cryptography

Article

Implantable Medical Device Security

Luigi Catuogno [1,†] and Clemente Galdi [2,*,†]

[1] Dipartimento di Scienze Economiche, Giuridiche, Informatiche e Motorie, University of Napoli Parthenope, 80133 Napoli, Italy; luigi.catuogno@uniparthenope.it
[2] Dipartimento di Studi Politici e Sociali, Università di Salerno, 84084 Fisciano, Italy
* Correspondence: clgaldi@unisa.it
† These authors contributed equally to this work.

Abstract: Implantable medical devices, or IMDs for short, are medical instruments that are placed into the human body through surgery. IMDs are typically used for treating chronic diseases. Currently available IMDs are capable of communicating using wireless channels with other devices, either in close proximity or even connected to the Internet, making IMDs part of the Internet of Medical Things. This capability opens the possibility of developing a wide range of services, like remote patient data control, localization in case of emergency, or telemedicine, which can improve patients' lifestyle. On the other hand, given the limited resources of such tiny devices, and the access to the Internet, there are numerous security issues to be considered when designing and deploying IMDs and their support infrastructures. In this paper, we highlight security problems related to Internet-connected IMDs, and survey some solutions that have been presented in the literature.

Keywords: medical IoT; ethical issues; machine learning; implantable devices; patient privacy; data security; device safety

Citation: Catuogno, L.; Galdi, C. Implantable Medical Device Security. *Cryptography* **2024**, *8*, 53. https://doi.org/10.3390/cryptography8040053

Academic Editor: Jim Plusquellic

Received: 30 September 2024
Revised: 11 November 2024
Accepted: 14 November 2024
Published: 15 November 2024

1. Introduction

The Internet of Medical Things (IoMT) refers to the network of medical devices interconnected through the internet or other network devices. These devices include medical instruments, sensors, diagnostic and therapeutic equipments, as well as wearable devices that collect medical data in real time. These devices, such as sensors and medical instruments with Wi-Fi/Bluetooth connections, enable communication among devices and are the basis of IoMT. Example applications of IoMT include remote patient monitoring for chronic diseases, tracking medication orders, locating patients in hospitals, and collecting data from wearable healthcare devices. Devices in this class might connect to cloud platforms where data are stored and analysed, supporting telemedicine and virtual assistance. The IoT market in healthcare is growing rapidly. It has been estimated with a value of more that USD 44 billion in 2023, with an estimated compound annual growth rate of 21.2% in the next 6 years [1]. IoMT profoundly impacts healthcare by improving asset management and enabling telemedicine for more flexible and accessible care. Used in hospitals, homes, and communities, IoMT facilitates continuous patient monitoring and rapid response to emergencies, overall improving the quality of healthcare and patients' lifestyles.

As the healthcare IoMT market grows, the number of attacks that are specifically targeting this class of devices is increasing. The America's Cyber Defence Agency, in its "Cybersecurity Alerts & Advisories" section [2], lists Healthcare and Public Health among the sectors of interest. CISA Industrial Control System Medical Advisory alerts are assigned a unique code of the form ICSMA-XX-YY-ZZ, that is associated with a short description of the vulnerability and pointers to CVE records. Similarly, the U.S. Food and Drug Administration (FDA) has recommended using industry standard cybersecurity techniques in implantable medical devices [3]. Guaranteeing the security of IoMT systems is a complex task because of a number of factors. First, of all, the IoMT includes highly heterogeneous devices, ranging from huge medical diagnostic devices like CT scanners, with relevant computing and communication capabilities, to tiny implantable medical devices (IMDs) that clearly provide different capabilities and allow diverse levels of protections. Given such heterogeneity, surveying the security of IoMT systems concretely requires the identification of specific, though wide, applications contexts that allow to restrict the attention to narrow, but real, threat scenarios. In this paper, we consider an orthogonal point of view. We restrict our attention to a specific type of devices in the IoMT, namely the IMDs, and survey the wide range of possible attacks and proposed solutions.

1.1. Implantable Medical Devices

Implantable medical devices (IMDs) are medical instruments that are partially or entirely placed into the human body through surgery. IMDs are intended to remain in place either temporarily, just for the expected duration of the treatment, or permanently, to support the treatment of chronic diseases. IMDs functionalities include continuous measurement of vital signs (such as heartbeat, blood pressure, glucose level, etc.) as well as automatically performing medical treatments such as electric stimulations or drug delivery.

Originally, implantable medical devices (IMDs) have been designed and built with the specific focus on the *safety* of the patient [4]. This means that, their sole goal was the proper execution of their programmed tasks. IMD devices need to communicate with the other devices for a number of reasons. First of all, doctors need a way to monitor the patient's reactions to the treatment, i.e., they need to read some patient's medical parameters and adapt the device behaviour if needed. Similarly, technicians need a way to monitor the device healthiness status and to reprogram it if needed, e.g., whenever there is a critical update to the device firmware. Early IMDs operated as stand-alone devices and were possibly connected to their controlling devices (the *programmer*) by means of wired electrodes or short range radio communication [5,6] (less than 10 cm). This means that the controlling device needed to be extremely close to the patient in order to be able to communicate with the IMD. Interactions mainly took place locally, under the physician's supervision. Device reconfigurations, upgrades, and repairs were performed by physically accessing the device, and often required surgery [7].

The security of first IMDs was essentially based on the security-by-obscurity paradigm [8–10]. In other words, communications between IMDs and external devices occurred by means of proprietary protocols. The idea was that, since the adversary does not know the communication protocol, they cannot understand the messages (passive security) or mount an active attack to let the IMD to deviate from its intended behaviour.

Nowadays, IMDs provide multiple interfaces and communication channels that are required to allow prompt and reliable interaction with the whole healthcare infrastructure and involved operators, including patients, in a less invasive way. Newer IMDs are able to use long-range (e.g., 2–5 m) wireless communications links. These newer devices, while being more comfortable for the patient, are open to the development of newer services that include multiple devices. In a modern-minimal setting, the IMDs communicate on the one hand with a programming station that is managed by the doctor/technician and, on the other hand with some sort of "home"-based communication device that allows the patient to monitor her device(s) and opens to the possibility of *telemedicine*. In Figure 1, we report a graphical representation of modern IMD infrastructures.

Communications can occur locally, i.e., in proximity to the patient, by contact (including sound, visual, tactile, and so-called Out-Of-Band signals), or through wireless network interfaces that connect the IMDs to: (a) the base station (the gateway that ensures communications with the physicians' equipment when the patient is at home); (b) any *mediating* device for the patient (e.g., a monitoring app on the mobile phone); or (c) any other medical device, both wearable and implanted, purposed to gather different physiological measurements.

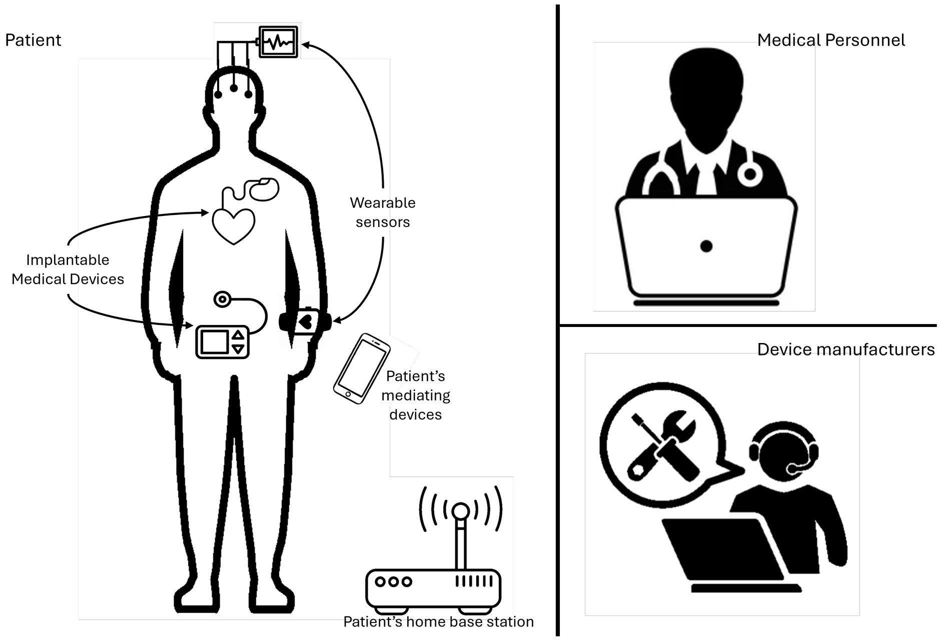
Patient
Wearable sensors
Implantable Medical Devices
Patient's mediating devices
Patient's home base station
Medical Personnel
Device manufacturers

Figure 1. Modern implantable medical device infrastructure.

Over time, this interoperability has become so important that it has led to the development of IMD ecosystems for the treatment of certain pathologies. Thus, modern devices are interconnected through real Body Area Networks (BANs), local short-range networks managed through standard multipurpose protocols (e.g., Bluetooth Low Energy).

Long-range communications take place between "local" devices on one side and (a) the healthcare infrastructure that is treating the patient, or possibly (b) the device's manufacturer, for diagnostics or updates purposes, on the other side. Such long-range communications leverage public network segments (e.g., mobile telephony or the Internet). At the same time, both healthcare institutions and the manufacturer may rely upon computational services provided by third parties, such as connectivity and cloud-based services. For this reason, while IMDs are tiny battery-operated devices whose primary design goal is to monitor patients' physiological signals and, possibly, take actions to correct specific needs, they have become part of a globally distributed ecosystems in which data storage and computation is possibly outsourced to partially trusted third parties.

Moreover, individuals' roles and duties, and devices' operating parameters, may vary over time, with the progress of the treatment or following specific events. These factors may require temporary modifications to the established access and authorization policy for the operators. For example, access to personal and medical data retained by the devices is usually allowed to authorized personnel only, whereas within an emergency scenario, any restriction should be relaxed, for the sake of saving the patient's life.

Such flexibility often conflicts with usual security goals. Potential solutions to this problem require extensions of the security concept for such kind of applications, in order to achieve acceptable trade-offs between devices safety, utility, and security. In fact, the design of IMDs (and, in particular, their security features) must take into account the strict constrains imposed to these devices, due to their critical physical environment. In [11,12], the authors highlight the nature and extent of such trade-offs, showing that, at first sight, needs raised to ensure patients' health and safety may conflict with the achievement of required security objectives. The authors mention some examples of such "tensions", firstly in relation to the patient's body's limited tolerance to exposure to overheating of the devices and prolonged emission of RF signals, or the need to prevent excessively fast depletion of the devices' battery, with respect to the adoption of computational intensive cryptographic primitives or communication intensive protocols for the sake of authentication and secure data transfer.

Despite the long-standing literature on secure system designs, as discussed below, it is possible to find numerous examples of very recent insecure devices.

In [9], the authors show how to reverse-engineer the communication protocol for an implantable cardiac defibrillator (ICD) and implement both passive and active attacks that impact on both patient safety and security. They also present possible countermeasures to such passive and active attacks, brought by both insiders and outsider adversaries, two of which require the patient to actively participate in the security process. One important point made by the authors is that security measures might, in principle, introduce safety hazards. For example, the use of cryptographic keys might protect user privacy but, at the same time, key unavailability might prevent authorized medical personnel access to user data during a critical condition that, in turn, is a safety-critical event to be properly managed.

In [10], the authors consider the case of a popular insulin pump, a device for controlling glucose levels in patient's blood that is used for the management of diabetes. This type of device actually consists of at least (a) a continuous glucose sensor, placed under the patient's skin, and (b) an insulin pump that injects insulin whenever necessary. Typically, this core system extends to one or more external devices, like a remote controller that is able to reprogram the pump, an external log system to store glucose levels, external glucose sensors in case of failure of the continuous sensor or, more recently, systems to monitor the patient's physical activity. The specific pump uses wireless links to connect with all such devices. In [10], the authors show that, using public available information and widely available off-the-shelf devices, it is possible to run both passive or active impersonation attacks against such devices. A more complex attack against a device of the same class is reported in [13].

In 2016, in [14], the authors considered different implantable cardiac defibrillators (ICDs) that use 2–5 m RF communication systems. The authors show that, using reverse engineering, it is possible to identify proprietary communication protocols implemented by these devices. Most importantly, the authors also show that such protocols present several implementation weaknesses that may be subject to different types of attacks. This show, once again, that security-by-obscurity is a paradigm that does not guarantee any security at all. Still, very recently, CISA reports vulnerabilities that span from data leakage (as in [15]) regarding unencrypted messages sent over BLE connections, to more critical and potentially life-endangering behaviours, like in [16].

Furthermore, when designing security protocols and measures to protect IMD, it is necessary to consider their impact on usability or acceptability from the patients. As observed in [17,18], although implantable devices have positive effects on the patients' quality of life, in some cases, measures taken to secure such devices make their usage unpleasant for different reasons, ranging from mistaken perceived security to cultural reasons or, as observed in [19], by social interactions.

1.2. Motivation

Securing IMDs is a complex task because of the inherent limitations of this class of devices, e.g., related to computing power, limited battery/bandwidth/communication range, and because of the criticality of the performed task, typically involving the possibility of the death of the patient. In general, techniques used to secure these devices can be based on different approaches. Some systems leverage the natural biometric nature of implantable devices, and use this property as a means for strong authentication/identification. Other approaches are based on the fact that specific technologies require limited distance between two devices in order communicate that, on the other hand, also prevents eavesdropping from devices that are far away from the target. More general approaches consider (typically lightweight) key management protocols, coupled with (lightweight) encryption schemes to ensure security properties. In some cases, anomaly detection systems can be used to prevent adversary attacks on specific devices. Finally, there exist solutions that use auditing techniques to monitor the system's behaviour, or external mechanisms or devices as enabling technologies for security properties.

In the literature, there exist different surveys on implantable devices. In [20], the authors first define security goals and adversarial goals, and then partition the threats into three possible categories, namely telemetry interference, software threats, and hardware and sensor interface threats. Then, for each threat category, the authors analyse the existing literature by listing a number of techniques that can be used to prevent it, providing an interesting dependency graph among the different existing proposals. An approach closer to our point of view can be found in [21], where the authors explicitly differentiate the normal from the emergency operational scenarios. Furthermore, the authors clearly mark the limitations and trade-offs related to the limited resources that are available on the IMD side. The authors consider four protection mechanisms, namely audit, security primitives, access control, and anomaly detection. An interesting literature analysis is carried out by analysing the existing solutions for each listed category. However, survey [21] does not consider results related to machine learning as a possible tool for IMD security.

In [22], the authors notice that plenty of studies addressed the security of IMDs in the general context of IoMT security. However, they restrict their study exclusively to IMDs, arguing that such devices have characteristics that are worth of a more in-depth and dedicated research. The authors precisely define the boundaries of the "IMD security domain", then provide a comprehensive survey of the security threats and a critical analysis of the main solutions currently on the shelf.

Nevertheless, minor attention is devoted to in-progress studies and future development; in particular, authors do not address the possibilities offered by the forthcoming application of machine learning.

In this paper, we systematize IMD security literature by partitioning solutions by security tool. We highlight what we believe are the most promising and important techniques that need to be considered when deploying a medical infrastructure that includes IMDs in the loop, and in particular we refer to currently available machine learning techniques as key enabler for modern IMD security.

2. Threat Model

Securing implantable medical devices and their support infrastructure (IMDs infrastructures, in short) is a quite challenging task for designers, due to complex nature of such equipment and their delicate field of application [23].

2.1. The Adversary

An extensive knowledge of adversaries' nature, objectives, targets, and capabilities in the specific field of IMDs is essential in order to identify the threats coming from them and to forecast potential attack patterns. At a glance, adversaries fall into two categories: insiders and outsiders.

Insiders may include any components of the medical staff: physicians, clinicians, practitioners, device maintainers/specialists and, obviously, patients themselves. Attacks by dishonest medical staff members could have the purpose of tampering with diagnostics, logging, and audit records in order to hide the causes of possible damages due to human errors and negligence, or simply to disclose sensitive data for monetary income. On the other hand, patients might try to exploit the device in order to modify the therapy (e.g., to increase the dose of certain drugs).

Insiders have legitimate, variously shaped access privileges to the IMD and its supporting equipment. Attacks mainly consists of device abuses with the purpose of circumventing access control and authorization systems. Moreover, insider attackers may take advantage of their physical proximity to the device.

Outsider adversaries include entities having any sort of interest in exploiting the IMD infrastructure. These adversaries may include terrorist or criminal organizations, competitors of the target IMD manufacturers, unscrupulous stakeholders, etc. They have the most diverse objectives, including causing physical harm to individuals (e.g., to kill them or for extortion purposes), causing trouble for any monetary advantage (e.g., to influence the stock markets), silently gathering sensitive information about patients or their pathology, tracking their movements, or pursuing discriminating actions against individuals with certain diseases.

Hassija et al. [24] discuss adversary types and motivations, the goals of the attacks, and the issues raised by a massive deployment of interconnected IMDs.

2.2. Attacks

Passive attacks are aimed at extracting any sort of information from the IMD infrastructure, mainly about patients (personal data, pathology, health status, current therapy . . .). Nevertheless, the target of a such attacks might be the IMD itself. In this case, adversaries are interested in discovering the type of device, its manufacturer, serial number, version, status, and any further information that can be used for subsequent intrusions.

Passive adversaries can proceed both locally, by silently observing the target equipment behaviour (e.g., by watching at its dashboard, listening to sound alerts, measuring any "side effect" of the device operation, intercepting short range communication occurring among IMDs [25]), or remotely, by eavesdropping the network traffic taking place within the whole infrastructure without interacting with any of its component.

The success chances for these kinds of attacks depend on the quality and strength of the security measures provided by the device and its support infrastructure. Problems mainly arise from those systems that store and disclose a vast amount of information without adequate access control policies and poorly protect its confidentiality.

Active adversaries leverage different means and techniques to violate an IMD infrastructure. Mainly, attacks are carried out remotely by either seeking and exploiting possible vulnerabilities in the IMDs' networking subsystem, or launched through those public network segments that connect its different components [26].

Locally, attacks can by mounted by unauthorized access to the infrastructure through illegally obtained devices [27] by hijacking any physical component with customized equipment. In this regard, Bruleson et al. [28] discuss the characteristics of three widespread types of IMDs, and briefly survey some of most common threats they are prone to. Particular attention is required for attacks targeting battery consumption [29], for which the available detection methods that are PC-like/mobile devices (e.g., ref. [30]) cannot be applied. To this regard, the human factor has its relevance. The attack surface might be affected by inexpert medical personnel and patients, and poorly designed (or enforced) security policies, practices, and guidelines [31–33].

3. Securing IMDs

As seen in the above discussion, until recently, there have been IMDs whose design and/or implementation allow for different types of attacks. In this section, we describe some tools and techniques that have been used in order to strengthen the security of IMDs.

3.1. Biometric Identification

One key problem related to IMDs is the identification of the patient during interactions. As we have seen, the IMD communicates with the outside world using short-/long-range communications. These communication channels might be used to obtain information directly from the devices, e.g., in an emergency situation for checking the patient conditions/device status, or from the infrastructure that stores patient secured data. In these cases, the system needs to prevent attacks to the privacy of the patient. At the same time, the communication channels can be used for reprogramming the specific device, based on the patient's medical conditions. It is thus mandatory to properly identify the patient in order to prevent the improper reconfiguration of the device.

In [34], the authors propose the use of the patient's biometrics to protect the IMD data. The authors specifically consider the case of medical emergencies in which the patient may not be conscious and, thus, may not be able to provide credentials to unlock the IMD data. The authors propose preloading the user biometrics, specifically the patient's fingerprints or the patient's iris, to protect the access to the IMD. In case of emergency, the medical staff may have easy access to such biometrics to unlock the IMD data. Notice that there exist dynamic access control techniques, e.g., ref. [35], that have been specifically designed for emergency situations, which might be coupled with biometric access control in an open environment. Furthermore, there exist specific solutions, e.g., refs. [36–38], to protect remotely stored encrypted data by means of secure protocols that allow for transfer and local decryption by means of locally measured biometrics.

In [39], the authors use the Inter-Pulse Intervals (IPIs) of heartbeats as a way to authenticate the proximity reader in case of emergency. The idea is that the external reader has access to the patient's heartbeats and can, thus, generate an Entity Identifier (EI). If such an identifier matches the one stored in the IMD, then the IMD data are released to the external reader.

In such cases, the use of biometrics can prevent passive or active attacks to the device. Whenever cardiac monitoring devices, like pacemakers or defibrillators, are used, the ECG data can be easily extracted and used as a biometric trait for user identification. However, ECGs are typically dynamic "non-random" signals and, thus, their plain or improper use in authentication protocols would lead to almost-deterministic protocols that, by definition, cannot considered secure. Indeed, deterministic protocols might be subject to eavesdropping and replay attacks. In [40], the authors present techniques to extract randomness from the ECG signals and provide a secure authentication protocols that uses the randomness and data from the ECG monitoring device.

In [41], the authors consider the security of the whole monitoring infrastructure, consisting of device, the communication channel, and the monitoring backend. Furthermore, the authors consider three different layers to be secured, namely the device, communication, and storage layers. In this paper, the authors use MLP neural networks for analysing the ECG signals. This solution proposes using a lightweight encryption scheme derived from direct sequence spread spectrum (DSSS) that is, essentially, a symmetric key encryption scheme obtained by using linear pseudo-random generators.

Current biometric authentication techniques guarantee high level of accuracy in the identification of a subject, especially when multi-modal identification, i.e., combination of multiple biometric signals, is available. For example, in [42] (resp., [43]), the authors show that combination of electrocardiography and photoplethysmography (resp., finger vein pattern) provides better results than unimodal systems. The real issue with biometric measurements is that they are really dependent on the sensor precision and the measurement context. For example. in the case of IMDs like ICDs or pacemakers, the device is naturally monitoring heart electric signals. However, the heart rate and electric behaviour is subject to external conditions like patient physical activity or mood. Furthermore, in case multiple sensors need to be used, one key issue is related to mechanical adjustments that physical (and possibly wearable) devices may require. One last issue to consider are spoofing attacks in which an adversary tries to impersonate a subject by using data recorded in previous identification sessions. Spoofing attacks are always possible when biometrics are used for identification. Some classical countermeasures to spoofing might not be applicable in the specific context of IMDs. For example, dynamic challenges, e.g., asking the subject to perform a specific action like blinking eyes during identification, might not be applicable in the context of cardiac IMDs, since the patient is not able to impose a specific action on their own heart. Instead, multi-modal systems might constitute a doable solution in the IMD setting.

3.2. Lightweight Cryptography and Key-Management

Modern IMDs are capable of connecting to other devices using some kind of wireless technology. The first such devices were designed and built to use proprietary technologies and communication protocols. However, such devices, as observed in [8], were typically insecure. Currently available devices use standard wireless technologies and protocols (e.g., BLE) that allow for the possibility of connecting with commonly available off-the-shelf devices. Such capability opens a wide range of possibilities for the cooperation of multiple services but, at the same time, it widens the attack surface.

It is clear that one crucial point in the security of each open ecosystem is the possibility of securely establishing cryptographic keys to protect communication and identification. The idea of using measurable physiological data to generate cryptographic keys for securing communication dates back to [44], who identified the Inter Pulse Interval, or IPI for short, as a good candidate. Indeed, IPI is sufficiently random for generating secure keys in a short amount of time. Furthermore, it can be easily measured anywhere on the patient's body. The latter property is extremely helpful whenever multiple sensors need to agree on a common key and have access to the same source of randomness. The authors of [40] use these properties to guarantee that only devices that are physically in contact with a patient (i.e., using an IMD), are authenticated and, thus, can communicate with other devices in the body network. Another approach has been used in [45], in which the cryptographic key in computed starting from the iris biometric. In [14], the authors argue about the common misleading assumptions that are made when designing a cryptographic protocol based on the measurement of physiological data. The first one considers the measurable data "as is" as source of randomness to be used in cryptographic protocols. It is well known that, in order to be used in cryptographic protocols, randomness sources need to withstand strict conditions. Informally, the elements in the generated streams need to be uniform and independent from each other. Human physiological measurable data are far from containing these properties. In [46], the authors introduced the fuzzy vault primitive, namely the possibility of locking a secret value using a set of secret elements in a way that it is possible to extract it only if the set used to unlock it is *close* to the original one. The "set of elements" used to lock a secret can be a set of biometric measurements of a person, and may be subject to some errors. The secret value can be extracted if, at decryption time, the biometric measurements of the encryptor are "not far" from the ones used to encrypt the value or, in other words, the subject who requested the decryption is the one who encrypted it. In [47] the authors provide a primitive, namely the *fuzzy extractor*, that can be used to turn any biometric data into cryptographically strong keys. This general primitive has been subsequently improved to be used in Body Sensor Networks [48]. In [49], the authors observe that modern IMDs are typically coupled with mobile devices owned by the patient, which are used to monitor or reconfigure the IMD and which communicate with an external controller. The authors propose a solution that considers this de facto (near future) standard configuration, and use the mobile device as key management centre and access policy decision point. In this way, the patient is always aware of all operations that her device is executing. One key issue is the establishment, in a secure way, of the "first" cryptographic key that is shared by the IMD and the mobile device owned by the patient. Starting from this architecture, the authors of [50] present a solution for an artificial pancreas system (APS). Such devices basically consist of three components: a continuous glucose monitor (CGM), an insulin pump, and a controller. For this type of device, the controller needs to securely communicate with the CGM and the insulin pump.

There exist a number of issues related to lightweight encryption and key management schemes in IMD/wearable devices [51]. First of all, one key measure in IMD devices is battery consumption. As stated above, current devices participate in a body area network, in which they exchange encrypted data. High-end devices in such networks, e.g., mobile phones, can easily withstand high energy-demanding schemes, since they can be easily recharged, while IMDs cannot. Every system deployment should consider the limitations of IMD devices within a body area network, provide different security levels that should depend on the specific devices' capabilities, and provide outsourcing capabilities to move heavy computations/communications to high-end devices in the network. In this context, the use of proxy re-encryption (e.g., ref. [52]) might provide a doable and efficient solution.

Regarding key management schemes, one key issue to be considered and explored is the peculiar need for rekeying. Body area networks essentially consist of two different types of devices: the ones that do not change frequently (e.g., IMDs), and the ones for which energy is not really an issue, i.e., they are connected to the power grid or it be easily recharged (e.g., user mobile phones). Furthermore, such devices may either use keys that, by their own nature, cannot change (e.g., biometric keys). Every key management scheme that needs to be deployed in a body area network that includes IMDs needs to be flexible enough to accommodate all such types of devices with different types of key requirements.

3.3. Out-of-Band Channels and OOBKey

Out-of-band channels make the communication between IMDs and external devices possible without relying (entirely) on wireless protocols. This has two main advantages: enabling the patient to be involved in the communication and being aware of what is going on (e.g., by notifying of certain events with an audible, visual, or tactile signal); and protecting short range sensitive data exchange from eavesdropping and interferences.

In [25], the authors discuss the limitations of recent key exchange mechanisms between IMDs and external devices, in terms of the lack of usability and deployability, and propose OOBKey, a key exchange mechanism that relies on out-of-band signalling. In particular, OOBKey features a two-step key exchange protocol: in the first, the IMD and the external device (a cellular phone) negotiates a short-term key (STK) through bodily motions of the patient's body. In the second step, the STK is used as a "password" in a PAKE protocol session, through which the endpoints establish a strong long-term key to be used to encrypt the communication.

3.4. External Devices

Given the limitations of IMDs, the use of external devices to support/protect/enhance the capabilities of implanted devices has been considered in different papers.

In [53], the authors propose the use of an external device, named the *shield*, to protect the wireless communications of an IMD. The key idea is to use the shield to jam incoming and outgoing communications so that outgoing messages are unreadable to any passive adversary. At the same time, messages by an active attacker are jammed by the shield and made useless, since the protected IMD will not recognize them as commands to be executed. At the same time, the shield is able to properly encode/decode messages whose destination is an authorized device. A similar approach has been adopted in [54], where an external wearable device, the *Guardian*, is able to protect the communications between an implantable cardiac device and a doctor, both during regular operations and in case of emergency ones. The key idea that both devices can derive a common encryption key from the patient's heartbeats. This approach allows the key regeneration in case the guardian is lost or malfunctioning. At the same time, any adversarial device cannot compute a shared key unless in physical contact with the patient.

In [55], the authors present a framework that prevents attacks on pacemakers by using a wearable device that monitors the Electrocardiogram (ECG) and Photoplethysmogram (PPG). More precisely, the authors present a formal runtime verification framework that, based on the ECG and PPG monitoring, is able to identify anomalies in the system behaviour, thus enforcing security policies to protect the patient. The framework simplifies the specification security policies that, by considering multiple physiological sensed data, are able to identify, and possibly block, attacks to a specific critical IMDs. The authors specify control policies using timed automata, and present a methodology for specifying pacemaker control policies with respect to ECG and PPG.

In [56], the authors present a proxy-based access control scheme that allows for the delegation of cryptographic computation intensive operations to an external proxy, e.g., a mobile, while guaranteeing the access to IMD.

Proxy re-encryption schemes can use different techniques and strategies. In principle, a semi-trusted proxy uses properties of a public key encryption scheme to re-encrypt a ciphertext from the public key of delegator to the public key a delegatee. There exist multiple security models, leading to encryption schemes of different complexities. As already stated above, resources needed to run the operations are fundamental, since IMDs have low computational resources. Recently (e.g., in ref. [56]), attribute-based encryption schemes have been successfully designed to implement proxy re-encryption for IoT devices. Improving these schemes might be beneficial for their deployment in contexts with IMDs, where biometrics might be used for device keys.

3.5. Machine Learning

Nowadays, machine learning (ML)-based systems are widely used to improve the security of medical equipment, including IMDs [57]. Supervised models are *trained* to recognize the correct operation of each component of the infrastructure. The training process is fed with specific *datasets*, i.e., data extracted from the target equipment, which can include commands and responses, telemetry, diagnostic signalling, medical measurements, and so on. Eventually, the model is able to realize if, because of a potential attack in progress, the infrastructure deviates from its expected behaviour, and to raise an alert to the decision maker.

Approaches leveraging machine learning differ from each other, depending on the device they monitor and the selection of data (features) used to analyse its behaviour. In particular, ML-based solutions have proved to be quite effective against attacks that consist of injecting malformed data into the infrastructure, in order to maliciously determine its actions or cause it to crash. For example, an adversary can replace vital signs collected by any IMD with altered measurements in order to force potentially harmful reactions.

The suitability of Deep Learning models that enable unsupervised learning and far more advanced analysis capability is investigated in [41]. In particular, the authors address the affordability of such models, in terms of computational capabilities and power consumption, for IMDs, which are generally resource constrained.

In [58], the authors define a small set of features suited to profile the communication among medical devices. The system analyses the type of exchanged messages, their timing and frequency, their origin, and other metadata, in order to detect possible anomalies (e.g., whenever a command is sent by a device located in an unexpected place).

HealthGuard [59] is presented as a security framework for *Smart Healthcare Systems*. HealthGuard monitors patients' vital sings, collected by means of multiple medical devices, and seeks evidence of potential misbehaving due to attacks against the medical infrastructure. HealthGuard is based on the assumption that vital signs do not change independently of each other. However, in accordance with the patient's health conditions, changes in any measurement are coherently reverberated through the others. The system is trained to recognize any variation in vital signs that is related to certain health conditions as "benign", and to raise an alarm whenever any incompatible measurement occurs. The event classification module leverages a machine learning model. Experiments compare the performance achieved with Multi-Layer Perceptron, Decision Tree, Random Forest, and K-Nearest Neighbour. The security model essentially concerns insider attacks. In fact, the considered threat model includes local forged data injection, physical device hijacking, and disconnection. Nevertheless, network-based attack patterns are out of this proposal's scope.

CardiWall [60] addresses the security of implantable cardiac defibrillators (ICD). CardiWall prevents a compromised programmer device to send harmful commands to the implanted device. The system consists of a trusted device that acts as a firewall placed between the devices, and analyses every command sent by the programmer to the ICD. In case of anomalies, an alert is raised, and the operator is asked to allow/deny the command delivery. Further approaches and solutions include those discussed in [61,62], which leverage both ML and DL models.

Machine learning-based solutions that mitigate attacks aiming at compromising the delivery of drugs for diabetes treatments include those discussed in [63–66]. Several proposals are designed to involve the patient in security actions. For example, in [67], whenever an anomalous command is issued to the pump, the patient is asked to allow or deny a consensus by making a predefined gesture.

In recent years, healthcare systems have become part of a globally distributed ecosystem. In principle, such systems might be used as the basis for a worldwide data distribution system that would provide AI scientists with a tremendous amount of medical research data to be analysed. However, it is easily understood that training such AI systems using classical centralized algorithms is impossible, due to privacy issues related to the very same nature of the medical data. A promising set of methodologies that can be used toward privacy-preserving machine learning in healthcare systems are the ones under the umbrella of federated learning [68,69]. The key idea is to allow model training to be executed distributively, while preserving data privacy. Each stakeholder locally trains a partial model using its own data. Partial models are then aggregated, either by a central authority, or distributively by all stakeholders. This would allow, for example, the engineering of diagnosis systems that are trained using medical (sensitive) data provided by different stakeholders [70,71], e.g., different hospitals. This approach has been already successfully used in specific cases; for example, for pneumonia detection [72], prediction of cardiac diseases [73], or for other IoMT applications [74]. Another possible application field is the engineering of intelligent systems that are used to block or prevent attacks to healthcare systems using data regarding previous attacks on participating stakeholders. It is obvious that such data are sensitive for each stakeholder, as its publication might affect the owner's reputation. In this context, compromised parties' agents might expose a Byzantine behaviour, trying to lead to a system that is unable to properly detect or prevent an attack. There exist solutions (e.g., [75]) that are able to limit the effect of Byzantine attacks, in the specific case by exploiting a supervisor that interacts with stakeholder agents by challenging shadow datasets in their training processes that allows for the removal of poisoned models.

In the context of low-capability devices like IMDs, the possibility offered by cloud storage and computing might allow for the engineering of solutions that would be impossible otherwise. Also in this field, federated learning might provide solutions (e.g., refs. [76,77]) that allow for the effective use of cloud resources for computing medical sensitive data while preserving their privacy.

The data privacy level each knowledge base representation is allowed to guarantee depends on specific assumptions about the knowledge that is available to each stakeholder/player. In other words, there exist theoretical frameworks that allow us to limit the information that can be inferred by a knowledge base (e.g., refs. [78,79]) if the only information that is available to the player is exactly the one that is represented by the knowledge base. However, each player may have access to external data sources, e.g., social networks or other data sources not belonging to the knowledge base, whose data might be coupled with the ones inferred by the knowledge base in order to obtain sensitive data that were impossible to obtgain without the side information.

In the context of IoMT (centralized/distributed federated) learning, the issue of designing privacy-preserving systems that are resilient against side information is crucial to guarantee patients' privacy. Different patients may have released personal data to different sets of data sources, and gaining control over all of them is practically impossible. Techniques for limiting the amount of sensitive information that can be inferred is an important open research problem.

3.6. Securing (Local and Remote) Software

Until now, we have discussed proposals for securing single IMDs, or how to couple each IMD with some helper devices. This step is clearly crucial and critical for securing the small world around the device. However, when securing an IMD, it is crucial to understand that each tiny device is an element in a global infrastructure. This means that attacks to the infrastructure may impact the security of each single IMD. Examples of this impact can be seen in [16], where a vulnerability in a software component on the server side allowed an attacker to read/modify or delete patient data. This type of vulnerability affects the data privacy or integrity on the healthcare organization side. More critical vulnerabilities have been identified on the Software Delivery Network, which is the network used by device manufacturer to distribute software updates. In this case, the vulnerability would allow an attacker to distribute malicious software directly to implanted devices. Secure firmware distribution and updates are one critical element in the device manufacturing industry [80,81]. Firmware is directly run on implanted devices, and its malfunctioning would immediately impact the patient's safety. A failure in the firmware/software distribution infrastructure allows for the deployment of insecure software. At a more general level, secure software production and distribution [82,83], guaranteeing protection against denial of service through improper device updates, have to be properly considered and put in place.

Recent results show either vulnerabilities in the firmware update mechanisms of specific IoT devices (e.g., refs. [84,85]), or vulnerabilities in the mechanisms used by the companion apps typically used to trigger the firmware updates in IoT devices [86].

As stated in [82], user education has to be carefully considered. First of all, user trust is subjective, and depends on a number of factors, some of which are background knowledge on the specific information, personal experience, application context, and so forth. This also holds for software update frameworks that need to be operated by people. In this regard, software developers might be tempted not to disclose a vulnerability in order to prevent distrust in a specific software component, and this should be clearly avoided by public company policies. On a more technical side, there is a need for (possibly) automatic verification of the firmware/software update procedures, specifically the ones triggered by mobile apps. Indeed, well-established globally available software distributions and update repositories have solid development teams. In contrast, firmware distribution systems and triggering apps for IoTs might be designed by personnel with limited experience in software distribution systems security that would, by itself, become a security threat to the whole infrastructure.

4. Ethical Aspects

The growing deployment of connected implantable medical devices increasingly raises ethical concerns regarding various aspects, ranging from safeguarding of patient welfare to ensuring the security and correct operation of the devices, as well as the protecting the privacy of patients' personal data.

As with every medical treatment, the use of IMDs adheres to ethical principles, such as respect for patients' *autonomy*, *non-maleficence*, *beneficence*, and *justice* [87]. Contrary to what one might expect at first sight, these principles have a significant and specific influence on the design of IMD infrastructures and their usage practices.

The principle of "autonomy" concerns every impact the therapy may have on the patients, primarily in terms of self-determination. In the context to IMDs, such a principle is implemented by providing the patient with comprehensive information related to the nature of the therapy, its effects, influences on lifestyle, and the risks associated with its adoption. Special emphasis is placed on issues related to device functionality and cybersecurity, ensuring that patients are fully aware of these aspects [31,88].

To this end, manufacturers of IMDs must make all instructions needed for correct device usage available, and promptly inform medical personnel and patients of any risks, defects, and vulnerabilities that may arise over time [89].

According to the principle of "non-maleficence", an implantable medical device should not cause harm to the patient due to design errors, malfunctions, or misuse. Manufacturers must ensure the proper functioning of the device through continuous monitoring, regular updates, and timely intervention in the event of failures or security breaches [90].

In this regard, increasing attention is devoted to identifying and enforcing roles and responsibilities for the different actors involved: device manufacturers, medical personnel, caregivers, and patients [91,92].

The principle of "beneficence" leads to the development of devices that effectively improve patients' quality of life, not only from a medical point of view, but also from a psychological one. In particular, to reduce the anxiety and insecurity that they may develop in relation to IMDs, some authors propose putting patients in the loop, by notifying them of events that may require attention, asking them questions, or prompting them to take actions aimed at checking their conditions or preventing security violations [25,67].

However, this could turn out as a double-edged sword. Indeed, inadequately skilled patients might experience anxiety and panic due to misinterpretation of the information provided by the device [93].

Finally, the principle of "justice" concerns guaranteeing fair access to IMD-based treatments, and to avoid patients with IMDs being subject of any form of discrimination.

Within the scope of this paper, fair access would mean preventing patients from considering any trade-off between device cost affordability and security. In fact, security features still noticeably affect the cost of devices, though research into low-cost and sustainable cryptography is a quite active field. However, in the short term, the main viable solutions require manufacturers, healthcare institutions, and regulatory boards cooperating in order to establish resource management policies and good practices for the sake of cost containment [94].

To prevent discrimination against patients with implantable medical devices, it is crucial to protect their personal data to avoid their identification, tracking, or recognition of their implanted device or therapy they are undergoing. Plenty of solutions are currently on the shelf for this purpose. Nevertheless, it is necessary to provide these tools of user interfaces that make the patients' comprehension and the definition of effective privacy policies easier [95].

5. Conclusions

In this paper, we have considered the security of implantable medical devices. This field has a number of intricacies due to the inherent need to guarantee safety and security of tiny battery-operated devices, with limited computational, storage, and communication capabilities, in a globally connected infrastructure, which may have a direct impact of patients' life. Our paper is far from being exhaustive, but highlights some issues that clearly emerge from the scientific literature.

From our point of view, a critical, urgent, and yet open issue is the design and standardization of a common middleware platform that allows for a transparent and secure deployment of tiny-to-medium devices in a body area network. Such a framework would immediately increase the security of all devices in the network if it is able to provide secure communication channels, secure outsourcing of data storage and computation, and a transparent layer for combining biometric measurements read by independent devices. Such primitives should be provided by manufacturers with a guaranteed minimum security level, and be specifically designed to be easily composable.

Author Contributions: Authors contributed equally to the preparation of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU—NGEU and by project Privacy Preserving Data Analysis (PPDA)—Growing Resilient Inclusive and Sustainable—GRINS (PE00000018) Spoke 0 AND 2—under the NRRP MUR program funded by the EU—NGEU.

Data Availability Statement: The original contributions presented in the study are included in the article, further inquiries can be directed to the corresponding author.

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

References

1. Grand View Research, Inc. Internet of Things in Healthcare Market Size, Share & Trends Analysis. 2023. Available online: https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market (accessed on 4 September 2024).
2. America's Cyber Defense Agengy. Cybersecurity Alerts & Advisories. 2023. Available online: https://www.cisa.gov/news-events/cybersecurity-advisories (accessed on 4 September 2024).

3. U.S. Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices. Technical Report. Guidance for Industry and Food and Drug Administration Staff. 2016. Available online: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf (accessed on 20 July 2024).
4. Sametinger, J.; Rozenblit, J.; Lysecky, R.; Ott, P. Security challenges for medical devices. *Commun. ACM* **2015**, *58*, 74–82. [CrossRef]
5. Greatbatch, W.; Holmes, C. History of implantable devices. *IEEE Eng. Med. Biol. Mag.* **1991**, *10*, 38–41. [CrossRef] [PubMed]
6. Majerus, S.J.A.; Fletter, P.C.; Damaser, M.S.; Garverick, S.L. Low-Power Wireless Micromanometer System for Acute and Chronic Bladder-Pressure Monitoring. *IEEE Trans. Biomed. Eng.* **2011**, *58*, 763–767. [CrossRef] [PubMed]
7. Narasimhan, S.; Wang, X.; Bhunia, S. Implantable electronics: Emerging design issues and an Ultra light-weight security solution. In Proceedings of the 2010 Annual International Conference of the IEEE Engineering in Medicine and Biology, Buenos Aires, Argentina, 31 August–4 September 2010; pp. 6425–6428. [CrossRef]
8. Marin, E.; Singelée, D.; Yang, B.; Verbauwhede, I.; Preneel, B. On the Feasibility of Cryptography for a Wireless Insulin Pump System. In Proceedings of the Sixth ACM Conference on Data and Application Security and Privacy, New Orleans, LA, USA, 9–11 March 2016; pp. 113–120. [CrossRef]
9. Halperin, D.; Heydt-Benjamin, T.S.; Ransford, B.; Clark, S.S.; Defend, B.; Morgan, W.; Fu, K.; Kohno, T.; Maisel, W.H. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In Proceedings of the 2008 IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, USA, 18–22 May 2008; pp. 129–142.
10. Li, C.; Raghunathan, A.; Jha, N.K. Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. In Proceedings of the 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, Columbia, MO, USA, 13–15 June 2011; pp. 150–156. [CrossRef]
11. Altawy, R.; Youssef, A.M. Security Tradeoffs in Cyber Physical Systems: A Case Study Survey on Implantable Medical Devices. *IEEE Access* **2016**, *4*, 959–979. [CrossRef]
12. Halperin, D.; Heydt-Benjamin, T.S.; Fu, K.; Kohno, T.; Maisel, W.H. Security and privacy for implantable medical devices. *IEEE Pervasive Comput.* **2008**, *7*, 30–39. [CrossRef]
13. Corporation, M. CVE-2022-43557. 2022. Available online: https://www.cve.org/CVERecord?id=CVE-2022-43557 (accessed on 24 September 2024).
14. Marin, E.; Singelée, D.; Garcia, F.D.; Chothia, T.; Willems, R.; Preneel, B. On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. In Proceedings of the 32nd Annual Conference on Computer Security Applications, ACSAC 2016, Los Angeles, CA, USA, 5–9 December 2016; Schwab, S., Robertson, W.K., Balzarotti, D., Eds.; ACM: New York, NY, USA, 2016; pp. 226–236.
15. Corporation, M. CVE-2024-34463. 2024. Available online: https://www.cve.org/CVERecord?id=CVE-2024-34463 (accessed on 24 September 2024).
16. Corporation, M. CVE-2023-31222. 2023. Available online: https://www.cve.org/CVERecord?id=CVE-2023-31222 (accessed on 24 September 2024).
17. Denning, T.; Borning, A.; Friedman, B.; Gill, B.T.; Kohno, T.; Maisel, W.H. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Atlanta, GO, USA, 10–15 April 2010; pp. 917–926.
18. Denning, T.; Kramer, D.B.; Friedman, B.; Reynolds, M.R.; Gill, B.; Kohno, T. CPS: Beyond usability: Applying value sensitive design based methods to investigate domain characteristics for security for implantable cardiac devices. In Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC '14, New Orleans, LA, USA, 8–12 December 2014; pp. 426–435. [CrossRef]
19. Shinohara, K.; Wobbrock, J.O. In the shadow of misperception: Assistive technology use and social interactions. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '11, Vancouver, BC, Canada, 7–12 May 2011; pp. 705–714. [CrossRef]
20. Rushanan, M.; Rubin, A.D.; Kune, D.F.; Swanson, C.M. SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks. In Proceedings of the 2014 IEEE Symposium on Security and Privacy, Berkeley, CA, USA, 18–21 May 2014; pp. 524–539. [CrossRef]
21. Camara, C.; Peris-Lopez, P.; Tapiador, J.E. Security and privacy issues in implantable medical devices: A comprehensive survey. *J. Biomed. Inform.* **2015**, *55*, 272–289. [CrossRef]
22. Kwarteng, E.; Cebe, M. A survey on security issues in modern Implantable Devices: Solutions and future issues. *Smart Health* **2022**, *25*, 100295. [CrossRef]
23. Kintzlinger, M.; Nissim, N. Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. *J. Biomed. Inform.* **2019**, *95*, 103233. [CrossRef]
24. Hassija, V.; Chamola, V.; Bajpai, B.C.; Zeadally, S. Security issues in implantable medical devices: Fact or fiction? *Sustain. Cities Soc.* **2021**, *66*, 102552. [CrossRef]
25. Zhang, M.; Marin, E.; Ryan, M.; Kostakos, V.; Murray, T.; Tag, B.; Oswald, D. OOBKey: Key Exchange with Implantable Medical Devices Using Out-Of-Band Channels. In Proceedings of the 2024 21st Annual International Conference on Privacy, Security and Trust, Vienna, Austria, 30 July–2 August 2024.
26. Yaqoob, T.; Abbas, H.; Atiquzzaman, M. Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 3723–3768. [CrossRef]

27. Hasan, R.; Zawoad, S.; Noor, S.; Haque, M.M.; Burke, D. How Secure is the Healthcare Network from Insider Attacks? An Audit Guideline for Vulnerability Analysis. In Proceedings of the 2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC), Atlanta, GA, USA, 10–14 June 2016; pp. 417–422. [CrossRef]
28. Burleson, W.; Clark, S.S.; Ransford, B.; Fu, K. Design challenges for secure implantable medical devices. In Proceedings of the 49th Annual Design Automation Conference, San Francisco, CA, USA, 3–7 June 2012; pp. 12–17.
29. Siddiqi, M.A.; Serdijn, W.A.; Strydis, C. Zero-Power Defense Done Right: Shielding IMDs from Battery-Depletion Attacks. *J. Signal Process. Syst.* **2021**, *93*, 421–437. [CrossRef]
30. Catuogno, L.; Galdi, C.; Pasquino, N. An Effective Methodology for Measuring Software Resource Usage. *IEEE Trans. Instrum. Meas.* **2018**, *67*, 2487–2494. [CrossRef]
31. Pycroft, L.; Aziz, T.Z. Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. *Expert Rev. Med. Devices* **2018**, *15*, 403–406. [CrossRef] [PubMed]
32. Khera, M. Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications. *J. Diabetes Sci. Technol.* **2017**, *11*, 207–212. [CrossRef] [PubMed]
33. Dawn Medlin, B.; Romaniello, A. An investigative study: Health care workers as security threat suppliers. *J. Inf. Priv. Secur.* **2007**, *3*, 30–46. [CrossRef]
34. Hei, X.; Du, X. IMD Access Control During Emergencies. In *Security for Wireless Implantable Medical Devices*; Springer: New York, NY, USA, 2013; pp. 19–35. [CrossRef]
35. Bonatti, P.A.; Galdi, C.; Torres, D. Event-driven RBAC. *J. Comput. Secur.* **2015**, *23*, 709–757. [CrossRef]
36. Catuogno, L.; Galdi, C.; Riccio, D. Flexible and robust Enterprise Right Management. In Proceedings of the IEEE Symposium on Computers and Communication, ISCC 2016, Messina, Italy, 27–30 June 2016; pp. 1257–1262. [CrossRef]
37. Catuogno, L.; Galdi, C.; Riccio, D. Off-line enterprise rights management leveraging biometric key binding and secure hardware. *J. Ambient Intell. Humaniz. Comput.* **2019**, *10*, 2883–2894. [CrossRef]
38. Catuogno, L.; Galdi, C.; Riccio, D. An Enterprise Rights Management System for On-the-Field Maintenance Facilities. *IEEE Access* **2020**, *8*, 95987–95996. [CrossRef]
39. Seepers, R.M.; Strydis, C.; Sourdis, I.; De Zeeuw, C.I. Adaptive entity-identifier generation for imd emergency access. In Proceedings of the First Workshop on Cryptography and Security in Computing Systems, Vienna, Austria, 20 January 2014; pp. 41–44.
40. Rostami, M.; Juels, A.; Koushanfar, F. Heart-to-heart (H2H): Authentication for implanted medical devices. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, CCS '13, Berlin, Germany, 4–8 November 2013; pp. 1099–1112. [CrossRef]
41. Rathore, H.; Fu, C.; Mohamed, A.; Al-Ali, A.; Du, X.; Guizani, M.; Yu, Z. Multi-layer security scheme for implantable medical devices. *Neural Comput. Appl.* **2020**, *32*, 4347–4360. [CrossRef]
42. Siam, A.I.; El-Shafai, W.; Abou Elazm, L.A.; El-Bahnasawy, N.A.; Abd El-Samie, F.E.; Abou Elazm, A.; El-Banby, G.M. Enhanced user verification in IoT applications: A fusion-based multimodal cancelable biometric system with ECG and PPG signals. *Neural Comput. Appl.* **2024**, *36*, 6575–6595. [CrossRef]
43. El-Rahiem, B.A.; El-Samie, F.E.A.; Amin, M. Multimodal biometric authentication based on deep fusion of electrocardiogram (ECG) and finger vein. *Multimed. Syst.* **2022**, *28*, 1325–1337. [CrossRef]
44. Poon, C.C.; Zhang, Y.T.; Bao, S.D. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Commun. Mag.* **2006**, *44*, 73–81. [CrossRef]
45. Riccio, D.; Galdi, C.; Manzo, R. Biometric/Cryptographic Keys Binding Based on Function Minimization. In Proceedings of the 12th International Conference on Signal-Image Technology & Internet-Based Systems, SITIS 2016, Naples, Italy, 28 November–1 December 2016; pp. 144–150. [CrossRef]
46. Juels, A.; Sudan, M. A fuzzy vault scheme. *Des. Codes Cryptogr.* **2006**, *38*, 237–257. [CrossRef]
47. Dodis, Y.; Ostrovsky, R.; Reyzin, L.; Smith, A.D. Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. *SIAM J. Comput.* **2008**, *38*, 97–139. [CrossRef]
48. Cao, C.; He, C.; Bao, S.; Li, Y. Improvement of fuzzy vault scheme for securing key distribution in body sensor network. In Proceedings of the 33rd Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBC 2011, Boston, MA, USA, 30 August–3 September 2011; pp. 3563–3567. [CrossRef]
49. Duttagupta, S.; Marin, E.; Singelée, D.; Preneel, B. HAT: Secure and Practical Key Establishment for Implantable Medical Devices. In Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy, CODASPY '23, Charlotte, NC, USA, 24–26 April 2023; pp. 213–224. [CrossRef]
50. Kim, J.; Oh, J.; Son, D.; Kwon, H.; Astillo, P.V.; You, I. APSec1.0: Innovative Security Protocol Design with Formal Security Analysis for the Artificial Pancreas System. *Sensors* **2023**, *23*, 5501. [CrossRef]
51. Salehi Shahraki, A.; Lauer, H.; Grobler, M.; Sakzad, A.; Rudolph, C. Access Control, Key Management, and Trust for Emerging Wireless Body Area Networks. *Sensors* **2023**, *23*, 9856. [CrossRef]
52. Li, X.; Xie, Y.; Wang, H.; Su, X.; Li, H. dAPRE:Efficient and Reliable Attribute-Based Proxy Re-Encryption Using DAG for Data Sharing in IoT. *IEEE Trans. Consum. Electron.* **2024**, *70*, 584–596. [CrossRef]

53. Gollakota, S.; Hassanieh, H.; Ransford, B.; Katabi, D.; Fu, K. They can hear your heartbeats: Non-invasive security for implantable medical devices. In Proceedings of the ACM SIGCOMM 2011 Conference, SIGCOMM '11, Toronto, ON, Canada, 15–19 August 2011; pp. 2–13. [CrossRef]
54. Xu, F.; Qin, Z.; Tan, C.C.; Wang, B.; Li, Q. IMDGuard: Securing implantable medical devices with the external wearable guardian. In Proceedings of the 2011 Proceedings IEEE INFOCOM, Shanghai, China, 10–15 April 2011; pp. 1862–1870. [CrossRef]
55. Panda, A.; Pinisetty, S.; Roop, P. Securing Pacemakers using Runtime Monitors over Physiological Signals. *ACM Trans. Embed. Comput. Syst.* **2024**. [CrossRef]
56. Wu, L.; Du, J. Designing novel proxy-based access control scheme for implantable medical devices. *Comput. Stand. Interfaces* **2024**, *87*, 103754. [CrossRef]
57. Newaz, A.I.; Sikder, A.K.; Rahman, M.A.; Uluagac, A.S. A survey on security and privacy issues in modern healthcare systems: Attacks and defenses. *Acm Trans. Comput. Healthc.* **2021**, *2*, 1–44. [CrossRef]
58. Gao, S.; Thamilarasu, G. Machine-learning classifiers for security in connected medical devices. In Proceedings of the 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–5.
59. Sundas, A.; Badotra, S.; Bharany, S.; Almogren, A.; Tag-ElDin, E.M.; Rehman, A.U. HealthGuard: An Intelligent Healthcare System Security Framework Based on Machine Learning. *Sustainability* **2022**, *14*, 11934. [CrossRef]
60. Kintzlinger, M.; Cohen, A.; Nissim, N.; Rav-Acha, M.; Khalameizer, V.; Elovici, Y.; Shahar, Y.; Katz, A. CardiWall: A trusted firewall for the detection of malicious clinical programming of cardiac implantable electronic devices. *IEEE Access* **2020**, *8*, 48123–48140. [CrossRef]
61. Levy-Loboda, T.; Rav-Acha, M.; Katz, A.; Nissim, N. Cardio-ML: Detection of malicious clinical programmings aimed at cardiac implantable electronic devices based on machine learning and a missing values resemblance framework. *Artif. Intell. Med.* **2021**, *122*, 102200. [CrossRef] [PubMed]
62. Krittanawong, C.; Rogers, A.J.; Johnson, K.W.; Wang, Z.; Turakhia, M.P.; Halperin, J.L.; Narayan, S.M. Integration of novel monitoring devices with machine learning technology for scalable cardiovascular management. *Nat. Rev. Cardiol.* **2021**, *18*, 75–91. [CrossRef] [PubMed]
63. Levy-Loboda, T.; Sheetrit, E.; Liberty, I.F.; Haim, A.; Nissim, N. Personalized insulin dose manipulation attack and its detection using interval-based temporal patterns and machine learning algorithms. *J. Biomed. Inform.* **2022**, *132*, 104129. [CrossRef]
64. Meneghetti, L.; Dassau, E.; Doyle, F.J., III; Del Favero, S. Machine learning-based anomaly detection algorithms to alert patients using sensor augmented pump of infusion site failures. *J. Diabetes Sci. Technol.* **2022**, *16*, 641–648. [CrossRef]
65. Ahmad, U.; Song, H.; Bilal, A.; Mahmood, S.; Alazab, M.; Jolfaei, A.; Ullah, A.; Saeed, U. A novel deep learning model to secure internet of things in healthcare. In *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 341–353.
66. Rathore, H.; Al-Ali, A.; Mohamed, A.; Du, X.; Guizani, M. DLRT: Deep learning approach for reliable diabetic treatment. In Proceedings of the GLOBECOM 2017-2017 IEEE Global Communications Conference, Singapore, 4–8 December 2017; pp. 1–6.
67. Ahmad, U.; Song, H.; Bilal, A.; Saleem, S.; Ullah, A. Securing insulin pump system using deep learning and gesture recognition. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1716–1719.
68. McMahan, B.; Moore, E.; Ramage, D.; Hampson, S.; Arcas, B.A. Communication-efficient learning of deep networks from decentralized data. In Proceedings of the Artificial Intelligence and Statistics, PMLR, Fort Lauderdale, FL, USA, 20–22 April 2017; pp. 1273–1282.
69. Bonawitz, K.; Eichner, H.; Grieskamp, W.; Huba, D.; Ingerman, A.; Ivanov, V.; Kiddon, C.; Konečný, J.; Mazzocchi, S.; McMahan, H.B.; et al. Towards Federated Learning at Scale: System Design. *arXiv* **2019**, arXiv:1902.01046.
70. Xu, J.; Glicksberg, B.S.; Su, C.; Walker, P.; Bian, J.; Wang, F. Federated learning for healthcare informatics. *J. Healthc. Inform. Res.* **2021**, *5*, 1–19. [CrossRef]
71. Zhao, L.; Xie, H.; Zhong, L.; Wang, Y. Explainable federated learning scheme for secure healthcare data sharing. *Health Inf. Sci. Syst.* **2024**, *12*, 49. [CrossRef]
72. Khan, S.H.; Alam, M.G.R. A Federated Learning Approach to Pneumonia Detection. In Proceedings of the 2021 International Conference on Engineering and Emerging Technologies (ICEET), Istanbul, Turkey, 27–28 October 2021; pp. 1–6. [CrossRef]
73. Bebortta, S.; Tripathy, S.S.; Basheer, S.; Chowdhary, C.L. FedEHR: A Federated Learning Approach towards the Prediction of Heart Diseases in IoT-Based Electronic Health Records. *Diagnostics* **2023**, *13*, 3166. [CrossRef]
74. Rani, S.; Kataria, A.; Kumar, S.; Tiwari, P. Federated learning for secure IoMT-applications in smart healthcare systems: A comprehensive review. *Knowl.-Based Syst.* **2023**, *274*, 110658. [CrossRef]
75. Zhao, P.; Jiang, J.; Zhang, G. FedSuper: A Byzantine-Robust Federated Learning Under Supervision. *ACM Trans. Sens. Netw.* **2024**, *20*, 1–29. [CrossRef]
76. Zhao, P.; Tao, J.; Lui, K.; Zhang, G.; Gao, F. Deep Reinforcement Learning-Based Joint Optimization of Delay and Privacy in Multiple-User MEC Systems. *IEEE Trans. Cloud Comput.* **2023**, *11*, 1487–1499. [CrossRef]

77. Quiñones, E.; Perales, J.; Ejarque, J.; Badouh, A.; Marco, S.; Auzanneau, F.; Galea, F.; González, D.; Hervás, J.R.; Silva, T.; et al. The DeepHealth HPC Infrastructure: Leveraging Heterogenous HPC and Cloud Computing Infrastructures for IA-based Medical Solutions. In *HPC, Big Data, and AI Convergence Towards Exascale: Challenge and Vision*; Terzo, O., Martinovič, J., Eds.; CRC Press: Boca Raton, FL, USA, 2022; Chapter 10, pp. 191–216. [CrossRef]
78. Biskup, J.; Bonatti, P.A.; Galdi, C.; Sauro, L. Inference-proof Data Filtering for a Probabilistic Setting. In Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web—Policy and Technology (PrivOn2017) Co-Located with 16th International Semantic Web Conference (ISWC 2017), Vienna, Austria, 22 October 2017; Volume 1951.
79. Biskup, J.; Bonatti, P.A.; Galdi, C.; Sauro, L. Optimality and Complexity of Inference-Proof Data Filtering and CQE. In Proceedings of the Computer Security—ESORICS 2014—19th European Symposium on Research in Computer Security, Wroclaw, Poland, 7–11 September 2014; Proceedings, Part II; Lecture Notes in Computer Science; Kutylowski, M., Vaidya, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; Volume 8713, pp. 165–181. [CrossRef]
80. Moran, B.; Tschofenig, H.; Brown, D.; Meriac, M. RFC 9019: A Firmware Update Architecture for Internet of Things. 2021. Available online: https://www.rfc-editor.org/info/rfc9019 (accessed on 24 September 2024).
81. Catuogno, L.; Galdi, C. Secure Firmware Update: Challenges and Solutions. *Cryptography* **2023**, *7*, 30. [CrossRef]
82. Hou, F.; Jansen, S. A systematic literature review on trust in the software ecosystem. *Empir. Softw. Eng.* **2023**, *28*, 8. [CrossRef]
83. Catuogno, L.; Galdi, C.; Persiano, G. Secure Dependency Enforcement in Package Management Systems. *IEEE Trans. Dependable Secur. Comput.* **2020**, *17*, 377–390. [CrossRef]
84. Cui, A.; Costello, M.; Stolfo, S.J. When Firmware Modifications Attack: A Case Study of Embedded Exploitation. In Proceedings of the 20th Annual Network and Distributed System Security Symposium, NDSS 2013, San Diego, CA, USA, 24–27 February 2013.
85. Andy, S.; Rahardjo, B.; Hanindhito, B. Attack scenarios and security analysis of MQTT communication protocol in IoT system. In Proceedings of the 2017 4th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), Yogyakarta, Indonesia, 19–21 September 2017; pp. 1–6.
86. Ibrahim, M.; Continella, A.; Bianchi, A. AoT—Attack on Things: A security analysis of IoT firmware updates. In Proceedings of the 2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P), Delft, The Netherlands, 3–7 July 2023; pp. 1047–1064. [CrossRef]
87. Beauchamp, T.L.; Childress, J.F. *Principles of Biomedical Ethics*; Oxford University Press: New York, NY, USA, 1994.
88. Torgersen, L.N.S.; Schulz, S.M.; Lugo, R.G.; Sütterlin, S. Patient informed consent, ethical and legal considerations in the context of digital vulnerability with smart, cardiac implantable electronic devices. *PLoS Digit. Health* **2024**, *3*, 1–17. [CrossRef]
89. Kramer, D.B.; Fu, K. Cybersecurity Concerns and Medical Devices: Lessons From a Pacemaker Advisory. *JAMA* **2017**, *318*, 2077–2078. [CrossRef]
90. Das, S.; Siroky, G.P.; Lee, S.; Mehta, D.; Suri, R. Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm.* **2021**, *18*, 473–481. [CrossRef]
91. Simon, D.A.; Kesselheim, A.S. Physician and Device Manufacturer Tort Liability for Remote Patient Monitoring Devices. In *Digital Health Care Outside of Traditional Clinical Settings: Ethical, Legal, and Regulatory Challenges and Opportunities*; Cambridge University Press: Cambridge, UK, 2024; pp. 109–122.
92. Radcliffe, J. Hacking medical devices for fun and insulin: Breaking the human SCADA system. In Proceedings of the Black Hat Conference, Las Vegas, NV, USA, 30 July–4 August 2011.
93. Ho, A.; Quick, O. Leaving patients to their own devices? Smart technology, safety and therapeutic relationships. *BMC Med. Ethics* **2018**, *19*, 1–6. [CrossRef]
94. Siddiqi, M.A.; Tsintzira, A.A.; Digkas, G.; Siavvas, M.G.; Strydis, C. Adding security to implantable medical devices: Can we afford it? In Proceedings of the International Conference on Embedded Wireless Systems and Networks, EWSN, Delft, The Netherlands, 17–19 February 2021; pp. 67–78.
95. Segura Anaya, L.; Alsadoon, A.; Costadopoulos, N.; Prasad, P. Ethical implications of user perceptions of wearable devices. *Sci. Eng. Ethics* **2018**, *24*, 1–28. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.