sustainability

Review

Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions

Mohamed Elhoseny [1], Navod Neranjan Thilakarathne [2,*], Mohammed I. Alghamdi [3], Rakesh Kumar Mahendran [4], Akber Abid Gardezi [5], Hesiri Weerasinghe [6] and Anuradhi Welhenge [6]

[1] Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt; melhoseny@ieee.org
[2] Department of ICT, Faculty of Technology, University of Colombo, Colombo 00700, Sri Lanka
[3] Department of Computer Science, Al-Baha University, Al-Bahah 1988, Saudi Arabia; mialmushilah@bu.edu.sa
[4] Department of Electronics and Communication Engineering, Vel Tech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Tamil Nadu 6000062, India; rakeshkumarmahendran@gmail.com
[5] Department of Computer Science, COMSATS University Islamabad, Islamabad 44000, Pakistan; akber.gardezi@comsats.edu.pk
[6] Faculty of Computing and Technology, University of Kelaniya, Colombo 00700, Sri Lanka; hesiri@kln.ac.lk (H.W.); anuradhiw@kln.ac.lk (A.W.)
* Correspondence: navod.neranjan@ict.cmb.ac.lk

Abstract: The rapid development and the expansion of Internet of Things (IoT)-powered technologies have strengthened the way we live and the quality of our lives in many ways by combining Internet and communication technologies through its ubiquitous nature. As a novel technological paradigm, this IoT is being served in many application domains including healthcare, surveillance, manufacturing, industrial automation, smart homes, the military, etc. Medical Internet of Things (MIoT), or the use of IoT in healthcare, is becoming a booming trend towards improving the health and wellbeing of billions of people by offering smooth and seamless medical facilities and by enhancing the services provided by medical practitioners, nurses, pharmaceutical companies, and other related government and non-government organizations. In recent times, this MIoT has gained higher attention for its potential to alleviate the massive burden on global healthcare, which has been caused by the rise of chronic diseases, the aging population, and emergency situations such as the recent COVID-19 global pandemic, where many government and non-government medical resources were challenged, owing to the rising demand for medical resources. It is evident that with this recent growing demand for MIoT, the associated technologies and its interconnected, heterogeneous nature adds new concerns as it becomes accessible to confidential patient data, often without patient or the medical staff consciousness, as the security and privacy of MIoT devices and technologies are often overlooked and undermined by relevant stakeholders. Hence, the growing security breaches that target the MIoT in healthcare are making the security and privacy of Medical IoT a crucial topic that is worth scrutinizing. In this study, we examined the current state of security and privacy of the MIoT, which has become of utmost concern among many security experts and researchers due to its rapid demand in recent times. Nevertheless, pertaining to the current state of security and privacy, we also examine and discuss a number of attack use cases, countermeasures and solutions, recent challenges, and anticipated future directions where further attention is required through this study.

Keywords: security; privacy; IoT; medical internet of things; smart health

Citation: Elhoseny, M.; Thilakarathne, N.N.; Alghamdi, M.I.; Mahendran, R.K.; Gardezi, A.A.; Weerasinghe, H.; Welhenge, A. Security and Privacy Issues in Medical Internet of Things: Overview, Countermeasures, Challenges and Future Directions. *Sustainability* **2021**, *13*, 11645. https://doi.org/10.3390/su132111645

Academic Editor: Simon Elias Bibri

Received: 26 August 2021
Accepted: 19 October 2021
Published: 21 October 2021

1. Introduction

Technology integration is becoming an integral part of our daily life as a result of the technological advancement of various technologies [1]. This results in less manual work and aids in ubiquitously interconnecting everyone, and IoT plays a major role, offering smooth and seamless ubiquitous services for everyone [2,3]. In general, the IoT refers to the networking of physical devices that are smart and interconnected [4] and comprises sensors, software, and network connectivity that enables it to collect and exchange data [5,6]. Currently, the IoT is shaping and transforming both the business and consumer worlds, finding its way into every global business and consumer domain. Apart from this, it is also being delivered in many other domains, including healthcare, smart cities, agriculture, the military, and so on [4–8]. Hence, the IoT may significantly enhance the way people interact with the world. Based on recent reports, the IoT market size was valued at USD 761.4 billion in 2020 and is projected to reach USD 1386.06 billion by 2026, which signifies its importance as a dominant technological paradigm towards improving the well-being of billions of people all around the world [9–12].

When it comes to the IoT in healthcare, or what is well known as MIoT, it refers to a wide variety of IoT devices whose main purpose is to facilitate and aid in fundamental patient care [7–11]. the global IoT in healthcare market size is USD 71.84 billion in 2020 and the market is projected to grow from USD 89.07 billion in 2021 to USD 446.52 billion by 2028 [9–12]. As of now, healthcare providers are utilizing various MIoT based applications and services for patient treatment, disease management, medical diagnosis, to improve patient care, and lower the costs of care [4–8], where they are capable of collecting various information such as vital body parameters from patients and monitor pathological details by implantable medical sensors or small wearable sensors that are worn by the patient [11–18]. With the aid of MIoT devices, patient condition can be monitored remotely and in real-time, and the captured data can then be analyzed and transmitted to the cloud data storage or the medical data centers for further processing and storage before offering services to various stakeholders such as physicians and other related medical staff, caregivers, and insurance service providers [18,19]. In general, MIoT applications include solutions that are designed for remote health monitoring, emergency patient care, healthcare management, the monitoring of elderly patients, clinical decision support systems, wireless capsule endoscopy, and so on [4,7,8,20–24]. Nevertheless, it is also evident that now the IoT has revolutionized healthcare organizations to expand their services to in-home patients where they can monitor, track, and treat the conditions of patients remotely while they are engaging with their daily activities. A typical MIoT system can be compartmentalized into several components [24–31]. For better understanding, an overview of a general MIoT system in healthcare is depicted in Figure 1.

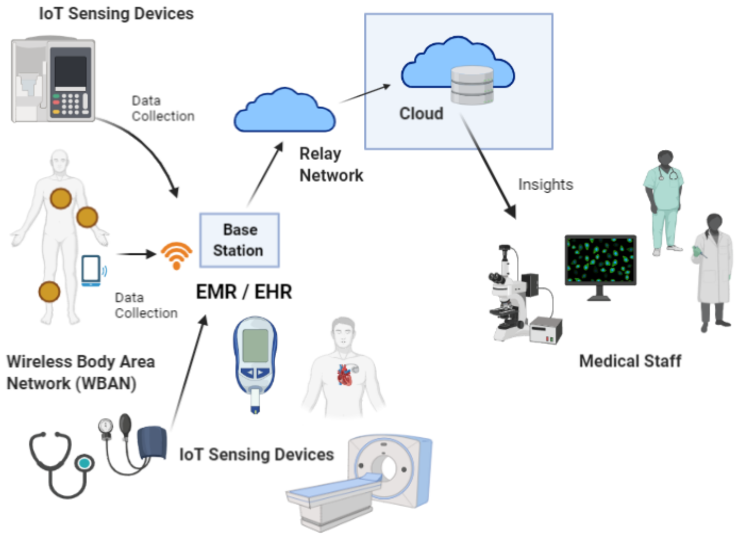


Figure 1. Overview of a general MIoT system in healthcare.

In general, a typical MIoT healthcare system comprises of a series of medical IoT devices that are embedded with various kinds of intelligent sensors that can perceive their surroundings [31,32]. The collected medical data can be processed either by a smart device itself or in the cloud, where a wireless medium is used to transfer the collected health information to the relevant stakeholders, which helps them to make decisions about the patient's condition [10,22,32–35]. In addition, such smart devices can be further connected to worldwide information networks for convenient and on-demand access.

The integration and the connectivity of physical things in the MIoT environment to the Internet means the possibility of remote access to the devices, which are made for the monitoring, analysis, forecasting, and storage of vital medical data [36,37]. On the other hand, these integrated IoT technologies introduce various vulnerabilities, owing to the rapidly evolving IoT threat landscape, where intruders can exploit and gain access to the MIoT network to further exploit the entire medical network/environment. This ultimately leads to situations where the security and privacy of the devices and patients are at risk. As the volume of data that is handled and generated by MIoT devices grows exponentially, it will eventually lead to the greater exposure of confidential medical data, which necessitates further study on the matter. Hence, the security and privacy of the data obtained from MIoT devices, which are either stored in the cloud or in remote servers or obtained during the transmission to the cloud or remote servers, are becoming a major unresolved concern in healthcare, where less attention is paid by the industry and the academic community [10,17]. Moreover, based on recent statistics [30–35], the healthcare sector leads in terms of the sectors that have been breached by cyber-attacks in recent times, as depicted in Figure 2 [15–20].

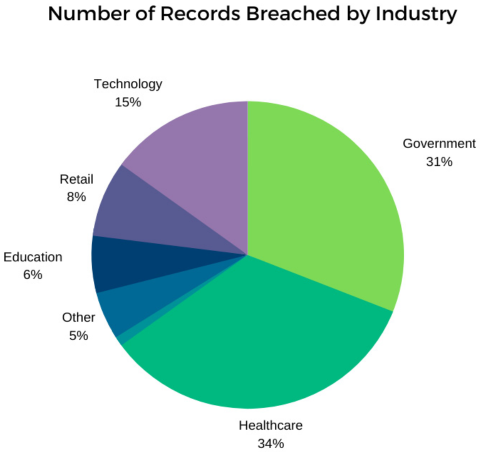


Figure 2. Latest statistics of the number of records breached by industry.

With the exponential growth of Internet-connected MIoT devices, confidential patient information is exposed to outside parties that can be accessible in numerous ways. For an instance, an intruder can eavesdrop through the wireless communication network and sniff for data that is being exchanged over the wireless network to access confidential patient data. In worst-case scenarios, intruders can remotely access the control unit of the medical device and can then control the device, jeopardizing the lives of patients [5,37]. Moreover, it would be a huge threat to the patient's privacy if a passive network observer could infer confidential patient information from the network traffic, especially when then inferred information can be used for abusive purposes following the attack [38,39]. It is evident that the lack of adequate knowledge about MIoT security among the end-users and the relevant stakeholders (e.g., medical staff, patients, caregivers) may also exacerbate vulnerabilities and may encourage attackers to further exploiting MIoT technologies, ultimately endangering the lives of patients in most cases [5,8,10,12]. Not only that, but in case of any cyber-attack, the biggest concerns or threats for healthcare would be data leakage or information loss, eventually resulting patient data being compromised, as depicted in Figure 3. Nevertheless, recent trends indicate that with the ever-increasing cyber-attacks that target healthcare, the healthcare IoT security market is expected to undergo rapid growth by the year 2025, with a total revenue of USD 100 billion, which also justifies our efforts to examine the current state of security and privacy of the MIoT through this study [38–41].

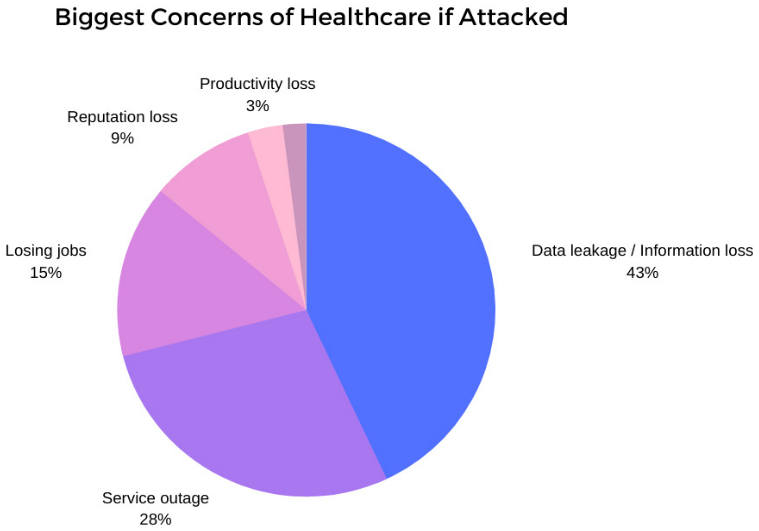


Figure 3. Biggest concerns in the healthcare sector if attacked.

On the other hand, in November of 2019, the entire world woke up to a deadly virus outbreak called COVID-19 that quickly spread to countries worldwide, posing worldwide chaos. Up to the moment where we are writing this, the virus has caused by worldwide population to decrease by almost 4 million people, posing huge doubt about the next phases of pandemic management when considering the current level of available medical resources. Global lockdowns have already been imposed, including country-wide and state-wide lockdowns, to contain the spread of the virus. In order to control and contain the spread of the virus, healthcare organizations, with the help of governments, introduced a variety of MIoT-based technologies to track and treat patients remotely, owing to the contagious nature of the virus and to reduce the strain on the medical facilities. As a result, the demand for MIoT devices and technologies have also grown during this pandemic season, has also led to a boost in MIoT security attacks, according to recent studies [40–45], which further motivated us towards compiling this study.

1.1. Motivation of Study

There is no question that a greater guarantee for the health and wellbeing of individuals is offered by the use of MIoT in healthcare, where it also puts a lot of strain on the security and privacy aspects of an MIoT-powered healthcare environment, with the lives of patients being endangered [45–47] if no countermeasures are taken. On the other hand, the usage of MIoT in healthcare is proliferating at a rapid phase, owing to rapid demand over recent years, which makes it impossible to address all security and privacy concerns in a timely manner, with many researchers and vendors currently working towards strengthening the security and privacy aspects of the MIoT ecosystem. Nevertheless, the MIoT concept itself is a novel concept where research activities are still in their early stages in terms of security and privacy. Thus, our motivation behind this study was to understand and collate the current level of knowledge pertaining to the security and privacy aspects of MIoT and to provide opportunities to conduct further research in this area that would be highly beneficial for researchers, academics, and vendors who are interested in the security and privacy aspects of MIoT.

1.2. Research Problems and Contribution

There have been rapid contributions in the area of MIoT towards proposing novel solutions for patient condition monitoring, disease diagnosis, and pandemic management, with many research studies and surveys being provided on the topic in general. When it comes to the security and privacy aspects, a few surveys have also been conducted on the topic in general, where it is not able to provide any significant knowledge to conduct future research and to devise sound security solutions towards improving the security and privacy of the pervasive MIoT environment. Hence, in order to address this research gap, this study provides an in-depth review of the security and privacy aspects of MioT, highlighting its ecosystem, key contributions, latest trends, countermeasures and solutions, challenges, and future directions. The following is a summary of our contributions:

1. We provide adequate knowledge about the underlying MIoT ecosystem and highlight its architecture, the key layers that the architecture itself is made out of, and the devices and technologies used in each layer.
2. We provide a discussion about the security and privacy requirements of the MIoT and highlight the latest trends to provide a better understanding of what is happening now.
3. We classify security and privacy attacks in terms of the MIoT layered architecture and suggest countermeasures and solutions to prevent these attacks in terms of the layered architecture.
4. We provide a brief comparison of the existing literature, highlighting its key contributions and limitations to justify our work.
5. In terms of the security and privacy of the MIoT, we highlight key challenges based on the layered architecture and also provide future directions as well.

1.3. Outline of Study

In order to provide a comprehensive review, as outlined in Section 1.2, the rest of the paper is organized as follows: In Section 2, we discuss the architecture of the MIoT, including the devices and technologies that have been employed thus far. In Section 3, we discuss the security and privacy requirements of the MIoT, highlighting why it has become an appealing target, including the latest trends. In Section 4, we elaborate on several attack scenarios to better understand attacks on the MIoT based on its layered architecture. Related work and contributions made by others are discussed and compared in Section 5. In Section 6, we describe countermeasures and solutions for solving current security and privacy problems in terms of the MIoT layered architecture. Challenges and future directions are presented in Section 7. Finally, the conclusions are presented in Section 8.

2. The Architecture of MIoT

As the main objective of this research study is to understand and review the current state of security and privacy aspects pertaining to the MIoT, it first is essential to have an understanding of the architecture and the devices and the technologies that are employed, as these creates a foundation towards better understanding the various security and privacy issues and their impact. Hence, in this second section, we mainly discuss the architecture of the MIoT and the devices employed in each layer in the architecture. As shown in Figure 4, the architecture of the MIoT can be seen as an abstraction of three hierarchical layers [11,13,16,24,42–47]. That is, the:

1. Perception layer.
2. Network layer.
3. Application layer.

According to the three-layered architecture, the bottommost layer is the perception layer, which is responsible for gathering the medical data from the physical MIoT devices, such as wearable's, smart blood glucose meters, ECG monitoring devices, and so on. Then, the network layer mainly consists of wireless, wired, and middleware systems, which facilitate the smooth delivery of gathered medical data, towards the destination. With the aid of underlying technological platforms, the network layer first processes and communicates the acquired data from the perception layer to the application layer, which is the topmost layer in the architecture. The application layer comprises medical data repositories to offer tailored and personalized medical services and to address the needs of end-users, who are patients, medical professionals, caregivers, and insurance companies [11,17]. An important fact is that the underlying technologies used by each of these layers are different from one another. Altogether, the MIoT devices and integrated technologies are used to provide a variety of services, each with its own requirements and limitations [13,17].

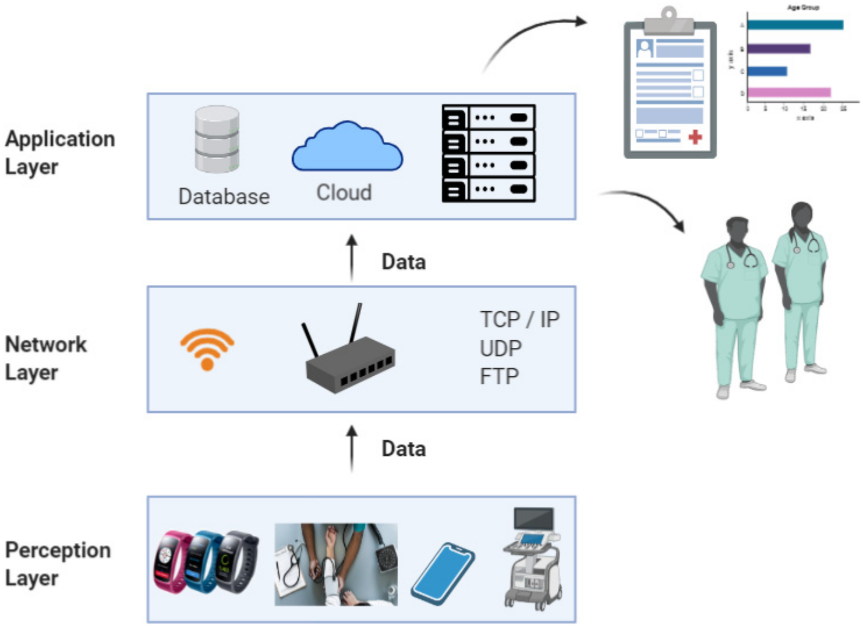


Figure 4. The three-layer architecture of the MIoT.

On the other hand, when it comes to effective service provisioning in MIoT, various protocols are being used, which hold a key place towards improving data transmission efficiency across the three layers and saving energy consumption during data transmission, while also providing security and privacy. The protocols used in each of these layers have their own purpose and characteristics, such as protocols for data transmission, which have connectivity between the MIoT sensors and gateways, and route where they should be evaluated based on the MIoT application type. In Table 1, we highlight the main protocols used in the application and network layers in MIoT solutions, and apportioned them according to the ISO/OSI model in order to generate better understanding.

Table 1. Main protocols used in MIoT solutions.

Network Layer	Application Layer
For network layer addressing IPv4/IPv6 protocols are used. For routing RPL, CARP, and CORPL protocols are used. The rest of the protocols used in network layer includes TCP, UDP, 6LoWPAN, IEEE 802.15.4 (e.g.: ZigBee) IEEE 802.15.1 (Bluetooth) LPWAN (e.g.: LoRaWAN) RFID, NFC, IEEE 802.11 (Wi-Fi).	MQTT, CoAP, DSS, AMQP, HTTP, HTTPS, TLS

2.1. Classification of Devices Based on the Architecture

The intention of this subsection is to provide readers a brief overview of the devices and technologies that are employed in each layer based on the three-layer architecture for the MIoT, as previously mentioned, in order to have an exact idea as to the security and privacy issues pertaining to the whole pervasive MIoT ecosystem [40–51].

2.1.1. Devices Employed in the Perception Layer

The perception layer is responsible for accumulating vital body parameters from the patients (e.g., body temperature, blood pressure range, blood oxygen level, heart rate, and blood glucose level, etc.) using physical MIoT devices. The accumulated data are then transferred to the network layer for transportation to the destination. Based on the state of the art, devices in this layer can further be categorized into four categories [13,26,33]:

1. Patient monitoring devices.
2. Remote wellness and chronic disease monitoring devices.
3. Real-time location service (RTL) devices.
4. Facility monitoring devices.

Based on this categorization, further examples are provided in the following subsection for better understanding.

Patient monitoring devices

The following Table 2, highlights examples for these patient monitoring devices.

Table 2. Patient monitoring devices.

Device Category	Examples
Clinical monitors	Heart rate monitors, ventilators, pulse oximetry monitors, electrocardiogram monitors, capnography monitors, depth of consciousness monitors
Medical devices	Ventilators, medical imaging devices (e.g., X-rays, computerized tomography (CT) scanners, and magnetic resonance imaging (MRI)), infusion pumps, incubators, smart medical devices, telemetry devices, smart stethoscopes
Virtual care devices	Remote ICU telemetry
Devices in smart patient rooms	Fall detection monitors, smart beds, personal hygiene monitors

Remote wellness and chronic disease monitoring devices

The following Table 3, highlights examples for these remote wellness and chronic disease monitoring devices.

Table 3. Remote wellness and chronic disease monitoring devices.

Device Category	Examples
Wearables	Wristbands, bio-energy patches, smart watches
Implantable devices	Pacemakers, defibrillators, neurostimulators, respiratory rate sensors, muscle activity sensors, swallowable camera capsules, embedded cardiac devices
Remote clinical monitors	Pulse oximeter monitors, ECG monitors, glucometers, fall detection monitors

Real-time location service (RTLs) devices

The following Table 4, highlights examples for these RTL devices used in MIoT based healthcare environment.

Table 4. Real-time Location Service (RTLs) devices.

Device Category	Examples
Devices for tracking employees	For tracking nursing staff, ancillary staff, physicians
Devices for tracking patients	Infant abduction, wandering systems, rehabilitation systems
Devices for tracking visitors	Way finding and digital signage
Devices for tracking assets	For wheelchairs, infusion pumps, smart cabinets, medication carts

Facility monitoring devices

The following Table 5, highlights examples for these facility monitoring devices in MIoT based healthcare environment.

Table 5. Facility monitoring devices.

Device Category	Examples
Devices used for environmental controls	Lighting (Daylight sensors), room control, humidity monitoring, water quality monitoring, HVAC
Devices used for building management	Elevators, power monitoring and power distribution
Devices used for security monitoring	Door locks and entry systems, fire alarms, video surveillance systems

2.1.2. Devices Employed in the Network Layer

The network layer has the responsibility of distributing content and routing the content to the destination as well as network addressing [13,46–49]. The devices used in this layer are as follows:

- Wired/Wireless media: It is evident that MIoT devices often use wired or wireless networks to connect to the end-user or the gateway [5,14]. In addition, MIoT devices can be connected to Wireless Sensor Networks (WSNs), which use a traditional Wi-Fi network or low-powered wireless personal area network (6LoWPAN). On the other hand, most devices that use wired connections are stationary (e.g., medical imaging devices) [26].
- Radio communication media: Some low-powered MIoT mobile devices use radio communication media such as Bluetooth, RFID, Bluetooth Low Energy (BLE), NFC, and all sorts of cellular communication networks to connect with each node and with end-users and the gateways. Many of the wearable medical IoT devices use BLE for short-range communication. Cellular networks (e.g., 2G, 3G, 4G, 5G) are used for long-range communication [14,25].

2.1.3. Devices Employed in the Application Layer

The application layer bridges physical MIoT devices and the end-users. When the integrated data from the perception layer come to the application layer via the network layer, the collated data are further processed into meaningful information and are saved in repositories in the cloud or dedicated servers in order to provide services as per stakeholder needs. It is evident that most device manufacturers switch their applications towards being hosted in the cloud, owing to the rapid elasticity, convenience, and high scalability that the cloud offers, as opposed to offering services through dedicated servers [13,14].

3. Security and Privacy Requirement of MIoT

It is no doubt that MIoT security and privacy play a vital role in modern ubiquitous healthcare [12,16,17], as most healthcare organizations do not devote the adequate time and necessary resources to safeguard security and privacy. A typical MIoT system is a complex ecosystem comprising heterogeneous components (e.g., medical information systems, gateways, cloud services, databases, and smart devices) that can leverage healthcare into the next level [7]. These devices pertaining to the ecosystem generate vast quantities of highly sensitive, real-time, and diversified data [14,35–48], which need to be protected by all means. The need for various strategies to ensure sufficient security and privacy is indicated by the fact that personal medical data are collected and distributed via public or private networks that are insecure most of the time. Thus, when developing robust and secure medical IoT systems, the following requirements should be considered and satisfied [4,5,7,9,11,17,19,20,28,42,50–57]:

- Confidentiality: Confidentially ensures that only authorized personnel have access to the medical data while hindering access for unauthorized personnel [11,42].
- Data integrity: Ensures that an adversary cannot attempt to alter or tamper medical data during transmission or storage [11,29].
- Data availability: Ensures that accurate data must be available to legitimate users so that reliable access to the resources are given to the appropriate users/nodes promptly [11,57].
- Resilience to attacks: MIoT systems must avoid a single point of failure and should have the ability to adapt to node failures. In addition, there should be an underlying protection schema that protects the devices or the information in the presence of an attack [4,5].
- Data usability: Data usability ensures that only authorized users can access the data [4,5].
- Access control: There should be an underlying access control mechanism for authenticated users [17].
- Data auditing: Auditing access to medical records is an important means of controlling the utilization of resources and a standard measure for the detection and monitoring of suspicious incidents or abnormalities [5,17].
- Data authentication: This ensures the confirmation of the origin and integrity of data [9,28].
- Privacy of patient information: Medical data can be apportioned into two categories, general records and sensitive data [17]. Sensitive data can also be called patient privacy information and includes details about infectious diseases, sexual orientation, mental status, drug addiction, and identity information. Because of the criticality and the sensitivity of this data, we need to ensure that these sensitive data are not exposed to unauthorized users or that unauthorized users do not have the capacity to understand the meaning of the data, even if the data are captured and intercepted [9,28,32,45].

Readers must note that the security and privacy of patient-related data are two separate concepts [17]. Data security ensures that data are safely stored and transmitted to guarantee their confidentiality and integrity. On the other hand, data privacy implies that data can only be accessed by the people who have proper authorization to access it. Hence, the successful development and deployment of MIoT must take security and privacy both as core considerations. If not, the lack of sufficient MIoT security and privacy would not only jeopardize the privacy of patients but may also jeopardize the lives of patients [6,15,18]. In the next section, we discuss the security attacks that can be expected if these security requirements are not met, based on the MIoT layered architecture. Before further discussing the types of attack that target each layer, readers need to understand why MIoT in healthcare is becoming an appealing target for intruder attacks. Hence, in the following, based on the state of the art, we list down the key reasons why it has become an appealing target [5,6]:

- The MIoT is an emerging technological paradigm where adequate research has not been conducted regarding security, where device manufacturers themselves rush to provide MIoT solutions without security in mind.
- The fact that highly confidential and sensitive data are always being transmitted across the MIoT ecosystem makes it a sound target for attackers.
- As most of the IoT devices are inbuilt with wireless communication capabilities, it puts most MIoT devices at risk for WSN security violations [4,5].
- In order to control, monitor, and operate, MIoT solutions encompass different applications. There is huge concern about the implementation risks in this application layer, such as breaches of access control and session hijacking as well as the general security functionalities of the applications.
- A large fraction of computational resources are consumed by certain security computations such as the execution of encryption algorithms. Due to the limited computing capacities (e.g., limited computing power and memory), many of these MIoT devices lack integrated encryption mechanisms, as execution cannot be completed in those resource-constrained environments. This lack of strong encryption mechanisms across devices makes devices susceptible to malicious attacks.
- The amount of financial profit that can be gained by exploiting the devices and data make these data a sound target for attackers by way of blackmailing someone, releasing the exploited data to the public, or selling it on the dark web [11].
- Personally identifiable information (PII) and personal health information (PHI), which can be contained within MIoT data, would make the entire MIoT ecosystem a sound target that could be exploited for profit [4].

As of now, according to the latest trends that have been witnessed, there have been various simulations and demonstrations of intruders attempting to insert malicious code directly into wearable devices using e programmable device interface or by trying to plant malware remotely to compromise the device and then obtain the sensitive data, monitor the device remotely, or control the device remotely, resulting in life-threatening circumstances [13]. Barnaby Jack demonstrated the hacking of an insulin pump at the McAfee conference in 2011 by overriding the device controls [18,50] to inject lethal insulin doses into the pump. Additionally, at the Melbourne Breakpoint security conference in 2012, he showed that a pacemaker transmitter could be reverse-engineered and hacked to produce a lethal electrical shock with a high voltage of 830 volts [18,51], resulting in a simulated cardiac arrest, clearly showing the repercussions of various vulnerabilities present with the MIoT. Moreover, according to *Wired* magazine [57–59], students at the University of Alabama demonstrated that they could hack the pacemaker in a robotic dummy patient and kill it theoretically. In 2016, a weakness in a St. Jude Medical cardiac device was discovered, where an intruder could send repetitive messages to the system until the battery was exhausted, a weakness that could eventually endanger the lives of patients [57–59]. While these examples illustrate the attacks that can be carried out on devices implanted in the human body, there are numerous vulnerabilities that are present on medical networks or terminal databases that have the ability to cause serious damage if the risk is not managed [18,56,57]. The following figure, Figure 5, depicts the top security threats that target healthcare cloud environments [57–65].

On the other hand, recent studies indicate that at least one security breach has been reported by nearly 90% of healthcare organizations involving MIoT devices [52]. Around 45% of all ransomware attacks that occurred in 2017 targeted healthcare organizations [53]. For example, the medical records in an Indiana hospital in the USA were encrypted by attackers, forcing the hospital to pay a USD 50,000 ransom to recover the data in 2017. By October 2016, 14 hospitals had reported ransomware attacks that had used medical devices as a gateway [58,59]. With more than 200,000 devices around the world, the biggest ransomware attack on medical systems was recorded in 2017 [12,54–56] and was known as WannaCry. It exploited vulnerabilities in the Windows OS and prevented medical staff from accessing affected computers [59–65], thus delaying critical patient care. Those ransomware attacks and hacking demonstrations imply that there is a high possibility of MIoT devices becoming compromised due to a lack of inbuilt security and a lack of user knowledge. In addition, the lack of environmental configurations in the MIoT ecosystem can also put MIoT devices at risk. Based on the latest statistics, it is evident that ransomware holds the first place among many other root causes that are responsible for the majority of healthcare data breaches, as depicted in Figure 6 [63,64,64–74].

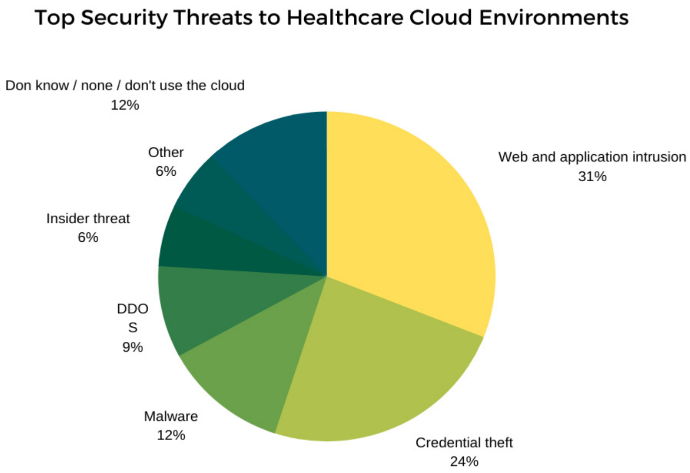


Figure 5. Top security threats to healthcare cloud environments.

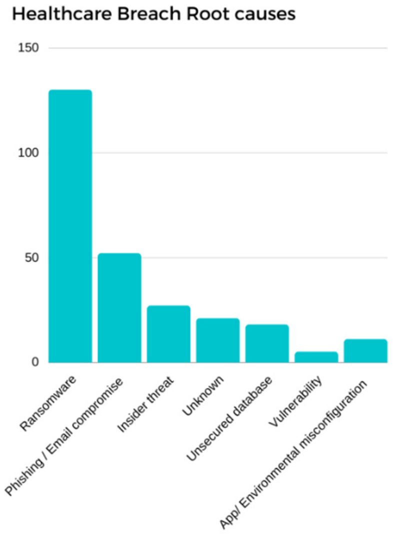
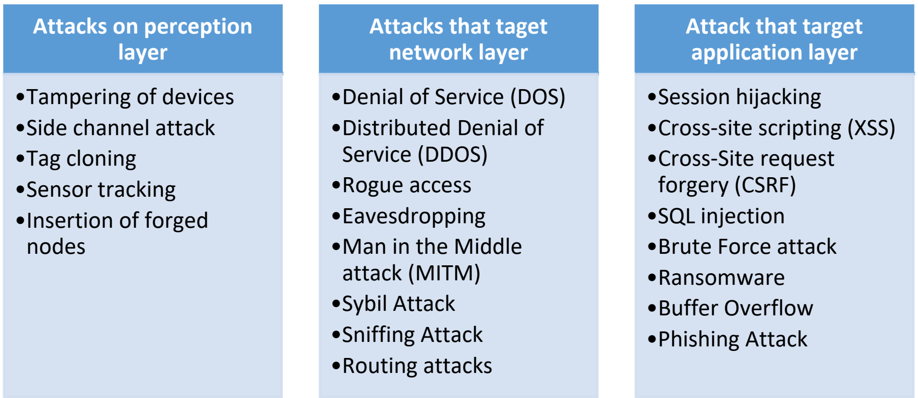


Figure 6. Root causes of healthcare data breaches.

4. Attack Classification Based on the Architecture

The intention of this subsection is to highlight the attacks targeting the MIoT ecosystem. Based on the state of the art, we have separated the attacks in terms of the MIoT layered architecture, into three sections, as in Figure 7 [18]. This is so that readers will have a better understanding of MIoT attacks and their implications as they pertain to each layer.



Attacks on perception layer

- Tampering of devices
- Side channel attack
- Tag cloning
- Sensor tracking
- Insertion of forged nodes

Attacks that taget network layer

- Denial of Service (DOS)
- Distributed Denial of Service (DDOS)
- Rogue access
- Eavesdropping
- Man in the Middle attack (MITM)
- Sybil Attack
- Sniffing Attack
- Routing attacks

Attack that target application layer

- Session hijacking
- Cross-site scripting (XSS)
- Cross-Site request forgery (CSRF)
- SQL injection
- Brute Force attack
- Ransomware
- Buffer Overflow
- Phishing Attack

Figure 7. Classification of security and privacy attacks in terms of the MIoT layered architecture.

4.1. Attacks on Perception Layer

The integrity and the privacy of data are compromised by attacks on these perception layer devices and can thus lead to adverse outcomes that can be fatal. Possible attacks that target the perception layer are listed below:

- **Tampering of devices**

The attacker can tamper physical MIoT sensing devices and can manipulate their functionality or can fully or partially stop their functionality [4,5]. Some of the firmware vulnerabilities allow attackers to further exploit these vulnerabilities, allowing them to then implant malware on the physical MIoT device and take control of the device [57].

- **Side channel attack**

It should be noted that attackers can utilize many techniques to perform a side-channel attack, such as monitoring the electromagnetic activity around the medical devices, by analyzing the power consumption and data movement timing [4,5,48]. A successful side-channel attack may lead to the exposure of underline confidential data.

- **Tag cloning**

Here, the attacker can use data obtained from a successful side channel attack or can duplicate the data from a pre-existing tag [48] to perform the attack. Unauthorized data, such as confidential patient information, is able to be accessed through the help of the cloned tag after the attack [4].

- **Sensor tracking**

During this kind of attack, attackers can exploit real-time location service devices to obtain patient location, which violates patient privacy [4]. These devices contain GPS tracking sensors to send the location of the patient in case of an emergency. If the device is vulnerable, the attacker may spoof the GPS data and will be able to determine the patient location [56,57].

- **Insertion of forged nodes**

To gain access and to gain further control over the MIoT network, an attacker can insert a falsified or malicious node between the actual network nodes in the MIoT network [5,13].

4.2. Attacks on Network Layer

- **Denial of Service (DOS)**

Medical IoT devices may have very limited capacity and capabilities, owing to the default miniaturized nature of the IoT. Hence, the attacker can use a successful DOS attack to interrupt the services performed by a MIoT network, endangering and delaying critical patient care [5]. This attack floods the system with a vast amount of service requests and disrupts the device functionality on the network [9]. Distributed denial of service

(DDOS) is an aggressive form of a denial of service attack [55–57] and uses a larger number of compromised nodes to flood the system, making it more difficult to determine the original source of the attack. Attackers can use automated tools such as botnets, which are comprised of infected IoT devices, to launch a wide variety of DDOS attacks [4]. (e.g., Telnet, Mirai)

- **Rogue access**

  Here, the attacker sets up a forged gateway and lures legitimate users to connect to the rogue access point and then intercepts the network traffic [4,13] to reveal the transmitting data.

- **Eavesdropping**

  The attacker first locates and intercepts the appropriate hardware devices so that he/she is able to successfully collect the data being transmitted through hardware devices. This unlawfully obtained data can be used to conduct different forms of attacks. Although this problem can be solved by encryption, strong encryption, particularly with low-powered MIoT devices, is not always practical due to a lack of processing power and memory [4,5,74–79].

- **Man in the Middle attack (MITM)**

  The MITM attack allows the attacker to exploit a possible vulnerability and view and listen to the data and thereafter secretly replay and alter the data that is being communicated. Since data are sent and retrieved by MIoT sensing devices, any modifications made to the data during transmission can lead to mistreatment (e.g., medication overdose) [5,13].

- **Replay attack**

  In this type of attack, an attacker is able to reuse a message that was previously shared between legitimate users for authentication. By breaching any of the network nodes or by eavesdropping, it is possible for the intruder to intercept the authentication message [5,13,57].

- **Sybil attack**

  This is a common attack that targets WSNs. A node in the network system provides the victim node with multiple identities, allowing the victim node to perform a single operation multiple times. As the attacker has multiple identities in the WSN, the victim node will transmit data through the compromised nodes exposing, the sensitive data [13,67].

- **Sniffing attack**

  Using sniffing devices or applications, the attacker tries to thieve or intercept the data in the network traffic and collect useful information for further attacks [4,5,66,67].

- **Routing attacks**

  The way that messages or data are routed is affected by this form of attack. The attacker may redirect, misdirect, spoof, or even drop the packets at the network layer in this form of attack [14].

4.3. Attacks on Application Layer

In the application layer, attacks primarily seek unauthorized access to sensitive user data, which ultimately violates user privacy. Attackers usually take advantage of software and device bugs (e.g., buffer overflow, code injection) on the application layer to compromise the services and applications offered by the application layer. In addition to these attacks, different forms of malware such as worms, viruses, and trojans often threaten applications and services. Further, other malicious programs (adware, key loggers, rootkit, and spyware, etc.) often undermine the privacy of the users [13]. In the following list, we discuss potential application-layer attacks:

- **Session hijacking**

Session hijacking is subjected to critical vulnerabilities in the session connection at the application interface, where an intruder can hijack the program session and can gain control over the application controls [4,5,13].

- **Cross-Site Scripting (XSS)**

Cross-site scripting attacks exploit applications by inserting malicious scripts to bypass access control through web pages, (e.g., web control pages) [13].

- **Cross-Site Request Forgery (CSRF)**

In CSRF attacks, the attacker forces an end user to execute unwanted actions on a web application on which they are currently authenticated, leading to devastating results such as revealing user credentials [4,13].

- **SQL injection**

In SQL injection attacks, the attacker attempts to attack the application-connected backend database by inserting malicious SQL statements. A successful SQL attack will lead the attacker to the backend database, where the attacker can exploit all of the critical patient data stored in the database [13].

- **Brute force attack**

Because of the weaker computational capacity possessed by most of the MIoT devices in a medical network, a simple brute force attack can easily compromise the device's access control and can open ways for attackers to further compromise the network, such as through planting malware on the devices [4,5].

- **Ransomware**

Ransomware encrypts all of the data in a system and asks for a ransom to be paid in order to redeem the compromised system. If appropriate security settings are not placed, ransomware may also start with one single compromised victim machine and may then spread across the entire network [4,5,18,51,79–85].

- **Buffer Overflow**

A buffer acts as a temporary area for data storage. When a software or device operation puts more data into the buffer, the extra data may overflow. This allows some of the information to leak into other buffers that may corrupt or overwrite any of the information that they carry. In a buffer overflow attack, the extra data sometimes hold specific instructions for actions intended by a hacker or malicious user (e.g., the data may trigger a reaction that destroys files, granting admin privileges, alters data, or exposes private information) [13,68].

- **Phishing attack**

An attacker pretends to be a legitimate person or an entity in a standard phishing attack and tries to access personal information, such as credit card data and user credentials. Email is extremely common as a medium that circulates these kinds of phishing attacks, where the attacker obtains confidential information when the user opens the email or email attachment [4,5,13].

Based on the literature that we have reviewed, it should be noted that there are a wide range of attacks, and they can take place on any of the layers. As such, we need to secure the entire MIoT ecosystem, not just specific technologies pertaining to one single layer, if we want to ensure optimal security [13,86–98].

5. Related Work and Contributions

In this section, we mainly highlight what exact contributions have been made by other researchers towards the state of the art by highlighting the title, scope of the study, key findings along with our observations, and whether the study is focusing on the IoT in general or specifically on MIoT. What we have understood is that even though there are previous studies related to MIoT security and privacy, none of the studies have been able to highlight security attacks in terms of the layered architecture of the MIoT, and none of them were able to highlight countermeasures and solutions in terms of recent security and privacy issues and that are related to the layered architecture in general. Hence, we believe that this study will be highly beneficial for researchers who are keen on learning about this subject. In the following table, Table 6, we highlight the contributions made by others towards the state of the art, which can be used to compare the current level of the status of the state of the art.

Table 6. Summary of contributions.

Reference and Year	Tittle	IoT in General	MIoT Specific	Scope	Contributions and Critique
[4], 2020	The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study		✓	A general systematic review that highlights security and privacy challenges.	The researchers discussed recent security and privacy challenges, pointing out the vulnerabilities that are present, but they did not put much effort towards discussing security and privacy requirements, countermeasures, and solutions.
[6], 2017	Security and privacy in the internet of medical things: taxonomy and risk assessment		✓	Taxonomy of security and privacy issues pertaining to MIoT is discussed.	A quantitative approach to identifying and assessing risks in MIoT is highlighted. Even though the researchers highlighted security and privacy issues, how to mitigate them was not discussed in detail in the study.
[7], 2017	Towards composable threat assessment for medical IoT (MIoT)		✓	A general analysis of MIoT threat assessment is discussed.	A framework for identifying, assessing, and evaluating threats in the MIoT environment is highlighted, whereas the study did not provide adequate knowledge about the security and privacy of MIoT.
[8], 2018	Secure medical data transmission model for IoT-based healthcare systems		✓	Proposed a hybrid security model for securing the content in medical images.	A security model based on the steganography technique with a hybrid encryption scheme is introduced towards protecting the security and data integrity of patient diagnosis data that are transmitted across MIoT networks.
[9], 2012	Internet of Things in healthcare: Interoperability and security issues		✓	A general discussion with regard to the security issues, benefits, and solutions in MIoT is provided.	Security challenges pertaining to the IoT in telemonitoring are highlighted. Even though the researchers provided a discussion in terms of the security of telemonitoring, this study did not provide adequate knowledge related to security attacks pertaining to MIoT-based telemonitoring solutions.
[10], 2018	An internet of things-based health prescription assistant and its security system design		✓	A theoretical framework for an MIoT health prescription assistant is proposed.	A security system for a health prescription assistance system is designed, implemented, and validated; this study only provides knowledge about the security aspects of MIoT-based telemedicine and not about the entire MIoT environment.
[11], 2019	A joint resource-aware and medical data security framework for wearable healthcare systems		✓	A security framework for resource-constrained wearable health monitoring systems is introduced.	A biometric-based security framework for a wearable health monitoring systems is introduced, and a performance comparison of the proposed model is also conducted. Even though the researchers conducted an experimental evaluation to test their framework, they failed to discuss security and privacy repercussions in terms of wearable MIoT, which is becoming a booming trend as of now.
[12], 2019	IoMT-SAF: Internet of medical things security assessment framework		✓	A web-based MIoT security assessment framework is developed.	The researchers developed a web-based framework that recommends security features in MIoT and assesses protection and deterrence based on ontology. Nevertheless, even though the featured web solution ranks the security solutions in terms of security and privacy, the study does not provide comprehensive knowledge about MIoT security and privacy.

Table 6. *Cont.*

Reference and Year	Tittle	IoT in General	MIoT Specific	Scope	Contributions and Critique
[13], 2018	Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice	✓		A summary of overall IoT security attacks is depicted.	The authors provide a taxonomy and classification based on IoT security attacks based on application domains, including healthcare, where they also highlight security and privacy requirements. Even though this provides a comprehensive overview of security and privacy attacks, countermeasures for the attacks are not featured in this study.
[17], 2018	Security and privacy in the medical internet of things: a review		✓	A review on security and privacy requirements and solutions with regard to the MIoT is provided.	Security and privacy requirements, open challenges, and anticipated future directions in terms of the security and privacy of MIoT are discussed, where this provides adequate knowledge about the underlying ecosystem, leading to security vulnerabilities.
[18], 2015	A review of security protocols in mHealth wireless body area networks (WBAN)		✓	Threats pertaining to the medical networks are discussed.	The latest trends and future directions are discussed as they pertain to medical networks, where the researchers were able to provide adequate knowledge about security requirements and mechanisms pertaining to medical networks. However, this features the security of MIoT networks only.
[21], 2016	A secure IoT-based healthcare system with body sensor networks		✓	A secure MIoT system is proposed in this study.	A secure MIoT system with a body sensor network is proposed and implemented using the Raspberry PI platform.
[28], 2015	BSN-Care: A secure IoT-based modern healthcare system using body sensor network		✓	Security concerns and requirements in the field of body sensor network-based healthcare systems are discussed.	The researchers proposed a secure MIoT healthcare system using a body sensor network (BSN) called BSN-Care.
[35], 2017	Internet of Medical Things (IOMT): applications, benefits and future challenges in healthcare domain		✓	Applications and challenges of MIoT are discussed, highlighting the security concerns.	A comprehensive review is presented in terms of MIoT applications and challenges to the domain, where the researchers do not put much emphasis on security as a key challenge.
[36], 2017	Internet of things for smart healthcare: Technologies, challenges, and opportunities		✓	A survey is conducted that highlights the state of the art related to the MIoT.	Security, privacy, wearability, and low-power operations related to MIoT are discussed, but the researchers do not provide that much focus on security and piracy as a key challenge.
[41], 2016	Security context framework for distributed healthcare IoT platform		✓	Context aware security framework is introduced for MIoT	The researchers introduce a security framework that can be used to secure data transmission across distributed MIoT platforms, whereas this does not feature any security and privacy attacks.
[43], 2014	The internet of things for healthcare monitoring: security review and proposed solution		✓	Security problems related to MIoT monitoring system are presented.	Proposed a security model for MIoT monitoring systems based on symmetric cryptography and network node authentication mechanisms, and authors provide decent knowledge in terms of security arracks and countermeasures.
[44], 2016	The internet of things in healthcare: Potential applications and challenges		✓	A review is provided in terms of MIoT applications.	Challenges are discussed in terms of the security and privacy MIoT applications as they pertain to MIoT solutions.
[47], 2013	Wattsupdoc: Power side channels to nonintrusively discover untargeted malware on embedded medical devices		✓	A research experiment is conducted with regard to MIoT platforms.	Proposed an add-on monitoring system for detecting malware that targets MIoT devices.
[60], 2015	The internet of things for health care: a comprehensive survey		✓	A survey is provided in terms of architecture, threat model, security requirements, and challenges.	Security and privacy issues, the latest trends pertaining to the MIoT ecosystem, are highlighted; this study provides a comprehensive survey about pervasive MIoT ecosystems. On the other hand, this study does not place much focus on security and privacy as key challenges.
[63], 2019	Security Requirements of Internet of Things-Based Healthcare System: a Survey		✓	In order to identify the security requirements pertaining to MIoT, a survey isconducted.	Features and concepts associated with security requirements for MIoT are highlighted, but this study only features security and privacy requirements.

Table 6. *Cont.*

Reference and Year	Tittle	IoT in General	MIoT Specific	Scope	Contributions and Critique
[70], 2018	Security Threats and Recommendation in IoT Healthcare		✓	Provides a review of various MIoT systems.	Security and privacy issues pertaining to MIoT systems and threats are discussed in terms of the layered architecture, and the researchers do not place much emphasis on challenges and future directions in terms of security and privacy.
[85], 2020	A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things		✓	Biometric authentication schema for MIoT body sensor network is introduced	Secure fuzzy extractor combined with fuzzy vault is introduced to protect sensitive patient data using encryption techniques.
[91], 2021	A privacy and session key based authentication scheme for medical IoT networks		✓	Network security schema for MIoT is introduced.	Secure addressing and mutual authentication protocol (SAMA) scheme is proposed and validated using formal and informal methods.
[92], 202.	Security and Privacy in IoT Smart Healthcare		✓	The current state of security and privacy of MIoT is analyzed.	The researchers provide a detailed discussion about challenges and security frameworks in terms of MIoT, and they also highlight security solutions in the study.
[93], 2021	Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology		✓	Smart-contract-enabled blockchain network is introduced	To protect the security and privacy of patient data, a blockchain-based methodology is proposed where the data can be stored on blockchain ledgers, towards enhancing data integrity and user privacy.

Based on the review that we conducted, when compiling this summary of contributions, we noted that most of the reviews and surveys only focused on reviewing the attack types and requirements and not solution. As such, the number of papers on the subject of solving the problems related to different attack types are minimal. On the other hand, most of these papers lack deep analysis about the security and privacy issues pertaining to the MIoT layered architecture. Hence, in order to fill this gap, in this study, we discuss the prevailing countermeasures and solutions in terms of layered architecture and also highlight challenges and future directions as well. Table 7 provides a comparison of the existing research work within our study for better understanding. In a nutshell, our study fulfills all of the criteria, which defines in the comparison table, which signifies our work among others.

Table 7. A comparison of related work with our study.

Reference and Year	Security and Privacy Requirements Are Discussed	Security and Privacy Attack Types Are Discussed	Countermeasures and Solutions for Attacks Are Discussed	Challenges Are Discussed in Terms of Security and Privacy	Recent Trends in Terms of Security and Privacy Are Highlighted	Future Directions Are Discussed in Terms of Security and Privacy
Thilakarathne, N. N., Kagita, M. K., and Gadekallu, D. T. R. (2020)	X	X	X	✓	✓	X
Alsubaei, F., Abuhussein, A., and Shiva, S. (2017)	✓	X	X	X	X	X
Darwish, S., Nouretdinov, I., and Wolthusen, S. D. (2017)	✓	X	X	✓	X	X
Tarouco et al. (2012)	✓	X	X	✓	X	X
Chenet al. (2018)	✓	✓	X	X	X	X
Sun et al. (2018)	✓	✓	✓	X	X	✓
Joyia et al. (2017)	X	X	X	✓	X	X
Baker, S. B., Xiang, W., and Atkinson, I. (2017).	X	✓	X	✓	X	X
Rghioui et al. (2014)	✓	✓	✓	X	X	X

Table 7. *Cont.*

Reference and Year	Security and Privacy Requirements Are Discussed	Security and Privacy Attack Types Are Discussed	Countermeasures and Solutions for Attacks Are Discussed	Challenges Are Discussed in Terms of Security and Privacy	Recent Trends in Terms of Security and Privacy Are Highlighted	Future Directions Are Discussed in Terms of Security and Privacy
Laplante, P. A., and Laplante, N. (2016)	X	✓	✓	✓	X	X
Islam et al. (2015)	X	✓	✓	✓	X	X
Nasiri S, Sadoughi F, Tadayon MH, and Dehnad A (2019)	✓	X	X	✓	X	X
Karunarathne et al. (2021).	✓	X	X	✓	X	X
Our review	✓	✓	✓	✓	✓	✓

6. Countermeasures and Solutions

The Open Web Application Security Project, or most popularly known as OWASP [69], has released a secure medical device deployment guide that was developed in conjunction with the Cloud Security Alliance. It provides a comprehensive overview about what kind of controls and precautions should be taken in order to strengthen the security of a medical IoT environment [4,62–70], such as having perimeter defense mechanisms, network security controls, device and OS update guidelines, device security controls, security testing plans (e.g., penetration testing), and proper incident response plans. In addition, the OWASP Internet of Things project [4,5] provides specific guidance for manufacturers, developers, and consumers to better understand the security challenges associated with the IoT and to allow them to make better security decisions when designing, deploying, or evaluating IoT technologies in any context [4,69,70].In order to guarantee better security and privacy within the entire MIoT ecosystem, the following criteria must be satisfied, and they should be integrated during the development and the deployment process of MIoT components that can be used to mitigate most of the threats [64,70–74].

- **Access control**

Access control specifies who has been authorized to access the medical data and MIoT devices, and how much access they are allowed and should be granted. Hence, it should verify the identity of the party attempting to access the data (e.g., using a password, fingerprint, etc.) [17,36]. As for that, well-designed access control must be implemented for IoT healthcare applications as well as devices to ensure maximum security and privacy [10,21,71]. On the other hand, when it comes to physical security, which is another aspect of access control, it should consider MIoT devices and medical data against physical theft, accidents, environmental hazards, and sabotage whenever it is necessary, adhering to all security and privacy requirements [70].

- **Data encryption**

Data encryption during data storage or transmission provides protection for the data. Solid data encryption would make it difficult for an attacker to read sensitive health data even if the attacker has access to the medical database or transmission media [20,36,41,64,71].

- **Data auditing**

Audits are very useful to determine the source of any security breach [19], allowing the underlying information to be examined (e.g., system notifications, network traffic, user access, etc.). On the other hand, the medical IoT network is extended towards the cloud and cannot be fully trusted. Hence, it is highly required to have an auditing mechanism in the cloud in order to identify the disruptions and anomalies happening across the cloud network [17].

- **IoT healthcare policies**

Policies and regulations play a pivotal role when transforming the healthcare sector to the next level by imposing various standards and regulations that everyone must comply with. As such, the United States has the Health Insurance Portability and Accountability Act (HIPAA), which was introduced in 1996, which defines the standards for protecting sensitive patient data and measures to be followed by any organization that deals with protected health information [19], whereas systems in the European countries must comply with Data Protection Directive, which was introduced in 1995.

- **Data search**

In order to preserve data privacy, confidential data must be encrypted prior to outsourcing, which outdates conventional data usage based on plaintext keyword searches [5,17].

- **Data minimization**

Data minimization suggests that the services provided by the Medical IoT should limit the collection of personal health information (PHI) to only the information that is needed, and they should also only retain the data for as long as is necessary to fulfill the purpose of the services that the users are requesting. Effective data minimization techniques in healthcare include minimizing the overall amount of patient personal data that are collected. On the other hand, only collecting the adequate and relevant amount of patient data and the amount that is in line with the intended purpose; deletion or masking obsolete or unnecessary personal data that are no longer needed; conducting periodic checkups to ensure the adequacy and relevance of the data that are collected are the other techniques that can be employed. As too much personal data may bring bigger risks, the effective utilization of data minimization would also help to lower the risks as well as lower the storage cost [5,21,25,45].

- **Data anonymization**

Data anonymization means the process of protecting private or sensitive information by erasing or encrypting identifiers that connect an individual to stored data. As an example, one can run a personally identifiable information (PII) information such as their name, social security number, and address through a data anonymization process that retains the data but keeps the source of the data anonymous [5,8,34].

- **Inventory devices**

Since healthcare organizations cannot secure what they cannot see, it is essential to create a full map of all the organizational assets. Many IoT devices are brought in without a proper risk assessment; hence, regular risk assessment must be conducted in order to identify potential risks. Some vendors provide inventory tools that can identify IoT devices on the network without disrupting their functionality [64,71].

- **Network segmentation**

System administrators in the organization must segment public networks from the rest of networks, limit access to virtual LAN assets and events, or segregate department-based traffic for providing effective organization wide security [64,71].

- **Follow the best practices**

Maintaining the best security practices, such as avoiding hard-coded passwords, deploying firewalls, and honeypots for luring and mitigating the attackers, and encrypting confidential data are highly essential when it comes to improving security in a typical MIoT setting. On the other hand, as these MIoT devices and applications are continuously being connected to networks, implementing intrusion prevention systems (IPSs), intrusion detection systems (IDSs), security sockets layer/transport layer security (SSL/TSL), and hypertext transfer protocol secure (HTTPS) communication mechanisms should be used in order to ensure network security [70]. Furthermore, before deploying devices, a risk assessment has to be completed in order to understand what vulnerabilities exist before setting up the environment. Moreover, devices and software must be updated regularly [64,71].

- **Wider awareness**

In general, employers in healthcare should have the necessary awareness of the principles of information security in order to provide security and necessary protection for MIoT applications and confidential patient data, and providing continuous medical staff training is essential towards improving the safety and wellbeing of patients. Staff training should comprise of providing them with adequate knowledge in data security and privacy and patient rights [70].

- **Continuous monitoring and reporting**

All MIoT applications and device-related logs must be collected to a centralized log management system for continuous network monitoring and Internet attacks. By having a central log management system, logs can be monitored, analyzed, and evaluated in real-time with the help of artificial intelligence (AI)-powered machine learning and deep learning techniques, resulting in preventing any security incidents from happening. This could be completed by implementing an organization-wide security information and event management system (SIEM), which would help to prevent attacks prior to when they are onset and give the capacity to respond to security incidents in a strong way in real time [3,4,70].

Next, based on the MIoT attacks that we have discussed, Table 8 provides a comprehensive summary of what sorts of countermeasures can be taken towards preventing attacks in terms of the MIoT layered architecture along with other types of measures that can be taken, along with our justification.

Table 8. Summary of countermeasures and solutions that can take against MIoT attacks, in terms of its layered architecture.

MIoT Attack Type	Related Layer	Access Control	Data Encryption	Data Auditing	IoT Healthcare Policies	Data Search	Data Minimization	Data Anonymization	Inventory Devices	Network Segmentation	Follow the Best Practices	Wider Awareness	Continuous Monitoring and Reporting	Justification/Other Measures That Can Take
Tampering of devices	Perception	✓			✓				✓		✓	✓	✓	As the tampering of devices deals with physical MIoT components, having access control mechanisms, anti-tampering mechanisms, implementing organization-wide healthcare policies and regularly monitoring the devices, and following up the best security practices can be taken as countermeasures.
Side channel attack	Perception		✓		✓		✓	✓			✓	✓	✓	As side-channel attacks are reliant on the relationship between information leaked through a side-channel and secret data, two types of countermeasures can be taken: eliminating or reducing the release of such information and eliminating the relationship between the leaked information and the secret data using some kind of data scrambling method.
Tag cloning	Perception	✓	✓		✓		✓	✓	✓		✓	✓	✓	Following a successful side-channel attack, a tag cloning attack can be performed, which can be mainly mitigated through the implementation of data encryption methods.
Sensor tracking	Perception	✓	✓		✓	✓	✓	✓	✓		✓	✓	✓	In order to avoid sensor tracking attacks, data that are mainly transmitted across MIoT networks can be encrypted, and access control mechanisms can be implemented. On the other hand, data search, anonymization, and minimization techniques can also be used.
Insertion of forged nodes	Perception	✓			✓				✓		✓	✓	✓	In order to avoid these types of attacks physical access control mechanisms, regularly monitoring devices can be conducted apart from adhering to healthcare policies and by following up with the best practices.
Denial of Service (DOS)	Network				✓					✓	✓	✓	✓	In order to prevent DOS attacks, network security can be strengthened by implementing next-generation firewalls, IPS, and IDS systems. Nevertheless, routers and firewalls can be configured to block malicious traffic, and unnecessary TCP/UDP services can be blocked to prevent DOS attacks.

Table 8. *Cont.*

MIoT Attack Type	Related Layer	Access Control	Data Encryption	Data Auditing	IoT Healthcare Policies	Data Search	Data Minimization	Data Anonymization	Inventory Devices	Network Segmentation	Follow the Best Practices	Wider Awareness	Continuous Monitoring and Reporting	Justification/Other Measures That Can Take
Distributed Denial of Service (DDOS)	Network				✓					✓	✓	✓	✓	The same measures that are used to counter DOS attacks can be used as countermeasures for DDOS attacks.
Rogue access	Network		✓		✓		✓	✓			✓	✓	✓	Apart from following up the best security practices and increasing user awareness, wireless intrusion prevention systems can be implemented to monitor the radio spectrum for unauthorized access points.
Eavesdropping	Network		✓		✓		✓	✓			✓	✓	✓	To prevent eavesdropping attacks, medical data can be encrypted. On the other hand, by using a personal firewall, keeping antivirus software updated, and using a virtual private network, these attacks can be prevented.
Man in the Middle attack (MITM)	Network		✓		✓		✓	✓			✓	✓	✓	Encrypting the medical data that transmit across the network and sticking with the best security practices would help to prevent MITM attacks.
Sybil Attack	Network	✓	✓		✓						✓	✓	✓	These attacks can be prevented by implementing ace control mechanisms and by following up with the best security practices.
Sniffing Attack	Network		✓		✓		✓	✓			✓	✓	✓	These attacks can be prevented using implementing access control mechanisms and by following up the best security practices.
Routing attacks	Network		✓		✓		✓	✓			✓	✓	✓	Routing attacks can be prevented using implementing network security mechanisms such as IDS.
Session hijacking	Application										✓	✓	✓	In order to prevent session hijacking attacks, the network data can be encrypted, and other network security protection mechanisms such as SSL/TLS and HTTPS schema can be implemented to secure the communication media.

Table 8. *Cont.*

MIoT Attack Type	Related Layer	Access Control	Data Encryption	Data Auditing	IoT Healthcare Policies	Data Search	Data Minimization	Data Anonymization	Inventory Devices	Network Segmentation	Follow the Best Practices	Wider Awareness	Continuous Monitoring and Reporting	Justification/Other Measures That Can Take
Cross-site scripting (XSS)	Application	✓									✓	✓	✓	XSS attacks can be prevented by having adequate application access control mechanisms, validating user inputs, and encoding output data.
Cross-Site request forgery (CSRF)	Application	✓			✓						✓	✓	✓	CSRF attacks can be prevented by having adequate network security mechanisms and by using anti-CSRF mechanisms.
SQL injection	Application	✓			✓						✓	✓	✓	These attacks can be prevented by implementing web application firewalls (WAF), IDS, and by having adequate application security controls, such as input validations.
Brute Force attack	Application	✓	✓				✓	✓			✓	✓	✓	Brute force attacks can be prevented by sticking with healthcare security policies, using adequate application security controls, and continuously monitoring logs through a SIEM.
Ransomware	Application				✓						✓	✓	✓	These attacks can be mitigated by increasing user awareness and by sticking with the best security practices, such as having anti-virus and anti-spyware solutions and using the inbuilt ransomware protection features of operating systems.
Buffer Overflow	Application	✓									✓	✓	✓	These attacks can be prevented by disabling unnecessary network services and by implementing firewalls and IPS systems.
Phishing Attack	Application		✓		✓		✓	✓			✓	✓	✓	In order to prevent phishing attacks, user awareness can be improved as the first defense, and antivirus and antispyware solutions can be installed on end-user machines to protect the organization's resources.

7. Challenges and Future Directions

The growing malware attacks pertaining the range of MIoT devices in healthcare are expected to rise in the forthcoming years, resulting in higher demand for robust IoT security. Among these malware attacks, ransomware and DDOS attacks are abundant. On the other hand, the latest studies and research indicate that the healthcare industry has a natural appeal to ransomware attacks due to the poor security configurations placed in the entire ecosystem. Nevertheless, placing appropriate and adequate security controls are challenging due to various factors. Hence, several challenges pertaining to the MIoT ecosystem need special attention in order to create stronger security within the MIoT ecosystem, where they would hinder the way of devising perfect security solutions. In the follow list, we discuss the main challenges that pertain to MIoT security and privacy and that need to be addressed with urgency [4,5,64,70–94].

- **Insecure network**

Due to convenience, high availability, and low cost, most medical IoT devices are rely heavily on wireless networks, such as WI-FI, which pose major security vulnerabilities, such as a factory fitted default username and passwords and weak authentication methods, which are a potential target for network-level attacks, such as sniffing, eavesdropping, and WI-FI password cracking attacks [3–5,70,71].

- **Limitation of resources**

In general, IoT healthcare devices are vary depending on their manufacturer, size, and complexity. When it comes to the internal design, most of the devices may have low-speed processors, low inbuilt memory, and storage capacities. Due to the constrained nature of the resources of most medical IoT devices, even a simple brute force attack can easily exploit and compromise the access control of such devices, leading to a mega comprise in the entire MIoT healthcare network. Hence, due to this resource-constrained nature and the complexity of device manufacturers, devising security solutions that minimize resource consumption over execution and that maximize security efficiency is a huge challenge [64,70–79].

- **Heterogeneous devices**

When it comes to most medical IoT devices, even devices that are made for a specific purpose will change based on the device manufacturer, as there is no constant or agreed-upon standards between device manufactures. Therefore, a MIoT device made for a specific purpose by manufacturer A would not be matched with a device made by manufacturer B, which increases the complexity of the devices, thus posing a challenge regarding devising unified secure schemes pertaining to the entire MIoT ecosystem [79–84].

- **Zero-day vulnerabilities and security patches**

Due to the intrinsic ubiquitous nature and rapidly changing threats, MIoT devices are highly likely to be exploited by zero-day vulnerabilities, which creates doubts about regularly updating devices to patch potential vulnerabilities before malicious attackers try to exploit them. Intruders, on the other hand, are always looking for weak places or weak links to exploit. For example, the outdated programs that are commonly found in the application layer are the most exposed to security attacks. Similarly, healthcare system providers seldom deliver the most recent firmware upgrades to physical MIoT devices, leaving end-user devices vulnerable to attack. As a result, to maintain high availability and prevent zero-day assaults, healthcare service providers should deliver regular updates to MIoT devices and applications [70,79–84].

- **High Mobility**

In general, most MIoT devices are highly mobile in nature. For example, if a patient is wearing a wearable heart rate monitor that is connected to the internet, then the device will send data to the cloud or to the patient's caregivers based on where the person is. When the person is at the office, it will connect to the office network, and it will connect to the home network when the person is at home. Hence, devising a sound security solution that focuses on the high mobile nature of MIoT is a tedious task, as depending on the environmental security configurations, threat mitigation approaches change [64,70–74].

- **Dynamic network topology**

Most of the MIoT devices connected to the main IoT network can leave the network either graciously (with proper notice of the exit) or disgracefully (suddenly), posing a doubt about applying universal security solutions for such complex dynamic network topologies [3–5,84–89].

- **Trust management**

Trust management is vital element in IoT and provides necessary security and privacy to the underlying data. As all of the devices in a typical IoT healthcare network connect to the Internet to send and retrieve data, IoT devices connected to the Internet must be trusted [3,4]. On the other hand, data collection trust is becoming a serious issue due to the large volume of data collected by these MIoT devices [70]. This vast volume of data is often known as big data, and the trust affiliated with big data is becoming a huge concern in healthcare as of now. Thus, researchers are currently studying the challenges of this trust management to prevent security and privacy attacks. These trust management issues impede the functionality of the network and application layer [64,70].

- **Social Engineering**

End-users, who are patients in this case, tend to disclose personal information openly on social media sites such as Facebook, Instagram, and others, as a result of the huge influence of social media. Cybercriminals on the other hand, perceive these sites as a new and profitable platform to distribute malware because of their enormous user base. As a result, end-users should avoid sharing personal information with strangers on these websites or over the phone [70,89–94].

Next, in Table 9, we provide a summary of challenges based on the MIoT layered architecture to provide a better understanding for our readers.

Table 9. Summary of challenges based on the layered architecture.

Challenge	Impede to the Functionality of			Related Work
	Perception Layer	Network Layer	Application Layer	
Insecure network		✓	✓	Research studies [2,3,6–8,10,12,18,21–23,28,32,35,41,48] mostly focus on this insecure network challenges in the MIoT environment. In this regard, the authors contributed in the form of surveys/reviews and proposed solutions for network data transmission.
Limitation of resources	✓	✓	✓	The research studies [4–7,9,32,35,47] mostly focus on this challenge, and most of the studies were surveys/reviews.
Heterogeneous devices	✓			These research studies [4–7,9,23,32,35] mostly focus on this challenging aspect, and most of them were surveys/reviews.
Zero-day vulnerabilities and security patches		✓	✓	These research studies [4–7,9,32,35] mostly focus on this challenging aspect, and most of them were surveys/reviews, and some of the studies proposed novel solutions.
High Mobility		✓		These research studies [4–6,9,32,35] mostly focus on this challenging aspect, and most of them were surveys/reviews.
Dynamic network topology		✓		These research studies [4–7,9,32,35] mostly focus on this challenging aspect, and some of the studies have proposed solutions to this problem.

Table 9. *Cont.*

Challenge	Impede to the Functionality of			Related Work
	Perception Layer	Network Layer	Application Layer	
Trust management		✓	✓	These research studies [4–7,9,27,32,35,47,62] most focus on this challenging aspect, and some of the authors have proposed trust management solutions by incorporating encryption mechanism among these studies.
Social Engineering			✓	Even though this was a rarely spoken subject, the research studies [4–7,9,32,35] provide some clues about this challenging aspect.

By highlighting the main challenges that hinder the ways of devising sound security solutions, next, we will discuss the anticipated future directions of MIoT that we can see in coming years.

Future Directions

In a nutshell, medical IoT-based innovations offer many useful services and applications to improve the efficiency of medical care and also facilitate improving the efficiency of healthcare facilities by delivering efficient services on-time [62]. In the following list, we highlight some of the key features and trends that we can anticipate in upcoming years in terms of Medical IoT security [14,17,28,61,63,77,94–99].

- In recent times, the emergence of AI has made a huge turning point in the IoT healthcare market and is helping to the growth of the MIoT market. Hence, it is evident that the significant use of AI-powered solutions will assist in real-time security monitoring [77,85]. Nevertheless, it is noted that MIoT security solutions rely on 03 aspects to successfully mitigate risks, such as the discovery of risks, network monitoring, and incident management, where AI would be an integral part of these solutions to provide an in-depth overview of threats and incidents and to provide the ability to respond to attacks in a timely manner while performing real-time monitoring.
- Since most medical IoT devices do not have enough computational power and memory on the devices themselves, for further data processing and storage, powerful and highly scalable computing and large storage infrastructure are needed [17,86–89]. As a result of that, due to high scalability and rapid elasticity, many healthcare organizations prefer to store their data and deploy their application servers in a stable cloud environment. As such, focus will be moved towards securing cloud environments where processing and storage happen at the same time in the same place [5,94,95].
- IoT Edge computing, which is known as data analysis, that is closer to the data source will combine with highly secured cloud environments for data storage and data processing [63,95].
- Blockchain-distributed ledger technology will be integrated with IoT to secure medical data, where the medical data and all the network transactions related data can be saved on blockchain ledgers in order to protect user privacy and data integrity [61,87,90].
- When designing MIoT devices and components, the focus will be moved towards embedded security rather and end-to-end security [88,90].
- Secure design will be an essential part of the medical IoT project development process [86,87].
- Security standards and regulations will be tighter to make sure that there are fewer gaps in the healthcare organizational security [96].
- The healthcare organizations will invest more and more in improving the organization's information security strategy in order to maintain their organizational image and to prevent any adverse security incidents beforehand [96].
- Traditional network routers provide some sorts of security capabilities such as firewall, password protection, and blocking unnecessary services, whereas modern network

routers will continue to become more secure and smarter, which is a better way to provide added network security at the network entry points [96–99].

- Biometric identity management is highly valued in healthcare settings, and its use is increasing. Along with multi-factor authentication, this is presently being investigated by more advanced healthcare organizations and pharmaceutical firms in order to improve their organizational security. Biometric applications in healthcare organizations is expected to expand in the next three to five years, and this would mostly be used as a method to add an extra security layer, govern identity management and access, and provide a more seamless clinical experience to all stakeholders [96–99].

8. Conclusions

The literature reviewed in this study leaves no question that security should be an integral part of potential MIoT system development and deployment. The new threat environment and the criticality of the MIoT ecosystem are seen in our review. Even though many studies have suggested enhancement and novel integrations for improving MIoT security, they still do not resolve the fundamental problem, which is the lack of adequate security within systems, which creates a gap in security and privacy. The COVID-19 pandemic has showcased how healthcare can move at fast pace in order to embrace new technologies. This agility in the healthcare sector will be one of the key legacies of the pandemic. It will encourage a continuous focus on innovation as the industry looks for new ways to improve outcomes for patients and healthcare professionals across the board. What the authors have understood is that effective security needs to be built-in, not patched. It has to be an integral part of the pervasive MIoT ecosystem. Even though great attention has been paid towards MIoT security, relevant standards and technical specifications are still improving and are far from reaching the optimal maturity level. Owing to the recent demands for the security and privacy of the MIoT, many researchers are currently working towards novel secure MIoT solutions that will offer many useful services and applications to improve the efficiency of medical care while maintaining security and privacy under any context. This would be fueled by the integration of AI, blockchain, essential secure design, focus on embedded security, and tight regulations in the long run. In summary, this study provides a comprehensive overview of privacy and security issues in the medical IoT with countermeasures and solutions that can be taken along with the key challenges and future directions. We believe that this will be useful and that it will provide assistance and open new ways for medical practitioners, researchers, academics and students, and other relevant stakeholders who are interested.

Author Contributions: Conceptualization, N.N.T., R.K.M., M.E., H.W., and A.W.; methodology, N.N.T., M.E., and A.A.G.; software, N.N.T.; M.I.A., and A.A.G.; validation, N.N.T.; formal analysis, N.N.T. and M.I.A.; investigation, N.N.T. and R.K.M.; resources, N.N.T.; data curation N.N.T., A.A.G.; writing—original draft preparation, N.N.T. and R.K.M.; writing—review and editing, N.N.T. and R.K.M.; visualization, M.E. and M.I.A.; supervision, M.E., A.A.G., H.W., and A.W.; project administration, N.N.T. and R.K.M.; funding acquisition, M.E. and M.I.A. 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.

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

References

1. Plachkinova, M.; Vo, A.; Alluhaidan, A. Emerging Trends in Smart Home Security, Privacy and Digital Forensics. 2016. Available online: https://aisel.aisnet.org/amcis2016/ITProj/Presentations/23/ (accessed on 20 July 2021).
2. Apthorpe, N.; Reisman, D.; Feamster, N. A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic. Available online: http://datworkshop.org/papers/dat16-final37.pdf (accessed on 20 July 2021).

3. Jacobsson, A.; Boldt, M.; Carlsson, B. A risk analysis of a smart home automation system. *Future Gener. Comput. Syst.* **2016**, *56*, 719–733. [CrossRef]
4. Thilakarathne, N.N.; Kagita, M.K.; Gadekallu, D.T.R. The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study. *Int. J. Eng. Manag. Res.* **2020**, *10*, 145–159. [CrossRef]
5. Thilakarathne, N.N. Security and Privacy Issues in IoT Environment. *Int. J. Eng. Manag. Res.* **2020**, *10*, 26–29. [CrossRef]
6. Alsubaei, F.; Abuhussein, A.; Shiva, S. Security and privacy in the internet of medical things: Taxonomy and risk assessment. In Proceedings of the 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), Singapore, 9–12 October 2017; pp. 112–120. [CrossRef]
7. Darwish, S.; Nouretdinov, I.; Wolthusen, S.D. Towards composable threat assessment for medical IoT (MIoT). *Procedia Comput. Sci.* **2017**, *113*, 627–632. [CrossRef]
8. Elhoseny, M.; Ramírez-González, G.; Abu-Elnasr, O.M.; Shawkat, S.A.; Arunkumar, N.; Farouk, A. Secure medical data transmission model for IoT-based healthcare systems. *IEEE Access* **2018**, *6*, 20596–20608. [CrossRef]
9. Tarouco, L.M.R.; Bertholdo, L.M.; Granville, L.Z.; Arbiza, L.M.R.; Carbone, F.; Marotta, M.; De Santanna, J.J.C. Internet of Things in healthcare: Interoperability and security issues. In Proceedings of the 2012 IEEE International Conference on Communications (ICC), Ottawa, ON, USA; 2012; pp. 6121–6125. [CrossRef]
10. Hossain, M.; Islam, S.R.; Ali, F.; Kwak, K.S.; Hasan, R. An internet of things-based health prescription assistant and its security system design. *Future Gener. Comput. Syst.* **2018**, *82*, 422–439. [CrossRef]
11. Pirbhulal, S.; Samuel, O.W.; Wu, W.; Sangaiah, A.K.; Li, G. A joint resource-aware and medical data security framework for wearable healthcare systems. *Future Gener. Comput. Syst.* **2019**, *95*, 382–391. [CrossRef]
12. Alsubaei, F.; Abuhussein, A.; Shandilya, V.; Shiva, S. IoMT-SAF: Internet of medical things security assessment framework. *Internet Things* **2019**, *8*, 100123. [CrossRef]
13. Chen, K.; Zhang, S.; Li, Z.; Zhang, Y.; Deng, Q.; Ray, S.; Jin, Y. Internet-of-Things security and vulnerabilities: Taxonomy, challenges, and practice. *J. Hardw. Syst. Secur.* **2018**, *2*, 97–110. [CrossRef]
14. El-hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) Authentication schemes. *Sensors* **2019**, *19*, 1141. [CrossRef]
15. Asplund, M.; Nadjm-Tehrani, S. Attitudes and perceptions of IoT security in critical societal services. *IEEE Access* **2016**, *4*, 2130–2138. [CrossRef]
16. Kumar, J.S.; Patel, D.R. A survey on internet of things: Security and privacy issues. *Int. J. Comput. Appl.* **2014**, *9*, 20–26.
17. Sun, W.; Cai, Z.; Li, Y.; Liu, F.; Fang, S.; Wang, G. Security and privacy in the medical internet of things: A review. *Secur. Commun. Netw.* **2018**, *2018*, doi. [CrossRef]
18. Kang, J.; Adibi, S. A review of security protocols in mHealth wireless body area networks (WBAN). In Proceedings of the Future Network Systems and Security: First International Conference, FNSS, Paris, France, 11–13 June 2015; Doss, R., Piramuthu, S., Zhou, W., Eds.; Springer: Cham, Switzerland, 2015; pp. 61–83.
19. AlMotiri, S.H.; Khan, M.A.; Alghamdi, M.A. Mobile health (m-health) system in the context of IoT. In Proceedings of the 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), Vienna, Austria, 22–24 August 2016; pp. 39–42. [CrossRef]
20. Azzawi, M.A.; Hassan, R.; Bakar, K.A. A review on Internet of Things (IoT) in healthcare. *Int. J. Appl. Eng. Res.* **2016**, *11*, 10216–10221.
21. Yeh, K.H. A secure IoT-based healthcare system with body sensor networks. *IEEE Access* **2016**, *4*, 10288–10299. [CrossRef]
22. Silva, C.A.; Aquino, G.S.; Melo, S.R.; Egídio, D.J. A fog computing-based architecture for medical records management. *Wirel. Commun. Mob. Comput.* **2019**, *2019*, 1968960. [CrossRef]
23. David, S.; Sagayam, K.M.; Elngar, A.A. Parasitic overview on different key management schemes for protection of Patients Health Records. *J. Cybersecur. Inf. Manag.* **2021**, *6*, 96–100.
24. Kodali, R.K.; Swamy, G.; Lakshmi, B. An implementation of IoT for healthcare. In Proceedings of the 2015 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Kerala, India, 10–12 December 2015; pp. 411–416. [CrossRef]
25. Rajput, D.S.; Gour, R. An IoT framework for healthcare monitoring systems. *Int. J. Comput. Sci. Inf. Secur.* **2016**, *14*, 451.
26. Maher, O.; Sitnikova, E. A Trustworthy Learning Technique for Securing Industrial Internet of Things Systems. *J. Intell. Syst. Internet Things* **2021**, *5*, 33–48.
27. Dimitrov, D.V. Blockchain applications for healthcare data management. *Healthc. Inform. Res.* **2019**, *25*, 51–56. [CrossRef]
28. Gope, P.; Hwang, T. BSN-Care: A secure IoT-based modern healthcare system using body sensor network. *IEEE Sens. J.* **2015**, *16*, 1368–1376. [CrossRef]
29. Milovanovic, D.; Bojkovic, Z. Cloud-based IoT healthcare applications: Requirements and recommendations. *Int. J. Internet Things Web Serv.* **2017**, *2*, 60–65.
30. Mahmud, R.; Koch, F.L.; Buyya, R. Cloud-Fog Interoperability in IoT-Enabled Healthcare Solutions. Available online: https://dl.acm.org/doi/10.1145/3154273.3154347 (accessed on 20 July 2021).
31. Sebestyen, G.; Hangan, A.; Oniga, S.; Gál, Z. eHealth solutions in the context of Internet of Things. In Proceedings of the 2014 IEEE International Conference on Automation, Quality and Testing, Robotics, Cluj-Napoca, Romania, 22–24 May 2014; pp. 1–6. [CrossRef]

32. Kumari, A.; Tanwar, S.; Tyagi, S.; Kumar, N. Fog computing for Healthcare 4.0 environment: Opportunities and challenges. *Comput. Electr. Eng.* **2018**, *72*, 1–13. [CrossRef]
33. Bui, N.; Zorzi, M. Health Care Applications: A Solution Based on the Internet of Things. Available online: https://dl.acm.org/doi/10.1145/2093698.2093829 (accessed on 20 July 2021).
34. Hassanalieragh, M.; Page, A.; Soyata, T.; Sharma, G.; Aktas, M.; Mateos, G.; Andreescu, S. Health monitoring and management using Internet-of-Things (IoT) sensing with cloud-based processing: Opportunities and challenges. In Proceedings of the 2015 IEEE International Conference on Services Computing, New York City, NY, USA, 27 June–2 July 2015; pp. 285–292. [CrossRef]
35. Joyia, G.J.; Liaqat, R.M.; Farooq, A.; Rehman, S. Internet of Medical Things (IOMT): Applications, benefits and future challenges in healthcare domain. *J. Commun.* **2017**, *12*, 240–247. [CrossRef]
36. Elsharkawy, M.; Al Masri, A.N. A Novel Image Encryption with Deep Learning Model for Secure Content based Image Retrieval. *J. Cybersecur. Inf. Manag.* **2019**, *0*, 54–64.
37. Zhao, W.; Wang, C.; Nakahira, Y. Medical Application on Internet of Things. In Proceedings of the IET International Conference on Communication Technology and Application (ICCTA 2011), Beijing, China, 14–16 October 2011.
38. Dimitrov, D.V. Medical internet of things and big data in healthcare. *Healthc. Inform. Res.* **2016**, *22*, 156–163. [CrossRef]
39. Hu, F.; Xie, D.; Shen, S. On the application of the internet of things in the field of medical and health care. In Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, Beijing, China, 20–23 August 2013; pp. 2053–2058. [CrossRef]
40. Gómez, J.; Oviedo, B.; Zhuma, E. Patient monitoring system based on internet of things. *Procedia Comput. Sci.* **2016**, *83*, 90–97. [CrossRef]
41. Sangpetch, O.; Sangpetch, A. Security context framework for distributed healthcare iot platform. In Proceedings of the Internet of Things Technologies for HealthCare, Västerås, Sweden, 18–19 October 2016; Springer: Cham, Switzerland, 2016; pp. 71–76.
42. Dohr, A.; Modre-Opsrian, R.; Drobics, M.; Hayn, D.; Schreier, G. The internet of things for ambient assisted living. In Proceedings of the 2010 Seventh International Conference on Information Technology: New Generations, Las Vegas, NV, USA, 12–14 April 2010; pp. 804–809. [CrossRef]
43. Rghioui, A.; L'aarje, A.; Elouaai, F.; Bouhorma, M. The internet of things for healthcare monitoring: Security review and proposed solution. In Proceedings of the 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), Tetouan, Morocco, 20–22 October 2014; pp. 384–389. [CrossRef]
44. Laplante, P.A.; Laplante, N. The internet of things in healthcare: Potential applications and challenges. *It Prof.* **2016**, *18*, 2–4. [CrossRef]
45. Li, C.; Hu, X.; Zhang, L. The IoT-based heart disease monitoring system for pervasive healthcare service. *Procedia Comput. Sci.* **2017**, *112*, 2328–2334. [CrossRef]
46. Dridi, A.; Sassi, S.; Faiz, S. Towards a semantic medical internet of things. In Proceedings of the 2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA), Hammamet, Tunisia,, 30 October-3 November 2017; pp. 1421–1428. [CrossRef]
47. Clark, S.S.; Ransford, B.; Rahmati, A.; Guineau, S.; Sorber, J.; Xu, W.; Fu, K. Wattsupdoc: Power Side Channels to Nonintrusively Discover Untargeted Malware on Embedded Medical Devices. Available online: https://www.semanticscholar.org/paper/WattsUpDoc%3A-Power-Side-Channels-to-Nonintrusively-Clark-Ransford/6c455f1daf739827c2e9af41c8f60cf93aaac84b (accessed on 20 July 2021).
48. Yasser, I.; Khalil, A.T.; Mohamed, M.A.; Khalifa, F. A New Chaos-based Approach for Robust Image Encryption. *J. Cybersecur. Inf. Manag.* **2021**, *7*, 51–64.
49. Jack, B. Wikipedia. 2020. Available online: http://en.wikipedia.org/wiki/Barnaby_Jack (accessed on 28 October 2020).
50. Zadrozny, B. The Good Hacker: Barnaby Jack Dies. *The Daily Beast 2013*. Available online: https://www.thedailybeast.com/the-good-hacker-barnaby-jack-dies (accessed on 28 October 2020).
51. 87% of Healthcare Organizations Will Adopt Internet of Things Technology by 2019. HIPAA J. 2017. Available online: https://www.hipaajournal.com/87pc-healthcare-organizations-adopt-internet-of-things-technology-2019-8712/ (accessed on 28 October 2020).
52. Learn More Cybersecurity Insights by Neil Weinberg, NW Securing IoT in Healthcare is Critical. *CSO Online* 2018. Available online: https://www.csoonline.com/article/3270948/data-breach/securing-iot-in-healthcare-is-critical.html (accessed on 28 October 2020).
53. Ryckaert, V. Hackers Held Patient Data Ransom, so Indiana Hospital System Paid $50,000. *USA Today 2018*. Available online: https://www.usatoday.com/story/tech/nation-now/2018/01/17/hackers-held-patient-data-ransom-so-indiana-hospitalsystem-paid-50-000/1042266001/ (accessed on 28 October 2020).
54. Hollywood Hospital Pays $17,000 in Bitcoin to Hackers; FBI Investigating. *Los Angeles Times* 2016. Available online: http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html (accessed on 28 October 2020).
55. Armerding, T. Medical Devices at Risk: 5 Capabilities That Invite Danger. *CSO Online* 2017. Available online: https://www.csoonline.com/article/3202081/security/medical-devices-at-risk-5-capabilities-that-invite-danger.html (accessed on 28 October 2020).
56. Securing the Internet of Healthcare Things. Available online: https://www.blackberry.com/us/en/forms/campaigns/ecp/healthcare (accessed on 28 October 2020).

57. Greenberg A How the Internet of Things Got Hacked. *Wired.*. Available online: https://www.wired.com/2015/12/2015-the-year-the-internet-of-things-got-hacked/ (accessed on 28 October 2020).
58. Center for Devices Radiological Health Cybersecurity. U.S. Food and Drug Administration. Available online: https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm (accessed on 28 October 2020).
59. Medical & IoT Device Security for Healthcare. *Armis* 2020. Available online: https://www.armis.com/resources/iot-security-white-papers/medical-iot-device-security-for-healthcare/ (accessed on 28 October 2020).
60. Islam, S.R.; Kwak, D.; Kabir, M.H.; Hossain, M.; Kwak, K.S. The internet of things for health care: A comprehensive survey. *IEEE Access* **2015**, *3*, 678–708. [CrossRef]
61. Zeadally, S.; Siddiqui, F.; Baig, Z.; Ibrahim, A. Smart healthcare: Challenges and potential solutions using internet of things (IoT) and big data analytics. *PSU Res. Rev.* **2019**, *4*, 149–168. [CrossRef]
62. IoT Security Forecasts and Trends: IoT, Security and Data Protection. 2020. Available online: https://www.i-scoop.eu/internet-of-things-guide/iot-security-forecasts/ (accessed on 28 October 2020).
63. Nasiri, S.; Sadoughi, F.; Tadayon, M.H.; Dehnad, A. Security Requirements of Internet of Things-Based Healthcare System: A Survey Study. 2019. Available online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7004290/ (accessed on 28 October 2020).
64. Electropages Medical IoT and Security. In: Latest Electronics News on Components and Electrical Engineering. Available online: https://www.electropages.com/blog/2020/08/medical-iot-and-security (accessed on 28 October 2020).
65. Elngar, A.; KRIT, S. Performance Analysis of Machine Learning based Botnet Detection and Classification Models for Information Security. *J. Cybersecur. Inf. Manag.* **2019**, *0*, 44–53.
66. Binance Academy. Sybil Attacks Explained. In: Binance Academy. 2020. Available online: https://academy.binance.com/en/articles/sybil-attacks-explained (accessed on 28 October 2020).
67. Buffer Overflow Attack with Example. *GeeksforGeeks* 2017. Available online: https://www.geeksforgeeks.org/buffer-overflow-attack-with-example/ (accessed on 28 October 2020).
68. OWASP Secure Medical Device Deployment Standard. Available online: https://owasp.org/www-project-secure-medical-device-deployment-standard/migrated_content (accessed on 28 October 2020).
69. OWASP Internet of Things. Available online: https://owasp.org/www-project-internet-of-things/ (accessed on 28 October 2020).
70. Eken, C.; Eken, H. Security Threats and Recommendation in IoT Healthcare. Available online: https://ep.liu.se/ecp/article.asp?issue=142&article=054&volume=0# (accessed on 20 July 2021).
71. Gloss, K. Healthcare IoT Security Risks and What to Do about Them. *IoT Agenda* 2020. Available online: https://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them (accessed on 28 October 2020).
72. Thilakarathne, N.N.; Kagita, M.K.; Gadekallu, T.R.; Maddikunta, P.K.R. The Adoption of ICT Powered Healthcare Technologies towards Managing Global Pandemics. *arXiv* **2020**, arXiv:2009.05716, preprint.
73. Kagita, M.K.; Thilakarathne, N.; Gadekallu, T.R.; Maddikunta, P.K.R. A Review on Security and Privacy of Internet of Medical Things. *arXiv* **2020**, preprint. arXiv:2009.05394.
74. Kagita, M.K.; Thilakarathne, N.; Rajput, D.S.; Lanka, D.S. A Detail Study of Security and Privacy issues of Internet of Things. *arXiv* **2020**, arXiv:2009.06341, preprint.
75. BioRender. BioRender App. Available online: https://app.biorender.com/ (accessed on 28 October 2020).
76. Navod, T. Review on the Use of ICT Driven Solutions Towards Managing Global Pandemics. *J. ICT Res. Appl.* **2021**, *14*, 207. [CrossRef]
77. Fortune Business Insights. IoT Security Market: Employment of Connected Medical Devices in Healthcare to Boost Market Amid COVID-19. *GlobeNewswire News Room.* Available online: https://www.globenewswire.com/news-release/2021/04/22/2214917/0/en/IoT-Security-Market-Employment-of-Connected-Medical-Devices-in-Healthcare-to-Boost-Market-Amid-COVID-19.html (accessed on 22 April 2021).
78. Healthcare IoT Security Market Applications, Share: Size Analysis 2027. Healthcare IoT Security Market Applications, Share | Size Analysis 2027. Available online: https://www.marketresearchfuture.com/reports/healthcare-iot-security-market-946 (accessed on 22 April 2021).
79. Reports and Data. IoT in Healthcare Market. *IoT in Healthcare Market Size, Trends & Growth, Industry Statistics.* 2020. Available online: https://www.reportsanddata.com/;https://www.reportsanddata.com/report-detail/iot-in-healthcare-market (accessed on 22 April 2021).
80. Kalra, R. Explore 3 IoT Trends in Healthcare for 2021. *IoT Agenda*. Available online: https://internetofthingsagenda.techtarget.com/feature/Explore-3-IoT-trends-in-healthcare (accessed on 28 December 2020).
81. O'Halloran, J.; 5G, IoT Technology to Transform Health and Social Care. ComputerWeekly.com. Available online: https://www.computerweekly.com/news/252492039/5G-IoT-technology-to-transform-health-and-social-care?ga=2.4808240.284146281.1623082131-1475437348.1621161510;https://blog.eccouncil.org/3-key-cyber-trends-that-the-healthcare-industry-should-avoid-to-combat-cyberattacks/ (accessed on 13 November 2020).
82. Certified Ethical Hacker: InfoSec Cyber Security Certification: EC-Council. EC. Available online: https://www.eccouncil.org/ (accessed on 22 April 2021).

83. Radware. Security Challenges for Healthcare Providers *Radware Blog*.. Available online: https://blog.radware.com/security/2020/08/security-challenges-for-healthcare-providers/ (accessed on 10 August 2020).
84. Infosecurity Magazine—Information Security & IT Security. Available online: https://www.infosecurity-magazine.com/ (accessed on 22 April 2021).
85. Mahendran, R.K.; Velusamy, P. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Comput. Commun.* **2020**, *153*, 545–552. [CrossRef]
86. Mahendran, R.K.; Velusamy, P.; Pandian, P. An efficient priority-based convolutional auto-encoder approach for electrocardiogram signal compression in Internet of Things based healthcare system. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e4115.
87. Srivastava, G.; Crichigno, J.; Dhar, S. A light and secure healthcare blockchain for iot medical devices. In Proceedings of the 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), Edmonton, AB, Canada, 5–8 May 2019; pp. 1–5. [CrossRef]
88. Shen, M.; Deng, Y.; Zhu, L.; Du, X.; Guizani, N. Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach. *IEEE Netw.* **2019**, *33*, 27–33. [CrossRef]
89. Thilakarathne, N.N.; Kagita, M.K.; Priyashan, W.M. Green Internet of Things: The Next Generation Energy Efficient Internet of Things. Available online: https://arxiv.org/ftp/arxiv/papers/2012/2012.01325.pdf (accessed on 10 August 2021).
90. Mustafa, M.M.; Parthasarathy, V.; Kumar, M.R.; Hemalatha, S. An Efficient DTDM H-MAC Protocol with Self-Calibrating Algorithm in BSN for Sporting Application. (2016). Available online: https://moam.info/an-efficient-dtdm-h-mac-protocol-with-self-_59c575931723ddde92385716.html (accessed on 10 August 2021).
91. Kumar, P.; Chouhan, L. A privacy and session key based authentication scheme for medical IoT networks. *Comput. Commun.* **2021**, *166*, 154–164. [CrossRef]
92. Karunarathne, S.M.; Saxena, N.; Khan, M.K. Security and Privacy in IoT Smart Healthcare. *IEEE Internet Comput.* **2021**, *25*, 37–48. [CrossRef]
93. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for internet of medical things (iomt) by leveraging blockchain and ipfs technology. *J. Supercomput.* **2021**, *77*, 1–40. [CrossRef]
94. Bhandari, K.S.; Ra, I.H.; Cho, G. Multi-topology based QoS-differentiation in RPL for internet of things applications. *IEEE Access* **2020**, *8*, 96686–96705. [CrossRef]
95. Bhandari, K.S.; Seo, C.; Cho, G.H. Towards Sensor-Cloud Based Efficient Smart Healthcare Monitoring Framework using Machine Learning. 2020. Available online: https://manuscriptlink-society-file.s3-ap-northeast-1.amazonaws.com/kism/conference/sma2020/presentation/SMA-2020_paper_129.pdf (accessed on 10 August 2021).
96. Sadek, I.; Rehman, S.U.; Codjo, J.; Abdulrazak, B. Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations. Available online: https://link.springer.com/chapter/10.1007/978-3-030-32785-9_1 (accessed on 10 August 2021).
97. Yaacoub, J.P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Future Gener. Comput. Syst.* **2020**, *105*, 581–606. [CrossRef]
98. Tawalbeh, L.A.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and security: Challenges and solutions. *Appl. Sci.* **2020**, *10*, 4102. [CrossRef]
99. Research, G.D.T. Cybersecurity in Medical: Cybersecurity Trends. Medical Device Network, Retrieved 30 September 2021. Available online: https://www.medicaldevice-network.com/comment/cybersecurity-in-medical-cybersecurity-trends/ (accessed on 22 April 2021).