Journal of
Cybersecurity and Privacy

MDPI

Review

Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis

Rachida Hireche [1,]*, Houssem Mansouri [1] and Al-Sakib Khan Pathan [2]

[1] Laboratory of Networks and Distributed Systems LRSD, Department of Computer Science, Faculty of Sciences, Ferhat Abbas University Sétif 1, Sétif 19000, Algeria
[2] Department of Computer Science and Engineering, United International University, Dhaka 1212, Bangladesh
* Correspondence: hireche.rachida@univ-setif.dz

Abstract: The Internet of Medical Things (IoMT) has become a strategic priority for future e-healthcare because of its ability to improve patient care and its scope of providing more reliable clinical data, increasing efficiency, and reducing costs. It is no wonder that many healthcare institutions nowadays like to harness the benefits offered by the IoMT. In fact, it is an infrastructure with connected medical devices, software applications, and care systems and services. However, the accelerated adoption of connected devices also has a serious side effect: it obscures the broader need to meet the requirements of standard security for modern converged environments (even beyond connected medical devices). Adding up different types and numbers of devices risks creating significant security vulnerabilities. In this paper, we have undertaken a study of various security techniques dedicated to this environment during recent years. This study enables us to classify these techniques and to characterize them in order to benefit from their positive aspects.

Keywords: authentication; healthcare; IoMT; IoT; internet; privacy; security; security management

check for updates

Citation: Hireche, R.; Mansouri, H.; Pathan, A.-S.K. Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. *J. Cybersecur. Priv.* **2022**, *2*, 640–661. https://doi.org/10.3390/jcp2030033

Academic Editor: Georgios Kambourakis

Received: 25 June 2022
Accepted: 8 August 2022
Published: 17 August 2022

1. Introduction

Various types of medical devices and applications are connected with the aid of Information Technology (IT) in an Internet of Medical Things (IoMT), which is designed to provide healthcare and e-healthcare services. The infrastructure of an IoMT involves various types of communications technologies and, in general, online networks. Wi-Fi technology could enable easy communication that can take place anywhere among the medical devices in such a setting. When cloud platforms are connected to the IoMT devices (for instance, Amazon Web Services), the sensor readings or various types of medical data can be stored and then analyzed.

One of the key objectives of the IoMT is to ensure minimal human intervention during various types of healthcare procedures and routine checkups of patients. For this, the automation of sensors and machine intelligence techniques are used. When invasive (i.e., can be inserted into human body) and non-invasive (implanted or attached to the skin) devices [1] collect enough information about a patient, that reduces the time for doctors to engage with the patient's diagnosis and frequency of hospital visits. Hence, IoMT can also reduce the costs for the patients and increase the efficiency of the healthcare professionals. For instance, it is possible to help sick elderly people by providing new assistance services in smart homes in order to continuously monitor their physiological conditions at a lower cost to detect the possible deterioration in their state of health.

The COVID-19 pandemic has shown the importance of the IoMT [1,2], with quarantine and lockdown measures which often needed remote healthcare facilities. In fact, such a situation has dramatically accelerated telemedicine and telehealth trends. It is expected that, in the coming years, IoMT will have more sophisticated technologies and applications for deeper and more precise diagnosis of diseases, efficient cost savings and faster healthcare added to it.

While the positive aspects of the IoMT are well enumerated in various studies, implementing the IoMT comes with its own set of challenges, the biggest being the security and privacy of the IoMT. Indeed, the medical data are often considered too sensitive and intrusive. Patients may often not like for their medical or health-related information to be leaked. Hence, the responsibility to protect such data is huge. The issue here, however, is that when we talk about IoMT that includes and welcomes various types of devices and applications in the setting; it would also make it more vulnerable to various types of security- and privacy-related attacks. The inadvertent inclusion of a single malicious device or a device run by a rogue entity could be enough to violate the strict requirement of the privacy of patients' information. Again, compromised data can lead to incorrect diagnoses and, thus, incorrect medications and treatment. This could even be life-threatening for targeted individuals such as national leaders or other important people with high influence or value in a society. Enemies could use the IoMT environment to obtain access to sensitive healthcare information and then cause indirect assassinations. Moreover, healthcare professionals could be wrongly accused of intentionally performing wrong treatments or modifying data and so on. Hence, security and privacy are of paramount importance in the IoMT. Indeed, to enable the wider adoption of IoMT, the security of the objects and networks used must be reinforced. Thus, new lightweight and robust mechanisms must be developed to counter the threats and attacks to which IoMT infrastructures are exposed. In fact, in a study, it was shown that the healthcare security market alone is expected to reach USA $8.7 billion by 2023 [3].

If we checked the most recent trends, we would notice that the attack surface is widening every day for the IoMT environment. On one hand, more and more medical devices are being connected to networks. On the other hand, healthcare establishments are a target favored by cyber-hackers, who are very interested in information about personal health —the most sensitive data of high value. Cybercriminals particularly covet this type of data [4] because of their great value and variety (e.g., credit card number, social security number, mailing address, email address, type of disease, medications, blood group type, things that are harmful to the patient, etc.).

In this study, we explored the area of IoMT and mainly focused on security and privacy issues. Some notable works have already been conducted in this domain. We examined and analyzed them and explored the use cases, vulnerabilities and countermeasures, solutions, and recent challenges, and then commented on the future direction of studies in this area. This study is a synthesis of what has been performed in the field of IoMT in the last few years, intended for relatively new researchers in this field, as well as for those who are interested in learning about recent advances and limitations of IoMT security issues and their solutions using new technologies. On the other hand, the comparison between different solutions based on new technologies provides a general overview of the future direction of security and privacy research in the IoMT field.

This paper is structured in ten sections. In Section 2, we introduce the context and architecture of IoMT systems. Section 3 defines the important communication protocols in the IoMT. In Section 4, we present IoMT-related technologies. In Section 5, we describe the security requirements to ensure reliability and robustness against various attacks. Then, in Section 6, we discuss different attacks against the IoMT system and classify them according to the presented IoMT architecture. Section 7 defines the categories of devices in the IoMT system and provides a classification of these devices based on their usage. It also presents the potential attacks against these devices. In Section 8, we review the IoMT security model. The classification and comparison between the different security schemes are shown in Section 9, before the paper is concluded in Section 10.

2. Architecture of IoMT

Not all applications and technologies use the same IoMT architecture. This is important to know before studying various aspects of IoMT. Each technology has its own set of guidelines and often claims to be the best [5] (for a particular case). Existing IoMT systems [6] typically have three main layers as shown in Figure 1: perception, network, and application. These layers include all the stages through which data pass, from the collection of patient information via sensors and wearable devices to the storage, analysis, and visualization stage by the patient and medical staff.

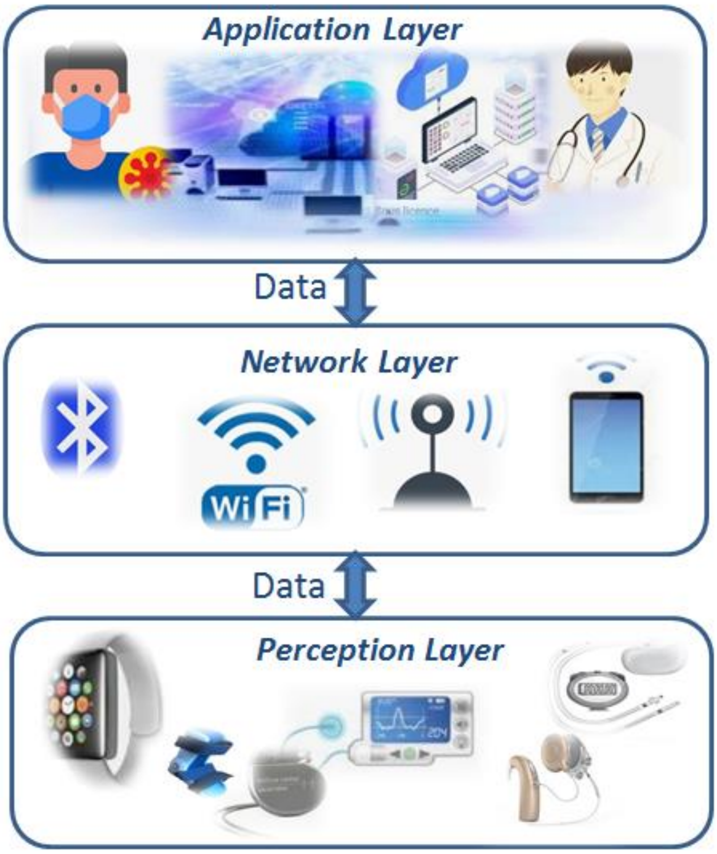

Figure 1. IoMT architecture.

The perception layer is the foundational layer of the IoMT architecture. This layer ensures the precise sensing of the parameters related to health issues [7]. Different types of sensors, especially those that can be implanted or attached to the body, such as a pacemaker, smart watch, etc., could be used to read and collect data about the patient(s). The collected data are transmitted as raw values, i.e., without any processing, via different communication technologies to the network layer [8]. This second layer forwards the data to the processing units (i.e., cloud) through the IoT gateway [9]. Next, the cloud basically performs the analysis. If some changes are detected for the patient's health data, this would carry important meaning [10]. The changes are then transmitted to the application layer and presented through remote monitoring, such as in a smartphone or a dedicated Access Point (AP), to the physicians for emergency response (such as, quantity, prescription or change of dosage of different medications) and to the patient(s) or for any further actions.

3. Communication Protocols in IoMT

With the increase in the number of smart devices present in IoT environments, especially for IoMT systems, the need to allow them to communicate quickly emerged. Again, to meet resource constraints (network, processing, storage, energy), new technologies and communication protocols have been developed or adapted to fulfil certain needs, such as low consumption and a large range, but also ease of implementation. Among the most important of these protocols, we mention ZigBee, Bluetooth, 802.11ac, Z-Wave, LoRaWAN, and Sigfox. Table 1 summarizes the main differences between these different communication technologies [11–13].

Table 1. Differences between different communication protocols in IoMT.

Protocol	ZigBee	Bluetooth	IEEE802.11ac	Z-Wave	LoRaWAN	Sigfox
Debits	250 kbps	2 Mbps	433–1300 Mbps	100 kbps	0.3–50 kbps	1 Mbps
Range	10–100 m	10–100 m	35 m (inside) and 300 m (outside)	30 m (inside) and 100 m outside)	20 km (rural area) and 8 km (urban area)	50 km (rural area) and 10 km (urban area)
Frequency	2.4 GHz	2.4 GHz	5 GHz	868 MHz (EU) 908 MHz (USA)	868 MHz (EU) 915 MHz (USA)	868 MHz (EU) 902 MHz (USA)
Security	AES 128 bits	AES 128 bits	WEP-WPA (AES 128 bits)	AES 128 bits	AES 128 bits	Partially addressed

The setting that we are discussing requires maintaining the maximum level of reliability for communications among the devices, as there could be thousands of Internet-connected devices of various types and resources. It is quite impossible to strictly regulate the types, models, and vendors of the users' and hospitals' used medical devices. Hence, there could often be critical differences among the devices. Therefore, an adaptable layered design is required. Various approaches for IoMT architectures and layers have been presented in the literature, including those that depend on the three aforementioned layers (if we project the IoMT system onto the Open Systems Interconnection, OSI reference model). We show, in Table 2, the primary protocols used in IoMT systems at the levels of each layer.

3.1. Perception Layer

The IEEE 802.15.4 standard [14] is the basis for the protocols at the perception layer. This standard is responsible for specifying the physical (PHY) and media access control (MAC) layers for many types of devices with minimal complexity, cost, and battery consumption limitations. Several IoMT-related protocols, such as 6LowPAN, ZigBee, and ISA 100.11a [15], are compatible with the IEEE 802.15.4 standard. To gather clinical data from sensors, healthcare systems employ several perception-layer protocols such as the Radio Frequency Identification (RFID) protocol, Near Field Communication (NFC) protocol, Bluetooth/BLE (Bluetooth Low Energy), Z-Wave, and Ultra-Wideband (UWB) protocol [16].

3.2. Network Layer

The majority of protocols at this layer are based on the IEEE 802.15 standard [17]. The network layer is in charge of sending and receiving medical data. As a result, this layer acts as the foundation for the healthcare platform's architecture. Network security is a huge problem in healthcare [18], since these network devices and communication lines/channels transmit sensitive data. At this layer, the most popular protocols for IoMT are WiFi and ZigBee. Bluetooth is also utilized; however, it is used less frequently since it cannot reach large areas such as hospitals. Technologies such as LoRaWAN and 6LoWPAN (IPv6 over Low-power Wireless Personal Area Networks) related to Wireless Sensor Networks [19] can also be utilized in some cases. Conventional cellular communication technologies (such as 3G/4G/5G or GPRS-General Packet Radio Service) can be utilized for data transfer over a considerable range.

3.3. Application Layer

The application layer is dedicated towards managing the smart medical platform. This includes customized interfaces and role-based control panels for diagnostic decision making. After collecting information from other layers, the application layer can transform the information into a suitable form that can be processed by the end-devices and medical servers [20]. The most commonly used application layer protocols are medical-data-encoding protocols such as HL7 (Health Level Seven) and XML (Extensible Markup Language) encode [21], CoAP (Constrained Application Protocol), MQTT (MQ Telemetry

Transport), and HTTP (Hypertext Transfer Protocol) secured with Transport Layer Security (TLS) [22].

3.4. Protocol Range and Data Transmission Rate in IoMT

Based on the technical information presented in [23], here we will make a comparison between the different protocols used in the healthcare systems, based on the range and data transmission rate.

- **Short-Range protocols:** ZigBee provides a mesh network structure. When it comes to setting and planning device energy use, ZigBee is easier than 6LowPAN. ZigBee also outperforms alternative protocols such as Z-Wave in terms of device hopping and energy usage [23]. In contrast to ZigBee networks, 6LoWPAN networks appear to have lower latency and packet loss rates, which make them suitable for medical services. When comparing 6LowPAN implementations in medical contexts to BLE implementations, a relevant research work [24] reveals that 6LowPAN is more efficient when employing IP-based applications, albeit there are connection concerns when barriers are present. When it comes to network communication, 6LoWPAN devices interact directly with one another, whereas LoRaWAN data is sent through gateways and routers. On the other hand, Z-Wave has a longer optimal range than ZigBee and 6LowPAN due to its sub-1 GHz band—this communication band also allows Z-Wave to have less interference. The disadvantage is its lower data-transmission rates.
- **Long-Range protocols:** For long-range protocols with low power consumption such as LoRaWAN and LTE-M (Long Term Evolution Machine Type Communication) networks, the main LPWAN (Low Power Wide Area Networks) technologies can also provide long-range connectivity of 10 km distances using subgigahertz (GHz) radio frequencies, even on a global scale as LTE-M networks provide a robust infrastructure and built-in security mechanism that can support most applications [25]. These technologies offer the manufacturers of connected objects to communicate data over long distances with low power consumption. Despite the need for specific hardware, LTE-M offers the best compromise between throughput and autonomy, which makes it ideal for multiple domains, including healthcare.

Table 2. The primary protocols used in IoMT systems at various levels.

Layer	Communication Protocols	Range Type	References
Perception Layer	RFID, NFC, Bluetooth/BLE, Z-Wave, UWB	Short-Range	[26,27]
Network Layer	IPV4, IPV6 protocols (for network addressing) For routing RPL, CARP, and CORPL protocols (for network routing) TCP, UDP, 6LoWPAN, WIA-PA	N/A	[28,29]
	NFC, RFID, IEEE 802.11 (Wi-Fi), IEEE 802.15.1 (Bluetooth), IEEE 802.15.4 (ZigBee),	Short-Range	
	LPWAN (LoRaWAN and LTE-M)	Long-Range	
Application Layer	HL7, CoAP, DSS, MQTT, HTTP, HTTPS, TLS	N/A	[30,31]

4. IoMT-Related Technologies

Wireless Sensor Networks (WSN) and Radio-Frequency IDentification (RFID) systems are two key IoMT technologies. In recent years, their integration with smart objects has offered new communication capabilities. Due to their benefits and use in IoT, we present them in brief in this section.

4.1. Wireless Sensor Networks (WSN)

A WSN consists of a set of self-powered sensor nodes with wireless computing and communication capabilities. The autonomous sensors often have limited energy resources and are capable of collecting, processing, analyzing, and disseminating information via radio waves (e.g., via ZigBee technology). A sensor node is usually composed of information-capture interfaces, a microprocessor, a memory unit, a communication interface, and a battery as a power source (Figure 2). These sensors can be attached to objects/persons or deployed in the environment according to the needs. There are several types of sensors depending on the phenomena monitored or the type of data such as temperature, humidity, position, or light sensors [12,23,32].

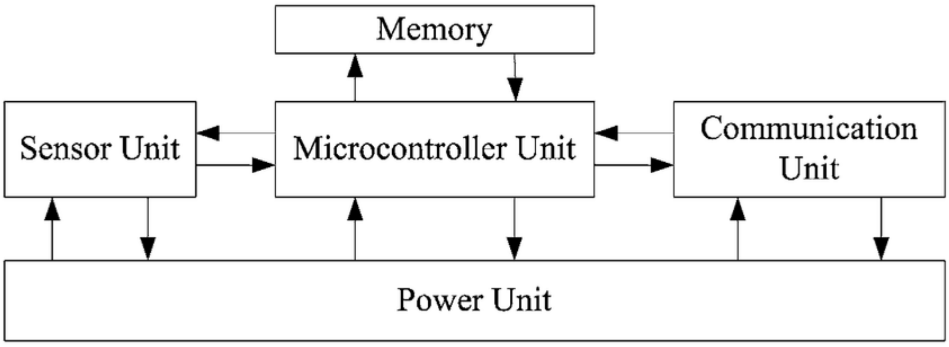

Figure 2. Sensor Architecture.

In a medical environment, sensors have become indispensable today, including in smart homes because they can be used to measure physical parameters of the monitored person (i.e., a patient) such as heartbeat, blood pressure, body temperature, and brain signals. The information collected and sent back via the network to the cloud is then processed and analyzed by the system before being transferred by the cloud via the Internet to the various actors (doctor, emergency services, etc.). This type of network, therefore, allows health professionals to remotely monitor the patient on the basis of the information received.

4.2. RFID Technology

The RFID technology allows, via radio frequencies, the automatic remote identification of objects equipped with RFID tags. An RFID system is mainly composed of two entities, which communicate between them, the reader (also called interrogator) and the label (also called “tag”). In its passive version, the reader will interrogate the tag via radio waves and the tag will then use the electromagnetic energy carried by the received signal to power itself and, at the end of the processing, to send its data in response to the reader [26,33,34].

RFID remains a promising technology for the implementation of smart health systems. Moreover, in addition to being a founding technology of the IoMT, it is an effective way to uniquely identify and manage objects. The use of RFID technology in the healthcare sector allows healthcare providers to facilitate decision-making and the accomplishment of tasks that are usually difficult in a complex clinical environment.

5. IoMT Security Requirements

We have already noted that security is of paramount importance for medical devices that are supposed to be used for wireless communications and remote communications for the healthcare or e-healthcare services. If there is any weakness or point of information leakage from the IoMT devices due to poor methods of authentication and access control, the entire setting can be seriously harmed both by incoming and outgoing data [35]. It is a fact that most of the IoMT devices do not have sufficient capability to detect and prevent attacks on their own. Hence, security measures must be implemented/deployed at strategic points of the entire network or system. Otherwise, the attackers who use sophisticated and often novel methods can easily evade security measures and gain unauthorized access to patient data [2]. Here, we present the security requirements for IoMT healthcare network infrastructures. We know the type of data that we would need what kind of protection is well defined within the CIANA (Confidentiality, Integrity, Availability, Non-Repudiation, and Authentication) considerations [9,36,37]. We discuss the requirements in light of CIANA and other aspects as described below.

- **Confidentiality**: In the context of the IoMT, confidentiality is about protecting the medical information that the patient shares with the personal physician or medical staff [19,38]. Such data must be protected from intrusion, eavesdropping, or from rogue entities that may harm the patient or use the medical information against him. While the standards give some general guidelines, the presence of network access control and data encryption is essential for guaranteeing the property of confidentiality for IoMT [9].
- **Privacy:** It ensures that patients' private data are protected against disclosure and attempts to exploit them illegally [15]. Currently, there are certain enacted rules in many countries for the collection and storage of patient's health data for privacy regulations. For instance, General Data Protection Regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) [2,39]. The IoMT system enforces these privacy regulations and allows users to access their private data.
- **Integrity**: Data integrity is a necessity for IoMT healthcare systems. It protects patient data from being altered or deleted by unauthorized parties; this primarily ensures that the data arrives at its intended destination without being altered during wireless transmission [40] and also remains unaltered via any unauthorized means when at rest. Healthcare organizations are more conscious of the necessity of data integrity than ever before. As data represent diagnoses, treatments, and health statuses, data integrity is critical in healthcare [38]. In this context, this property can also be defined as the capacity to identify unlawful data tampering or distortion that causes permanent damage [41]. To prevent hostile attempts from modifying sent data, proper data integrity safeguards must be included.
- **Availability:** Availability is the ability of servers and medical equipment to make services and data available to users when they need it [42]. It is an important component in healthcare systems, especially when a patient's health must be monitored on a continual basis. As a result, in order to assure availability, the system must be updated to offer suspect data storage or transmission channels in the event of DoS/DDoS (Denial-of-Service/Distributed Denial-of-Service) assaults, as well as to strengthen its permanence and capacity to promptly resolve any issues [41].
- **Non-Repudiation:** This is the ability to hold any authorized user responsible for his activities. Simply expressed, non-repudiation guarantees that no system activity may be rejected [9]. This criterion prevents authorized users from canceling earlier system commitments or activities [38]. This metric measures the system's capacity to confirm the existence or absence of an action. To simplify even further, an entity cannot deny completing a task after completing it and must take responsibility for any action or its consequence. The easiest approach to achieving this criterion is to use digital signature techniques [9].
- **Authentication:** When a user logs into the system, the user's identity should be verified. Message authentication, on the other hand, is the act of confirming that a user is the original source of the provided data from a previous time. Mutual authentication is the most secure type of security; before transferring secure keys or data, the client and server must first authenticate each other. Lightweight authentication algorithms are becoming increasingly common as a result of a shortage of memory capacity in certain IoMT devices or a lack of CPU (Central Processing Unit) strength to conduct the cryptographic operations required by classic authentication protocols [14].

- **Authorization:** As mentioned before, medical data must be protected from unauthorized access due to the sensitivity of such data [43]. Hence, in our context, only trusted parties (with the required skill or expertise) should be given permission to complete certain actions, such as giving commands to medical IoMT devices or updating the software or installing security patches on medical IoMT devices.
- **Anonymity:** When unauthorized users engage with the system, this requirement guarantees that the identity of the patient or physician stays concealed, i.e., both the patient and the physician should remain anonymous. When a patient and a physician are communicating, their identities should not be revealed [35]. Passive attacks are only able to observe what a person does, not who a person is.

6. Classification of Attacks in IoMT

IoMT applications rely on a wide range of technologies with different types of embedded features, each of which has its own set of security vulnerabilities [31]. Hence, many widely used IoT protocols now lack fundamental security procedures. There are various types of attacks that not only compromise the patient's privacy, but can also cause irreparable financial and reputational damage [41]. As a recorded case, in October 2016, an IoT botnet conducted a DDoS attack on a DNS (Domain Name System) service provider. Mirai was the malware employed by the botnet. Large parts of the Internet, including Twitter, the Guardian, Netflix, Reddit, and CNN, were shut down as a result of the latter [44]. According to a recent Comparitech report, these attacks have cost the healthcare industry more than $160 million since 2016 [44,45]. It was also alleged that attacks on brain implants result in death [45]. The number of ransomware attacks against healthcare organizations increased by 94 percent between 2021 and 2022 according to a report from cybersecurity firm Sophos. More than two-thirds of U.S. healthcare organizations reported experiencing a ransomware attack in 2021; according to the study, this was up from 34 percent in 2020 [46]. Table 3 displays the attacks classified according to the IoMT's targeted layer and their influence on the system's security requirements. As a result of the heightened danger of a cyber-attack on the IoMT system, the creation and development of robust security solutions has become necessary.

Table 3. IoMT potential attacks for each layer and their influence on the system's security requirements.

Type Layer	Attack	Brief Description	Effects	References
Perception	**Side-channel attack**	The information is obtained from the side channels of the encryption device.	Confidentiality, Integrity	[47,48]
	Tampering devices	The IoMT device is physically accessed to modify the data (modification in a device using RFID or communication link).	Confidentiality, Integrity	[49]
	Tag cloning	An attacker might exploit data obtained through a successful side-channel attack or replicate data from a previously used tag. The cloned tag, for example, might be used to gain access to an unlawful facility or data, such as medical data (Using simple technologies, attackers may clone RFIDs).	Confidentiality, Authorization, Integrity	[50]
	Sensor tracking	This form of attack invades patients' privacy. Attackers might obtain access to patients' whereabouts or fake GPS data by using unsecured equipment. Other sensors, such as those used in fall detection, wheelchair management, and remote monitoring systems, can also be utilized to divulge sensitive data about patients.	Confidentiality, Authorization, Integrity, Privacy	[51]

Table 3. *Cont.*

Type Layer	Attack	Brief Description	Effects	References
Network	**Eavesdropping**	An attacker intercepts and tracks the necessary hardware and communication to capture data. Data obtained in this manner (unlawfully) can be utilized in a variety of ways.	Confidentiality, Non-repudiation, Privacy	[50]
	Replay	An attacker can use an authentication message that was previously transmitted between two legitimate users. In this situation, an attacker can intercept a signed packet and send it back to target multiple times.	Authorization	[52,53]
	Man-in-the-middle	It's a cyber-attack that targets two IoMT devices' communication and gains access to their private data. The attacker can listen in on or monitor the communication between the two devices in this attack. The attacker can alter the intercepted data before they are transmitted to their intended destination.	Confidentiality, Authorization	[54]
	Rogue access	A fake gateway is placed inside the wireless network range in this attack to give genuine users access and intercept traffic.		[55]
	DoS/DDoS	Unlike DoS attacks, which are carried out by a single node, a DDoS attack is carried out by several sources, flooding a specified target with messages or connection requests with the purpose of rendering the service inaccessible to legitimate users.	Availability	[56,57]
	Sinkhole	A malicious node attracts traffic in this attack by offering a better connection quality. Once the attack is successful, other attacks (such as eavesdropping or selective forwarding) can be launched, in which the malicious node isolates specific nodes by discarding packets that pass through them.		[35]
	Sniffing	Data transferred between two nodes is passively intercepted by sniffing attacks. Due to the fact that the attacker can observe the data passed between the system's layers.	Confidentiality	[58]
	Selective Forwarding	A malicious node may simply change, drop, or selectively forward some messages to other nodes in the network. As a result, the information received by the destination is incomplete.	All	[52,59]
Application	**Brute Force**	The attackers usually use automated tools to create multiple password combinations until they succeed. The dictionary attack is an example of a serious vulnerability for IoMT devices.	Confidentiality, Integrity	[60,61]
	SQL injection	An SQL injection attack involves introducing a faulty SQL statement into the application's backend database. A successful SQL injection attack can compromise or change sensitive patient data.	All	[58,62]
	Account hijacking	At the network level, many IoT devices communicate in transparent text or with insecure encryption. Intercepting the packet when an end user is authenticating allows an attacker to undertake account hijacking.	Confidentiality, Integrity	[43]
	Ransomware	Ransomware encrypts important information and demands a large fee to unlock it. In return for money, attackers can encrypt sensitive data such as health information and keep the decryption key.	Integrity, Availability	[35]

7. IoMT Devices and Potential Attacks

IoMT systems can be useful for a wide range of medical conditions. In the IoMT, smart medical devices are classified into four categories based on where they are used on the human body [63].

- **Implantable Medical Devices (IMDs):** These are devices that are implanted to replace or sustain a biological structure that is absent or damaged. Furthermore, an IMD can be utilized to improve a biological structure that already exists. The primary function of such implanted devices is to monitor and transmit signals from the patient's body to other medical systems [63]. They are primarily composed of small wireless modules and health sensors that capture information such as temperature, mobility, blood glucose, and blood pressure. The pacemaker, for example, can be particularly beneficial for managing aberrant cardiac rhythms [64], and infusion pumps, such as enteral, PCA, and insulin infusion pumps, can be utilized in a range of therapies [32,65]. Infusion pumps have been linked to a number of patient-safety issues. As a result, authentication procedures need to be developed [66]. Although a wireless connection may enhance the security risks associated with these electronic devices, it is nevertheless the most preferred communication method for their installation [11].
- **Internet of Wearable Devices (IoWDs):** These devices are worn by people to track their biometrics, which may help them improve their overall health. This category includes a variety of IoMT systems. Examples could include EEG (electroencephalography) and ECG (electrocardiography) [67,68]. As we know, EEG can be used to monitor and record brain activities while an ECG can monitor the condition of the heart's rhythm and electrical activity. Other examples could include, for instance, smart watches that are quite popular nowadays for monitoring biometrics such as heart rate and movement; fitness trackers; activity, accelerating, and respiratory rate sensors [32,69]; and so on. However, due to battery-life limitations and sensor accuracy, these devices are unlikely to be used to replace IMDs in critical situations [12].
- **Ambient Devices:** Although ambient devices are not used for patient treatment and monitoring, they sense the patient's environment to monitor patterns of activity and manage environmental conditions near the patient. They include [70] patient identification devices, motion detection devices, monitoring devices, implantable device chargers, and alarm devices.
- **Stationary Devices:** Devices that are not generally carried by the patient are classified as stationary devices. Although such devices were previously unconnected, they may now be managed remotely to enable telemedicine treatments [71]. Examples of stationary devices include imaging devices (such as, magnetic resonance imaging (MRI), computerized tomography (CT) scanners, and X-rays) and surgical devices [72].

Low-power wireless network technologies (such as Bluetooth or Bluetooth/BLE, NFC, Zigbee, Z-Wave, and RFID) are commonly used to communicate between the body network and the personal server. Bluetooth is mostly used in wearable devices, while RFID and NFC use a short-range, low-power communication topology. Therefore, they are frequently used in implanted devices [73,74]. On the other hand, long-range wireless technologies such as Wi-Fi, LoRa, and GSM are used by the IoMT system to provide the connection between the personal server gateway and the medical server. Different network attacks can compromise IoMT devices. This is due to a lack of standards and security controls in device production, as well as the nature of the devices and the IoMT network. Memory space, energy, and low power limits preclude them from supporting the calculation of typical cryptographic security methods. Furthermore, as the IoMT network is heterogeneous and uses multiple protocols at each layer, a single security solution will not work for all devices. Table 4 shows the device categories, their locations, examples for each category, and potential attacks. In the table, we have used '✓' (tick) and 'N/A' to mean whether an attack is possible to be launched or not.

Table 4. IoMT device categories, their locations, examples for each category, and potential attacks.

Device Type		**Implantable Medical Devices**	**Internet of Wearable Devices**	**Ambient Devices**	**Stationary Devices**
Device Location		In human tissues	On the human body	Close to the human body	Inside treatment rooms and hospitals
Examples of Devices		Pacemaker, deep brain implants, insulin pump	EEG and ECG, fall detection band, blood pressure monitors, smart watches, accelerating sensors, respiratory rate sensors, fitness trackers	Motion sensors, pressure sensors, vibration sensors, gyroscope sensors, daylight sensors, and pressure sensors	Imaging devices (such as, MRI, CT scanners, and X-rays) and surgical devices
Perception Layer Potential Attacks/Difficulty	**Side channel**	✓	✓	N/A	✓
	Tag cloning	N/A	✓	N/A	N/A
	Tampering devices	N/A	✓	✓	✓
	Sensor tracking	✓	✓	N/A	N/A
Network Layer Potential Attacks/Difficulty	**Eavesdropping**	✓	✓	✓	✓
	Replay	✓	✓	✓	✓
	Man-in-the-middle	✓	✓	✓	✓
	Rogue access	✓	✓	✓	N/A
	DoS	✓	✓	✓	✓
	Sinkhole	✓	✓	✓	N/A
Application Layer Potential Attacks/Difficulty	**SQL injection**	✓	✓	✓	✓
	Account hijacking	✓	✓	✓	✓
	Ransomware	✓	✓	✓	✓
	Brute force	✓	✓	✓	✓

8. IoMT Security Model

During the last decade, several researchers have concentrated on IoMT security challenges and solutions. Two of the key technologies considered for such an environment are Blockchain and Artificial Intelligence (AI). The objective was mainly to ensure secure transactions and data processing at the cloud layer [75]. As these two technologies showed promise to secure the financial sector, a similar level concern has been considered for IoMT. Blockchain technology is employed in IoMT systems as a security-management solution for sharing information between patients and other parties, such as doctors. Intrusions or unusual activity in patient data and network traffic can be detected by AI systems. This section of the paper examines the critical aspects of some of the most recent research works on IoMT systems. The selection of studies reviewed is based on the most current, relevant studies that best meet the security and privacy criteria of the IoMT system, as well as the different ways various technologies are used to meet them.

8.1. Blockchain Models

Pournaghi et al. [76] proposed a secure scheme which they named as “MedSBA”. It includes the application of attribute-based encryption methods combined with blockchain technology for sharing and storing medical data among patients, hospitals, and other stakeholders. This scheme applies two types of attribute-based encryptions, KP-ABE (Key-Policy Attribute-Based Encryption) and CP-ABE (Ciphertext-Policy Attribute-Based Encryption), to control patients’ access to their own medical data. It also includes two PBFT (Practical Byzantine Fault Tolerance) consensus-based private blockchains in two forms: permissionless and permissioned. The former is used to distribute public medical information and the structure for the authorized access to medical data, and the latter is to set the information of key and storage places on the cloud-storing systems. The system’s functionality was proven using BAN (Burrows–Abadi–Needham) logic, while the security was proven using formal design. Simulating MedSBAs with OPNET software demonstrates the system’s efficiency in terms of computing complexity and storage. However, the system did not facilitate the exchange of cryptocurrency for data sharing between data-consumer organizations and individuals.

Garg et al. [77] designed an authentication key agreement scheme termed as "BAKMP-IoMT", based on blockchain for the IoMT environment. It provides secure key management for cloud servers, personal servers, and medical implantable devices. Furthermore, the system enables secure access to critical healthcare data and guarantees that only authorized individuals have access to it. Legitimate people can also securely access healthcare data via cloud servers. This is accomplished by keeping all sensitive healthcare information in a blockchain that is managed by cloud servers. To demonstrate the system's ability to withstand many types of hypothetical attacks, a comprehensive formal security study has been performed using a widely recognized automated tool, AVISPA (automated validation of Internet security protocols and applications), as well as formal and informal security analyses. BAKMP-IoMT is compared with other existing schemes, and it also performs better in terms of security and functionality, lower communication and communication costs for authentication, and key management phases compared to other schemes. In addition, the simulation of BAKMP-IoMT is performed to demonstrate its impact on performance parameters.

Tahir et al. [78] proposed a lightweight framework for authentication and permission to complement current blockchain-based IoT networks in the healthcare sector. The authentication method, which is bound by conditional joint probability, employs random numbers. This enables the system to create a secure link between IoT devices for data collection. Extensive simulations with the AVISPA tool and the Cooja simulator are used to assess and evaluate the suggested model. The technology improves access control while also providing excellent mutual authentication. When weighed against each other, it also minimizes transmission costs and computing overheads, as seen in the testing findings. The suggested framework, on the other hand, is not assessed on hardware in a realistic context, making it less efficient (or its practicality is still questionable).

Xu et al. [79] proposed a blockchain-based privacy-preservation scheme (Healthchain) for large-scale health data. This scheme encrypts health data using fine-grained access control. In particular, the user transaction is used for key management that can allow users to add or revoke authorized physicians. In addition, it introduces two blockchains to avoid medical disputes, such as physician diagnoses. The IoT data cannot be modified or deleted once stored in the blockchain. The results of the experiment and security assessment confirmed that the system can meet the expected security requirements and can be applied to mobile health systems. However, insider attacks are neglected by the system.

8.2. Authentication Model

Deebak and Al-Turjman [80] presented the smart service authentication (SSA) framework to cross-examine the communication entities' common secret session key and improve mutual authenticity. It provides an authentic signature for conducting encrypted transfers between communication nodes and ensuring enhanced data security between the patients and physicians. Formal and informal verifications were used to investigate the security attributes. The suggested SSA framework has been implemented utilizing a Field Programmable Gate Array (FPGA) and Moteiv TMote Sky-Mote to demonstrate the system's security and performance efficiency. The importance of the SSA framework model's ability to withstand security threats such as health-report forgery, health-report reveal, server-spoofing, and so on is demonstrated by formal and informal security analysis. As a result, it is shown to be a good fit for the telecare medical information system (TMIS).

Lone et al. [13] proposed a secure communication scheme for medical applications utilizing Attribute-Based Encryption (ABE) for authentication in a Heterogeneous Network (HetNet) at the network layer. Health-related information is protected using ABE. This not only reduces transmission costs, but also protects health data from intruders [21]. It incorporates a third-party server that assists in the authentication and storage of patient data. A high-level protocol-specification language (HLPSL) is used to implement the complete security method. The AVISPA automated tool is used to validate the system codes. However, in this scenario, the users communicate through a third-party trusted authority. If this third party is hacked, all the data become subject to hostile attacks.

Yanambaka et al. [81] proposed a lightweight and robust authentication scheme based on the physical unclonable function (PUF) for IoMT. This technique does not save any data from IoMT devices in server memory. In this mechanism, the devices are completely authenticated within 1.2 to 1.5 s. A hybridized oscillator arbiter PUF is used to accomplish system validation. Based on the PUF used during system validation, the number of keys used for authentication was around 240. As the technique is lightweight, it may be used in a variety of designs to enable scalability and resilience. However, the system failed to verify that the client could authenticate the server's communications.

Xin et al. [82] proposed a multimodal biometric identification approach for IoMT. The system's effective matching technique was based on the Fishers vector's secondary calculation (FV). In addition, the system made use of three biometric techniques: finger vein, fingerprint, and face. These methods are combined at the feature level. Again, the system used a bogus feature in the feature fusion process, which often occurs in the real world. The liveness detection is added to the system, which uses DCT (Discrete Cosine Transform) to determine whether the image is genuine or false, and then removes the fake image to improve the system's robustness. The developed framework shows a relatively higher recognition rate. When compared to unimodal biometric systems, which are particularly important for an IoMT platform, it provides superior security. However, the system's accuracy ratings still remain low.

8.3. Privacy Model

Cano and Cañavate-Sanchez [83] proposed a novel method to include a dual signature in the elliptic curve digital-signature algorithm (ECDSA) for IoMT systems. Using edge-computing servers, this system preserves the confidentiality of data transmitted from the IoMT to the cloud. In particular, the captured health data is hidden by the edge device, and the identity of the IoMT devices, namely wearable or smart devices, remains anonymous to the cloud. Since this solution is based on the elliptic-curve cryptography (ECC) approach, its implementation on IoMT devices was feasible and affordable. This technique confirms that, while the anonymity of the data source is ensured from the cloud perspective, the integrity and authentication of the origin of the collected data is also ensured. In addition, the computational requirements and complexity are minimized.

Gull et al. [84] proposed a reversible dual-frame data-hiding technique with high capacity for IoMT-based networks. Initially, the Huffman coding scheme was used to preprocess the captured secret data. A codebook of "d" bits is generated after the Huffman coding to encode the indices which are decimal values. For double steno-image acquisition, the value of the indices is divided into two parts and embedded in two images similar to each other. Although the scheme showed a very high payload, it maintained the perceptual quality at a high level. The scheme provides an average improvement in *embeddability* of 33.2%, with a signal-to-noise ratio (SNR) improvement of 1.32%. The average structural similarity index (SSIM) value is 0.8873. A significant improvement was offered by the system and was also computationally efficient, which allowed it to be used in the IoMT network. However, there was no effective strategy to control the underflow and overflow problems.

Huang et al. [85] proposed a practical system that reliably authenticates patients with noisy ECG signals and simultaneously provides differential privacy. With respect to the current motion status, the system can identify the motions and adapt the algorithm. By ensuring indistinguishability, the privacy of ECG patterns has been protected. This system preserves the speed of authentication by implementing lightweight online algorithms. On the other hand, it effectively disaggregates noise from ECG signals to ensure reliable authentication. It ensures indistinguishability via differential privacy to prevent adversaries from deducing patients' ECG information. This system also improves accuracy by applying soft thresholding while maintaining the claimed privacy guarantee. Online datasets were used to evaluate and validate the effectiveness of the system. In addition, a pilot study on human volunteers was conducted to validate the system. However, the system was not scalable enough for the attack.

Wang et al. [86] investigated an efficient blind-batch encryption scheme based on the Computational Diffie–Hellman hypothesis, which has been shown to be secure. For secure and privacy-preserving medical services in Smart Connected Health (SCH), the scheme used a protocol. With six classical attacks, the system analyzed the protocol and ran the prototype on the Intel Edison platform. Experiments revealed that the system was effective for "cheap" communication protocols and resource-constrained devices. For storage-limited devices, the system could require a high cost.

In a recent work, Ahamad and Pathan [2] consider the confidentiality issue for message exchange in the IoMT environment and propose SPMHF (Security and Privacy-aware Mobile Healthcare Framework). Alongside confidentiality/privacy, the mechanism ensures the integrity of the message, offers the strategy of audit control and ensures patient authentication, access control, data availability, transparency, and freshness of health data. To add more to these, the framework requires taking the patient's consent for allowing information exchange. In this work, the HIPAA standard is strictly maintained, and the authors show that several known attacks could be thwarted in that kind of environment.

8.4. Machine Learning Model

In order to predict the different patterns of attacks in deep brain stimulation (DBS), Abdaoui et al. [87] built a full prototype of an embedded system to lessen the attacks on these devices. This system does not only distinguish real alarms from fake ones, but it also classifies the different attacks using deep learning and Raspberry Pi3. Deep learning has been proved to indicate an accuracy of 97% in learning and predicting false signals. The feasibility of real-time attack-detection can be clearly demonstrated when this system is deployed on a cloud.

Ben Amor et al. [88] proposed an anomaly in terms of data detection and a separation approach designed for smartphone healthcare, called AUDIT. A pre-processing phase and a real-time processing step were used in the study. Using PCA (Principal Component Analysis) and correlation coefficient, the feature was selected and extracted. This allows the system to detect erroneous physiological measurements and to distinguish between real and false medical features.

Priya et al. [89] classified networked assaults using a hybrid PCA-GWO (Principal Component Analysis-Grey Wolf Optimization) technique for selecting features and a deep neural network (DNN) classifier. The proposed solution is suitable for IoMT devices with a single IP address. The input data was preprocessed using the One-Hop coding strategy. The two algorithms were then applied successively for data reduction, followed by prediction using well-known classifiers. The proposed model outperformed and outclassed other current learning algorithms, with a 15% gain in detection accuracy and a 32% reduction in training and classification time.

As a system to detect possible intrusions, Manimurugan et al. [90] proposed a Deep Belief Network (DBN) algorithm model. In that study, the metrics they used were F1 score, precision, recall, and detection rate, as well as accuracy. In comparison to other techniques, the proposed model obtained positive results for all variables. This model is claimed to have the possibility of being extended to detect different attack patterns against both various databases and IoT devices. For the normal class, the proposed method obtained 99.37% accuracy; for the Botnet class, it reached 97.93%; for the Dos/DDoS class, the percentage was 96.67%; as for the Port scan class, it was 97.71%; 97.71% for the Brute Force class, 96.37% for the Infiltration class; and finally, the method was able to obtain 98.37% for the Web attack.

To obtain features from the ECG signal, and thus reduce the computational cost, Barros et al. [91] used only the fiducial points detected during signal capture. For classification, a number of machine-learning approaches were applied. The results of the evaluation reveal that the suggested solution is efficient because of its accuracy of more than 98.2% in the continuous authentication and identification scenario and reduced complexity using less than 10 features. This appears to be a viable approach for improving the security of many critical services and applications.

9. Classification and Comparison

Throughout this study, a systematic review of literature was conducted on the privacy and security issues of IoMT as well as the different ways that various technologies are used to address them. By analyzing the results of the study, including the technologies and tools used, the benefits, evaluations and limitations of each proposed solution, Table 5 provides a classification and comparison between the security schemes discussed in the security model. This comparison provides a general overview of the future direction of privacy and security research in the field of IoMT. From this review, we can conclude that numerous schemes are published to secure IoMT devices. Most of these studies concentrated on securing the network layer of the device or the body since intrusions into devices such as IMDs can have a serious effect on the patient's health and life. Some suggested solutions to secure these devices are device authentication, sensor anomaly detection, and access control. In addition, studies which used attack and malware detection strategies observed and studied how to secure the network layer. The findings also show that the blockchain, the ECC algorithm, and light-weight authentication are the best for security in comparison to traditional algorithms. We concluded that traditional ML techniques may not be efficient enough when given metrics are not considered (such as time complexity, energy consumption, and resource complexity) [90]. We have also noticed that most studies ignore these criteria and do not take them into consideration when evaluating their proposed models. Therefore, how to use ML in an appropriate way to fit the nature of IoMT had better be the focus of future studies in this domain. Nowadays, as IoMT devices often find the authentication process computationally intensive, the present research direction is headed to apply lightweight mechanisms with the use of physiological data from sensors to decrease the computational load on the device [91]. Table 5's comparison provides a general overview of the future direction of security and privacy research in IoMT.

Table 5. The summary of the studies reported on the security and privacy model.

Security Model	Ref	Technologies and Techniques Used	Security Requirement	Benefits of the Proposed Scheme	Evaluation of the Proposed Scheme	Challenges in Proposed Scheme
Blockchain Model	[76]	Attribute-based encryption methods combined(ABE) with private blockchain technology; BAN logic; OPNET software	Privacy, accessibility, authorization, authentication, and integrity.	Securely share and store medical data between patients, hospitals and other stakeholders.	Efficiency in terms of computing complexity and storage.	The complexity of cryptocurrency exchange for data sharing.
	[77]	Blockchain technology, AVISPA automated tool,	Authentication, confidentiality, and privacy	Provides secure key management among different communicating entities for IoMT environment	Efficient in terms of security and functionality, reducing communication and communication costs for the authentication and key management phase.	Does not meet all security requirements

Table 5. *Cont.*

Security Model	Ref	Technologies and Techniques Used	Security Requirement	Benefits of the Proposed Scheme	Evaluation of the Proposed Scheme	Challenges in Proposed Scheme
Blockchain Model	[78]	Blockchain technology, AVISPA automated tool, Cooja simulator	Mutual authentication	Lightweight framework for authentication and permission to complement current blockchain-based IoT networks in the healthcare sector	Minimization of transmission costs and computing overhead	Not assessed on hardware in a realistic context, making it less efficient
	[79]	Blockchain technology, fine-grained access control	Privacy, confidentiality, and integrity	large-scale health data privacy preserving scheme based on blockchain technology	System can meet the expected security requirements and can be applied to mobile health systems	Insider attacks are neglected by the system.
Authentication Model	[80]	Cloud Environment (CE), FPGA, Moteiv TMote Sky-Mote	Mutual authenticity	Framework for cross-reviewing the common secret session key of communication entities and establishing mutual authenticity for TMIS system using the cloud environment (CE)	Security and performance efficiency, resistance to security threats, reduces computational cost, and good fit adaptation to the TMIS system	Intended for TMIS systems, and does not meet all security requirements
	[13]	Attribute-based encryption (ABE), HLPSL language, AVISPA automated tool	Authentication, and privacy	A secure communication for medical applications utilizing ABE for authentication in HetNet at the network layer	Better protection of health data against intruders, minimization of transmission costs and computational load	Attribute threshold requirement for authentication, use of a third-party trusted authority (if this third party is hacked, all data is subject to hostile attacks)
	[81]	Physical unclonable functions (PUFs)	Authentication	A lightweight and robust authentication scheme based on the physical non-clonable function (PUF) for the IoMT, which does not store any data from the IoMT devices in the server memory	The proposed authentication scheme increases the robustness of the design while being lightweight for deployment in various designs and supports scalability	The system failed to verify that the client could authenticate the server's communications
	[82]	Biometric techniques, fisher Vector (FV), DCT	Authentication	A multimodal biometric system for person recognition using face, fingerprint, and finger vein images, in the IoMT.	Excellent recognition rate and higher security than a unimodal biometric-based system	Low system accuracy rates
	[83]	ECDSA Algorithm, ECC cryptography, dual signature method	Privacy, confidentiality, and authentication	Include a double signature in the ECDSA algorithm to enhance security and preserve data privacy in communications between IoMT devices and the cloud via edge computing devices	Calculation requirements and complexity are minimized	Ensuring the integrity and authentication of the origin of the data collected, is linked to ensuring the anonymity of the data source from a cloud perspective

Table 5. *Cont.*

Security Model	Ref	Technologies and Techniques Used	Security Requirement	Benefits of the Proposed Scheme	Evaluation of the Proposed Scheme	Challenges in Proposed Scheme
Authentication Model	[84]	Huffman coding scheme	Privacy, confidentiality, and authentication	A reversible high-capacity dual-frame data hiding technique for IoMT networks based on the Huffman coding scheme	The system offers significant improvement and computational efficiency, which allowed it to be used in the IoMT network	No effective strategy to control overflow and underflow problems
	[85]	Electrocardiogram (ECG) signal, online datasets	Privacy, confidentiality, and authentication	A practical system that reliably authenticates patients with noisy ECG signals and simultaneously provides differential privacy	Allows an efficient and effective authentication of the patient while guaranteeing the confidentiality of the model	The system was not scalable enough for the attack
	[86]	Computational Diffie-Hellman (CDH)	Privacy, confidentiality	Suitable for cheap communication protocol and resource-constrained devices	Cost effective solution suitable for devices with limited resources	The mechanism can be costly for devices with constrained storage/memory
	[2]	AES (Advanced Encryption Standard), ECDSA (Elliptic Curve Digital Signature Algorithm), Transport Layer Security (TLS)	Privacy, confidentiality, authentication, integrity, non-repudiation	Confidentiality, integrity of the message, audit control, effective patient authentication, data availability, access control, transparency, freshness of health data	Allows secure exchange of message maintaining all security requirements. Data freshness is ensured. HIPAA standard maintained	There may be end-to-end delay on some occasions
Machine learning Model	[87]	Keras and Tensor flow In Python, Deep Learning	Privacy, confidential-ity, authentication, integrity	An embedded system prototype for predicting distinct attack patterns in deep brain stimulation	Anomaly based false alarm detection; high accuracy; the ability to detect attacks in real time	High computation overhead; high False Positive Rate (FPR)
	[88]	R and Java, Languages, AUDIT module	Privacy, confidentiality, authentication, integrity	Detects inaccurate measurements in real time and distinguishes between defects or errors and health events for smart mobile healthcare	Lightweight, real time, improved accuracy and False Positive Rate (FPR)	Energy and CPU usage is not taken into account, lack of detection of attacks at the server and transmission level
	[89]	GWO and PCA algorithms, Deep Learning classifier	Privacy, confidentiality, authentication, authorization, integrity, availability	A deep neural network (DNN) is used to develop an effective intrusion detection system (IDS) to classify and predict unexpected cyber-attacks in the IoMT environment	High accuracy (15%) and low training and classification time (32%)	Overhead in terms of memory and CPU, limited to IoMT devices with a single IP address
	[90]	Deep Belief Network (DBN), CICIDS2017 dataset	Privacy, confidentiality, integrity, availability	A Deep Belief Network (DBN) algorithm model based on deep learning for the intrusion detection system	High accuracy, precision, F1 and recall, positive results for all variables compared to other techniques, extended to the detection of several forms of attacks	High training overhead, False Positive Rate (FPR) and performance overhead ignored

Table 5. *Cont.*

Security Model	Ref	Technologies and Techniques Used	Security Requirement	Benefits of the Proposed Scheme	Evaluation of the Proposed Scheme	Challenges in Proposed Scheme
Machine learning Model	[91]	Waikato Environment for Knowledge Analysis (WEKA), Naive-Bayes (NB), Support Vector Machine (SVM), MultiLayer Perceptron Artificial Neural Network (MLP), Random Forest (RF)	Authentication and security	Reduce computational cost by extracting features from the ECG signal and using only the landmarks calculated directly from the signal acquisition	Accuracy of over 98.2%, and reduced complexity using less than 10 features	Accuracy reduction, high training costs, as well as uncalculated performance costs, difficult to put into practice using several sensors

10. Conclusions and Future Directions

The use of IoMT is a reality today. Many hospital systems are adopting it or in the process of adopting it. The majority of current research activities focuses on how medical and health-monitoring technologies can help reduce healthcare costs while improving patient health. This is also an objective of many developed hospitals and medical facilities. As a result, protecting this technology has become critical, as the IoMT is vulnerable to a variety of attacks due to its reliance on wireless communications. These attacks have the potential to compromise the system and breach patient's privacy, as well as compromise the confidentiality, integrity, and availability of medical services. The major security difficulties, challenges, and drawbacks of IoMT were reported and discussed in this paper. We have also discussed how to improve IoMT services by securing IoMT domains and their related assets using various and suitable security methods, as well as how to improve patient health and experience using various strategies. We also highlighted the importance of a good security strategy for the many wireless-communication protocols used by the IoMT system to keep it secure, private, reliable, and accurate.

In a nutshell, the objective of this paper is to review the current state of security and privacy in IoMT, which has become a major concern for many security experts and researchers due to its rapid demand in recent times. Nevertheless, with respect to the current state of security and privacy, we have also reviewed and discussed a number of attack use cases, countermeasures and solutions, recent challenges, and anticipated future directions that require further attention in this area. We concluded that current techniques may fail if certain parameters, such as resource complexity, time complexity, and energy consumption, are not considered. We found that a large majority of studies have ignored these criteria in evaluating their proposed models. However, future studies should focus on how to use these new technologies appropriately to make concessions for the nature of IoMT. More work is needed to be able to address global needs, especially in the security domain.

Author Contributions: Conceptualization, R.H., H.M. and A.-S.K.P.; investigation, R.H., H.M. and A.-S.K.P.; resources, R.H., H.M.; writing—original draft preparation, R.H.; writing—review and editing, H.M. and A.-S.K.P.; visualization, R.H.; supervision, H.M. and A.-S.K.P.; project administration, H.M. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Khan, R.A.; Pathan, A.-S.K. The state of the art wireless body area sensor networks: A survey. *Int. J. Distrib. Sens. Netw.* **2018**, *14*, 1–23. [CrossRef]
2. Ahamad, S.S.; Pathan, A.-S.K. A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19 like pandemic. *Connect. Sci.* **2021**, *33*, 532–554. [CrossRef]
3. Vaiyapuri, T.; Binbusayyis, A.; Varadarajan, V. Security, privacy and trust in IoMT enabled smart healthcare system: A systematic review of current and future trends. *Int. J. Adv. Comput. Sci. Appl.* **2021**, *12*, 731–737. [CrossRef]
4. Rasool, R.U.; Ahmad, H.F.; Rafique, W.; Qayyumd, A.; Qadir, J. Security and privacy of internet of medical things: A contemporary review in the age of surveillance, botnets, and adversarial. *J. Netw. Comput. Appl.* **2022**, *201*, 103332. [CrossRef]
5. Gubbi, J.; Buyya, R.; Marusic, S.; Palaniswami, M. Internet of things (IoT): A vision, architectural elements, and future directions. *Future Gener. Comput. Syst.* **2013**, *29*, 1645–1660. [CrossRef]
6. Jahankhani, H.; Ibarra, J. Digital forensic investigation for the Internet of medical things (IoMT). *Forensic Leg. Investig. Sci.* **2019**, *5*, 1–6. [CrossRef]
7. Al Shorman, O.; Al Shorman, B.; Al-khassaweneh, M.; Alkahtani, F. A review of internet of medical things (IoMT)—Based remote health monitoring through wearable sensors: A case study for diabetic patients. Indones. *J. Electr. Eng. Comput. Sci.* **2020**, *20*, 414–422.
8. Dhiyya, A.J.A. Architecture of IoMT in healthcare. In *The Internet of Medical Things (IoMT): Healthcare Transformation*; Hemalatha, R.J., Akila, D., Balaganesh, D., Paul, A., Eds.; Wiley: Hoboken, NJ, USA, 2022; pp. 161–172.
9. Ghubaish, A.; Salman, T.; Zolanvari, M.; Unal, D.; Al-Ali, A.; Jain, R. Recent advances in the internet of medical things (IoMT) systems security. *IEEE Internet Things J.* **2020**, *8*, 8707–8718. [CrossRef]
10. Din, I.U.; Guizani, M.; Hassan, S.; Kim, B.-S.; Khan, M.K.; Atiquzzaman, M.; Ahmed, S.H. The Internet of things: A review of enabled technologies and future challenges. *IEEE Access* **2018**, *7*, 7606–7640. [CrossRef]
11. Ferguson, J.E.; Redish, A.D. Wireless communication with implanted medical devices using the conductive properties of the body. *Expert Rev. Med. Devices* **2011**, *8*, 427–433. [CrossRef]
12. Kos, A.; Milutinović, V.; Umek, A. Challenges in wireless communication for connected sensors and wearable devices used in sport biofeedback applications. *Future Gener. Comput. Syst.* **2019**, *92*, 582–592. [CrossRef]
13. Lone, T.A.; Rashid, A.; Gupta, S.; Gupta, S.K.; Rao, D.S.; Najim, M.; Srivastava, A.; Kumar, A.; Umrao, L.S.; Singhal, A. Securing communication by attribute-based authentication in hetnet used for medical applications. *EURASIP J. Wirel. Commun. Netw.* **2020**, *146*, 146. [CrossRef]
14. Alrawais, A.; Alhothaily, A.; Hu, C.; Cheng, X. Fog computing for the internet of things: Security and privacy issues. *IEEE Internet Comput.* **2017**, *21*, 34–42. [CrossRef]
15. Hameed, S.S.; Hassan, W.H.; Abdul Latiff, L.; Ghabban, F. A systematic review of security and privacy issues in the internet of medical things; the role of machine learning approaches. *Peer. J. Comput. Sci.* **2021**, *7*, e414. [CrossRef] [PubMed]
16. Kagita, M.K.; Thilakarathne, N.; Gadekallu, T.R.; Maddikunta, P.K.R. A review on security and privacy of internet of medical things. In *Intelligent Internet of Things for Healthcare and Industry*; Ghosh, U., Chakraborty, C., Garg, L., Srivastava, G., Eds.; Springer: Berlin/Heidelberg, Germany, 2022; pp. 171–187.
17. Poongodi, T.; Rathee, A.; Indrakumari, R.; Suresh, P. IoT sensing capabilities: Sensor deployment and node discovery, wearable sensors, wireless body area network (WBAN), data acquisition. In *Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm*; Peng, S.L., Pal, S., Huang, L., Eds.; Springer International Publishing: Cham, Switzerland, 2020; pp. 127–151.
18. Choudhary, G.; Jain, A.K. Internet of things: A survey on architecture, technologies, protocols and challenges. In Proceedings of the International Conference on Recent Advances and Innovations in Engineering, Jaipur, India, 23–25 December 2016.
19. Benslimane, Y.; Benahmed, K.; Benslimane, H. Security mechanisms for 6LoWPAN network in context of internet of things: A Survey. In *Renewable Energy for Smart and Sustainable Cities*; Hatti, M., Ed.; Springer International Publishing: Cham, Switzerland, 2019; pp. 49–69.
20. Ahmadi, H.; Arji, G.; Shahmoradi, L.; Safdari, R.; Nilashi, M.; Alizadeh, M. The application of internet of things in healthcare: A systematic literature review and classification. *Univ. Access Inf. Soc.* **2019**, *18*, 837–869. [CrossRef]
21. Islam, S.M.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
22. Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and privacy issues in medical internet of things: Overview, countermeasures, challenges and future directions. *Sustainability* **2021**, *13*, 11645. [CrossRef]
23. Toscano, E.; Bello, L.L. Comparative assessments of IEEE 802.15. 4/ZigBee and 6LoWPAN for low-power industrial WSNs in realistic scenarios. In Proceedings of the 9th IEEE International Workshop on Factory Communication Systems, Lemgo, Germany, 21–24 May 2012.
24. Tabish, R.; Mnaouer, A.B.; Touati, F.; Ghaleb, A.M. A comparative analysis of BLE and 6LoWPAN for U-HealthCare applications. In Proceedings of the 7th IEEE GCC Conference and Exhibition, Doha, Qatar, 17–20 November 2013.
25. Haxhibeqiri, J.; De Poorter, E.; Moerman, I.; Hoebeke, J. A survey of LoRaWAN for IoT: From technology to application. *Sensors* **2018**, *18*, 3995. [CrossRef]

26. Sundaresan, S.; Doss, R.; Zhou, W. RFID in healthcare–current trends and the future. In *Springer Series in Bio-/Neuroinformatics*; Kasabov, N., Ed.; Springer: Berlin/Heidelberg, Germany, 2015; Volume 5, pp. 839–870.
27. Sarigiannidis, P.; Karapistoli, E.; Economides, A.A. Detecting sybil attacks in wireless sensor networks using UWB ranging-based information. *Expert Syst. Appl.* **2015**, *42*, 7560–7572. [CrossRef]
28. Peng, H. WIFI network information security analysis research. In Proceedings of the 2nd IEEE International Conference on Consumer Electronics, Communications and Networks, Yichang, China, 21–23 April 2012.
29. Yang, X.; Karampatzakis, E.; Doerr, C.; Kuipers, F. Security vulnerabilities in LoRaWAN. In Proceedings of the IEEE/ACM 3rd International Conference on Internet-of-Things Design and Implementation, Orlando, FL, USA, 17–20 April 2018.
30. Duggal, A. HL7 2. x security. In Proceedings of the 8th Annual HITB Security Conference, Amsterdam, The Netherlands, 10–14 April 2017.
31. Flury, M.; Poturalski, M.; Papadimitratos, P.; Hubaux, J.P.; Le Boudec, J.Y. Effectiveness of distance-decreasing attacks against impulse radio ranging. In Proceedings of the 3rd ACM Conference on Wireless Network Security, Hoboken, NJ, USA, 22–24 March 2010.
32. Navya, V.; Deepalakshmi, P. Threshold-based energy-efficient routing for transmission of critical physiological parameters in a wireless body area network under emergency scenarios. *Int. J. Comput. Appl.* **2021**, *43*, 367–376. [CrossRef]
33. Nanayakkara, N.; Halgamuge, M.N.; Syed, A. Security and privacy of internet of medical things (IoMT) based healthcare applications: A review. In Proceedings of the 262nd IIER International Conference, Istanbul, Turkey, 6–7 November 2019.
34. Chen, X.; Zhu, H.; Geng, D.; Liu, W.; Yang, R.; Li, S. Merging RFID and blockchain technologies to accelerate big data medical research based on physiological signals. *J. Healthc. Eng.* **2020**, *2020*, 2452683. [CrossRef] [PubMed]
35. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
36. Kasyoka, P.; Kimwele, M.; Mbandu Angolo, S. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *J. Med. Eng. Technol.* **2020**, *44*, 12–19. [CrossRef] [PubMed]
37. Belkhouja, T.; Sorour, S.; Hefeida, M.S. Role-based hierarchical medical data encryption for implantable medical devices. In Proceedings of the IEEE Global Communications Conference, Waikoloa, HI, USA, 9–13 December 2019.
38. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C.I. Review of security and privacy for the internet of medical things. In Proceedings of the International Conference on Distributed Computing in Sensor Systems, Santorini, Greece, 29–31 May 2019.
39. Hash, J.; Bowen, P.; Johnson, L.; Smith, C.; Steinberg, D. *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*; Special Publication (NIST SP); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008.
40. Koutras, D.; Stergiopoulos, G.; Dasaklis, T. Security in IoMT communications: A survey. *Sensors* **2020**, *20*, 4828. [CrossRef] [PubMed]
41. Sun, Y.; Lo, F.P.-W.; Lo, B. Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Access* **2019**, *7*, 183339–183355. [CrossRef]
42. Papaioannou, M.; Karageorgou, M.; Mantas, G.; Sucasas, V.; Essop, I.; Jonathan, R.; Dimitrios, L. A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). *Trans. Emerg. Telecommun. Technol.* **2022**, *33*, e4049. [CrossRef]
43. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. *J. Supercomput.* **2021**, *77*, 7916–7955. [CrossRef]
44. Davis, J. Ransomware Attacks Cost Healthcare Sector at Least $160M Since 2016. Health IT Security. Available online: https://healthitsecurity.com/ (accessed on 23 June 2022).
45. Rathore, H.; Al-Ali, A.K.; Mohamed, A.; Du, X.; Guizani, M. A novel deep learning strategy for classifying different attack patterns for deep brain implants. *IEEE Access* **2019**, *7*, 24154–24164. [CrossRef]
46. 'Lives Are at Stake': Hacking of US Hospitals Highlights Deadly Risk of Ransomware, The Guardian. Available online: https://www.theguardian.com/technology/2022/jul/14/ransomware-attacks-cybersecurity-targeting-us-hospitals (accessed on 5 August 2022).
47. Saif, S.; Biswas, S.; Chattopadhyay, S. Intelligent, secure big health data management using deep learning and blockchain technology: An overview. In *Deep Learning Techniques for Biomedical and Health Informatics*; Dash, S., Acharya, B., Mittal, M., Abraham, A., Kelemen, A., Eds.; Springer International Publishing: Cham, Switzerland, 2020; Volume 68, pp. 187–209.
48. Maji, S.; Banerjee, U.; Fuller, S.H.; Abdelhamid, M.R.; Nadeau, P.M.; Yazicigil, R.T.; Chandrakasan, A.P. A low-power dual-Factor authentication unit for secure implantable devices. In Proceedings of the IEEE Custom Integrated Circuits Conference, Newport Beach, CA, USA, 22–25 March 2020.
49. Andrea, I.; Chrysostomou, C.; Hadjichristofi, G. Internet of things: Security vulnerabilities and challenges. In Proceedings of the IEEE Symposium on Computers and Communication, Larnaca, Cyprus, Greek, 6–9 July 2015.
50. Abosata, N.; Al-Rubaye, S.; Inalhan, G.; Emmanouilidis, C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors* **2021**, *21*, 3654. [CrossRef]
51. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 127072.

52. Kalyani, G.; Chaudhari, S. An efficient approach for enhancing security in Internet of Things using the optimum authentication key. *Int. J. Comput. Appl.* **2020**, *42*, 306–314. [CrossRef]
53. Burhan, M.; Rehman, R.A.; Khan, B.; Kim, B.-S. IoT elements, layered architectures and security issues: A comprehensive survey. *Sensors* **2018**, *18*, 2796. [CrossRef] [PubMed]
54. Salem, O.; Alsubhi, K.; Shaafi, A.; Gheryani, M.; Mehaoua, A.; Boutaba, R. Man-in-the-Middle Attack Mitigation in Internet of Medical Things. *IEEE Trans. Ind. Inform.* **2022**, *18*, 2053–2062.
55. Agyemang, I.O.; Kponyo, J.J.; Klogo, G.S.; Boateng, J.O. Lightweight rogue access point detection algorithm for WiFi-enabled internet of things (IoT) devices. *Internet Things* **2020**, *11*, 100200. [CrossRef]
56. Khader, R.; Eleyan, D. Survey of DoS/DDoS attacks in IoT. *Sust. Eng. Innov.* **2021**, *3*, 23–28. [CrossRef]
57. Sharma, M.; Arora, B. Detection and prevention of DoS and DDoS in IoT. In *Lecture Notes in Networks and Systems*; Singh, P.K., Wierzchoń, S.T., Tanwar, S., Ganzha, M., Rodrigues, J.J.P.C., Eds.; Springer: Singapore, 2021; Volume 203, pp. 845–855.
58. Sethuraman, S.C.; Vijayakumar, V.; Walczak, S. Cyber-attacks on healthcare devices using unmanned aerial vehicles. *J. Med. Syst.* **2020**, *44*, 29. [CrossRef]
59. Pathan, A.-S.K.; Lee, H.-W.; Hong, C.S. Security in wireless sensor networks: Issues and challenges. In Proceedings of the 8th International Conference on Advanced Communication Technology (IEEE ICACT 2006), Gangwon, Korea, 20–22 February 2006; Volume II.
60. Marin-Jiménez, M.J.; Castro, F.M.; Guil, N.; De la Torre, F.; Medina-Carnicer, R. Deep multi-task learning for gait-based biometrics. In Proceedings of the IEEE International Conference on Image Processing, Beijing, China, 17–20 September 2017.
61. Schwartz, O.; Mathov, Y.; Bohadana, M.; Elovici, Y.; Oren, Y. Opening pandora's box: Effective techniques for reverse engineering IoT Devices. In Proceedings of the International Conference on Smart Card Research and Advanced Applications, Lugano, Switzerland, 13–15 November 2017.
62. Pathan, A.-S.K.; Kindy, D.A. Lethality of SQL injection against current and future internet-technologies. *Int. J. Comput. Sci. Eng.* **2014**, *9*, 386–394. [CrossRef]
63. Haghi, M.; Thurow, K.; Habil, A.; Stoll, R.; Habil, M. Wearable devices in medical internet of things: Scientific research and commercially available devices. *Healthc. Inform. Res.* **2017**, *23*, 4–15. [CrossRef]
64. Altawy, R.; Youssef, A.M. Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices. *IEEE Access* **2016**, *4*, 959–979. [CrossRef]
65. Larson, B.R.; Zhang, Y.; Barrett, S.C.; Hatcliff, J.; Jones, P.L. Enabling safe interoperation by medical device virtual integration. *IEEE Des. Test* **2015**, *32*, 74–88. [CrossRef]
66. Sicari, S.; Rizzardi, A.; Coen-Porisini, A. How to evaluate an internet of things system: Models, case studies, and real developments. *Software Pract. Exp.* **2019**, *49*, 1663–1685. [CrossRef]
67. Scarpato, N.; Pieroni, A.; Di Nunzio, L.; Fallucchi, F. E-health-IoT universe: A review. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2017**, *7*, 2328–2336. [CrossRef]
68. Neethirajan, S. Recent advances in wearable sensors for animal health management. *Sens. Bio-Sens. Res.* **2017**, *12*, 15–29. [CrossRef]
69. Suranthaa, N.; Davidc, P.A.; Wicaksono, M. A Review of wearable internet-of-things device for healthcare. *Procedia Comput. Sci.* **2020**, *179*, 936–943. [CrossRef]
70. Lee, J.H.; Seo, D.W. Development of ECG monitoring system and implantable device with wireless charging. *Micromachines* **2019**, *10*, 38. [CrossRef]
71. Limaye, A.; Adegbija, T.A. Workload Characterization for the internet of medical things (IoMT). In Proceedings of the IEEE Computer Society Annual Symposium on VLSI, Bochum, Germany, 3–5 July 2017.
72. Alsubaei, F.; Shiva, S.; Abuhussein, A. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 42nd IEEE Conference on Local Computer Networks Workshops, Singapore, 9 October 2017.
73. Lakafosis, V.; Vyas, R.; Mariotti, C.; Le, T.; Tentzeris, M.M. Integrating tiny RFID- and NFC-based sensors with the Internet. In *Green RFID Systems*; Roselli, L., Ed.; Cambridge University Press: Cambridge, UK, 2014; pp. 152–175.
74. Bhanushali, J.; Dinde, P.; Chakraborty, S. Internet of things: Machine to machine communication with emphasis on role of RFID and NFC. *Int. J. Sci. Eng. Res.* **2015**, *6*, 779–785.
75. Nasiri, S.; Sadoughi, F.; Tadayon, M.H.; Dehnad, A. Security requirements of internet of things-based healthcare system: A survey study. *Acta. Inform. Med.* **2019**, *27*, 253–258. [CrossRef]
76. Pournaghi, S.M.; Bayat, M.; Farjami, Y. MedSBA: A novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption. *J. Ambient Intell. Humaniz. Comput.* **2020**, *11*, 4613–4641. [CrossRef]
77. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.; Park, Y. Bakmp-iomt: Design of blockchain enabled authenticated key management protocol for internet of medical things deployment. *IEEE Access* **2020**, *8*, 95956–95977. [CrossRef]
78. Tahir, M.; Sardaraz, M.; Muhammad, S.; Saud Khan, M. A lightweight authentication and authorization framework for blockchain enabled IoT network in health-informatics. *Sustainability* **2020**, *12*, 6960. [CrossRef]
79. Xu, J.; Xue, K.; Li, S.; Tian, H.; Hong, J.; Hong, P.; Yu, N. Healthchain: A blockchain-based privacy preserving scheme for largescale health data. *IEEE Internet Things J.* **2019**, *6*, 8770–8781. [CrossRef]
80. Deebak, B.; Al-Turjman, F. Smart mutual authentication protocol for cloud based medical healthcare systems using internet of medical things. *IEEE J. Sel. Areas Commun.* **2020**, *39*, 346–360. [CrossRef]

81. Yanambaka, V.P.; Mohanty, S.P.; Kougianos, E.; Puthal, D. Pmsec: Physical unclonable function-based robust and lightweight authentication in the internet of medical things. *IEEE Trans. Consum. Electron.* **2019**, *65*, 388–397. [CrossRef]
82. Xin, Y.; Kong, L.; Liu, Z.; Wang, C.; Zhu, H.; Gao, M.; Zhao, C.; Xu, X. Multimodal feature-level fusion for biometrics identification system on iomt platform. *IEEE Access* **2018**, *6*, 21418–21426. [CrossRef]
83. Cano, M.D.; Cañavate-Sanchez, A. Preserving data privacy in the internet of medical things using dual signature ecdsa. *Secur. Commun. Netw.* **2020**, *2020*, 4960964. [CrossRef]
84. Gull, S.; Parah, S.A.; Muhammad, K. Reversible data hiding exploiting huffman encoding with dual images for IoMT based healthcare. *Comput. Commun.* **2020**, *163*, 134–149. [CrossRef]
85. Huang, P.; Guo, L.; Li, M.; Fang, Y. Practical privacy-preserving ECG-based authentication for IoT-based healthcare. *IEEE Internet Things J.* **2019**, *6*, 9200–9210. [CrossRef]
86. Wang, Z. Blind batch encryption-based protocol for secure and privacy-preserving medical services in smart connected health. *IEEE Internet Things J.* **2019**, *6*, 9555–9562. [CrossRef]
87. Abdaoui, A.; Al-Ali, A.; Riahi, A.; Mohamed, A.; Du, X.; Guizani, M. Secure medical treatment with deep learning on embedded board. In *Energy Efficiency of Medical Devices and Healthcare Applications*; Mohamed, A., Ed.; Elsevier: Amsterdam, The Netherlands, 2020; pp. 131–151.
88. Ben Amor, L.; Lahyani, I.; Jmaiel, M. AUDIT: Anomalous data detection and Isolation approach for mobile healthcare systems. *Expert Syst.* **2020**, *37*, e12390. [CrossRef]
89. Priya, R.M.S.; Maddikunta, P.K.R.; Parimala, M.; Koppu, S.; Reddy, T.; Chowdhary, C.L.; Alazab, M. An effective feature engineering for DNN using hybrid PCA-GWO for intrusion detection in IoMT architecture. *Comput. Commun.* **2020**, *160*, 39–149.
90. Manimurugan, S.; Almutairi, S.; Aborokbah, M.M.; Chilamkurti, N.; Ganesan, S.; Patan, R. Effective attack detection in internet of medical things smart environment using a deep belief neural network. *IEEE Access* **2020**, *8*, 77396–77404. [CrossRef]
91. Barros, A.; Rosário, D.; Resque, P.; Cerqueira, E. Heart of IoT: ECG as biometric sign for authentication and identification. In Proceedings of the 15th International Wireless Communications & Mobile Computing Conference, Piscataway, NJ, USA, 24–28 June 2019.