For computer vision models (such as CNNs), these maps highlight the key areas of images that have had the most significant impact on the decisions.
3. **Sensitivity Analysis**: This method investigates how changes in inputs lead to changes in model outputs, helping users understand which features significantly influence the final decision.

Importance of XAI:

• Reliability: Transparency in decision-making increases users' trust in AI systems.

• Privacy and Fairness: Explaining models can uncover and correct hidden biases, preventing unfair decisions.

• Regulatory Compliance: In some instances, such as data protection laws, it is necessary to explain the reasoning behind decisions made by AI systems to individuals.

Similarly, the authors [21] focus on the use of AI as a cybersecurity tool in the healthcare sector, while the authors [22] discuss the security aspects of Federated Learning (FL) in IoMT applications within smart healthcare ecosystems. Enhancing cybersecurity performance through AI involves using advanced technologies to improve threat detection, response time, adaptability to evolving threats, and the overall robustness of security measures. Integrating AI is crucial

when addressing challenges from a complex threat landscape, enabling effective cybersecurity operations.

The primary aim of this review is to fill the gap in the relevant literature concerning modern cybersecurity technologies that utilize AI techniques to enhance performance and mitigate security and privacy vulnerabilities. Considering the numerous advantages of AI technologies compared to their traditional cybersecurity counterparts—including blockchain, anomaly detection, homomorphic encryption, differential privacy, federated learning, and more—we provide a structured overview of current scientific trends.

3. Networked Medical Devices

In the distinct realm of IoMT, Networked Medical Devices (NMDs) encompass a wide range of interconnected devices via the Internet and wireless communication channels. These include Implantable Medical Devices (IMDs), Wearable Medical Devices (WMDs), Remote Patient Monitoring (RPM) systems, and Hospital Network Devices (HNDs).

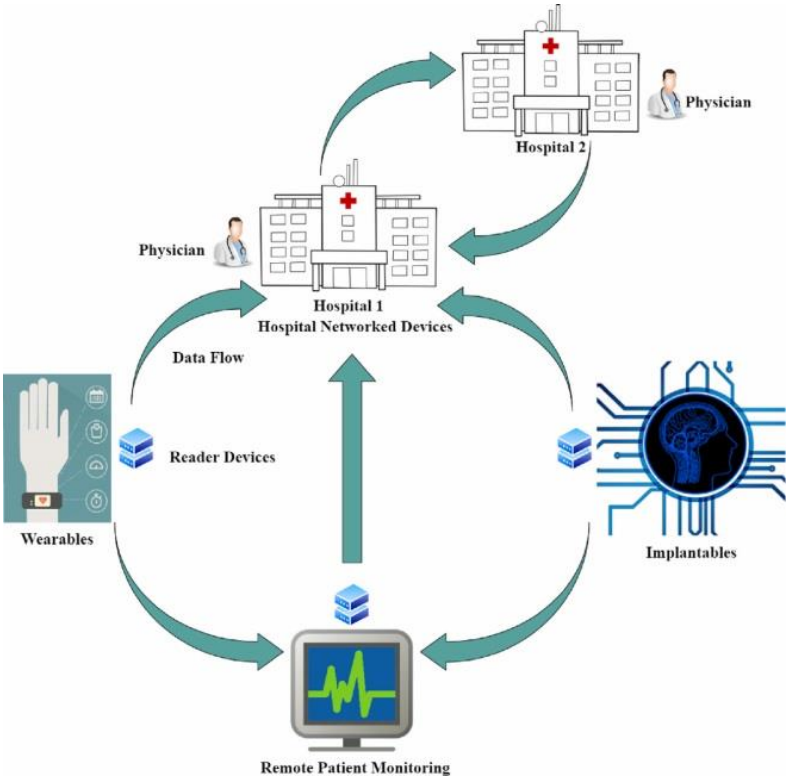

Figure 1: Internet of Things ecosystem

The emerging IoMT ecosystem and its corresponding NMDs are illustrated in Figure 1, where a network of hospitals can exchange medical data for clinical and research purposes. This enables

physicians and researchers to benefit from medical information obtained from a more significant number of patients.

The Internet of Things ecosystem is diverse and includes various components, and its development is impossible without identification and communication between the components. The IoT ecosystem is based on different layers: hardware, communication, security, platforms, information storage, processing, and software.

3.1. Implantable Medical Devices (IMDs):

IMDs are surgically placed within a patient's body for several purposes: (1) to address specific medical conditions by replacing or augmenting the function of a damaged organ or anatomical structure, (2) to monitor various bodily functions, and (3) to deliver medications or other therapies directly to a targeted area. IMDs can be classified into the following categories [23]:

- **Cardiovascular Devices**: Used to treat heart and vascular-related diseases.
- **Neurological Devices**: Used for treating conditions related to the nervous system, including epilepsy, Parkinson's disease, and chronic pain.
- **Orthopedic Devices**: Used to treat conditions related to bones and joints.
- **Cochlear Devices**: Used for the treatment of hearing loss.
- **Implantable Drug Delivery Devices**: These devices deliver medications directly to targeted areas of the body, such as tumors, through implantable pumps.

IMDs are typically made from biocompatible materials and are often powered by batteries or other energy sources. It is important to note that patients who are candidates for IMDs must be closely monitored to ensure the device's proper function and to address potential issues, such as device rejection or malfunction [24]. Although IMDs have significantly improved healthcare and brought revolutionary advancements in saving lives, they also present notable security challenges.

3.2. Wearable Medical Equipment (WMDs):

WMDs are a rapidly growing category of healthcare technology that can be worn on the body to monitor, track, or detect various health parameters. They often utilize advanced sensors and wireless connectivity to collect and transmit data. In addition, WMDs offer several benefits, including real-time health monitoring, increased patient engagement, and improved healthcare outcomes. They have been utilized in research and clinical trials to collect objective data, track patient progress, and evaluate treatment effectiveness. Among WMDs, fitness trackers are the

most popular due to their ability to monitor activity levels, heart rate, sleep patterns, and calories burned. Continuous glucose monitors are devices designed to track glucose levels in individuals with diabetes, providing real-time data to manage blood sugar levels and facilitate informed treatment decisions [25].

By continuously tracking vital signs and identifying irregularities or patterns, WMDs have the potential to facilitate early detection of potential health issues, enabling timely medical interventions. However, WMDs may also pose significant security concerns. The sensitive health data they generate inherently raises privacy and confidentiality issues, necessitating robust encryption and secure data storage.

3.3. Remote Patient Monitoring Systems (RPMs):

RPM systems monitor patients and collect relevant medical data remotely. They utilize multiple sensors to transmit data from the patient to healthcare professionals, enabling continuous monitoring and timely intervention. It is noteworthy that RPM systems provide patients access to secure online portals or mobile applications to view their health data, track their progress, receive educational materials, and communicate with healthcare providers remotely [26].

RPMs are based on wireless technologies such as Bluetooth, Wi-Fi, and cellular networks, while the transmitted data is typically encrypted to protect privacy and confidentiality. Additionally, the transferred patient data is stored and analyzed using specialized software [27]. Consequently, complex algorithms are employed to process the data, identify potential anomalies, and send alerts to medical staff if necessary, thereby preventing data leaks and enhancing patient safety.

3.4. Hospital Network Devices (HNDs):

HNDs consist of devices and tools medical professionals use in hospitals and other clinical settings for diagnosing, treating, and monitoring patients. Like IMDs and WMDs, HNDs can vary significantly based on patient needs and the conditions being treated.

Common HNDs include:

- **Diagnostic and Imaging Equipment**: Such as X-ray machines, computed tomography (CT) scanners, magnetic resonance imaging (MRI) machines, and ultrasound scanners, as well as laboratory equipment for analyzing blood, urine, and other bodily fluids.
- **Monitoring Devices**: For example, blood pressure monitors, ECG machines, and pulse oximeters.

- **Infusion Pumps**: Used to deliver medications, fluids, and other substances directly into a patient's bloodstream.
- **Rehabilitation Equipment**: Including physical therapy devices, exercise equipment, splints, braces, and more.
- **Patient Positioning Equipment**: Hospital beds and stretchers are used to position patients for various medical procedures and to ensure comfort during their hospital stay.

Ensuring medical equipment security in hospitals is critically important in the modern healthcare environment, which is becoming increasingly interconnected. As more medical devices join hospital networks, the exposure to cyberattacks rises, making them vulnerable to cybercriminals seeking to exploit software or hardware weaknesses. Malicious attacks on medical equipment in hospitals can have serious consequences, such as compromising patient safety and privacy and disrupting hospital operations.

4. Security and Privacy of IoMT devices

Although IoMT devices offer numerous benefits, they also present challenges due to their vulnerability to security threats and attacks. It is essential to identify such threats and attacks to ensure the integrity, availability, confidentiality, and privacy of sensitive patient health data.

The interconnected nature of IoMT devices can expose them to various cyber risks, including unauthorized access, data breaches, and potential manipulation of device functionalities. As these devices collect and transmit sensitive health information, any compromise can lead to severe consequences, including breaches of patient confidentiality, disruptions in healthcare delivery, and even risks to patient safety.

To address these challenges, it is crucial to implement robust security measures that encompass encryption, secure communication protocols, access control mechanisms, and regular security assessments. Additionally, healthcare providers must foster a culture of security awareness among staff and patients to effectively mitigate risks associated with IoMT devices.

4.1. Security and Privacy Threats

As modern medical devices have evolved from standalone sensors to more integrated devices, their security is broadly understood through a layered approach that connects various technologies, devices, sensors, and systems via electrical, electronic, and wired or wireless connections. The structure and functionality of each layer are described in Figure 2.

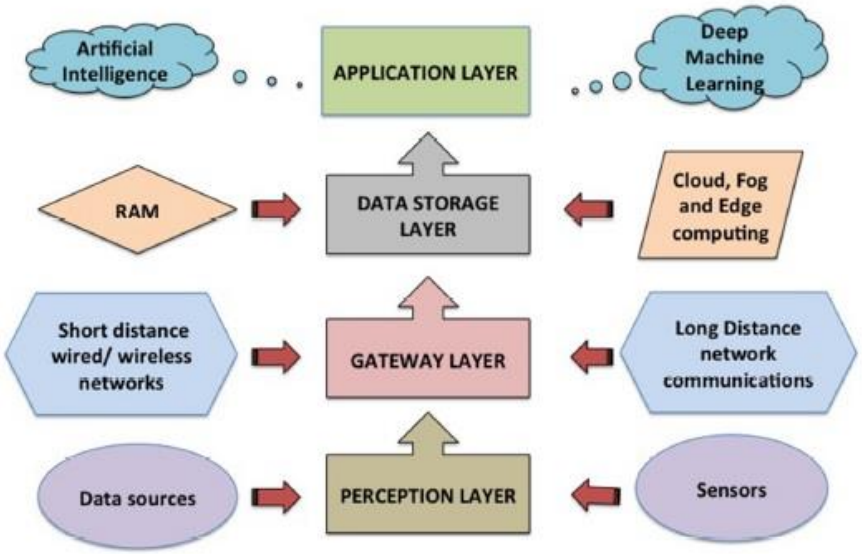

Figure 2: IoMT network layers

• **Perception Layer - Sensor systems for Data Collection**

The perception layer, often called the physical layer, is the lowest layer of the IoMT ecosystem. It comprises data sources such as smart objects, health monitoring devices, and mobile applications integrated with sensors like infrared, medical, smart device, cameras, and Global Positioning Systems (GPS). These sensor systems detect environmental changes, identify objects, locations, and measurements, and convert information into digital signals. They can also store data for future use.

In the perception layer, unauthorized physical access to medical devices can pose significant security risks. Additionally, malicious actors may attempt to manipulate medical devices by physically altering their components or configurations.

This can include accessing the internal components of a device, manipulating hardware or the operating system, or inserting malicious components. Threats at the physical layer may also manifest as intentional or unintentional interference with the operation of medical devices caused by electromagnetic interference, power outages, or intentional jamming of wireless signals. From a network layer perspective, Networked Medical Devices (NMDs) must be secure to protect patient data and ensure device functionality. Spoofing, Distributed Denial of Service (DDoS) attacks, Sybil attacks, and sinkhole attacks are the primary types of threats typically identified at this layer [28].

• **Network layer - Gateway layer**

As mentioned, sensors require a connection to a gateway that facilitates communication through networks, storing information either locally or centrally. Communications can occur at various frequencies and be short-range, such as RFID, wireless sensor networks, Bluetooth, Zigbee, and low-power Wi-Fi, or longer-range, such as cloud computing and blockchain.

Networks can include Personal Area Networks (PAN) like Zigbee, Bluetooth, and Ultra Wideband (UWB), or Local Area Networks (LAN) such as Ethernet and Wi-Fi connections. Wide area networks (WANs) like Global System for Mobile Communications (GSM) do not require direct connectivity but utilize servers and backup applications. Wireless Sensor Networks (WSN) are particularly useful for supporting many sensor nodes, especially in sensors that require low power connectivity and data rates.

• **Transfer Layer - Data Storage**

The transport layer plays a crucial role in the communications of the IoMT network. It receives data from applications and segments it for transmission into smaller packets, ensuring data integrity and reliability by detecting and correcting errors. The transport layer also manages the flow of data to prevent network congestion and allows multiple applications to share the same network connection [5]. This layer provides two main protocols: the Transmission Control Protocol (TCP), which prioritizes reliability, and the User Datagram Protocol (UDP), which enhances speed for real-time applications. It is important to note that the transport layer enables smooth and efficient data transfer between IoMT devices.

• Application Layer

The application layer plays a crucial role in data processing, user interaction, and device functionality for NMDs. The primary function of this layer is to interpret data and provide specific application services. It utilizes AI and deep learning to understand electronic health record data and monitor trends and changes in the collected data (data repository). However, this layer is susceptible to various security threats that can compromise patient data, device integrity, and system accessibility.

4.2. Active and passive attacks

The security and privacy threats outlined in the previous section are closely related to passive and active attacks on NMDs. Passive attacks, such as eavesdropping, are employed by potential attackers to gain unauthorized access to sensitive data, such as patient health records and treatment plans exchanged between NMDs [29]. Attackers may passively intercept

communications to obtain valuable information, jeopardizing the patient's right to privacy and confidentiality. Furthermore, through passive attacks, attackers often intercept and alter transmitted data, leading to misdiagnoses, incorrect medication dosages, or other adverse consequences.

Active attacks, such as injection attacks (SQL injection, code injection, and others), exploit vulnerabilities in NMD application software to inject malicious code. This can lead to unauthorized access, data corruption, and system compromise. Active attacks include denial-of-service (DoS) attacks, where attackers overwhelm NMDs with large volumes of malicious traffic or requests. As a result, devices may become unavailable, disrupting vital medical services. In this context, active malware attacks threaten the operation of networked medical devices and can facilitate unauthorized access or control. Malware may be introduced through various means, including infected software updates and compromised network connections [30]. A detailed classification of attacks against NMDs is provided in the following paragraphs.

4.2.1. Malware Attacks

The term "malware" generally refers to malicious software that can infect medical devices and compromise their security and functionality. Malware may jeopardize sensitive data, manipulate device behavior, or potentially cause physical harm to patients.

Ransomware is a relatively popular malware attack that can encrypt the data on a medical device and render it inoperable until a ransom is paid. Ransomware attacks on medical devices can lead to significant disruptions in patient care and may compromise the confidentiality and integrity of sensitive medical data [16]. Additionally, Trojan horses are malicious programs that appear to be legitimate software but typically contain hidden malware that can jeopardize the security of a medical device. Trojan attacks can steal sensitive data or gain unauthorized access [31]. Botnets are networks of infected devices that an attacker can control. Botnets can launch DDoS attacks, steal sensitive data, or utilize the medical device as a proxy for other attacks. Another type of malware attack involves backdoors, vulnerabilities intentionally embedded in middleware or device software, allowing unauthorized access to the device.

4.2.2. Sybil Attacks

Sybil attacks are a security threat when an attacker creates multiple fake identities, referred to as "Sybil nodes," to infiltrate a network and gain access to sensitive information. In the context of

IoMT, Sybil attacks can be particularly challenging as they may compromise the connected devices and the data they collect.

Popular defensive strategies against Sybil attacks include social graph-based Sybil detection, behavior classification-based Sybil detection, and mobile Sybil detection. By implementing authentication mechanisms, reputation-based systems, distributed consensus algorithms, secure routing protocols, and machine learning-based techniques, healthcare organizations can mitigate the risk of Sybil attacks and ensure the security of their IoT networks.

Identity-based Sybil attacks are specific types of Sybil attacks in which the attacker creates multiple fake identities based on the same physical identity, making it difficult to identify and localize the attack [32].

4.2.3. Routing Attacks

Routing attacks threaten the confidentiality, integrity, and availability of sensitive medical data, potentially endangering patient health. One type of routing attack, a Man-in-the-Middle (MitM) attack, involves intercepting and modifying the communication between a medical device and its intended destination. This allows the attacker to steal or alter sensitive medical data.

Additionally, routing table attacks may attempt to manipulate a medical device's routing table, causing it to send data to an unintended destination or preventing it from communicating with other devices on the network [33]. Denial-of-Service (DoS) attacks aim to disrupt the normal functioning of a medical device by overwhelming its routing infrastructure with traffic, rendering it unresponsive or even shutting it down.

An attacker may also exploit vulnerabilities in the routing protocol used by a medical device to gain unauthorized access, steal sensitive data, or manipulate its behavior. DoS attacks have been extensively studied in the literature. Variants of DoS attacks include battery depletion, botnets, and several others. Flooding is recognized as a type of DoS attack that leads to resource blockage and overload in the healthcare environment. Different types of DoS attacks can be categorized based on their target network layer.

4.2.4. Battery Drain Attacks

Attacks on implantable and wearable devices maliciously aim to drain the battery of these devices, potentially harming patients who rely on them for monitoring or treatment. Closely related to other attacks, battery drain can occur due to malware infecting a device, causing it to consume excessive energy.

DDoS attacks may also overload the communication channels of implantable devices, forcing them to expend more energy to maintain connectivity. An attacker could physically manipulate a wearable or implantable device to reduce energy-saving features or increase power consumption. Regular software updates can typically help address security vulnerabilities in these devices. Proper encryption can protect wearables or implantables from malware attacks that lead to faster battery drainage. At the same time, access control measures, such as multi-factor authentication, can prevent unauthorized access and manipulation of implantable devices [34, 35].

4.2.5. Firmware modification

Firmware is the software used to control the hardware of a device. Due to its inherent software nature, this operating system is vulnerable to various digital attacks. An attacker can exploit such vulnerabilities to gain access to the operating system's core [36].

Specifically, an attacker may access, modify components, or entirely replace the software to steal information, corrupt data, recreate routing rules, create a launchpad for further attacks, etc. Operating system attacks in IoMT are quite common and generally include the following:

(a) **Unauthorized Access:** The attacker gains access to the device and sensitive personal data and information.

(b) **Device Control:** The attacker takes partial or full control of the device.

(c) **Malware Installation:** The attacker installs malware alongside the software, which can be transferred to other devices or used as a starting point for further attacks.

(d) **DDoS Attacks:** Changes to the device's operating system turn it into a bot that supports potential DDoS attacks on the network.

(e) **Data Loss:** Operating system attacks can lead to the loss or corruption of data/information stored on the device.

(f) **Physical Damage:** Since the operating system controls the hardware, tampering with it can physically damage the device or specific components. Attackers can also reverse-engineer the operating system of a medical device to find vulnerabilities or modify the system to suit their needs. Additionally, they can exploit vulnerabilities during the update process of a medical device to install unauthorized operating system updates that change the device's behavior or even introduce new vulnerabilities [37].

4.2.6. Eavesdropping

Eavesdropping occurs when a hacker intercepts, deletes, or modifies data transmitted between two devices. This type of attack is also known as a spying attack. Eavesdropping relies on insecure network communications to access data in transit between devices. Through eavesdropping attacks, sensitive information is obtained due to insecure communication channels.

Several medical and wearable devices, such as blood pressure monitors and smartwatches, have vulnerabilities that allow attackers to obtain sensitive information. To further explain the definition of "eavesdropping attack," it usually occurs when a user connects to a network where traffic is not secure or encrypted and sends sensitive data to a colleague. Data is transmitted over an open network, allowing the attacker to exploit and intercept a vulnerability through various methods.

Detecting eavesdropping attacks is often difficult. Unlike other forms of cyber attacks, a bug or eavesdropping device may not negatively impact the performance of devices and networks. With eavesdropping, attackers can employ various methods to carry out attacks, typically involving using different devices to listen to conversations and monitor network activities [38].

4.2.7. Cloud attacks, Device Simulation, and Sensor Spoofing

Cloud attacks target cloud-based service platforms, such as computing services, storage services, or hosted applications. Cloud computing is a computational model where computing resources (like servers, storage, and data processing) are provided over the Internet from centralized data centers. Users can access these resources via the Internet without needing physical hardware. Key features of cloud computing include scalability, remote accessibility, and reduced infrastructure costs.

Features of Cloud Computing:

• Data processing and storage in centralized data centers.

• Suitable for applications that require heavy processing.

• Dependent on an internet connection with a relatively longer delay.

• Suitable for processing massive data and performing complex calculations.

Cloud attacks can have severe consequences, including data breaches, data loss, unauthorized access to sensitive information, and service disruptions. As more organizations and individuals

rely on cloud computing for data storage and processing, the number of potential targets for attackers also increases. Many organizations may be unaware of the risks and vulnerabilities associated with cloud computing or may not have adequate measures to protect against these threats.

Cloud attacks include modifying cloud infrastructure, a technology that has been relatively recently integrated into healthcare. Device simulation involves mimicking devices to perform malicious activities within the IoMT environment. If a successful attack occurs, the attacker gains control of a sensor and alters the medical device's functionality, potentially jeopardizing patient safety and data integrity [39].

4.2.8. Perception Attacks

Perception attacks are associated with vulnerabilities at the lowest level of the transmitted signal, regardless of the medium used. Perception attacks often manifest as multiple access (MAC) layer attacks.

At the perception layer, attackers may manipulate the data generated by medical devices or sensors, making vital signs appear stable when they are not. This can lead healthcare providers to make incorrect decisions based on false information, potentially endangering patients' lives.

4.2.9. Bluetooth Attacks

Bluetooth attacks can be classified into several categories, mainly because Bluetooth technology implements its layered architecture. Several attacks of this particular type include blue smacking (DoS), Blues nerfing and Bluebugging (data breach), Bluejacking (spoofing), and Blueprinting (sniffing).

Bluejacking is an attack in which Bluetooth sends unsolicited messages to a medical device. Messages can steal sensitive data or cause unpredictable device behavior [40].

Bluesnarfing exploits vulnerabilities in the Bluetooth protocol to gain unauthorized access to a medical device. Once an attacker gains access, they can steal sensitive data or manipulate the behavior of that device. Users of medical programs are often required to log into an online account, where they enter their medical information provided by WMD or IMD. The relevant information has been collected and stored. If malicious agents gain access to these credentials, they can alter or manipulate medical data in various ways, posing a significant risk to patient health monitoring [41].

Due to numerous security attacks on NMD, From passive attacks, such as eavesdropping, to active attacks, such as malware infiltration, it is clear that protecting these devices' integrity, confidentiality, and availability is paramount. These attacks are a significant risk to patient privacy and the effectiveness of medical treatments. By examining these vulnerabilities and their implications, it is clear that advanced technologies must be developed to enhance NMD defenses. Are used. With its ability to analyze large amounts of data, the ML algorithm can detect anomalies and predict possible security breaches. In the next section, we will examine the application of AI techniques in IoMT cyber security. We strive to ensure optimal performance and reliability while mitigating multiple threats and attacks.

5. Artificial intelligence to increase IoMT security

Increasing exposure to NMD against security threats and attacks, as described in Section 4, highlights the necessity of improving the performance and effectiveness of cyber security. To address this growing concern, this section presents the central role of ML and DL methods in increasing the security of IoMT devices. We will check. AI effectively contributes to the most advanced cybersecurity technologies, from anomaly detection and intrusion detection systems to homomorphic encryption, and can reduce risks, increase patient safety, and protect sensitive medical data. We aim to provide a comprehensive review of the use of ML technologies and DL To create secure and sustainable IoMT ecosystems.

5.1. Blockchain

Blockchain (BC) comprises a series of modules that store data. Modifying data becomes exceptionally challenging once data is added to a block, making blockchain an extremely secure information network. In a blockchain network, interactions between nodes occur through transactions, which are subsequently collected into information blocks after being verified by designated network nodes. The recorded data blocks are secured against tampering using a consensus mechanism, enabling decentralized usage. Interactions with other devices or peers do not require central authentication, allowing healthcare applications to exchange patient healthcare data securely.

In this context, BC-based methods to mitigate DDoS attacks can be classified based on their deployment locations as network-based, near the attacker, near the victim, or a combination, emphasizing IoT and SDN architectures [42].

The structure of a block consists of three components:

- **Data**: Sender, receiver, and transaction amount.
- **Hash**: This is a unique code for each block, akin to a fingerprint.
- **Previous Block Hash**: Each block is linked to the others, creating a chain.

Therefore, a minor change in one block can profoundly affect the entire blockchain. An additional security layer has been implemented to reduce the risk of unauthorized access by hackers.

A significant challenge to integrating BC into IoMT arises from the limited computational resources of NMDs, as BC typically does not operate in real time. However, it has been shown that BC can enhance healthcare [43]. Combining artificial intelligence with BC technology in the context of NMDs improves security by providing real-time threat detection, adaptive security measures, and data protection. Nevertheless, it is essential to consider computational requirements, data privacy concerns, and the need for continuous model updates when implementing AI models for security in healthcare environments.

In [44], a three-layer neural network (TNN) and BC technology were combined into a single framework that ensures the integrity and privacy of transmitted medical data. Additionally, [45] introduced an integrated approach using a bidirectional long short-term memory (LSTM) model and BC technology to provide early stress detection for NMD users. A new secure authentication approach utilizing K-Nearest Neighbors (KNN) and ML has also been proposed, improving computation time compared to traditional KNN algorithms [46].

5.2. Authentication Schemes

In healthcare systems, authentication and authorization mechanisms are critical security components [47]. Upon successful authentication, an entity is granted access to the healthcare system by verifying unique attributes or confidential information. Given the necessity for privacy in healthcare systems, IoMT must encrypt patient data using a secure encryption key. Distributing a secure key, especially in symmetric encryption environments involving numerous participants, is daunting. In asymmetric encryption, the key distribution challenge is resolved using a pair of keys—one public and one private—although these keys are generally larger.

ML enables the development of adaptive authentication systems that continuously evaluate user behavior and adjust authentication requirements accordingly. For example, a system can detect changes in typing behavior or login location for healthcare providers and initiate additional authentication if necessary. This could facilitate biometric authentication methods in medical

devices, such as fingerprint, facial, or voice recognition [48]. These biometric factors are unique to individuals and provide a higher security level than traditional authentication methods.

Decentralized authentication for patient-authorized wearable devices is facilitated using ML techniques to predict and transmit authentication features to the next trusted reference. In [49, 50], a multi-layer security authentication scheme is proposed, encompassing data, network, and application layers. Feature extraction at the application layer involves using a QRS set from ECG signals, applying Legendre approximation, and a custom multi-layer perceptron for classifying ECG data. Conversely, [51] discusses a lightweight hybrid authentication scheme incorporating Supervised ML (SML) followed by an encryption and decryption scheme for secure data transmission through wireless communication channels. SML facilitates decentralized authentication for patient-authorized wearable devices to minimize computational costs, authentication time, and communication expenses, particularly during data transfer between different data collection areas.

A privacy-preserving deep learning neural network framework, as described in [52], is implemented to safeguard data transmission against adversarial attacks while reducing encryption/decryption times. A new privacy-preserving method based on a ciphertext policy has been introduced, integrating the advantages of private, public, and master keys to create patient-centric access control. In study [53], the authors propose a privacy-preserving scheme for collecting patient data from IoMT devices in disease prediction systems. Following the initial authentication phase, elliptic curve cryptography based on log-of-round values is applied to enhance security during data transmission. A deep learning neural network utilizing an advanced genetic swarm algorithm is employed for disease prediction. Lastly, [47]presents research on delivering reliable ECG data by applying domain customization attacks within a supervised learning platform. After receiving data from devices, a combination of unique features is considered as input in a support vector machine (SVM) with various data preprocessing techniques to refine the platform's verification process.

5.3. Anomaly Detection (AD)

Anomaly detection algorithms are crucial in intrusion detection systems, monitoring and identifying attacks or unusual activities within IoMT devices. These algorithms operate on the premise of detecting anomalies, defined as extraordinary events that significantly deviate from the normal behavior of a system. The complexity of anomaly detection in IoMT arises from the

diversity and multitude of interconnected devices and sensors, each with varying computational resources, communication protocols, and capabilities.

Integrating ML and DL algorithms is proposed as a promising strategy to mitigate these complexities. In [54], the authors introduce a biometric security framework based on ML that utilizes features from ECG signals to authenticate users during the testing phase. This approach leverages unique biometric identifiers derived from polynomial coefficient approximations.

5.4. Homomorphic Encryption (HE)

Homomorphic encryption (HE) refers to a set of cryptographic techniques that allow for computations on encrypted data without decryption. This capability ensures that the results of computations remain encrypted, facilitating data processing without compromising the associated privacy. HE's ability to preserve privacy in outsourced storage and computation is particularly noteworthy, as it allows data to remain encrypted even when processed in cloud environments.

Recent studies indicate that the effectiveness of HE in IoMT is enhanced through the integration of MLand DL techniques. For instance, a design for efficient privacy-preserving text search in cloud-based IoMT systems, utilizing HE and bilinear mapping, was proposed in [55]. This design aims to establish a relational context for query keywords on encrypted data, further enhanced by security analysis through term frequency-inverse document frequency (TF-IDF) for information retrieval.

Additionally, an advanced privacy-preserving data fusion strategy (PDFS) was introduced in [56], which involves classifying sensitive tasks, evaluating task completion, designing work contracts based on incentive mechanisms, and integrating HE-based data. PDFS employs a privacy-preserving classification mechanism based on K-means clustering, demonstrating greater effectiveness than conventional methods.

Moreover, the authors of [57] explored the development of a secure and searchable blockchain database based on deep learning that employs HE, facilitating secure access to data and key management through smart contracts, utilizing a Variational Autoencoder (VAE) for classification purposes.

Cryptographic tools such as HE are essential for protecting local models in federated learning and ensuring the privacy of medical data against various attack vectors. This includes a resilient mechanism that guarantees system integrity despite multiple active clients.

5.5. Differential Privacy (DP)

Differential privacy (DP) is a data science and ML method aimed at protecting individuals' personal information within datasets. This technique ensures that even if an individual's data is included in a dataset, specific information about that individual remains confidential and difficult to access.

In differential privacy, noise (error) is added to the data to prevent direct identification of individuals. This method guarantees that the output of data analyses will be nearly identical, whether or not the information of a specific individual is present in the dataset. By introducing randomness, DP effectively obfuscates individual data points while allowing for useful aggregate insights.

DP establishes specific constraints on the information that can be revealed about an individual's data in a database, thereby protecting personal privacy. In healthcare, the primary goal of DP is to safeguard patient privacy, especially when medical data is shared with healthcare providers or researchers. The integration of artificial intelligence (AI) can enhance DP protection mechanisms.

For instance, a strategy for multi-regional task allocation, enhanced with privacy, referred to as PMTA, is proposed in [58]. This strategy employs DP to introduce noise into patient data, which is then utilized to train a deep Q-network that leverages a spectral clustering algorithm for optimal classification.

5.6. Federal Learning (FL)

The increasing volume of data generated by modern healthcare infrastructures poses specific challenges for traditional AI, which typically focuses on centralized data processing. Federated Learning (FL), a form of distributed learning, has become a popular solution for intelligent healthcare systems that involve IoMT devices. It allows for the collaborative training of global models while keeping private data secure from potential adversaries.

FL is a decentralized approach to ML that enables models to be trained without the need to collect raw data in a central location. In this method, data remains on local devices such as smartphones or computers, and the model is trained directly on each device. Instead of sharing data, only updates to the model (weights and learning parameters) are synchronized with a central server [59].

This approach is particularly beneficial in terms of privacy preservation and reducing data transmission costs, as sensitive data never leaves the local devices. FL is especially useful in applications involving smartphones, healthcare, and the Internet of Things (IoT), where data is dispersed and confidential.

By leveraging FL, healthcare organizations can build more robust AI models that learn from a wider array of data sources while maintaining patient privacy. This decentralized framework also addresses data sovereignty concerns, as data can remain within its originating jurisdiction, complying with local regulations.

Furthermore, FL can enhance model performance by aggregating knowledge from multiple local models, leading to a more generalized understanding of patterns and trends across diverse patient populations. As healthcare systems increasingly adopt IoMT devices, FL offers a scalable and privacy-preserving way to harness the power of data for better health outcomes [60].

5.7. Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) are tools designed to monitor networks and computer systems for suspicious activities, cyberattacks, or security breaches. The primary goal of IDS is to detect and alert on unauthorized or suspicious activities, allowing for prevention of potential intrusions and threats. Innovative IDS, particularly those incorporating artificial intelligence techniques, are increasingly important in enhancing the cybersecurity of IoMT, especially given the advanced complexities of cyberattacks [61]. There are two main types of IDS:

1.Signature-based IDS: These systems utilize a database of known attack patterns and signatures. If an activity matches one of these known signatures, the IDS generates an alert. While this type of system is effective for detecting known attacks, it struggles with identifying new or unknown threats.

2. Anomaly-based IDS: This type of system monitors the normal behavior of a network or system and identifies any abnormal deviations from this behavior as potential threats. This method can detect new and unknown attacks, but it may also generate a higher number of false positives due to its reliance on deviations from established norms.

6. Discussion

As highlighted in the previous section, artificial intelligence significantly enhances the security of IoMT (Internet of Medical Things). However, despite the remarkable advancements, the integration of AI into IoMT necessitates a thorough reassessment of the underlying technologies

and their implementation. This integration is not as straightforward as its advancements might suggest. In this regard, there are limitations and challenges associated with the implementation of AI algorithms in IoMT devices that warrant comprehensive examination, including hardware implementation, quantum computing, training AI models, and various ethical concerns.

One significant barrier to integrating AI into the IoMT ecosystem is the inadequacy of existing hardware. Effective implementation of AI algorithms requires high-performance computational capabilities and demands devices specifically designed for healthcare environments. Without the appropriate hardware infrastructure, the potential benefits of AI can be severely limited, hampering its effectiveness in real-time monitoring and decision-making processes.

Another limitation involves the training of AI models in the context of IoMT. These models require large and accurate datasets, often constrained in healthcare due to privacy concerns. Such restrictions limit training data availability and raise ethical issues surrounding data collection, consent, and the use of sensitive patient information. This is particularly critical in the healthcare sector, where the stakes are high, and ethical standards must be upheld rigorously.

Challenges in AI Integration

6.1. Hardware implementation:

In addition to the advantages offered by IoMT devices, such as reduced overall costs and efficient data exchange facilitated by 5G technologies, these devices also possess inherent limitations. Specifically, their cost-effective design imposes resource constraints, impacting computational capacity, memory allocation, and energy consumption. More specifically:

1. **Computational Capacity**: DL and ML algorithms are inherently computationally expensive due to their reliance on multiplication and accumulation operations and non-linear activation functions. This complexity makes their execution a challenging task, particularly as miniaturization of IoMT devices is crucial.
2. **Memory Allocation**: As the complexity of AI algorithms increases, the number of trainable parameters also rises accordingly. Therefore, the available memory must have sufficient capacity to accommodate the large number of involved parameters.
3. **Energy Consumption**: Given their computational demands, DL and ML algorithms consume significant amounts of energy, leading to reduced battery life in IoMT devices. This results in the need for frequent recharging and complementary use of energy harvesting techniques to extend their operational lifespan.

6.2. Quantum computing

Quantum computing represents a type of computation based on the principles of quantum mechanics, a branch of physics that describes the behavior of particles at very small scales, such as atoms and photons. Unlike classical computers, which process information using bits (which can be either 0 or 1 at any moment), quantum computers use qubits that can simultaneously exist in both 0 and 1 states, a concept known as superposition [62].

Key Features of Quantum Computing:

1. **Superposition**: A qubit can be in multiple states at the same time. This feature allows quantum computers to perform complex calculations simultaneously, significantly increasing their computational power.
2. **Entanglement**: Qubits can become "entangled" so that the state of one qubit can instantaneously affect the state of another, regardless of the distance between them. This feature enables more efficient computations.
3. **Interference**: Quantum computations use wave interference to enhance correct results while diminishing incorrect outcomes.

The advantages of quantum computing include extremely high speeds in solving complex problems, such as factoring large numbers, simulating complex molecules, and optimizing at levels beyond classical computers' capabilities. However, quantum computing is still in the research and development phase, facing significant challenges in creating practical and stable quantum computers.

This technology has widespread applications in areas such as cryptography, artificial intelligence, quantum chemistry, and optimization, and it could fundamentally change the landscape of technology and computing in the future.

Quantum computing has the potential to significantly impact cybersecurity, both in terms of breaking existing cryptographic methods and providing new solutions for secure communications. Quantum computers could disrupt current encryption systems, necessitating the development of quantum-resistant algorithms. It is expected that quantum computing will transform cybersecurity and could potentially affect the security of medical devices and patient data in the context of IoMT. Thus, security measures for IoMT must evolve to stay ahead of the potential risks posed by quantum computing. The combination of ML with quantum computing

may yield tools that are not only more accurate and efficient but also more resilient against quantum attacks.

The emerging field of Quantum ML (QML) utilizes quantum mechanics as defense mechanisms. While early results in this new area appear promising, there are still barriers to developing these quantum tools for practical and real-world applications.

6.3. Training AI Models

Training is one of the most critical aspects of AI models, especially when used in the context of IoMT. It is important to note that when environmental conditions or the features of IoMT devices change, AI models must be retrained and parameterized. Additionally, DL and ML algorithms trained on limited data may lead to overfitting, resulting in poor model performance. Given these considerations, healthcare professionals have raised concerns about the performance capabilities of AI models deployed in these devices. When AI algorithms receive incorrect IoMT data, they may produce inaccurate results, potentially harming patients. Moreover, it is notable that high false positive rates in diagnostic systems can generate misleading alerts for healthcare personnel. As a result, the trust of healthcare professionals in IoMT devices is contingent upon the accuracy and reliability of the embedded AI models, especially regarding clinical decision-support systems [63].

Accuracy ensures that AI can correctly identify real threats (true positives) and non-threats (true negatives), while precision indicates that the identified threats are relevant and do not include false positives. One potential solution for increasing trust among medical professionals is the use of Explainable AI (XAI). XAI may empower healthcare professionals to understand AI models and potentially trust them, enabling them to verify the proposed outcomes. For this purpose, glass-box models may provide interpretability of AI system processes by identifying potential vulnerabilities, thus facilitating the reduction of associated security risks and paving the way for a reliable IoMT environment.

6.4. Ethics

The integration of AI into IoMT raises significant ethical considerations, particularly regarding patient privacy, data integrity, and the potential for bias in decision-making processes. In our efforts to enhance the security of IoMT through AI, we must address these ethical challenges. The deployment of AI in IoMT should be thoroughly evaluated for its ethical implications.

Concerns such as data usage, algorithmic bias, and AI-driven decision-making arise prominently with the incorporation of AI into IoMT devices [64].

To realize the full potential of AI in healthcare in the near future, four key ethical issues must be addressed: (1) obtaining informed consent for data use, (2) ensuring safety and transparency, (3) addressing algorithmic fairness and bias, and (4) protecting privacy. Consequently, given the application of AI in high-stakes areas like healthcare, the confidentiality of processed data is of primary importance, emphasizing the need for the development and governance of AI systems that are responsible, fair, and transparent.

7. Conclusion

IoMT (Internet of Medical Things) represents a transformative paradigm in healthcare, with the potential to revolutionize patient care, diagnosis, and treatment. However, the expansion of IoMT devices brings significant security and privacy challenges. Motivated by the promising potential of AI-related technologies, this work investigates the implementation of AI methods to mitigate cybersecurity challenges and enhance the security and privacy of IoMT.

Recent research indicates a substantial increase in interest in the literature concerning IoMT security. In this context, we systematically gathered and classified extensive research in this field. Our comprehensive review highlights that integrating ML and DL techniques can significantly improve the cybersecurity of IoMT. This improvement could be beneficial for enhancing the security and privacy of IoMT devices.

Furthermore, considering the numerous advantages of AI technologies, we provide a systematic overview of the current scientific trends in this emerging field, in contrast to their primary cybersecurity counterparts. The promising potential of AI-based cybersecurity in the IoMT landscape is expected to play a crucial role in protecting patient data, ultimately fostering a new era of personalized and data-driven healthcare.

By addressing the security and privacy concerns associated with IoMT, AI can safeguard sensitive patient information and enhance the overall effectiveness of healthcare delivery systems. The ongoing evolution of AI methodologies offers a hopeful outlook for the future of healthcare, where technology and patient care can merge to create safer, more efficient environments for providers and patients.

Resources

[1] Ashton, K.J.R.j., That ‘internet of things’ thing. 2009. 22(7): p. 97-114.

[2] Atzori, L., A. Iera, and G. Morabito, The Internet of Things: A survey. Computer Networks, 2010. 54(15): p. 2787-2805.
[3] Mavrogiorgou, A., et al., IoT in Healthcare: Achieving Interoperability of High-Quality Data Acquired by IoT Medical Devices. 2019. 19(9): p. 1978.
[4] Ghodsizad, T., et al., Spatiotemporal registration and fusion of transthoracic echocardiography and volumetric coronary artery tree. International Journal of Computer Assisted Radiology and Surgery, 2021. 16(9): p. 1493-1505.
[5] Koutras, D., et al., Security in IoMT Communications: A Survey. 2020. 20(17): p. 4828.
[6] Talayeh, G., et al., Temporal Registration of Cardiac Multimodal Images Using Locally Linear Embedding Algorithm. Frontiers in Biomedical Technologies, 2021. 8(4).
[7] Yaacoub, J.-P.A., et al., Securing internet of medical things systems: Limitations, issues and recommendations. Future Generation Computer Systems, 2020. 105: p. 581-606.
[8] Islam, S.M.R., et al., The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 2015. 3: p. 678-708.
[9] Sun, Y., F.P.W. Lo, and B. Lo, Security and Privacy for the Internet of Medical Things Enabled Healthcare Systems: A Survey. IEEE Access, 2019. 7: p. 183339-183355.
[10] Healthcare data breach statistics. 2023.
[11] Marks, M. and C.E. Haupt, AI Chatbots, Health Privacy, and Challenges to HIPAA Compliance. JAMA, 2023. 330(4): p. 309-310.
[12] Institute, P., Cost of a data breach report 2022. 2022, IBM Corporation Armonk, NY, USA.
[13] Ghubaish, A., et al., Recent Advances in the Internet-of-Medical-Things (IoMT) Systems Security. IEEE Internet of Things Journal, 2021. 8(11): p. 8707-8718.
[14] Martínez, A.L., M.G. Pérez, and A. Ruiz-Martínez, A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. 2023. 55(12 %J ACM Comput. Surv.): p. Article 249.
[15] Gatouillat, A., et al., Internet of Medical Things: A Review of Recent Contributions Dealing With Cyber-Physical Systems in Medicine. IEEE Internet of Things Journal, 2018. 5(5): p. 3810-3822.
[16] Papaioannou, M., et al., A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). 2022. 33(6): p. e4049.
[17] Hernandez-Jaimes, M.L., et al., Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures. Internet of Things, 2023. 23: p. 100887.
[18] Ameen, A.H., M.A. Mohammed, and A.N. Rashid, Dimensions of artificial intelligence techniques, blockchain, and cyber security in the Internet of medical things: Opportunities, challenges, and future directions. 2023. 32(1).
[19] Khalid, N., et al., Privacy-preserving artificial intelligence in healthcare: Techniques and applications. Computers in Biology and Medicine, 2023. 158: p. 106848.
[20] Naresh, V.S. and M. Thamarai, Privacy-preserving data mining and machine learning in healthcare: Applications, challenges, and solutions. 2023. 13(2): p. e1490.
[21] Gopalan, S.S., A. Raza, and W. Almobaideen. IoT Security in Healthcare using AI: A Survey. in 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA). 2021.
[22] Rani, S., et al., Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. Knowledge-Based Systems, 2023. 274: p. 110658.
[23] Kwarteng, E. and M. Cebe, A survey on security issues in modern Implantable Devices: Solutions and future issues. Smart Health, 2022. 25: p. 100295.
[24] Gaobotse, G., et al., Non-invasive smart implants in healthcare: Redefining healthcare services delivery through sensors and emerging digital health technologies. Sensors International, 2022. 3: p. 100156.

[25] Yaqoob, T., H. Abbas, and M. Atiquzzaman, Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. IEEE Communications Surveys & Tutorials, 2019. 21(4): p. 3723-3768.
[26] Said, A.M., A. Yahyaoui, and T. Abdellatif, Efficient Anomaly Detection for Smart Hospital IoT Systems. 2021. 21(4): p. 1026.
[27] Boikanyo, K., et al., Remote patient monitoring systems: Applications, architecture, and challenges. Scientific African, 2023. 20: p. e01638.
[28] Pöhn, D. and W. Hommel, Towards an Improved Taxonomy of Attacks Related to Digital Identities and Identity Management Systems. 2023. 2023(1): p. 5573310.
[29] Hireche, R., H. Mansouri, and A.-S.K. Pathan, Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. 2022. 2(3): p. 640-661.
[30] Wasserman, L. and Y. Wasserman, Hospital cybersecurity risks and gaps: Review (for the non-cyber professional). 2022. 4.
[31] Rathore, H., et al. A review of security challenges, attacks and resolutions for wireless medical devices. in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC). 2017.
[32] David, D.S. and T.J.J.A.E.R.E.T. George, Identity-based Sybil attack detection and localization. 2020. 1: p. 94-98.
[33] Nidhya, R., S. Karthik, and G. Smilarubavathy. An End-to-End Secure and Energy-Aware Routing Mechanism for IoT-Based Modern Health Care System. 2019. Singapore: Springer Singapore.
[34] Newaz, A.I., et al., A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses. 2021. 2(3 %J ACM Trans. Comput. Healthcare): p. Article 27.
[35] Rushanan, M., et al. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. in 2014 IEEE Symposium on Security and Privacy. 2014.
[36] Srihith, I.V., et al., Firmware Attacks: The Silent Threat to Your IoT Connected Devices. International Journal of Advanced Research in Science, Communication and Technology, 2023. 3: p. 2581-9429.
[37] Van Devender, M.S., Risk Assessment Framework for Evaluation of Cybersecurity Threats and Vulnerabilities in Medical Devices. 2023, University of South Alabama.
[38] Algarni, A., A Survey and Classification of Security and Privacy Research in Smart Healthcare Systems. IEEE Access, 2019. 7: p. 101879-101894.
[39] Deogirikar, J. and A. Vidhate. Security attacks in IoT: A survey. in 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). 2017.
[40] Zhang, C., H. Shahriar, and A.B.M.K. Riad. Security and Privacy Analysis of Wearable Health Device. in 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC). 2020.
[41] Jones, D.N., Understanding and Decreasing Security Breaches in the Healthcare Industry: A Qualitative Case Study Exploring Network-Connected Medical Devices in a Large Hospital. 2022, Northcentral University.
[42] Chaganti, R., B. Bhushan, and V. Ravi, A survey on Blockchain solutions in DDoS attacks mitigation: Techniques, open challenges and future directions. Computer Communications, 2023. 197: p. 96-112.
[43] Rehman, A., et al., A secure healthcare 5.0 system based on blockchain technology entangled with federated learning technique. Computers in Biology and Medicine, 2022. 150: p. 106019.
[44] Alsemmeari, R.A., et al., Resilient Security Framework Using TNN and Blockchain for IoMT. 2023. 12(10): p. 2252.
[45] Qi, P., et al., A blockchain-based secure Internet of medical things framework for stress detection. Information Sciences, 2023. 628: p. 377-390.
[46] Al-Otaibi, Y.D., K-nearest neighbour-based smart contract for internet of medical things security using blockchain. Computers and Electrical Engineering, 2022. 101: p. 108129.

[47] Dhanke, J., et al., Heterogeneous sensor data fusion acquisition model for medical applications. Measurement: Sensors, 2022. 24: p. 100552.
[48] Zafar, S., et al., Securing Bio-Cyber Interface for the Internet of Bio-Nano Things using Particle Swarm Optimization and Artificial Neural Networks based parameter profiling. Computers in Biology and Medicine, 2021. 136: p. 104707.
[49] Almaiah, M.A., et al., A Novel Hybrid Trustworthy Decentralized Authentication and Data Preservation Model for Digital Healthcare IoT Based CPS. 2022. 22(4): p. 1448.
[50] Rathore, H., et al., Multi-layer security scheme for implantable medical devices. Neural Computing and Applications, 2020. 32(9): p. 4347-4360.
[51] Adil, M., et al., An AI-Enabled Hybrid Lightweight Authentication Scheme for Intelligent IoMT Based Cyber-Physical Systems. IEEE Transactions on Network Science and Engineering, 2023. 10(5): p. 2719-2730.
[52] Kathamuthu, N.D., et al., Deep Q-Learning-Based Neural Network with Privacy Preservation Method for Secure Data Transmission in Internet of Things (IoT) Healthcare Application. 2022. 11(1): p. 157.
[53] Padinjappurathu Gopalan, S., et al., An Efficient and Privacy-Preserving Scheme for Disease Prediction in Modern Healthcare Systems. 2022. 22(15): p. 5574.
[54] Pirbhulal, S., et al. Towards Machine Learning Enabled Security Framework for IoT-based Healthcare. in 2019 13th International Conference on Sensing Technology (ICST). 2019.
[55] Shen, M., et al., Secure Phrase Search for Intelligent Processing of Encrypted Data in Cloud-Based IoT. IEEE Internet of Things Journal, 2019. 6(2): p. 1998-2008.
[56] Lin, H., et al., Privacy-Enhanced Data Fusion for COVID-19 Applications in Intelligent Internet of Medical Things. IEEE Internet of Things Journal, 2021. 8(21): p. 15683-15693.
[57] Ali, A., et al., Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography. 2022. 22(2): p. 528.
[58] Wang, X., et al., A Privacy-Enhanced Multiarea Task Allocation Strategy for Healthcare 4.0. IEEE Transactions on Industrial Informatics, 2023. 19(3): p. 2740-2748.
[59] Houssein, E.H. and A. Sayed, Boosted federated learning based on improved Particle Swarm Optimization for healthcare IoT devices. Computers in Biology and Medicine, 2023. 163: p. 107195.
[60] Sun, L., et al., A federated learning and blockchain framework for physiological signal classification based on continual learning. Information Sciences, 2023. 630: p. 586-598.
[61] Sultana, N., et al., Survey on SDN based network intrusion detection system using machine learning approaches. Peer-to-Peer Networking and Applications, 2019. 12(2): p. 493-501.
[62] West, M.T., et al., Towards quantum enhanced adversarial robustness in machine learning. Nature Machine Intelligence, 2023. 5(6): p. 581-589.
[63] Belhadi, A., et al., BIoMT-ISeg: Blockchain internet of medical things for intelligent segmentation. 2023. 13.
[64] Díaz-Rodríguez, N., et al., Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. Information Fusion, 2023. 99: p. 101896.