sustainability

MDPI

Review

Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends

Bharat Bhushan [1,*], Avinash Kumar [2], Ambuj Kumar Agarwal [1], Amit Kumar [3], Pronaya Bhattacharya [4] and Arun Kumar [5]

[1] Department of Computer Science and Engineering, School of Engineering and Technology, Sharda University, Greater Noida 201310, Uttar Pradesh, India
[2] SITAICS, Rashtriya Raksha University, Lavad 382305, Gujarat, India
[3] Department of Computer Science and Applications, School of Engineering and technology, Sharda University, Greater Noida, 201310, India
[4] Department of Computer Science and Engineering, Amity School of Engineering and Technology, Amity University, Kolkata 700135, West Bengal, India
[5] Galgotias College of Engineering and Technology, Greater Noida 201310, Uttar Pradesh, India
* Correspondence: bharat_bhushan1989@yahoo.com; Tel.: +91-995-897-3930

Abstract: Recent advances in machine-to-machine (M2M) communications, mini-hardware manufacturing, and micro computing have led to the development of the Internet of Things (IoT). The IoT is integrated with medical devices in order to enable better treatment, cost-effective medical solutions, improved patient monitoring, and enhanced personalized healthcare. This has led to the development of more complex and heterogeneous Internet of Medical Things (IoMT) systems that have their own operating systems and protocols. Even though such pervasive and low-cost sensing devices can bring about enormous changes in the healthcare sector, these are prone to numerous security and privacy issues. Security is thus a major challenge in these critical systems, one that inhibits their widespread adoption. However, significant inroads have been made by the on-going research, which powers the IoMT applications by incorporating prevalent security measures. In this regard, this paper highlights the significance of implementing key security measures, and essential aspects of the IoMT that make it useful for interconnecting various internal and external working domains of healthcare. This paper presents state-of-the-art techniques for securing IoMT systems, in terms of data transmission, collection, and storage. Furthermore, the paper also explores various security requirements, inherent design challenges, and various security techniques that could make the IoMT more secure and sustainable. Finally, the paper gives a panoramic view of the current status of research in the field and outlines some future research directions in this area.

Keywords: Internet of Medical Things (IoMT); security; privacy; healthcare; medical devices; cyber security

Citation: Bhushan, B.; Kumar, A.; Agarwal, A.K.; Kumar, A.; Bhattacharya, P.; Kumar, A. Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. *Sustainability* **2023**, *15*, 6177. https://doi.org/10.3390/su15076177

Academic Editors: Stavros Shiaeles, Amir Masoud Rahmani, Firuz Kamalov and Seyedeh Yasaman Hosseini Mirmahaleh

Received: 23 January 2023
Revised: 29 March 2023
Accepted: 30 March 2023
Published: 3 April 2023

1. Introduction

The Internet of Medical Things (IoMT) has emerged from the existing Internet of Things (IoT) technology, specifically dealing with the healthcare of patients. Similar to the IoT, the IoMT is also interconnected to various devices for communication with each other. The communication could be wireless, wired, or both, depending upon the devices and infrastructure developed. Smart cities are emerging at a rapid pace, and hence the need for the IoMT is also increasing [1]. The IoMT has the potential to reduce expenses incurred in the healthcare sector [2]; the sector is predicted to make a saving of USD 300 billion through the use of IoMT-based systems [3]. The revenue that was generated by IoMT-based systems in the year 2017 was USD 28 billion, and it is expected to grow up to USD 135 billion [4]. This will lead to a huge increase in the number of investors in IoMT-based systems.

Security, in any system, is a must, as it not only protects the client's data and information, but also protects the reputation of the organization [5]. Therefore, the IoMT needs to be protected from various types of cyber-attacks. The probability of cyber-attacks increases in the case of the IoMT because it works on the concept of the IoT, in which devices, protocols, and operating systems all distinctly constitute the heterogeneous environment [6]. The heterogeneity makes the system more vulnerable to cyber-attacks [7,8]. The main motivation for an attack on the IoMT is the value of the data stored within it, for the monitoring and treatment of patients. The average cost of IoMT data is estimated to be 50 times higher than in other sectors. This high value of IoMT data creates a greater risk of cyber-attack. Moreover, the devices used in IoMT-based system, such as closed-circuit television (CCTV) cameras, do not have patch update facilities, and thus require replacement if a vulnerability is found.

Considering the above two points, securing the IoMT is a necessity. Various techniques are used for achieving security and preserving privacy in IoMT-based systems. Symmetric key cryptography could be used as one of the solutions for preserving security in the IoMT [9]. The asymmetric key cryptography concept could also be used for protecting against data leakage in IoMT-based systems [10]. Apart from these two key-based techniques, key-less techniques could also be used for dealing with security and privacy issues in the IoMT [11]. These key-less techniques include token-based security, biometric-based security, proxy-based security, and blockchain-based security [7,12]. These security concepts are very useful as they are particularly sensitive to anomalies in the system. This anomaly detection helps the IoMT system, not only in detecting previously occurred cyber-attacks, but also in detecting new ones [13–16].

Limaye et al. [17] introduced innovative microarchitectures and suggested improvements that will allow for the efficient execution of future IoMT applications. Pritam et al. [18] proposed a comprehensive taxonomic review of current IoT-based sensor systems developed by the IoT market cap for taxonomic representations. Their research highlights the security and privacy challenges related to sensor data, and future strategies for enhancing the existing security vulnerabilities. Al-Turjman et al. [19] provided an overview of the IoMT, emphasizing future development, research objectives, and related applications. Authors presented a generalized IoMT structure that includes the three elements of data gathering, communication gateways, and servers/cloud. Sun et al. [20] aimed to efficiently use high quality healthcare resources, while working within the constraints of the present medical environment and medical-related equipment, to process and evaluate medical big data in a timely manner. They also concentrated on the improvements that cloud computing, edge computing, and artificial intelligence technologies have brought to the IoMT. In another work, Guangjun et al. [21] showed a triple topic intent-based security control (TS-PBAC) that is suitable for blockchain-enabled reliable transaction networks. Authors lay out an individual-centric security and confidentiality mechanism for access control, with various purposes and roles in IoMT scenarios. Ghubaish et al. [2] demonstrated cutting-edge methods for securing information in IoMT systems. The work provides a detailed analysis of potential physical and network threats that could endanger IoMT systems. The majority of security precautions do not take various forms of attacks into consideration. Ashfaq et al. [22] presented an extensive analysis of the numerous studies carried out to develop and improve the IoMT. They also included in-depth analysis of the benefits and downfalls of the various communication technologies now in use. In another work, Awad et al. [23] presented an in-depth analysis of an MEC (mobile edge computing)-based IoMT healthcare system. However, although the IoMT has been widely applied over the last 3 years, not enough comprehensive studies shed light on its security and privacy aspects. In contrast to the works discussed above, this paper brings forth a holistic approach for IoMT applications, highlighting motive, security requirements, concerns, and future research directions. In summary, the major contributions of this paper are as follows.

- This work presents the background of the IoMT and the motives for its wide acceptance to build the foundation for an understanding of the heterogeneous features of the IoMT.
- This work presents the various parameters that make the IoMT vulnerable to cyber-attacks.
- This work scrutinizes various security and privacy requirements in IoMT-based systems.
- This work discusses the major design challenges in an IoMT environment, and outlines various techniques used for resolving such security issues.
- This work presents a state-of-the-art solution using various methods to make the IoMT safer for application with humans.
- Finally, this work outlines several open research challenges that can help future researchers working in this emerging research area.

The remainder of the paper is organized as follows: Section 2 represents the background of the IoMT. Section 3 deals with the security requirements and design challenges of the IoMT. Section 4 presents security techniques in the IoMT. Section 5 presents a taxonomy of security protocols in the IoMT. Finally, Section 7 presents the future research directions, followed by a conclusion in Section 8.

2. Background of the IoMT

The rise in interconnected devices for human activities has led to a burgeoning exchange of data. The Internet of Things (IoT) has become a platform for various systems, including the Internet of Medical Things (IoMT), which is one of the most important areas in terms of human benefit [24]. The IoMT is useful for interconnecting medical devices and applications associated with them [2]. The IoMT is particularly useful for the remote monitoring of patients and the analysis of medical information [25]. Real-life data analysis is vital when gathering medical data in order to prevent a sudden attack in patients. The IoMT has increased the life expectancy of humans by monitoring patients' health at consistent times. The below sub-sections contain an in-depth discussion of the IoMT.

2.1. Defining the IoMT

Systems based on the IoMT concept typically have three levels, namely, the sensor, the personal server, and the server. Figure 1 presents the architectural view of this three-layer IoMT-based system. Importantly, most of the recently proposed work uses this architecture [26]. Sensors, along with other medical devices, are placed at the sensor level; these build up the local network and are termed the body sensor network (BSN) [27]. To provide services such as low powered Bluetooth communication (LPBC), and radio frequency identification (RFID), as well as near field communication (NFC), layers such as the sensor and personal server levels are used. LPBC is particularly useful, as it could be implemented in both star as well as mesh topologies. Those devices which are implantable could be improved using NFC and RFID. NFC and RFID are useful in device-to-device communication within a short distance. The physiological data and information are vital, and these are gathered using medical devices and transmitted to personal servers. The personal servers consist of on-body and off-body devices. The on-body devices include smart phones, tablets, etc., and off-body devices include routers, gateways, etc. These personal servers are useful in processing as well as storing the data at a local level before transferring it to the centrally located medical server (MS). The personal server must operate without any issues when connectivity to the MS is lost because of network issues. Various healthcare systems based on the concept of the IoMT have been proposed, among which BSN-Care is one of the most recent [28].

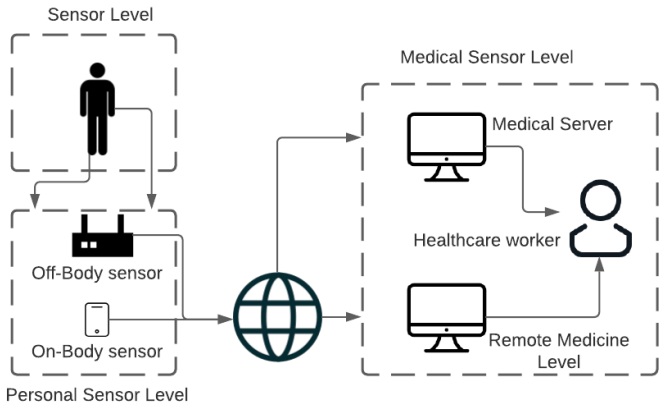

Figure 1. IoMT architecture.

2.2. Motives for IoMT Acceptance

Acceptance of the IoMT is essential to its application and use in the field of technology. The points below cover the important rationale that led to the adoption of the IoMT, as stated by Gus Vlahos [29].

- The use of the IoMT enhances the quality of the clinic. The Memorial Hermann Health System, located in Texas, in the United States, has adopted the IoMT for various activities, such as sending messages, scanning barcodes, and transmitting images.
- The perception of the generally functional and efficient automation of the IoMT helps in empowering efficient connectivity. One example could be the use of smart pills that can send messages, as well as alert signals, to the doctors who are associated with patient monitoring.
- Practical implementations of the IoMT can also be found in remote monitoring, which is performed via gathering data and transferring it to the relevant analyst, which could assist them in managing the patient's illness before it becomes more complicated. A practical example could be seen in the form of UCLA Health and Children's Health, located in Dallas.
- The IoMT also helps in conserving bodily health by accumulating and sending a person's health data to their healthcare practitioner. Practical implementation of this could be seen in the Apple Watch 6, which provides the user with alerts regarding the presence of oxygen in their blood.

2.3. IoMT Types

The IoMT is essential for the improvement of services relevant to various medical conditions. Devices such as pacemakers are implantable devices, whose performance can be enhanced greatly. The IoMT is broadly categorized into two types, Implantable Medical Devices (IMD) and the Internet of Wearable Devices (IoWD). These are thoroughly discussed in the below points.

- IMD refers to those devices which could be used to replace, support, or enhance the biological structure. One practical implementation could be seen in controlling the abnormal rhythm of the human heart using a pacemaker. The pacemaker supports the body by maintaining a consistent heartbeat in the case of an increase or decrease in heart rate from the normal human range [30]. A pacemaker will last longer if its power consumption is less; typically, they tend to last from 5 to 15 years, approximately [31].
- An example of the IoWD is typically worn by individuals to monitor their biometric data, such as heart rate, which could help to enhance their overall health. Devices such as blood pressure monitors (BPM), electrocardiogram monitors (ECG), smartwatches, etc., are examples of the IoWD [32]. Nutrition has become one of the major concerns for humans, and noncritical patients are widely monitored using fall detection and ECG readers [33,34].

2.4. Sensors for the IoMT

The IoMT-based application relies on the filed sensor and other sensors to carry out their designated task as per the IoMT architecture. The sensors used in the system are the most vital elements, as they are the first receptors for IoMT-based applications. In the case of the IoMT, there are various categories of e-healthcare sensors, such as disposable e-health sensors, connected e-health sensors, IoT-market cap sensors, and miscellaneous sensors.

Disposable e-health sensors that can respond to temperature, pressure, integral signals, etc., come under this category. MAX30205 and MLX90614 sensors fall under this category [35]. Connected e-health sensors of the IoMT should be connected at all times to ensure consistency in the communication transmitted over the network [36]. The pressure, position, temperature, etc., are the essential attributes measured by this sensor in the IoMT. IoT-Market cap sensors have flourished in the market. Smart Thermometer (ST) and Kardia Heart (KH) monitoring systems are some of the popular home-based health monitoring systems. Wearable fitness sensors are abundant on e-commerce websites. Miscellaneous sensors play a vital role in the life of pregnant women. The Internet of DNA (IoDNA) is another milestone achievement for genome mapping used for advanced medication systems. Synthesis of genetics using smart DNA (SDNA) could be utilized taking DNA measurements that could be uploaded over IoT-genome DNA for analysis. This concept is also used for predicting genetic defects in newborns. Figure 2 presents the classification of sensors. Table 1 presents the comparison of various sensors in terms of their performance and usage.

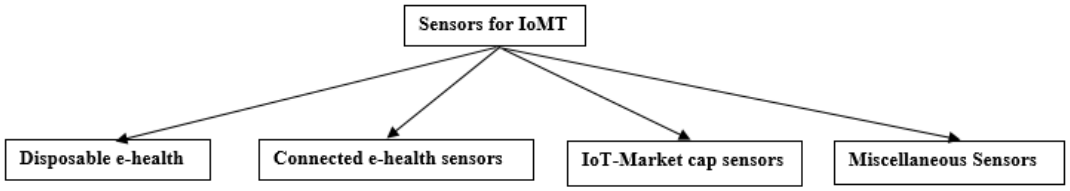

Figure 2. Types of sensors in the IoMT.

Table 1. Sensors and their parameters.

S. No	Product	Type of Sensor	Reference	Support Priority	Disease/Monitoring	Cost	Data Usability	Energy Consumption
1	Proteus Digital Monitor	Clinical biometric	https://www.proteus.com/, accessed on 10 January 2023	Yes	Hypertension, diabetes	Very high	Average	Very high
2	Obaa	Clinical	https://www.obaawoman.com/, accessed on 10 January 2023	Yes	Patient waiting time reduction	Low	High	Average
3	OMsignal	Brain and fitness	http://omsignal.com/, accessed on 10 January 2023	Yes	Wellness care	High	Average	High
4	Thalmic Labs	Home monitoring	https://www.bynorth.com/, accessed on 10 January 2023	Yes	Virtual reality of health status	High	High	High
5	BabyBe	Sleep, infant and woman care	http://www.babybemedical.com/, accessed on 10 January 2023	Yes	Bio signal between mother and premature infant	High	Average	Low
6	AdhereTech	Clinical	https://www.adheretech.com/, accessed on 10 January 2023	Yes	Regular medication	Low	Average	Average
7	Pacifier	Sleep, infant and woman care	https://bluemaestro.com/, accessed on 10 January 2023	Yes	Body temperature	High	High	High
8	CYCORE	Clinical biometric	http://cycore.ucsd.edu/, accessed on 10 January 2023	Yes	Cancer	Average	High	Very high
9	Zeeq	Sleep, infant and woman care	https://sleeptrackers.io/zeeq-smart-pillow/, accessed on 10 January 2023	Yes	Sleep	Average	Low	Average
10	Halo Neuroscience	Brain and fitness	https://www.haloneuro.com/, accessed on 10 January 2023	Yes	Cognitive task management	Average	Low	Average
11	Voluntis	Clinical	https://www.voluntis.com/, accessed on 10 January 2023	Yes	Cancer self management	Very high	Average	Very high

Table 1. *Cont.*

S. no	Product	Type of Sensor	Reference	Support Priority	Disease/Monitoring	Cost	Data Usability	Energy Consumption
12	TuringSense	Home monitoring	https://www.turingsense.com/, accessed on 10 January 2023	Yes	Rehabilitation, posture correction, virtual reality	Average	Low	High
13	Quantus	Clinical biometric	https://quanttus.com/, accessed on 10 January 2023	Yes	Sleep, diabetes, blood pressure	Low	Low	Low
14	Triggerish	Brain and fitness	https://www.sensimed.ch/sensimedtriggerfish/, accessed on 10 January 2023	Yes	Irregular fitness tracking	Low	Average	Average
15	Teletracking	Clinical	https://www.teletracking.com/, accessed on 10 January 2023	Yes	Patient–doctor communication	Average	High	High
16	Cue Health	Home monitoring	https://www.cuehealth.com/, accessed on 10 January 2023	Yes	Inflammation, influenza, fertility, testosterone	Low	High	Low
17	Biostrap	Brain and fitness	https://biostrap.com/, accessed on 10 January 2023	Yes	Sleep recovery and performance management	Low	High	Low
18	Sotera Wireless	Clinical biometric	http://storeawireless.com/, accessed on 10 January 2023	Yes	Blood pressure, fall detection	Average	Very high	Low
19	Beddit	Sleep, infant and woman care	https://www.beddit.com/, accessed on 10 January 2023	Yes	Sleep and wellness	Average	High	Low
20	BioSerenity	Home monitoring	https://www.bioserenity.com/, accessed on 10 January 2023	Yes	Epilepsy monitoring	Very high	Average	Average
21	MC10	Clinical biometric	http://mc10inc.com/, accessed on 10 January 2023	Yes	Sleep, posture, heart rate	Low	Low	Low
22	Ovia	Sleep, infant and woman care	https://www.oviahealth.com/, accessed on 10 January 2023	Yes	Ovulation	Low	High	Average
23	Breezhaler	Home monitoring	https://www.medicines.org.uk/emc/product/3496/smpc, accessed on 10 January 2023	Yes	Asthma	Average	Low	Average
24	NeuroSky	Brain and fitness	http://neurosky.com/, accessed on 10 January 2023	Yes	Mental and physical integration	Low	Average	Low
25	Evermind	Clinical	http://evermind.us/, accessed on 10 January 2023	Yes	Daily activity	High	Low	High

2.5. State-of-the-Art Strategy for Telesurgery or Remote Surgery

Tele-surgery has emerged as a possibility with the advancement of communication linked to the transition from 4G to 5G. This has made possible remote treatment in societies where the movement of specialists is complex. The 5G-enabled tactile internet (TI)-based tele-surgery system operates over a network, for Healthcare 4.0-based state-of-the-art applications [37]. The tele-surgery system works using the principle of a master–slave system, consisting of an operation site robot, which is responsible for performing the desired surgery task based on the command and control provided by the human system interface. the system works in concert with the haptic device, earphones for receiving audio input commands, and a video console. Therefore, the need for consistent connectivity is particularly crucial for any IoMT-based infra-structure where there is a use of remote connection to tackle medical emergencies in case of the unviability of medical services in that particular geographical location. Additionally, in the age of cyber war among nations, there are possibilities that a nation's critical assets, which may include healthcare, will be targeted and thus it is highly important to safeguard against jamming or channel-based attacks. Additionally, all remote or tele-surgery activities involve the use of a command and control server (C2 server), which is one of area of great interest for hackers. Such systems are vulnerable to distributed denial of service (DDoS) attacks, which may include ping of death (PoD), UDP flooding, IP address spoofing, SYN flood, etc., and any of these attacks, performed on the C2 servers could lead to catastrophic loss of human life. Therefore, in order to understand the threats presented by the use of remote connection, it is vital to investigate and dive deep into the important medical services carried out remotely.

2.5.1. Teleoperation

This method of tele-surgery is based upon the concept whereby the master or controller transmits position commands, and the salve manipulator is responsible for adhering to the command. Apart from the server and processor, the system is comprised of the master manipulator (MM), salve manipulator (SM), and servo system (SS) [38,39]. The MM is responsible for controlling the robot, whereas the SS and SM are responsible for operating the robot. The SS tackles the output-controlled data of the SM. Software is used to analyze the bulk of the analog signals (AS), and also constructs the position coordinates.

2.5.2. Endoscopic Telesurgery

This tele-surgery technique, in comparison to earlier methods of tele-surgery, is more evolved. Laparoscopic cholecystectomy is considered to be the first robot-assisted surgery. Later, the Da Vinci surgical robot emerged and was considered to be extremely efficient for short-distance remote surgery. Despite the short range of the Da Vinci surgical robot, it could be used over larger distances, by using procedure control (PC) as well as including the remote guidance system (RGS). The Raven II System, as well as the Lapabot System, are two more widely used robots in tele-surgery [40,41].

2.5.3. Neurosurgical Telesurgery

This deals specifically with remote surgery on neurosystems. The Socrates Robot Remote Cooperative System was the first system developed that was mainly responsible for surgical training [42]. Neuro-Arm is another tele-neurosurgery-based system that is useful in fusing MRI data with a 3D view, but it is also useful in short-distance tele-neurosurgery [43]. China has developed tele-robotic-directed neurosurgery, which is one of its kind and is capable of all fourth-generation tele-surgery features [43].

2.5.4. Orthopedic Telesurgery

In this method of tele-surgery, there are two main components involved, namely a high-end 3D camera, and a robot responsible for tackling the master–slave-based communication. The surgeon performs the task, first by visualizing the patient, by looking at the screen, and then, in order to control the remote robot, the surgeon uses a haptic arm (HA). In response to this, the robot arms interpret the instructions given by the surgeon, who is sitting remotely. This arrangement is useful for treatment, as the robot mimics the natural movement of the surgeon. The main factor enabling this transition of input from surgeon to robot is haptic technology (HT). HT has become more efficient with the inclusion of artificial intelligence and virtual reality [44].

3. Security Requirements and Design Challenges

Security is a vital issue for data exchange between medical devices in IoMT-based systems. The data of the patient are very sensitive, as they are particularly personal. The medical history and symptoms of the patients are processed and recorded in IoMT-based systems. Therefore, this data must be protected from the attacker. In order to better understand the various security parameters [45–48], the four most important are discussed in the below enumeration.

3.1. Security Requirements

- Confidentiality/Privacy: Confidentiality, or privacy, is the top priority, as a huge amount of sensitive and personal data is processed and stored across IoMT devices. These data should be accessible to the authorized user via a proper authentication mechanism; furthermore, the stored data should be encrypted to avoid ease of access by an adversary. The encryption adopted must be secure enough to safeguard from attackers [46].
- Integrity: The integrity of data in the IoMT is essential, as these inputs are used for the treatment of the patients. Integrity ensures that the data has not been modified,

either during transmission or during the storage process. The modification of data may consist of deleting it, adding false values, etc. It is important to safeguard the sensitive data of the IoMT to stop unauthorized access.

- Authentication: The validation of authorized users for communication is key to performing identity authentication. To authenticate an identity, both communicating parties must mutually verify themselves. The transfer of data and information occurs after mutual authentication. The IoMT consists of various services, including the cloud, that need adequate authentication. The authentication mechanism may vary according to the various IoMT-based applications [47].
- Non-Repudiation: This is particularly crucial because an illegal entity could not deny the validity of the messages. To validate the messages, the proof of origin is mentioned along with the integrity of the data. The denying of the message becomes extremely tough when the source or origin is mentioned. The concept of a digital signature is widely used for implementing non-repudiation.
- Availability: This feature ensures that the information and services are accessible to authorized users only. The availability feature is exploited by the adversary or attacker by executing a denial-of-service (DoS) attack. This attack is generally launched when confidentiality and integrity of the system remain intact and the attacker is unable to compromise these two features [48].
- Backward and Forward Secrecy: The backward and forward features are an integral part of the IoMT-based system since it consists of hardware devices in large numbers. Forward secrecy suggests that, if any device leaves the IoMT system, then it should be discontinued, so that it could not access any communication within the existing system. Moreover, in case of backward secrecy, newly installed devices in IoMT systems should not have any access to previously transmitted messages.

3.2. Design Challenges in the IoMT

- Postural body movement: The sensors which are used in on-body medical devices, as well as other sensors, are usually placed in a group. The movement of the patients using these devices and sensors is not consistent, as they are highly mobile. The transmission used to monitor postural body movement could be optimized by a quality change associated with the movement of the patient [49].
- Temperature rise: A temperature rise is generally observed in any hardware-based system. In the case of the IoMT, two main factors raise the temperature of the system. Radiation through the antenna is the first cause, while the consumption of power is the other major cause [50].
- Energy efficiency: Energy efficiency is preserved in IoMT-based systems by designing them in such a way as to make optimal use of energy on local devices or sensor nodes, and also optimize the energy consumption of the overall network across its lifetime. This implementation is especially important in the case of surgical devices in IoMT-based systems, where the battery is the main source of energy [51].
- Transmission range: The transmission, when it occurs across a very short range along with movement of the body, sometimes leads to disconnection, as well as re-partitioning in the sensor present in the IoMT. There is a need to minimize the total number of sensors on the patient's body to reduce disconnection. IBS is one of the methods whereby transmission is made more optimal [52].
- Heterogeneous environment: IoMT-based systems are generally comprised of various devices and sensors, which are manufactured by different manufacturing companies. These devices use different architectures for their operation. Thus, the system becomes highly heterogeneous. Therefore, the network must be capable enough to tackle these heterogeneities to route the data and information properly in the IoMT-based system.

3.3. Concerns in the IoMT

Security concerns are high in IoMT-based systems as the system is heterogeneous, and also consists of wireless communication, thus making it vulnerable to wireless network-based attacks. The eavesdropping and man-in-the-middle (MitM) attacks are two main major attacks that are possible against wireless-based communication. Privacy concerns are high in the case of the IoMT, and attacks on network traffic aiming to gain sensitive information about patients are a serious threat to IoMT-based systems. Passive attacks are more prevalent in systems where there is a possibility of identity theft. Trust concern relates to trust management, and deals with the accountability of the service provider to the users. Any breach of sensitive and private data results in the loss of the trust of the user in the service providers. A lack of training among healthcare workers and employees could lead to permanent damage to the patients, and might also result in loss of life. Data falsification, or the transmission of wrong data, could result in delivering the wrong drugs, or the wrong amount of drugs, into a patient's body, which might create serious issues. Accuracy becomes paramount when robots are used in an IoMT-based system, as their mishandling could have fatal results.

3.4. Prevalent Attacks in the IoMT

Although there exist some state-of-the-art techniques to secure IoMT systems, nowadays the adversaries are also equipped with advanced techniques to exploit them. There are various aspects through which the IoMT can be targeted by cyber-attacks [53]. In general, adversaries try to compromise the confidentiality–integrity–availability (CIA) triad of an IoMT network. Thus, their attacks can be either active or passive, and are categorized as attacks against data confidentiality, privacy, device authentication, and many more [54]. The Sybil attack is also a prominent tool used to target IoMT networks [55]. Table 2 presents various cyber-attacks prevalent against the IoMT.

Table 2. Cyber-attacks in the IoMT.

Category	Attacks	Possible in IoMT
Data confidentiality attacks [2,56]	Man-in-the-middle (MitM) Packet sniffing	Yes
Social engineering attacks [24]	Pretexting Baiting attack	Yes
Privacy attacks [57]	Black-box attack White-box attack	Yes
Availability attacks [58]	Distributed DoS (DDoS) Flooding attacks	Yes
User or device authentication attacks [59]	Brute forcing, masquerading, replay attacks, session hijacking, rainbow attacks, dictionary	Yes
Malware attacks [60]	Spyware, Trojan, rootkit	Yes

3.5. Existing Security Framework for IoMT-Based Applications

Security of the IoMT is crucial, as this type of infrastructure consists of particularly sensitive and private data that ranges from the personal health condition of a person to his/her insurance details. According to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), it is necessary for any organization dealing with the medical data of a user to safeguard the data, and only give privilege for the electronic transfer of data to a third party for processing when the user has given their consent for the same [61]. Therefore, if the IoMT system includes data from a US Citizen, this Act needs to be followed by the organization. Additionally, if the IoMT infrastructure falls within the European Union, the IoMT-based organization must then abide by the General Data Protection Regulation (GDPR) [62].

J. Rauscher et al. [63] proposed a framework model on security for the IoMT, known as the IoT safety and security architecture analysis framework (IoT- S2A2F). This model is useful in analyzing existing IoMT infrastructure, as well potential new infrastructure, for vulnerability assessment in order to tackle threat vectors. Additionally, models such as the architecture analysis and design language (AADL) are very crucial for threat hunting and finding vulnerabilities in a system based on the IoT infrastructure [64]. The misbehavior detection system (MDS) is yet another important model that deals with the privacy, as well as security, of the IoMT system. S. Rahmadika et al. [65] proposed a blockchain-based framework for enhancing the intrusion detection capability of blockchain. This model is especially effective when the system is very heterogeneous, as the blockchain can detect even slight changes in the value of the asset, and thus making the model very sensitive to intrusion upon the system. The security of the IoMT is critical because various devices of different architecture and protocols communicate with each other within it; therefore, it is important to segregate the network into layers. The use of the layered security model (LSM) would be helpful for pen-testers investigating points of weakness in IoMT-based applications. The safeguard of MDS is very crucial in avoiding harmful injection attacks, as a harmful SQL injection could lead to the complete credentials of patents being compromised. Choudhary et al. [66] have proposed a lightweight misbehavior detection scheme that relies on formal verification and automatic model checking in a medical cyber physical system. In another work, Astillo et al. [67] aimed to mitigate security threats, by using a specification-based misbehavior detection model, and validate the data integrity using outlier detection algorithms.

3.6. Risk Analysis and Threat Mapping

The risk analysis is a very crucial aspect of the security efforts, as it helps to analyze the level of threat. This analysis could be performed using the threat mapping technique, whereby the threats are mapped according to their severity. Table 3 depicts the threat and risk associated with the various IoMT elements.

Table 3. Threat and risk mapping.

IoMT Assets	Possible Threat Entry	References	Risk	Severity
Gateway	Attack from WAN	Gao et al. [68]	The ARP table could be poisoned that is exiting in Gateway router	High: as it may reveal important IP of internal switches and routers
Helpdesk Workstation	LAN and WAN	Gopal et al. [69]	Virus could be inserted or phishing mail could be sent to reception.	Low: as generally this workstation does not consists of any permanent data, only appointment times and patient names
Web Server	WAN	Shah et al. [70]	Consist of the web application on which IoMT website and application would be running	High: this may lead to complete failure hospital management system and bring the organization back to pen and paper mode
MD	LAN and WAN	G. M et al. [71]	Consist of admin and other users' passwords	High: as it can compromise the complete digital infrastructure.
Filed Sensors	Hardware means	Elmahi et al. [72]	Jammer could be used to create noise	Moderate: this can reduce the efficiency of reporting of data to the centralized server performed by Filed Sensors
SIEM	WAN and LAN	-	If the monitoring framework itself becomes compromised then, then all internal and external attacks would not be visible	High: this will create problems in the monitoring of logs, networks and other vulnerable areas where attacks could take place.

4. Security Techniques in IoMT

The above-explained attacks suggest that there is a strong need for securing the IoMT, as it could be vulnerable to cyber-attacks. The below subsections explain various vital security techniques required for securing the IoMT.

4.1. Symmetric Key Cryptography

Symmetric cryptographic algorithms are based on shared/secret keys between the communicating nodes, and require prior key generation. These algorithms are useful in IoMT systems for initiating secure connections and hierarchically accessing the patient's data. Furthermore, these facilitate two-factor authentication, in which other techniques, such as pattern-based and facial recognition, act as the second factor [73]. The role of symmetric key algorithms in IoMT systems is discussed in the subsections below.

4.1.1. Hierarchical Access

This technique provides role-based authorization and facilitates hierarchical access to patients' data using a hierarchical role-based architecture. For instance, any nurse can administer medicines, but only an authenticated doctor can prescribe a new medication. The model requires a hierarchical security technique of relatively low complexity that enciphers the patient's personal information and deciphers only part of the data. Belkhouja et al. [74] proposed a role-based encryption standard that guarantees hierarchical access to patients' data and also overcomes the computational shortcomings of implantable medical devices (IMDs). Their standard achieves the desired encryption hierarchy by using the Chinese remainder theorem (CRT), where the users can access the patient's data according to the assigned privilege [75]. A more privileged user can access any data, whereas users with restricted privilege can access only the relevant data.

4.1.2. Biometric Systems

Most IoMT systems rely on facial scanning for authenticating users in a continuous role-based authentication process. The shared keys serve as the first authentication factor, while facial recognition serves as the subsequent authentication factor. This enables a secure connection between the medical controller and the sensor [76]. Further, the system is capable of securing the overall medical setting and preventing the staff from having limited privilege to access the data. In another work, Belkhouja et al. [77] proposed an elliptic curve cryptography (ECC)-based authentication scheme that allows secure access to implanted devices and protects wireless key exchange. This works by using integrated fingerprint and electrocardiogram to create a lightweight, efficient, and secure authentication scheme for IMDs.

4.1.3. Gait-Based Scheme

This scheme generates unique symmetric keys using the human walking pattern. Sun et al. [78] proposed a novel biometric cryptosystem that uses an artificial neural network (ANN) and gait signal energy variations for securing wireless communications in implantable and wearable healthcare devices. Their approach extracts similar features from the body sensors, and aims to generate on-demand binary keys without any manual intervention. The proposed scheme outperforms the existing state-of-the-art techniques in terms of the number of bits generated per gait cycle. A 128-bit key is generated to secure communications between the access points and IoMT sensors. Furthermore, the generation of binary keys at different times adds randomness to the keys without any direct system–user interaction.

4.1.4. Cryptographic Hash Function (CHF)

CHF is a one-way function that maps an arbitrary size input to fixed-size data [79]. In healthcare scenarios, the initial parameters (such as a shared key and node ID) can be XORed together (to verify if one of the operands is different), and then hashed. The hash value is then shared with the gateway and sensor nodes to generate their keys [80]. IoMT systems can use authenticated key agreement protocols and secure communications by integrating the XOR operator, a symmetric key, and the CHF. Xu et al. [81] proposed a lightweight authentication technique that guarantees forward secrecy in wireless body area networks (WBANs) without exploiting asymmetric encryption standards. The proposed

scheme incurred low computational costs and is less vulnerable to security attacks, as compared to other lightweight security schemes. Alzahrani et al. [82] proposed a provably secure and reliable key agreement-based health monitoring protocol that is resistant to some of the most prominent attacks against WBANs, such as key compromised impersonation attacks and replay attacks.

4.2. Asymmetric Key Cryptography

Asymmetric cryptographic algorithms include two keys: a private key (for decryption/signature), and a public key (for encryption/validation). Everyone knows the public key, whereas only the owner knows the private key. Figure 3 depicts the process of encryption/decryption in asymmetric key cryptography. Some of the most widely accepted algorithms in this category include elliptic curve cryptography (ECC) and Rivest–Shamir–Adleman (RSA) [83]. ECC in particular is useful in securing IoMT systems, owing to its lightweight features. Furthermore, asymmetric keys can also provide two-factor authentication. Asymmetric keys can act as the first factor, and are supported by various techniques (such as smart cards used in hospitals) that serve as the second factor. The role of asymmetric key algorithms in IoMT systems is discussed in the subsections below.

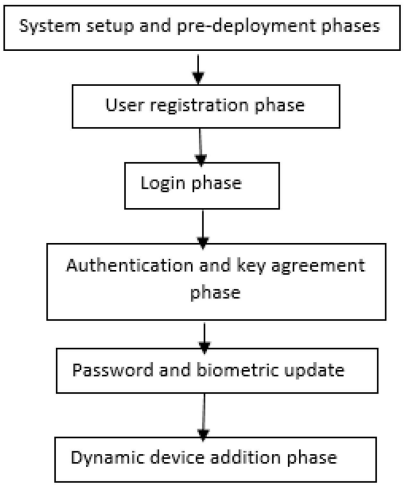

Figure 3. User device management in the IoMT.

4.2.1. Homomorphic Encryption (HE)

HE ensures data confidentiality and mitigates the mathematical complexity linked to data encryption. In IoMT settings, it maintains data privacy and allows only the patient to access their data by storing the encrypted data in the cloud layer. For example, IoMT sensors in smartwatches allow continuous data encryption and reveal the relevant data to medical staff only during an emergency, when necessary to perform a proper diagnosis. Sun et al. [84] fully leveraged HE to encipher patient data in a mobile healthcare network, in order to achieve computations on the cipher text. In another work, Jiang et al. [85] utilized HE to achieve privacy preservation in medical diagnosis. Farooqui et al. [86] proposed a human-centered model to identify and treat mental healthcare patients by integrating an encrypted cloud computing paradigm and emerging IoT wearable technologies. Guo et al. [87] proposed a homomorphic encryption-based privacy-preserving scheme that prevents the leakage of cluster center data and the disclosure of participants' privacy. Kara et al. [88] proposed a full HE scheme based on magic number fragmentation and twin key encryption. The proposed scheme is resistant to brute-force attacks and effective against cryptanalytic attacks in smart city applications.

4.2.2. CHF with ECC

Integration of ECC keys and CHF function can help in realizing a certificateless secure channel between medical doctors and their patients. This integration allows the sharing of

keys securely between the key generation server (KGS) and nodes in IoMT layers. Node ID, ECC public key, and other preliminary parameters are hashed with the help of CHF. The hashed value is then sent to the nodes in the IoMT gateway and sensor layers. Asymmetric keys can be generated from the received hash values, thereby solving the prominent issues of secret key sharing in symmetric cryptographic techniques [89]. Furthermore, this can mitigate the certificate management overhead for data sharing and storage in the cloud [90]. Considering the substantial increase in IoMT data sizes, it is advantageous to divide the medical data into subsets and share them securely using CHF and ECC keys. Maria et al. [91] integrated ECC and other software implementations to designing secure and privacy-preserving solutions for IoMT communications. The proposed scheme guarantees origin authentication, integrity, and data source anonymity, with complexity and computational requirements within acceptable limits. Zheng et al. [92] aimed to preserve data integrity using ECC and data encryption standards (DES) in electrocardiogram (ECG) monitoring systems. Ogundokun et al. [93] presented a crypto-stegno model to preserve the confidentiality of the patient's EHRs in an IoMT environment. Sowjanya et al. [94] designed a lightweight, robust, and anonymous ECC-based authentication protocol for securing medical data in WBANs.

4.2.3. Digital Signatures

Digital signatures have been employed for verifying data authenticity in a small IoMT system using the public and private keys of the sender for verification and signature respectively [95]. These can be integrated with the sensor's firmware in IoMT systems with an add-on to intercept and validate wireless communication [96]. This method mandates the storage of public keys of authorized users in the sensor's firmware for validation. Farahat et al. [97] aimed to guarantee secure authentication and data privacy using digital signatures and key rotation schemes. Kumar et al. [98] proposed a smart, escrow-free, identity-based cloud-centric IoMT system that gathers patients' data and outsources it to a medical cloud server after sign-encrypting and aggregating them.

4.3. Keyless Algorithm

Security schemes based on blockchain technology, proxy-based techniques, and biometrics guarantee security without the need for pre-shared keys. The role of keyless algorithms in IoMT systems is discussed in the subsections below.

4.3.1. Blockchain Technology

Blockchain technology is employed in IoMT systems for security management and data sharing. However, due to strict communication requirements and larger data chunks, blockchain is susceptible to communication overhead, latency, and storage issues [99]. Nguyen et al. [100] designed a smart contract-based access control mechanism for securely sharing EHRs in IoMT systems. Similarly, Garg et al. [101] proposed a blockchain-enabled key agreement scheme aimed at providing secure key exchange between cloud servers, personal servers, and medical devices. In another work, Meng et al. [102] utilized blockchain for detecting malicious nodes by enhancing trust management in medical smartphone networks. Gao et al. [103] proposed an integration of blockchain technology and edge computing for safeguarding the confidentiality of data analysis in IoMT systems. The proposed framework relies on blockchain for authenticating the cloud service providers and IoMT devices in the network. Egala et al. [104] proposed a blockchain-based, decentralized, and automated access control technique for IoMT systems. The proposed technique utilizes a hybrid computing paradigm and solves the issues related to latency, high cost, and single point of failure. In another work, Jin et al. [105] presented a blockchain-based cross-cluster federated learning solution for secure data sharing in IoMT systems. Similarly, Awad et al. [106] integrated blockchain and edge computing to optimize the computational cost and latency of medical record sharing between entities.

4.3.2. Proxy-Based Systems

Proxy-based systems facilitate full duplex secure communication, and rely on a middleware device for controlling the communication between devices such as medical controllers and sensors. Kulac et al. [107] aimed to secure communications in implantable medical device (IMD) systems and provide full duplex secure transmissions using a protective security belt. Verma et al. [108] presented a provably secure and efficient proxy signature scheme for e-healthcare systems. In another work, Bhatia et al. [109] proposed a proxy-based, pairing-free, and lightweight re-encryption scheme for securely sharing the EHRs with the public cloud. In the proposed scheme, patients use the public key to encrypt data before outsourcing it to the cloud. Kulac et al. [110] aimed to protect IMDs from adversaries and achieve full duplex secure communications using a middleware device, named the protector jacket. The protector jacket uses spoofing-based beamforming techniques to support longer battery life and higher power efficiency. In another work, Li et al. [111] integrated the concept of public key encryption and proxy re-encryption to search healthcare records securely and flexibly.

4.3.3. Biometrics

One of the most widely accepted techniques to enhance security in IoMT systems is the use of biometric sensors. Patients and the medical staff can access the medical records only after biometric authentication in a medical setting. ECG-based sensors and fingerprints are the most commonly used biometrics. ECG-based sensors encrypt data based on heartbeat activities and fingerprint sensors rely on reading the fingerprint image. Fingerprint sensors are superior to ECG-based techniques in terms of computational overhead and message size. Zheng et al. [112] proposed a finger-to-heart authentication technique that aims to utilize the patient's fingerprint for granting access to the IMD. In another work, Zheng et al. [113] used fingerprint information to safeguard elderly people suffering from memory loss and protect them from malicious adversaries in IoMT systems. Shakil et al. [114] proposed a biometric-based authentication scheme to secure health data using a behavioral biometric signature.

The major security advances in IoMT scenarios are summarized in Table 4.

Table 4. Recent security advances in IoMT scenarios.

Security Techniques in IoMT	References	Year	Major Contribution
Symmetric key cryptography	Liu et al. [73]	2019	Lightweight NTRU public key cryptography-based security protocol
	Belkhouja et al. [74]	2019	Role-based encryption standard to Overcome the computational shortcomings of IMDs
	Tutari et al. [76]	2019	Role-based authentication for IMDs
	Belkhouja et al. [77]	2019	Secure access to implanted devices and protects the wireless key exchange.
	Sun et al. [78]	2019	Biometric cryptosystems that use ANN and gait signal energy variations
	Xu et al. [81] proposed a	2019	Lightweight authentication technique to guarantee forward secrecy in WBANs
	Alzahrani et al. [82]	2020	Provably secure and reliable key agreement-based health monitoring protocol

Table 4. *Cont.*

Security Techniques in IoMT	References	Year	Major Contribution
Asymmetric key cryptography	Sun et al. [84]	2017	Fully homomorphic encryption in healthcare networks
	Jiang et al. [85]	2019	Privacy-preserving in IoT
	Farooqui et al. [86]	2019	Human-centered model to identify and treat mental healthcare patients
	Guo et al. [87]	2020	Homomorphic encryption to prevent leakage of patients' data
	Kara et al. [88]	2021	Magic number fragmentation and twin key encryption
	Kasyoka et al. [89]	2020	Pairing-free authentication protocol for WBANs
	Bhatia et al. [90]	2020	Healthcare data sharing using incremental proxy re-encryption
	Maria et al. [91]	2020	Secure and privacy-preserving solutions for IoMT communications
	Zheng et al. [92]	2020	Preserves data integrity in healthcare monitoring systems
	Ogundokun et al. [93]	2021	Preserves data confidentiality using crypto-stegno model.
	Sowjanya et al. [94]	2021	ECC-based authentication protocol for securing medical data in WBANs.
	Easttom et al. [96]	2019	Cyberthreats in implantable medical devices
	Farahat et al. [97]	2018	Secure authentication using digital signatures and key rotation schemes.
	Kumar et al. [98]	2020	Identity-based cloud-centric IoMT system
	Nguyen et al. [100]	2019	Smart contract-based access control mechanism for securely sharing EHRs
	Garg et al. [101]	2020	Blockchain-enabled key agreement scheme
	Meng et al. [102]	2020	Blockchain-based trust management in medical smartphone networks
	Gao et al. [103]	2021	Blockchain technology and edge computing to maintain confidentiality in IoMT systems.
Keyless algorithm	Egala et al. [104]	2021	Automated access control technique for IoMT systems
	Jin et al. [105]	2021	Blockchain-based cross-cluster federated learning solutions for secure data sharing in IoMT systems
	Awad et al. [106]	2021	Optimize computational cost and latency of medical record sharing
	Kulac et al. [107]	2017	Protective security belt to provide full duplex secure transmissions
	Verma et al. [108]	2017	Proxy signature scheme for e-healthcare systems
	Bhatia et al. [109]	2018	Lightweight re-encryption scheme for securely sharing the EHRs
	Kulac et al. [110]	2019	Protector jacket to protect IMDs from adversaries
	Li et al. [111]	2020	Public key encryption and proxy re-encryption for securely searching healthcare records
	Zheng et al. [112]	2019	Use the patient's fingerprint for granting access to the IMD
	Zheng et al. [113]	2020	Fingerprint information to safeguard elderly people suffering from memory loss
	Shakil et al. [114]	2020	Behavioral biometric signature to secure health data

5. Taxonomy of Security Protocols in IoMT

The taxonomy discussed in this section focuses on various protocols that are vital for the IoMT. Moreover, the other function of security protocols in IoT communication environments, apart from providing security, is to store, as well as exchange, data. The optimality of security features is a crucial part, not only in the IoMT, but rather in every system which relies on channels of communication for their desired end task. Here, in the case of the IoMT, since the data are more sensitive (mental health of patient, drugs used by him or her) and more private (his relationship, as mentioned in insurance documents), this creates an area of interest for adversaries, and the weak protocol becomes a particularly vulnerable point for such a system. Protocol attacks, which are also sometimes referred to as

state-exhaustion attacks, are very dangerous. Therefore, it is important to use more secure protocols in the case of the IoMT. It is crucial to understand how the least privilege is being tackled using the access control (AC) concept and how the cryptography plays important role in making the protocols more resilient in detecting, preventing and mitigating state-exhaustion attacks.

Figure 4 shows the taxonomy of security protocols in the IoMT. The below subsections discuss the vital aspects of security protocols for the IoMT.

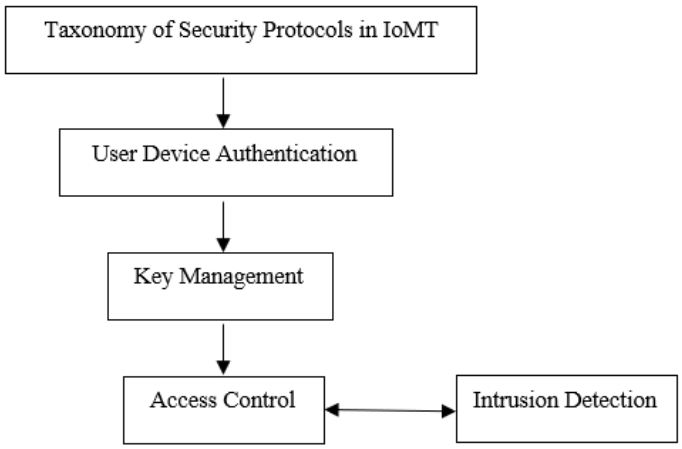

Figure 4. Taxonomy of security protocols in IoMT.

5.1. Key Management

The role of the key management (KM) protocol is to create, manage, and distribute cryptographic keys between the entities interacting with one another in the IoT/IoMT environment. Based on the requirements, the whole process is classified into various phases, such as key generation, key exchange, key usage, and key revocation. A "cryptographic technique" is followed by the key management mechanism that supplies the details of various static or mobile users, different IoT devices, as well as key servers. For secure communication, robust key management plays the most significant role in this context [115]. KM goes through four different phases. Figure 5 presents the various phases of key management in IoMT-based systems.

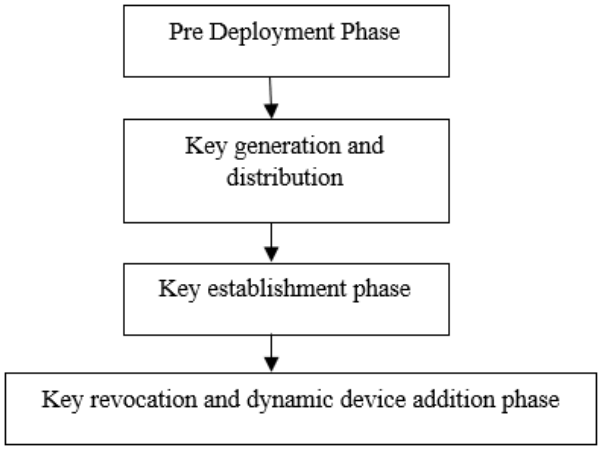

Figure 5. Key management in the IoMT.

5.2. User Device Authentication

The process of identifying and verifying the identities of the communication parties is known as user authentication. Often, in device or user authentication, the communicating parties carry out this verification among themselves before establishing the session key for

communication. This is termed mutual authentication [116]. Figure 3 explains the working scenario of user device management in IoMT-based systems.

5.3. Access Control

Permission management is crucial to avoid the mishandling of data and resources in any system. This is frequently implemented using an access control mechanism. Access control is intended to limit and manage access to resources that include data, devices, and networks. In the case of the IoMT, the devices are granted the privilege to access the resources. This is intended to improve the smooth functioning of the IoMT-based system. The longevity of the IoMT-based system could be increased by adding new devices, which could be generic or smart. This is required, as many devices are battery based and their batteries degrade with time. The physical attack could be performed when the adversary replaces the original device in the network with the infected one [117]. To secure such devices, the designing of IoMT-based systems should follow an access control mechanism [118–120]. The access control is implemented using node authentication (NA) and key establishment (KE). NA is essential in avoiding physical attacks upon the addition of a new device to the existing IoMT system, as it should first authenticate itself with the neighboring devices to confirm to them that it is an authentic device, not an illicit one. Moreover, KE helps to secure future communication across the whole system when a new device is added. This is achieved by enabling secret key sharing between the existing and newly added devices. Apart from these, it is very important to grant access to legitimate users only.

5.4. Intrusion Detection

Detection of intrusion in a system is vital for the normal function of the system. Intrusion detection system (IDS) is very helpful in the analysis of malicious activities that occur inside the network of the targeted system. The IDS is capable of detecting and preventing various types of attacks attempted against the system. The IDS, when installed in the IoMT system, monitors the network and detects any anomalies initiated in the traffic. If an anomaly is detected, IDS will then alert the system and corresponding devices will take appropriate action based on this alert. The IDS could send a message to the admin to block an IP that seems malicious [121]. The adversary can sometimes physically access the device and replace it with an infected one. Moreover, a power analysis attack could be used by the adversary to gain sensitive information from the system [122,123]. This could give credential information to the adversary and, using these gained credentials, the adversary could implant his own devices. These maliciously crafted devices could be used by an adversary to execute a more devastating attack. The IoMT could also be attacked by various types of viruses and malware. Moreover, new malware could also attack the existing IoMT system. Further details of the detection mechanism are discussed in the below enumerations.

6. Future Research Directions

The IoMT is increasing the efficiency and accuracy of the treatment of patients through real-time monitoring of patients' healthcare data. Despite the IoMT being an extremely recent and advanced technology, the system is vulnerable to cyber-attacks because of its heterogeneous nature. The below subsections present a few vital points to be incorporated into future research.

6.1. Scalability of Malware Detection

The IoMT is a combination of a huge number of heterogeneous devices, networks, applications, and paradigms for data transfer that have distinct features and requirements. The detection of malware in a such complex environment is a very challenging task. The use of an "electronic health recorder (EHR)" to store the information of users over the IoT-based cloud for processing is one way to resolve heterogeneity issues in the IoMT.

Moreover, the BAN also produces a enormous amount of data in the IoMT environment. Therefore, in order to detect malware in a such complex environment, there is a need to develop a more specific method. Hence, more research is needed.

6.2. Cross-Platform Malware Detection

The deployment of malware detection tools in the IoMT environment is difficult because of its heterogeneity. It becomes tough to design such tools and mechanisms that could detect malware in a cross-platform environment. For instance, if there is an exchange of data and information from smart homes to smart healthcare to monitor the patients, the system becomes more convoluted, and, therefore, the detection of malware becomes a tedious task. Therefore, uninterrupted network-based malware techniques need to be developed.

6.3. Security Assessment

The methods of performing security research are versatile in their parameters. Different research groups or individuals carrying out research on the IoMT use different parameters for the analysis of security. Hence, there is no uniformity in the research. The use of adversarial analysis concepts and tools used by researchers does not consider the same parameters and inputs between different researchers. Therefore, comparing the proposed work of each individual or research group is quite challenging. Consequently, future research is required to define a set of parameters that could be used for research to strengthen the security of the IoMT.

6.4. Paradigm Shift in IoMT Sensors

The transition in society occurs at a faster pace when the new technologies emerge at a faster rate. The shifting from traditional to newer technologies, such as the IoMT, is the result of such a transition. A transition is currently taking place, from a generic method of tracking patients' health to clinical data integration, where sensors play a vital role in IoMT-based systems. Mobility in the IoMT is the principal feature that has revolutionized the tracking and caring of patients' health.

6.5. Security and Privacy

A significant amount of private and sensitive data is present in IoMT-based systems, and, over time, this considerable volume of data is increasing. The use of blockchain technology and cryptography are two vital elements that could make an IoMT-based system safer. The use of SHA-256 makes data integrity more efficient. The use of blockchain has entered into various fields of technology, and its use in IoMT would be very useful to achieve the integrity of data.

6.6. Blockchain for Healthcare Data Sharing

The data used in the IoMT-based system are highly sensitive. Apart from the healthcare employees, the patients are the complete controllers of these data. Therefore, there is always a chance of the leakage of data. The use of a time-stamped feature of blockchain could be very useful in detecting the integrity of such data and information. Once these data are stored in a distributed ledger, the detection of an anomaly in patients' data could be tackled efficiently.

6.7. Heterogeneity in an IoMT Communication Environment

The IoMT consists of a huge range of distinct devices and systems, such as full-edged systems, workstations, tablets, smartphones, RFID tags, etc. Communication occurs between these devices using an inter-connected network, and these devices use various protocols to communicate among themselves. These devices have their own differing storage capability, range of communication, and operating system, as well as power con-

sumption rate. Therefore, the detection of attacks in such a system needs to develop in a more specialized manner.

7. Research Challenges and Lessons Learned

The IoMT is evolving continuously, with the development of more digital medical devices and the advancement of new network security devices. Future research needs to focus on the below discussed points.

- The research on the network is very important for the IoMT. The backbone of the IoMT is the network through which each device communicates with others to yield the desired task. Therefore, if the device has to operate in a real-time scenario, as in the case of tele-surgery, the delay in transmission could result in the loss of human life. Hence, latency is one of the main concerns in such a scenario, where the healthcare worker is performing surgery through a haptic arm. Moreover, channel-based attacks are very deadly, as they could compromise the data on transit, and, hence, the integrity of the original data could be compromised. Therefore, it is crucial to deal with zero-day-based attacks over the communicating medium in the IoMT.
- The next area of concern for the future is the devices that are a part of the IoMT system. As we know that there is no standard architecture to be followed by everyone implementing IoT applications, so the same goes for the IoMT. There are devices, such as CCTV cameras and filed sensors, that do not have the capacity to update their software, and therefore become obsolete in terms of security after a particular time. Consequently, it is necessary to replace them with more advanced and newer versions. Hence, there could be future research on updating these devices while connected to the IoMT, rather than replacing them, in order to reduce the cost of implementing visual surveillance within the IoMT.
- The next area of research, which plays an important role in the function of the IoMT, is the application software and system software, which work, either as intermediates between the hardware and software or on top of them, for various medical processes. Some of the most widely used software in medical environments are electronic health records (EHR), hospital management systems (HMS), telemedicine software, etc. It is important to identify, on a regular basis, any vulnerabilities in the codes of these software, and there is therefore a need for a proper standardized framework to define the security check in this software. Moreover, there is a need to inspect the operating system code involved in the devices which are involved in the IoMT, in order to identify the existence of any zero-day attacks.
- The use of secure communicating channels, identification of vulnerabilities in the system at the right time, and the use of appropriate software and hardware to protect the IoMT application would not be possible without having effective governance, risk, and compliance (GRC) processes. These policies play a crucial role in the efficient working of the organization. Since, in the case of the IoMT, various more personal and sensitive data are involved, both locally and also remotely, it become very important to understand which of the patient's data require explicit permission from the patient for access, so that his/her fundamental rights are not violated. Furthermore, the policy should clearly identify the authorization domain for each employee, in order to safeguard against data breaches that may occur due to weak policy. Therefore, the use of efficient policy specifically for the IoMT is needed in future.

8. Conclusions

IoT-based connected medical and e-healthcare solutions, such as the IoMT, are proving to be revolutionary for the healthcare industry. The growth in related applications has been of immense help to the healthcare providers, such as clinics, hospitals, practitioners, and care givers, in providing patients with the most accurate, predictive, and effective medication strategies. Therefore, IoT-based solutions for e-healthcare services are emerging as a vital component to help match the demanding needs of the digital society. The IoMT

assists in real-time patient monitoring and allows all the related domains of healthcare to work together as one unit, with the help of an interconnected network. Furthermore, to maintain a high level of privacy, security, accuracy, and trust, it is highly recommended and essential to train IT and medical staff to ensure that they do not fall victim to cyber-attacks. Therefore, the main aim of this paper is to tighten the ties between the varied non-technical and technical solutions to enable increasingly efficient, secure, and sophisticated IoMT systems. In this paper, we discuss the security requirements, design challenges, novel attacks, and state-of-the-art security techniques that are essential to making IoMT-based systems more secure. The paper explores three vital security techniques required for securing IoMT systems, namely, asymmetric key algorithms, symmetric key algorithms, and keyless algorithms. Finally, the paper discusses various future research directions that will guide future researchers working in this area.

Author Contributions: Conceptualization, B.B. and A.K. (Avinash Kumar); methodology, A.K.A., P.B. and A.K. (Avinash Kumar); formal analysis, A.K. (Arun Kumar), A.K. (Amit Kumar) and A.K. (Avinash Kumar); investigation, P.B., A.K. (Amit Kumar) and A.K.A.; resources, A.K. (Avinash Kumar), B.B. and P.B.; writing—original draft preparation, A.K. (Avinash Kumar), A.K. (Arun Kumar) and B.B.; writing—review and editing, A.K.A., P.B. and A.K. (Amit Kumar); supervision, B.B.; funding acquisition, B.B. 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. Vishnu, S.; Ramson, S.R.J.; Jegan, R. Internet of medical things (IOMT)—An overview. In Proceedings of the 2020 5th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 5–6 March 2020. [CrossRef]
2. 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.* **2021**, *8*, 8707–8718. [CrossRef]
3. Dilibal, C. Development of edge-IOMT computing architecture for smart healthcare monitoring platform. In Proceedings of the 2020 4th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT), Istanbul, Turkey, 22–24 October 2020. [CrossRef]
4. Joshi, S.; Joshi, S. A sensor based secured health monitoring and alert technique using IOMT. In Proceedings of the 2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), Jaipur, India, 28–29 September 2019. [CrossRef]
5. Rizk, D.; Rizk, R.; Hsu, S. Applied layered-security model to IOMT. In Proceedings of the 2019 IEEE International Conference on Intelligence and Security Informatics (ISI), Shenzhen, China, 1–3 July 2019. [CrossRef]
6. Hatzivasilis, G.; Soultatos, O.; Ioannidis, S.; Verikoukis, C.; Demetriou, G.; Tsatsoulis, C. Review of Security and privacy for the internet of medical things (IOMT). In Proceedings of the 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, 29–31 May 2019. [CrossRef]
7. Wazid, M.; Das, A.K.; Rodrigues, J.J.; Shetty, S.; Park, Y. IOMT malware detection approaches: Analysis and research challenges. *IEEE Access* **2019**, *7*, 182459–182476. [CrossRef]
8. Karmakar, K.K.; Varadharajan, V.; Tupakula, U.; Nepal, S.; Thapa, C. Towards a security enhanced virtualised network infrastructure for internet of medical things (IOMT). In Proceedings of the 2020 6th IEEE Conference on Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020. [CrossRef]
9. Sittampalam, G.; Ratnarajah, N. Enhanced symmetric cryptography for IOT using novel Random secret key approach. In Proceedings of the 2020 2nd International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 10–11 December 2020. [CrossRef]
10. Sowjanya, K.; Dasgupta, M. Survey of symmetric and asymmetric key management schemes in the context of IOT based healthcare system. In Proceedings of the 2020 First International Conference on Power, Control and Computing Technologies (ICPC2T), Raipur, India, 3–5 January 2020. [CrossRef]
11. Mursi, K.T.; Zhuang, Y.; Alkatheiri, M.S.; Aseeri, A.O. Extensive examination of XOR arbiter pufs as security primitives for resource-constrained IOT devices. In Proceedings of the 2019 17th International Conference on Privacy, Security and Trust (PST), Fredericton, NB, Canada, 26–28 August 2019. [CrossRef]

12. Ray, I.; Kar, D.M.; Peterson, J.; Goeringer, S. Device identity and trust in IOT-sphere forsaking cryptography. In Proceedings of the 2019 IEEE 5th International Conference on Collaboration and Internet Computing (CIC), Los Angeles, CA, USA, 12–14 December 2019. [CrossRef]
13. Bao, Q.; Li, B.; Hu, T.; Sun, X. A survey of Blockchain Consensus Safety and Security: State-of-the-art, Challenges, and future work. *J. Syst. Softw.* **2023**, *196*, 111555. [CrossRef]
14. Khanday, A.M.U.D.; Rabani, S.T.; Khan, Q.R.; Rouf, N.; Din, M.M.U. Machine learning based approaches for detecting COVID-19 using clinical text data. *Int. J. Inf. Tecnol.* **2020**, *12*, 731–739. [CrossRef]
15. Roukounaki, A.; Efremidis, S.; Soldatos, J.; Neises, J.; Walloschke, T.; Kefalakis, N. Scalable and configurable end-to-end collection and analysis of IOT security data: Towards end-to-end security in IOT Systems. In Proceedings of the 2019 Global IoT Summit (GIoTS), Aarhus, Denmark, 17–21 June 2019. [CrossRef]
16. Yadav, A.K.; Singh, K.; Amin, A.H.; Almutairi, L.; Alsenani, T.R.; Ahmadian, A. A comparative study on consensus mechanism with security threats and future scopes: Blockchain. *Comput. Commun.* **2023**, *201*, 102–115. [CrossRef]
17. Limaye, A.; Adegbija, T. HERMIT: A Benchmark Suite for the Internet of Medical Things. *IEEE Internet Things J.* **2018**, *5*, 4212–4222. [CrossRef]
18. Ray, P.P.; Dash, D.; Kumar, N. Sensors for internet of medical things: State-of-the-art, security and privacy issues, challenges and future directions. *Comput. Commun.* **2020**, *160*, 111–131. [CrossRef]
19. Al-Turjman, F.; Nawaz, M.H.; Ulusar, U.D. Intelligence in the Internet of Medical Things era: A systematic review of current and future trends. *Comput. Commun.* **2020**, *150*, 644–660. [CrossRef]
20. Sun, L.; Jiang, X.; Ren, H.; Guo, Y. Edge-cloud computing and artificial intelligence in internet of medical things: Architecture, technology and application. *IEEE Access* **2020**, *8*, 101079–101092. [CrossRef]
21. Wu, G.; Wang, S.; Ning, Z. Blockchain-enabled privacy-preserving access control for data publishing and sharing in the internet of medical things. *IEEE Internet Things J.* **2021**, *9*, 8091–8104. [CrossRef]
22. Ashfaq, Z.; Rafay, A.; Mumtaz, R.; Zaidi, S.M.H.; Saleem, H.; Zaidi, S.A.R.; Haque, A. A review of enabling technologies for Internet of Medical Things (IoMT) Ecosystem. *Ain Shams Eng. J.* **2022**, *13*, 101660. [CrossRef]
23. Awad, A.; Fouda, M.M.; Khashaba, M.M.; Mohamed, E.R.; Hosny, K.M. Utilization of mobile edge computing on the Internet of Medical Things: A survey. *ICT Express* **2022**. [CrossRef]
24. Almogren, A.; Mohiuddin, I.; Din, I.U.; Almajed, H.; Guizani, N. Ftm-iomt: Fuzzy-based trust management for preventing sybil attacks in internet of medical things. *IEEE Internet Things J.* **2020**, *8*, 4485–4497. [CrossRef]
25. Khosravi, M.R.; Samadi, S. Mobile multimedia computing in cyber-physical surveillance services through UAV-borne Video-SAR: A taxonomy of intelligent data processing for IoMT-enabled radar sensor networks. *Tsinghua Sci. Technol.* **2022**, *27*, 288–302. [CrossRef]
26. Yeh, K.-H. A secure IOT-based healthcare system with Body Sensor Networks. *IEEE Access* **2016**, *4*, 10288–10299. [CrossRef]
27. Yang, G. *Body Sensor Networks*; Springer: London, UK, 2006. [CrossRef]
28. Gope, P.; Hwang, T. BSN-care: A secure IOT-based modern healthcare system using Body Sensor Network. *IEEE Sens. J.* **2016**, *16*, 1368–1376. [CrossRef]
29. Gus Vlahos. 5 Reasons IoMT Devices Make Sense for Health Care Organizations. Available online: https://healthtechmagazine.net/article/2020/04/5-reasons-iomt-devicesmake-sense-HealthCare-organizations (accessed on 29 September 2020).
30. Deloitte. Medtech and the Internet of Medical Things: How Connected Medical Devices are Transforming Health Care. 2018. Available online: https://www.medigy.com/news/2020/04/08/healthtechmagazine-5-reasons-iomt-devices-make-sense-for-healthcare-organizations/ (accessed on 20 October 2020).
31. Dilawar, N.; Rizwan, M.; Ahmad, F.; Akram, S. Blockchain: Securing internet of medical things (IOMT). *Int. J. Adv. Comput. Sci. Appl.* **2019**, *10*, 82–89. [CrossRef]
32. Dubovitskaya, A.; Xu, Z.; Ryu, S.; Schumacher, M.; Wang, F. How blockchain could empower eHealth: An application for radiation oncology. In *Data Management and Analytics for Medicine and Healthcare*; Springer: Cham, Switzerland, 2017; pp. 3–6. [CrossRef]
33. Ben Sasson, E.; Chiesa, A.; Garman, C.; Green, M.; Miers, I.; Tromer, E.; Virza, M. Zerocash: Decentralized anonymous payments from Bitcoin. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014. [CrossRef]
34. Medical Device Radiocommunications Service (MedRadio), Federal Commun. Commission (FCC), Washington, DC, USA. Available online: https://www.fcc.gov/medical-deviceradiocommunications-service-medrad (accessed on 18 November 2020).
35. Thiyagarajan, K.; Rajini, G.K.; Maji, D. Cost-effective, disposable, flexible and printable MWCNT-based wearable sensor for human body temperature monitoring. *IEEE Sens. J.* **2021**, *22*, 16756–16763. [CrossRef]
36. Wu, F.; Wu, T.; Yuce, M.R. Design and implementation of a wearable sensor network system for IOT-connected safety and health applications. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019. [CrossRef]
37. Gupta, R.; Tanwar, S.; Tyagi, S.; Kumar, N. Tactile-Internet-Based Telesurgery System for Healthcare 4.0: An Architecture, Research Challenges, and Future Directions. *IEEE Netw.* **2019**, *33*, 22–29. [CrossRef]
38. Satava, R.M. Emerging technologies for surgery in the 21st century. *Arch. Surg.* **1999**, *134*, 1197–1202. [CrossRef]
39. Oboe, R.; Slama, T.; Trevisani, A. Telerobotics through Internet: Problems, Approaches and Applications. *An. Univ. Din. Craiova. Mec. Electroteh* **2007**, *4*, 81–90.

40. Lum, M.J.H.; Friedman, D.C.W.; Sankaranarayanan, G.; King, H.; Fodero, K.; Leuschke, R.; Hannaford, B.; Rosen, J.; Sinanan, M.N.; King, H.-S.H. The RAVEN: Design and validation of a telesurgery system. *Int. J. Robot. Res.* **2009**, *28*, 1183–1197. [CrossRef]
41. Choi, J.; Park, J.W.; Kim, D.J.; Shin, J.; Park, C.Y.; Lee, J.C.; Jo, Y.H. Lapabot: A compact telesurgical robot system for minimally invasive surgery: Part I. System description. *Minim. Invasive Ther. Allied Technol.* **2012**, *21*, 188–194. [CrossRef] [PubMed]
42. Mendez, I.; Hill, R.; Clarke, D.; Kolyvas, G.; Walling, S. Robotic long-distance telementoring in neurosurgery. *Neurosurgery* **2005**, *56*, 434–440. [CrossRef] [PubMed]
43. Nanah, A.; Bayoumi, A.B. The pros and cons of digital health communication tools in neurosurgery: A systematic review of literature. *Neurosurg. Rev.* **2020**, *43*, 835–846. [CrossRef]
44. Memos, V.A.; Minopoulos, G.; Psannis, K. *The Impact of IoT and 5G Technology in Telesurgery: Benefits & Limitations*; IEEE: New York, NY, USA, 2019.
45. Iqbal, W.; Abbas, H.; Daneshmand, M.; Rauf, B.; Bangash, Y.A. An in-depth analysis of IOT security requirements, challenges, and their countermeasures via software-defined security. *IEEE Internet Things J.* **2020**, *7*, 10250–10276. [CrossRef]
46. Chanal, P.M.; Kakkasageri, M.S. Hybrid algorithm for data confidentiality in internet of things. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019. [CrossRef]
47. Cherupally, S.R.; Boga, S.; Podili, P.; Kataoka, K. Lightweight and scalable DAG based distributed ledger for verifying IOT Data Integrity. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Republic of Korea, 13–16 January 2021. [CrossRef]
48. Shah, T.; Venkatesan, S. Authentication of IOT device and IOT server using secure vaults. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018. [CrossRef]
49. Chen, C.-M.; Liu, S.; Li, X.; Islam, S.K.H.; Das, A.K. A provably-secure authenticated key agreement protocol for remote patient monitoring iomt. *J. Syst. Archit.* **2023**, *136*, 102831. [CrossRef]
50. Karar, M.E.; Khan, Z.F.; Alshahrani, H.; Reyad, O. Smart IOMT-based segmentation of coronavirus infections using lung CT scans. *Alex. Eng. J.* **2023**, *69*, 571–583. [CrossRef]
51. Das, A.K.; Zeadally, S. Data Security in the Smart Grid Environment. In *Pathways to a Smarter Power System*; Taşcıkaraoğlu, A., Erdinç, O., Eds.; Elsevier: Amsterdam, The Netherlands, 2019; pp. 371–395. [CrossRef]
52. Zang, W.; Li, Y. Gait-cycle-driven transmission power control scheme for a Wireless Body Area Network. *IEEE J. Biomed. Health Inform.* **2018**, *22*, 697–706. [CrossRef]
53. Nisarga, B.L.; Manishankar, S.; Sinha, S.; Shekar, S. Hybrid IOT based Hazard Detection System for buildings. In Proceedings of the 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, 2–4 July 2020. [CrossRef]
54. Mutescu, P.-M.; Petrariu, A.I.; Lavric, A. Wireless Communications for IOT: Energy efficiency survey. In Proceedings of the 2021 12th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, Romania, 25–27 March 2021. [CrossRef]
55. Pullmann, J.; Macko, D. Increasing energy efficiency by minimizing collisions in long-range IOT networks. In Proceedings of the 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 1–3 July 2019. [CrossRef]
56. Rahman, A.; Hossain, M.S.; Alrajeh, N.A.; Alsolami, F. Adversarial examples—Security threats to covid-19 deep learning systems in medical IOT devices. *IEEE Internet Things J.* **2021**, *8*, 9603–9610. [CrossRef]
57. Yaacoub, J.-P.A.; Noura, M.; Noura, H.N.; Salman, O. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
58. Zachos, G.; Essop, I.; Mantas, G.; Porfyrakis, K. An anomaly-based intrusion detection system for internet of medical things networks. *Electronics* **2021**, *10*, 2562. [CrossRef]
59. Wang, Z.; Zhu, H.; Sun, L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods. *IEEE Access* **2021**, *9*, 11895–11910. [CrossRef]
60. Jalwana, M.A.A.K.; Akhtar, N.; Bennamoun, M.; Mian, A. Orthogonal Deep Models as Defense Against Black-Box Attacks. *IEEE Access* **2020**, *8*, 119744–119757. [CrossRef]
61. Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Centers for Disease Control and Prevention. 2022. Available online: https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient\T1\textquoterights%20consent%20or%20knowledge (accessed on 20 February 2023).
62. Official Legal Text. General Data Protection Regulation (GDPR). 2022. Available online: https://gdpr-info.eu/ (accessed on 20 February 2023).
63. Rauscher, J.; Bauer, B. Safety and Security Architecture Analyses Framework for the Internet of Things of Medical Devices. In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018; pp. 1–3. [CrossRef]

64. Wortman, P.A.; Tehranipoor, F.; Karimian, N.; Chandy, J.A. Proposing a modeling framework for minimizing security vulnerabilities in IoT systems in the healthcare domain. In Proceedings of the 2017 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI), Orlando, FL, USA, 16–19 February 2017.
65. Rahmadika, S.; Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Sharma, V.; You, I. Blockchain-Based Privacy Preservation Scheme for Misbehavior Detection in Lightweight IoMT Devices. *IEEE J. Biomed. Health Inform.* **2023**, *27*, 710–721. [CrossRef]
66. Choudhary, G.; Astillo, P.V.; You, I.; Yim, K.; Chen, I.R.; Cho, J.H. Lightweight Misbehavior Detection Management of Embedded IoT Devices in Medical Cyber Physical Systems. *IEEE Trans. Netw. Serv. Manag.* **2020**, *17*, 2496–2510. [CrossRef]
67. Astillo, P.V.; Choudhary, G.; Duguma, D.G.; Kim, J.; You, I. TrMAps: Trust Management in Specification-Based Misbehavior Detection System for IMD-Enabled Artificial Pancreas System. *IEEE J. Biomed. Health Inform.* **2021**, *25*, 3763–3775. [CrossRef]
68. Gao, W.; Sun, Y.; Fu, Q.; Wu, Z.; Ma, X.; Zheng, K.; Huang, X. ARP Poisoning Prevention in Internet of Things. In Proceedings of the 2018 9th International Conference on Information Technology in Medicine and Education (ITME), Hangzhou, China, 19–21 October 2018; pp. 733–736. [CrossRef]
69. Gopal, S.B.; Poongodi, C.; Nanthiya, D.; Kirubakaran, T.; Logeshwar, D.; Saravanan, B.K. Autoencoder based Architecture for Mitigating phishing URL attack in the Internet of Things (IoT) using Deep Neural Networks. In Proceedings of the 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 21–22 April 2022; pp. 427–431. [CrossRef]
70. Adil, M.; Jan, M.A.; Mastorakis, S.; Song, H.; Jadoon, M.M.; Abbas, S.; Farouk, A. Hash-MAC-DSDV: Mutual Authentication for Intelligent IoT-Based Cyber–Physical Systems. *IEEE Internet Things J.* **2022**, *9*, 22173–22183. [CrossRef]
71. Gowtham, M.; Pramod, H.B. Semantic Query-Featured Ensemble Learning Model for SQL-Injection Attack Detection in IoT-Ecosystems. *IEEE Trans. Reliab.* **2022**, *71*, 1057–1074. [CrossRef]
72. Elmahi, E.; Salekzamankhani, S.; Sharma, M. In-Depth Analysis of Signal Jammers' and Anti-Jamming Effect on 5G Signal. In Proceedings of the 2019 7th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Istanbul, Turkey, 26–28 August 2019; pp. 1–6. [CrossRef]
73. Liu, W.; Zheng, J.; Shen, W.; Lu, Y.; Liang, R.; Li, J.; Hu, Y.; Ni, D. Research on application layer security communication protocol based on lightweight NTRU public key cryptography. In Proceedings of the 2019 International Conference on Intelligent Computing, Automation and Systems (ICICAS), Chongqing, China, 6–8 December 2019. [CrossRef]
74. Belkhouja, T.; Sorour, S.; Hefeida, M.S. Role-based hierarchical medical data encryption for implantable medical devices. In Proceedings of the 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
75. Chinese Remainder Theorem, Wikipedia. Available online: https://en.wikipedia.org/wiki/Chinese_remainder_theorem (accessed on 18 November 2020).
76. Tutari, V.H.; Das, B.; Chowdhury, D.R. A continuous role-based authentication scheme and data transmission protocol for implantable medical devices. In Proceedings of the 2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP), Gangtok, India, 25–28 February 2019; pp. 1–6.
77. Belkhouja, T.; Du, X.; Mohamed, A.; Al-Ali, A.K.; Guizani, M. Biometric-based authentication scheme for implantable medical devices during emergency situations. *Future Gener. Comput. Syst.* **2019**, *98*, 109–119. [CrossRef]
78. Sun, Y.; Lo, B. An artificial neural network framework for gait-based biometrics. *IEEE J. Biomed. Health Inform.* **2019**, *23*, 987–998. [CrossRef] [PubMed]
79. Cryptographic Hash Function, Wikipedia. Available online: https://en.wikipedia.org/wiki/Cryptographic_hash_function (accessed on 18 November 2020).
80. XOR Gate, Wikipedia. Available online: https://en.wikipedia.org/wiki/XOR_gate (accessed on 18 November 2020).
81. Xu, Z.; Xu, C.; Liang, W.; Xu, J.; Chen, H. A Lightweight Mutual Authentication and key agreement scheme for Medical Internet of Things. *IEEE Access* **2019**, *7*, 53922–53931. [CrossRef]
82. Alzahrani, B.A.; Irshad, A.; Albeshri, A.; Alsubhi, K. A provably secure and Lightweight Patient-healthcare authentication protocol in Wireless Body Area Networks. *Wirel. Pers. Commun.* **2020**, *117*, 47–69. [CrossRef]
83. Homomorphic Encryption, Wikipedia. Available online: https://en.wikipedia.org/wiki/Homomorphic_encryption (accessed on 18 November 2020).
84. Sun, X.; Zhang, P.; Sookhak, M.; Yu, J.; Xie, W. Utilizing fully homomorphic encryption to implement secure medical computation in Smart Cities. *Pers. Ubiquitous Comput.* **2017**, *21*, 831–839. [CrossRef]
85. Jiang, L.; Chen, L.; Giannetsos, T.; Luo, B.; Liang, K.; Han, J. Toward practical privacy-preserving processing over encrypted data in IOT: An assistive healthcare use case. *IEEE Internet Things J.* **2019**, *6*, 10177–10190. [CrossRef]
86. Farooqui, M.; Gull, H.; Ilyas, M.; Iqbal, S.Z.; Khan, M.A.; Krishna, G.; Ahmed, M.S. Improving mental healthcare using a human centered internet of things model and embedding homomorphic encryption scheme for cloud security. *J. Comput. Theor. Nanosci.* **2019**, *16*, 1806–1812. [CrossRef]
87. Guo, X.; Lin, H.; Wu, Y.; Peng, M. A new data clustering strategy for enhancing mutual privacy in healthcare IOT Systems. *Future Gener. Comput. Syst.* **2020**, *113*, 407–417. [CrossRef]
88. Kara, M.; Laouid, A.; Yagoub, M.A.; Euler, R.; Medileh, S.; Hammoudeh, M.; Eleyan, A.; Bounceur, A. A fully homomorphic encryption based on magic number fragmentation and el-gamal encryption: Smart healthcare use case. *Expert Syst.* **2021**, *39*, e12767. [CrossRef]

89. Kasyoka, P.; Kimwele, M.; Angolo, S.M. Certificateless pairing-free authentication scheme for wireless body area network in healthcare management system. *J. Med. Eng. Technol.* **2020**, *44*, 12–19. [CrossRef]
90. Bhatia, T.; Verma, A.K.; Sharma, G. Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing. *Concurr. Comput. Pract. Exp.* **2020**, *32*, e5520. [CrossRef]
91. 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]
92. Zheng, L.; Wang, Z.; Tian, S. Comparative study on electrocardiogram encryption using elliptic curves cryptography and data encryption standard for applications in internet of medical things. *Concurr. Comput. Pract. Exp.* **2020**, *34*, e5776. [CrossRef]
93. Ogundokun, R.O.; Awotunde, J.B.; Adeniyi, E.A.; Ayo, F.E. Crypto-stegno based model for securing medical information on IOMT platform. *Multimed. Tools Appl.* **2021**, *80*, 31705–31727. [CrossRef]
94. Sowjanya, K.; Dasgupta, M.; Ray, S. Elliptic curve cryptography based authentication scheme for internet of medical things. *J. Inf. Secur. Appl.* **2021**, *58*, 102761. [CrossRef]
95. Digital Signature, Wikipedia. Available online: https://en.wikipedia.org/wiki/Digital_signature (accessed on 18 November 2020).
96. Easttom, C.; Mei, N. Mitigating implanted medical device cybersecurity risks. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 0145–0148.
97. Farahat, I.S.; Tolba, A.S.; Elhoseny, M.; Eladrosy, W. A secure real-time internet of medical smart things (IOMST). *Comput. Electr. Eng.* **2018**, *72*, 455–467. [CrossRef]
98. Kumar, M.; Chand, S. A Secure and Efficient Cloud-Centric Internet-of-Medical-Things-Enabled Smart Healthcare System with Public Verifiability. *IEEE Internet Things J.* **2020**, *7*, 10650–10659. [CrossRef]
99. Bhushan, B.; Sinha, P.; Sagayam, K.M.; Andrew, J. Untangling blockchain technology: A survey on state of the art, security threats, privacy services, applications and future research directions. *Comput. Electr. Eng.* **2021**, *90*, 106897. [CrossRef]
100. Nguyen, D.C.; Pathirana, P.N.; Ding, M.; Seneviratne, A. Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems. *IEEE Access* **2019**, *7*, 66792–66806. [CrossRef]
101. Garg, N.; Wazid, M.; Das, A.K.; Singh, D.P.; Rodrigues, J.J.P.C.; 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]
102. Meng, W.; Li, W.; Zhu, L. Enhancing Medical Smartphone Networks via Blockchain-Based Trust Management Against Insider Attacks. *IEEE Trans. Eng. Manag.* **2020**, *67*, 1377–1386. [CrossRef]
103. Gao, Y.; Lin, H.; Chen, Y.; Liu, Y. Blockchain and SGX-Enabled Edge-Computing-Empowered Secure IoMT Data Analysis. *IEEE Internet Things J.* **2021**, *8*, 15785–15795. [CrossRef]
104. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things with Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731. [CrossRef]
105. Jin, H.; Dai, X.; Xiao, J.; Li, B.; Li, H.; Zhang, Y. Cross-Cluster Federated Learning and Blockchain for Internet of Medical Things. *IEEE Internet Things J.* **2021**, *8*, 15776–15784. [CrossRef]
106. Abdellatif, A.A.; Samara, L.; Mohamed, A.; Erbad, A.; Chiasserini, C.F.; Guizani, M.; O'Connor, M.D.; Laughton, J. MEdge-Chain: Leveraging Edge Computing and Blockchain for Efficient Medical Data Exchange. *IEEE Internet Things J.* **2021**, *8*, 15762–15775. [CrossRef]
107. Kulaç, S. Security belt for wireless implantable medical devices. *J. Med. Syst.* **2017**, *41*, 172. [CrossRef]
108. Verma, G.K.; Singh, B.B.; Singh, H. Provably secure message recovery proxy signature scheme for wireless sensor networks in e-healthcare. *Wirel. Pers. Commun.* **2017**, *99*, 539–554. [CrossRef]
109. Bhatia, T.; Verma, A.K.; Sharma, G. Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud. *Trans. Emerg. Telecommun. Technol.* **2018**, *29*, e3309. [CrossRef]
110. Kulac, S. A new externally worn proxy-based Protector for Non-Secure wireless implantable medical devices: Security jacket. *IEEE Access* **2019**, *7*, 55358–55366. [CrossRef]
111. Li, W.; Jin, C.; Kumari, S.; Xiong, H.; Kumar, S. Proxy re-encryption with Equality Test for secure data sharing in internet of things-based Healthcare Systems. *Trans. Emerg. Telecommun. Technol.* **2020**, *33*, e3986. [CrossRef]
112. Zheng, G.; Yang, W.; Valli, C.; Qiao, L.; Shankaran, R.; Orgun, M.A.; Mukhopadhyay, S.C. Finger-to-heart (F2H): Authentication for wireless implantable medical devices. *IEEE J. Biomed. Health Inform.* **2019**, *23*, 1546–1557. [CrossRef]
113. Zheng, G.; Yang, W.; Johnstone, M.; Shankaran, R.; Valli, C. Securing the elderly in cyberspace with fingerprints. In *Assistive Technology for the Elderly*; Suryadevara, N.K., Mukhopadhyay, S.C., Eds.; Elsevier: Amsterdam, The Netherlands, 2020; pp. 59–79. [CrossRef]
114. Shakil, K.A.; Zareen, F.J.; Alam, M.; Jabin, S. BAMHealthCloud: A biometric authentication and data management system for healthcare data in cloud. *J. King Saud Univ.—Comput. Inf. Sci.* **2020**, *32*, 57–64. [CrossRef]
115. Li, J.; Chen, X.; Li, M.; Li, J.; Lee PP, C.; Lou, W. Secure deduplication with efficient and reliable convergent key management. *IEEE Trans. Parallel Distrib. Syst.* **2014**, *25*, 1615–1625. [CrossRef]
116. He, D.; Kumar, N.; Khan, M.K.; Wang, L.; Shen, J. Efficient Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services. *IEEE Syst. J.* **2018**, *12*, 1621–1631. [CrossRef]

117. Wazid, M.; Das, A.K. A secure group-based blackhole node detection scheme for hierarchical wireless sensor networks. *Wirel. Pers. Commun.* **2016**, *94*, 1165–1191. [CrossRef]
118. Das, A.K.; Wazid, M.; Yannam, A.R.; Rodrigues, J.J.; Park, Y. Provably secure ECC-based device access control and key agreement protocol for IOT environment. *IEEE Access* **2019**, *7*, 55382–55397. [CrossRef]
119. Ding, S.; Cao, J.; Li, C.; Fan, K.; Li, H. A novel attribute-based access control scheme using blockchain for IOT. *IEEE Access* **2019**, *7*, 38431–38441. [CrossRef]
120. Riad, K.; Hamza, R.; Yan, H. Sensitive and energetic IOT access control for Managing Cloud Electronic Health Records. *IEEE Access* **2019**, *7*, 86384–86393. [CrossRef]
121. Sahu, N.K.; Mukherjee, I. Machine learning based Anomaly Detection for IOT network: (anomaly detection in IOT network). In Proceedings of the 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (48184), Tirunelveli, India, 15–17 June 2020. [CrossRef]
122. Bovenzi, G.; Aceto, G.; Ciuonzo, D.; Persico, V.; Pescape, A. A hierarchical hybrid intrusion detection approach in IOT scenarios. In Proceedings of the GLOBECOM 2020–2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020. [CrossRef]
123. Sharma, V.; You, I.; Yim, K.; Chen, I.-R.; Cho, J.-H. Briot: Behavior rule specification-based misbehavior detection for IOT-embedded cyber-physical systems. *IEEE Access* **2019**, *7*, 118556–118580. [CrossRef]