International Journal of Computing and Digital Systems
2025, VOL. 17, NO.1, 1-15

http://dx.doi.org/10.12785/ijcds/1571024987

Investigational Study for Overcoming Security Challenges in Implantable Medical Devices

Muawya Naser[1], Hussein Al Bazar[2] and Hussein Abdel-Jaber[3]

[1]*Department of Cybersecurity, Princess Sumaya University for Technology, Amman, Jordan*
[2,3]*Faculty of Computer Studies, Arab Open University (AOU), Riyadh, Saudi Arabia*

Received 27 April 2024, Revised 12 October 2024, Accepted 25 October 2024

Abstract: Implantable Medical Devices are getting popular each passing day. Their telemetry makes them the most appropriate choice for both patients and doctors. But, like every other networked device, these devices, too, are vulnerable to security breaches. Security threats to these devices can be, in some cases, threats to human life. Therefore, their security needs to be vigilant. Researchers continue to overcome these vulnerabilities. All of the proposed solutions are not very practical solutions to the security issues of these devices because of the constraints attached to these devices. The utmost constraint is their battery. This paper has attempted to review battery-efficient security solutions. A vast range of literature has been surveyed for this purpose. This paper can be used as a reference for research in this field.

Keywords: Implantable Medical Devices, Security, Privacy, Threats.

1. Introduction

We are living in a cyber age. Technology is all around us. From kitchen chores to defense hallmarks, technology has to play key role everywhere [1], [2], [3], [4], [5], [6], [7], [8]. As people use technology more and more, it undergoes versatility and improvements. Healthcare also is one of the most promising fields where technology is rapidly advancing [9],[10], [11], [12], [13]. From online appointments with doctors to remote surgery, are the applications of technology in healthcare [14], [15], [16]. Implantable Medical Devices (IMDs) are one such example.

IMDs are specialized microchips that get implanted within the human body and are used for regulating and monitoring various human physiological activities, such as monitoring heartbeat rate, regularly measuring the blood pressure level, looking at brain conditions, and maintaining insulin at an optimum level as shown in Figure 1 [17], [18], [19], [20]. The device records these activities and sends them back to a receiving device called a programmer. The concerned doctor takes insights from these readings and takes action if needed. Some common types of IMDs are Pacemakers, Cardioverter Defibrillators, Cochlear implants, and Insulin pumps etc.[21]

The importance of these medical devices has reached an undeniable degree. They have become a necessary part of our lives. IMDs offer numerous aids and assistance to humans. These aids can be in the form of offering support to the handicapped, reporting variations in the health metrics, supplying drugs to the internal and hardly accessible body parts, and replacing the disabled organ as well. These devices have become essential for many. Some people use them as just aiding devices, but they are considered survival tools for many. It has become impractical not to consider them as part of human lives.

IMDs are coming in to assist both doctors and patients. For the doctor, it is easier to examine the patient with most minor physical contact and more accuracy [22], [23]; for the patient, it is an efficient and very precise and instant therapy [24], [25]. 5G and IOT (Internet of Things) have proliferated the use of IMDs [26], [27]. According to estimates, the global IMD market is valued at US115$billion; in2027, itisenvisagedtoreachUS$ 155 billion by 2027, as shown in Figure 2 [28]. Now that these devices have become an essential part of human lives, they must be used responsibly. Network connectivity of these devices makes them prone to security threats [29]. Former US Vice President Dick Cheney had disabled wireless connectivity of his IMD to avoid any danger [30]. Any security threat to these devices can be as lethal as a threat to human life in the worst case, mainly in the case of cardiac IMDs [31], [32], [33].

E-mail address: M.Aldalaien@psut.edu.jo, halbazar@arabou.edu.sa, habdeljaber@arabou.edu.sa

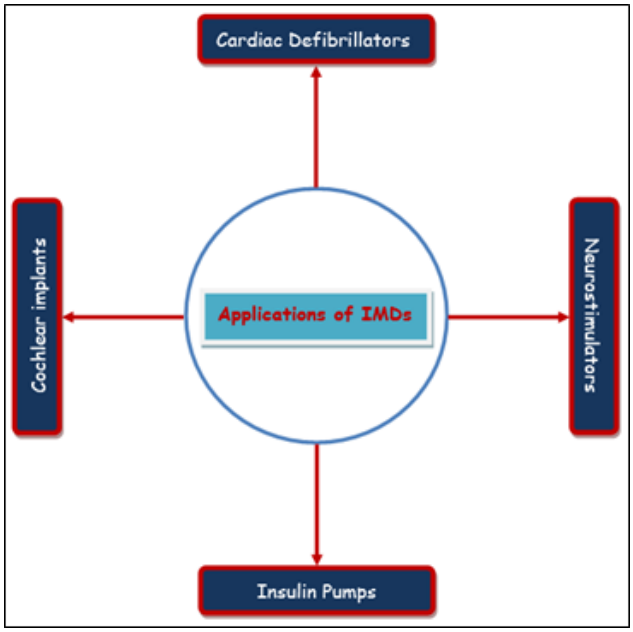

Figure 1. Common applications of IMDs

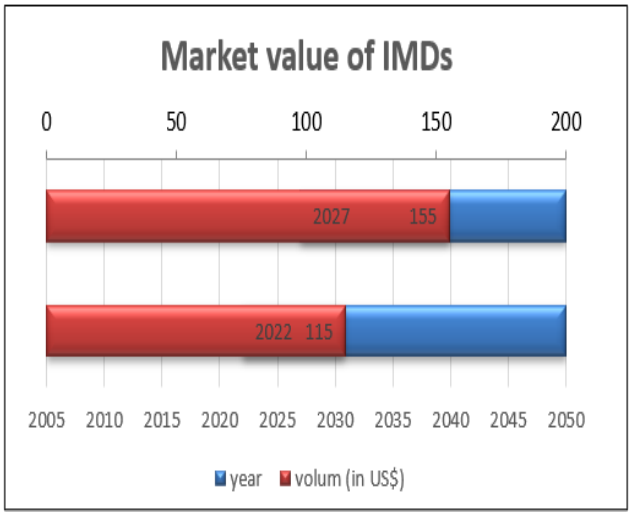

Figure 2. IMDs market in 2022 vs 2027

Researchers, on the other hand, continue to discover and overcome these security issues [34],][35]. There is also a handful of research on unearthing the security challenges [36], [37], [38]. These research pieces have also been reviewed by other researchers. On the other hand, many researchers have put efforts to combat these challenges [39], [40], [41]. So far, there needs to be more focus on reviewing the research that proposes solutions to these challenges. This survey paper focuses on reviewing these available solutions and looking at their shortcomings. Among the many possible solutions to IMD security, power-efficient solutions are the most viable ones, for the battery is the most precious resource in IMDs. The main focus of this research is to reveal the most power-efficient solutions. This paper is aimed at serving as a reference point for future research.

This paper aims to distinguish between power-efficient and non-power-efficient solutions for addressing the security challenges of Implantable Medical Devices and to provide valuable insights for researchers interested in this topic. Moreover, this paper's contributions include reviewing solutions that do not focus on power efficiency and those that emphasize power-efficient approaches to IMD security. Additionally, the paper compares these solutions, highlighting their respective advantages and shortcomings.

The rest of the paper is organized as section 2 provides a background of IMDs; section 3 discusses the security architecture of IMDs; in section 4, some common security threats to IMDs have been discussed; section 5 discusses the methodology of research; section 6 is the discussion section of the reviewed literature; section 7 provides the proposed solutions discussion and future work; research recommendations provided in section 8; section 9 concludes the paper.

2. Background

Several components are involved in working an IMD: the sensor, the stimulator, the wireless transceiver, memory, external devices, and the battery. It is also noteworthy that the sensor, transceiver, memory, battery, and stimulator are mostly part of a single chip, as shown in Figure 3. Their individual explanations are below.

1) **Sensor:** The sensor has to sense the physiological conditions of the specific body part (like sensing heartbeat in the case of a defibrillator) [42].
2) **Transceiver:** This wireless device sends the signals generated by the sensor and receives the signal sent to the chip from any external device. The process of sending and receiving these measurements is called telemetry [43].
3) **Memory:** A small amount of memory is also needed in IMDs to store the instructions for and from the sensor [44].
4) **Battery:** This is an intensive part of the IMD. It is needed to power the functioning of the IMD. Nowadays, wirelessly rechargeable batteries are being used the most.
5) **External devices:** Some external devices are also connected to the IMD. These external devices can include the patient's cellphone, the doctor's cellphone, and the programmer. The programmer is a computing device that the IMD communicates with most frequently. The IMD sends data to the programmer, and the doctor reads this data to take appropriate action.
6) **Stimulator/Actuator:** The IMD chip also includes a small stimulator. The purpose of a stimulator is to implement an action proposed by the doctor. For example, in the case of an insulin pump, increasing the insulin supply would be done using the stimulator.

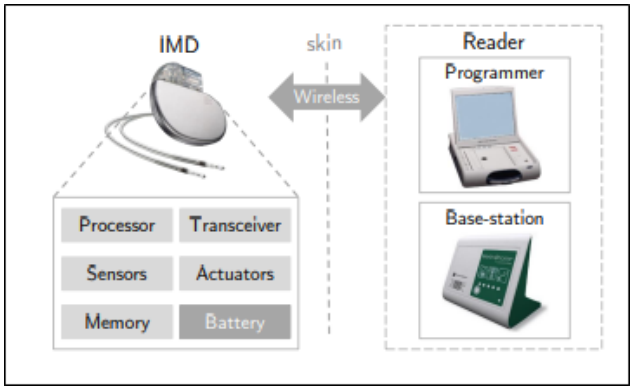

Figure 3. Working of IMDs [45].

3. Security Architecture of IMDs

Since IMDs are mostly attached to life-critical body parts, their security is of utmost importance [46]. Most IMDs today have multi-layer security approaches [47]. Some common security layers in IMDs are discussed below and shown in Figure 4.

1) **Authentication:** This process should ensure that an authorized person is accessing the IMD. This is usually ensured through a password or some biometric verification [48].
2) **Secure Communication:** Since IMD transmits very critical information through a wireless channel, it is necessary that the communication be secure. The communication is encrypted using different techniques [49], [50].
3) **Data Integrity:** The user's data should be stored in such a format that it must not be misused, forged, or stolen. An appropriate encryption technique like RSA should be applied to it.
4) **Securing the device physically:** It is also equally important that the IMD must be secured from any physical harm. This is ensured as part of human personal security.
5) **Updating the firmware:** The firmware of the IMD should be able to install the updates offered by the manufacturer.

4. Common Threats of IMDs

Some prevalent threats to IMDs are based on the security features that can be exploited. These vulnerabilities can be in the network or even in the IMD itself [51], [52]. Some of these threats are discussed as follows and shown in Table 1.

1) **Eavesdropping:** When an unauthorized person records the data communication between the IMD and programmer exploiting network vulnerability, it is called eavesdropping. It is generally overcome by employing some cryptographic technique [53].
2) **Unauthorized Access:** To operate the IMD, the authorized person (like a physician) proves identity by entering a password or another biometric authentication. If someone succeeds in manipulating the authentication process illegitimately, it is considered unauthorized access. This can even endanger the patient's life in the worst-case scenario [54].
3) **Battery Drain:** Some attacks aim at draining the battery of the IMD. These attacks have the adverse impact that the patient would have to undergo surgery (in most cases) or other hard medical procedures (in a few cases) to replace the battery. Thus, these attacks intend to harm the patient physically. Attacks like Denial-of-Service (DoS) are carried out to inflict this harm on the patient [55].
4) **Manipulating the Firmware:** Some attackers try to change the firmware settings of the IMD. This helps them take control of the device [41].
5) **Man-in-the-Middle:** An IMD can be easily exploited if another programmer is brought near it. It can communicate with any programmer with a similar configuration to the one it was initially connected to [56].
6) **Stealing Data:** Attackers can also succeed in stealing the data generated by the IMD. This data is generally stored in an IMD or on some hospital server. This type of attack typically occurs when no proper data encryption is in place.
7) **Malware:** Like every other modern device, the IMD is also at risk of malware attacks. Different types of malware, from viruses and spyware to trojans, are being injected into the IMDs. This malware can steal data from the IMD and tamper with it [38].
8) **Physical Attack:** An IMD can also face physical attacks. These attacks can include stealing the IMD, tampering with the IMD, or even damaging its parts (leads, circuits, etc.).

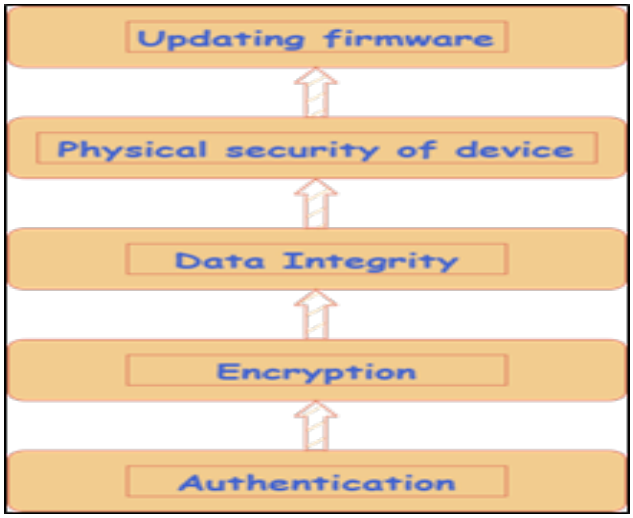

Figure 4. Security layers of IMDs

TABLE I. Security Threats vs Vulnerabilities of IMDs

Security Threat	Against Vulnerability
Eavesdropping	Network protocols
Unauthorized Access	Authentication
Battery Drain	Network and device security
Manipulating the Firmware	Penetrating through network and exploiting the device's inadaptability
Man-in-the-Middle	Network surveillance and channel vulnerabilities
Stealing Data	Data Integrity
Malware	Security loopholes in device
Physical Attack	Human body directly

5. Methodology

During this research, the primary sources consulted were MDPI [57], IEEE Xplore [58], ACM Digital Library [59], and Science Direct [60] as shown in Figure 5. Many keywords searched on Google Scholar search engine are 'zero-power solutions to IMDs,' 'Powerless security solutions to IMDs,' 'Enhancing the security of IMDs,' 'security-power trade-off in IMDs,' 'Zero-power security solutions to IOMTs,' 'power-efficient security solutions to IMD/Internet of Medical things.' These keywords are briefly presented in tabular form in Table 2. Many research studies were returned, among which were selected as the most relevant to real-world implementation. The methodology of this research is presenting a literature review of nonpower efficiency and power efficiency solutions for security problems in IMDs. This comprehensive literature review covers the advantages and disadvantages of these solutions. Moreover, The tools used for achieving the literature review of this research work are searching for recent research that has solved security problems in IMDs and critically analyzing the literature review. The techniques used for producing this literature review are searching for cutting-edge literature, checking cutting-edge literature, identifying relevant works, analyzing relevant works, and finally producing the literature review.

Literature has been reviewed in reverse chronological order, where the latest researches were prioritized the most. This is because that old research may not be compatible with and applicable to modern devices. All the relevant proposed solutions were reviewed for their advantages and shortcomings.

6. Literature Review

This section reviews the most important works regarding IMD security. The focus is on techniques that consider power efficiency, although some of the techniques do not, so a comparison can be drawn. Table 3 presents an overview of all the reviewed literature.

A. solutions with no focus on power-efficiency

I. Almazyad et al

Data security has been brought under experiment in this research. The authors have proposed three data transmission

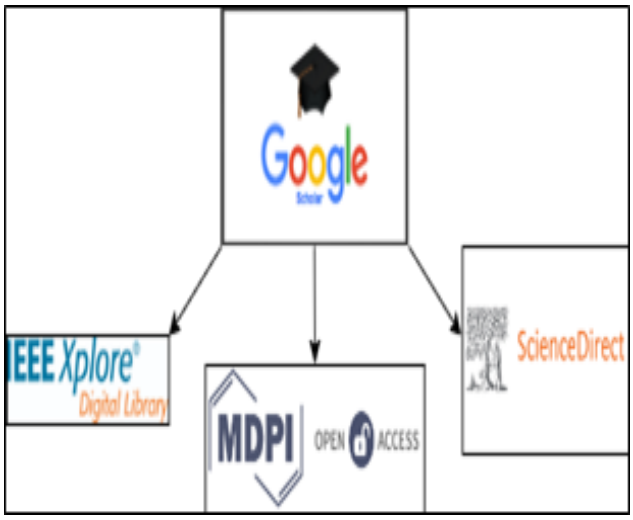

Figure 5. Main sources consulted for the research

modes for doctors from IMD. The modes are mode 0, mode 1, and mode 2, where mode 0 has the most critical data. The Adaptive Mode Selection (AMS) mechanism is proposed to select an appropriate mode for data transmission. A Priority-Queue-based (PQ-based) mechanism has been used to stop dangerous data from spreading to the rest of the system. The Adaptive Protocol Selection (APS) chooses a transmission mechanism. Experiments have shown that the three methods combined deliver very efficient performance while securing the data [61].

G. Zheng et al.

The authors of this research have drawn a comparison of two key generation techniques. The key generation considered here is based on electrocardiogram (ECG). The two cryptographic schemes under study are the fuzzy commitment and the fuzzy vault. Similarities and differences between the two techniques have been investigated. For doing so, for both the said techniques, an IMD has transmitted an ECG signal; it has been processed; ECC encoding has been done; key validation is carried out; and at last, key commitment and key revealing are performed. The performance of both techniques has been evaluated based

TABLE II. Keywords Searched

S. No	Keyword Searched
1	Zero-power solutions to IMDs
2	Powerless security solutions to IMDs
3	Enhancing security of IMDs
4	Security-power trade-off in IMDs
5	Zero-power security solutions to IOMTs
6	Power-efficient security solutions to IMD/ Internet of Medical things

on three parameters: temporal variance, False Acceptance Rate (FAR), and false rejection rate. Results show that FAR in the case of Fuzz Commitment is zero. Along with that, it also requires the least resources. Contrarily, fuzz vault has an acceptable false reject rate of 5% [62].

L. Pycrof et al.

The authors of this paper have proposed a theoretical framework for securing the IMD. A four-step course of action has been recommended for consideration while manufacturing an IMD. The first and foremost thing to be incorporated in IMD design is record keeping of all its activities, called 'auditing.' The second step in this direction is reporting any bug in the IMD. Another very important recommendation is to include multi-factor authentication in the IMD design. Last but not least, there is a dire need to increase IMD security awareness among manufacturers and clinicians [30].

M Zhang et al.

In this paper, the authors have uncovered some common security challenges in IMDs and proposed solutions. The first challenge they discussed was possible software or hardware failure, while standard solutions presented to it were a fault-tolerant design and formal verification of the device after manufacturing. A security attack discussed is the radio attack, which means an attack on the communication channel. Four solutions have been suggested for these attacks: various cryptographic solutions, low-range communication based on RFID, etc., deploying some external devices like a Security Guard and removing the battery constraints. Another threat to IMD arises from the malware. The possible solutions to these threats are a secure execution environment of applications and runtime monitoring, such as intrusion detection, which needs to be implemented. An intimidating security breach is a side-channel attack. System-level countermeasures have been proposed to combat it [63].

C. Li et al.

This part of the literature sought security bugs in an IMD and presented two-step defenses against these vulnerabilities. The authors experimented on glucose monitoring and insulin delivery pumps. The unearthed vulnerabilities include eavesdropping and tampering with the information stored on the IMD. The possible solutions presented are cryptographic protection and body-coupled communication. A rolling code mechanism has been used as part of cryptographic protection. Body-coupled communication needs the insulin meter to be very close to the patient's body. It can thwart any remote attack. Both combined have demonstrated that they can significantly secure an IMD against security threats [64].

F. Xu et al.

The proposed method in this research has been called IMDGuard. In the said model, an external wearable device called 'Guardian' has been deployed. This external device has been deployed to authenticate the IMD and the programmer based on the patient's ECG. The main aim of the Guardian is to utilize the randomness of the ECG. The randomness of the authentication would aid in overcoming the drawbacks of pre-shared, non-rewritable keys. In an emergency, the doctor must physically remove the Guardian from the patient. A mechanism has also been implemented in the proposed model to avoid spoofing. The authors have performed experiments on TelosB and TinyOS 2.1. Results show that the proposed model does not need additional hardware to run, making it very viable [65].

L. Wu et al.

[66] proposed for IMDs a proxy-based fine-grained access control scheme that can extend the age of IMDs by giving the proxy device heavy cryptographic calculations. Moreover, the fine-grained access control is enforced by using the ciphertext policy attribute-based encryption (CP-ABE). Thus, the IMDs can be accessed solely by authorized and/or qualified individuals. The implementation of the proposed scheme is conducted upon actual emulator devices.

M. Zhang et al.

[67] proposed protocols for IMD key exchange to offer a secured communication channel for IMD devices. In addition, the proposed IMD key exchange protocols benefit from an Out-Of-Band (OOB) channel like physiological, audio, and vibration signals. [67] Performed a deep analysis of the existing OOB depending on solutions for IMDs, and relying upon discoveries, a protocol for IMD key exchange, which contains a new class for OOB channels depending upon human bodily motions, is proposed. The prototypes have been implemented, and a user study with 24 participants has validated the designs.

B. Wan et al.

The study's goal in [68] is obtaining vision for every attribute as introduced in the IMDs value. In addition, they measure the strengths of attributes and identify their relative importance. Also, the determinants for stakeholders' favorites should be specified. The design of combined methods has been utilized to determine the attributes and levels that reflect the favorite of stakeholders in the direction of the IMDs value. The design mixed the consultation of experts, literature reviewing, pilot testing, and the interactions based one-on-one with stakeholders [68]. Six attributes, along with their levels, are specified, relying upon this design. These attributes are clinical effectiveness, safety, innovation, disease severity, implementation capacity, and cost. Thirty ideal selection sets have been developed from one hundred and forty-four hypothetical profiles. Moreover, patients and healthcare professionals, such as stakeholders in China, were surveyed. Professionals of healthcare include experts in health technology assessment, decision-makers, medical doctors, and hospital administrators. One hundred thirty-four respondents contributed to the survey. The results are analyzed by combining logit and conditional logit models. The combined logit model presented its results, which displayed that all attributes influence respondents' selections of IMDs. Furthermore, the respondents are ready to pay the highest cost for the medical devices in case they have enhancements in clinical safety, then raise clinical effectiveness, cure severe diseases using technology, enhanced implementation capacity, and the technology that is innovative with no alternatives [68].

DS Bhavani and K Venkata Raju

In this paper, the authors examine the security vulnerabilities of IMDs and propose a series of enhanced security protocols to address these issues. They emphasize the need for robust authentication mechanisms, such as lightweight cryptographic solutions like Elliptic Curve Cryptography (ECC), which can effectively safeguard sensitive patient data while maintaining low energy consumption [69]. These proposed solutions improve patient safety by preventing unauthorized access and protecting against data breaches, enhancing trust in using IMDs. The suggested protocols' lightweight nature makes them suitable for the resource-constrained environment of IMDs, ensuring that security measures do not compromise device performance. However, implementing these security protocols may face limitations due to IMDs' inherent resource constraints, which could impact their ability to support complex security mechanisms [69].

B. Power-efficient solutions

M. Prematilake et al.

In this research, a hardware and software-based security solution is adopted. The proposed method monitors the readings of the sensor and the IMD itself. The approach adopted offers a two-pronged security solution. First, a set of rules is established to classify safe and unsafe operations, and a rule-check mechanism is established to see if the rules are abided by. The rule-checking should be, in part, done during the development phase of the IMD, and the remaining rules set should be verified once the IMD becomes operational. The verification of rules runs in an independent environment so that the unsafe activity may not harm the device. The experiment was performed on an artificial pancreas. Results show that it has delivered very good performance where the verification delay in insulin pump was 253 ms, which is considered relatively low [70].

M. A. Siddiqi et al.

This research focuses on providing zero power immunity to IMDs against battery DoS attacks. Since the attacker can drain the battery of an IMD by generating frequent illicit authorization requests to the IMD, this drains the device's battery. The authors have developed a zero-power defense based on an energy harvesting model. A design model has been proposed that has to be applied to zero-power defenses in the context of IMDs. A survey of such existing systems has also been conducted. Finally, a security mechanism against battery-DoS attacks has been proposed [45].

N. Ellouze et al.

The authors of this piece of research have proposed a zero-power solution to IMD security. The primary contribution of this research is ECG-based key authentication, which has to be backed by the power harvested from the RFID system. The ECG-based key must be matched at IMD and the programmer for authorization. This research has specifically been aimed at Cardiac IMDs. In their approach, the first thing that the authors did was add extra hardware to the IMD. This additional hardware is called a Wireless Identification and Sensing Platform (WISP). The fundamental purpose of deploying WISP is to decode the ECG signal for mutual authentication. WISP does not come with extra power overhead. Instead, it uses the energy of RFID. An RFID reader and a set of cardiac sensors have been deployed on the programmer's part. Separate mechanisms are being proposed for regular situations as well as for emergency situations. In this way, it has been ensured that there is no unauthorized access to the IMD. Besides that, the proposed solution is also defiant to other attacks, such as replay or desynchronization [71].

W. Choi et al.

An energy-efficient key exchange solution has been proposed in this research. The key is generated using inter-pulse intervals. In the proposed solution, the heartbeat rate is measured at IMD and the programmer; then, this measured inter-pulse interval is adjusted using an error correction code as part of self-recovery. At the end of IMD, there is no need to add communication overhead for error correction. To verify the proposed model. The authors have conducted experiments on the ECG signals dataset named PhysioBank [72]. For security analysis, the Secure Sketch mechanism was used [73]. The proposed model was proven to satisfy many security parameters like entropy. Further, the energy that this model required for transmitting a single bit was 3.79 mJ while receiving a single bit required 1.83 mJ [74].

M. Yasin et al.
The authors of this research have combined two separately proposed solutions. The two separately proposed solutions are security solutions and overcoming power issues. This study proposes a power-efficient secure mechanism for predicting ventricular arrhythmia almost three hours before the attack. On the aspect of prediction, the Naïve Bayes classifier has been used. The prediction has achieved an accuracy of 86%. An ECG-based random key extraction technique has been employed on the security side. It has a multi-layer security approach. Overall, the proposed chip consumes 62.2% less power and occupies 16% less space [75].

Y. Kim et al.
The authors have sought to establish a secure communication channel and a viable key exchange model in this research. The proposed channel is a vibration-based side channel and key exchange mechanism called SecureVibe. The advantage of a vibration-based system is its short range and ease of perceptibility to the host. For exchanging (AES) keys with a faster bitrate, the On-Off Keying (OOK) demodulation scheme was used. These techniques combined (especially vibration-based channels) make the communication power-efficient and resistant to any battery drain attack. Key exchange only ensures authorized connection establishment, while a vibration-based channel awakens the host-patient against infiltration. For carrying the experiment, nRF51822 RF SoC IMD was used; a Nexus 5 smartphone was used as an external device [76].

Q. Yang et al.
A promising zero-power solution has been proposed by Q. Yang et al. This study proposes a practical implementation of a zero-power authentication mechanism. According to the proposed scheme, a security guard device facilitates communication between the IMD and the programmer. The security guard device gets power wirelessly from the programmer. The primary function of the security guard device is to authenticate the device that is accessing the IMD. Amplitude shift keying with pulse width modulation (ASK-PWM) is used for data encoding. This ensures low power consumption. For security, the SHA-1 algorithm is used. Experiments have shown that the system transmitted data with a speed of 500Kbps [77].

T. Xu et al.
The authors have proposed a physical unclonable functions (PUFs) based approach in this research. PUFs work on complex, unpredictable mathematical functions. This research uses two PUF-based circuits; one is to be deployed inside the patient's body integrated with the IMD, while the other is deployed externally with the programmer. Input-output mapping of both PUFs is performed for authentication purposes. The ultra-low power consumption of these PUFs gives an edge to this model over many other proposed hardware-based models [78].

M. Zhang et al.
A wireless channel monitoring and detection of malicious traffic strategy has been proposed in this research. According to the authors, the existing security solutions for IMDs are power-expensive. They have proposed a general security framework called MedMon (Medical security monitor). MedMon can be a dedicated device or embedded into an existing device like a smartphone. The device would monitor all the data packet exchanges between the IMD and the programmer. It has a multi-layered approach to detecting anomalous traffic. It has two-stage mechanisms for responding to the attack: the first is passive, where the patient is notified of malicious activity; in the second stage, MedMon blocks the wannabe. Anomalies have been classified into two classes: physical anomaly and behavioral anomaly. The authors have experimented with glucose monitoring and insulin delivery IMD [79].

D. Halperin et al.
In this research, the authors have first exploited a few vulnerabilities in IMDs and then proposed defenses to these loopholes. The vulnerabilities they have found include intercepting communication and inferring critical personal information of the patient and therapeutic information. Further, the authors have exploited the issue of unauthorized access to the IMD by an external device. This can change commands stored on the IMD, disordering the therapy. Besides that, it would also eat up the battery. To counter these loopholes, the authors have proposed a three-faceted security model: first, the patient is notified about suspicious activity, then a symmetric cryptographic technique is used to stop unauthorized access, and last, the patient physically facilitates key exchange. The noteworthy feature of the proposed security model is that it is a zero-power defense, which means it does not further power. The experiment was performed on the "Medtronic Maximo DR VVEDDDR (7278)" model cardiac defibrillator [31].

S Duttagupta et al.
In this paper, the authors identified security challenges in IMDs and proposed a Hash-based Access Token (HAT), a practical solution for key establishment in IMDs. The HAT system shifts access control to an external device, such as a smartphone, which acts as a Key Distribution Center (KDC). This external device issues hash-based access tokens that personal devices use to establish secure communication channels with the IMD. The approach enables dynamic and fine-grained access control, allowing the patient to manage which devices can connect to the IMD and revoke or delegate access when necessary [80]. This solution's advantages include minimal energy and memory overhead, making it suitable for resource-constrained IMDs. It also provides robust security by preventing unauthorized access through cryptographic token-based authentication. Additionally, HAT supports flexible access management, allowing personal devices to be updated or revoked dynamically, enhancing usability in real-life scenarios. However, the system relies on an external device, introducing a single

point of failure. If the external device is lost, compromised, or unavailable, access to the IMD may be disrupted, although backup mechanisms like QR codes can mitigate this risk. Furthermore, frequent session key renewals may impose some energy demands on the IMD over long-term use [80].

N Karimian, et al.
This paper proposes an ECG-based key generation scheme and a blockchain-based authentication protocol for securing IMDs. The key is generated from a single heartbeat using fiducial features like amplitude and time differences between ECG peaks. This approach drastically reduces the key generation time to about one second, a significant improvement compared to previous methods that required around 30 seconds [81]. The advantages of this system include efficient key generation, improved randomness as verified by statistical tests, and secure communication through dynamic key updates. The proposed blockchain-based authentication protocol also allows secure interactions between patients and healthcare providers in various scenarios, including emergencies, without requiring physical proximity. However, this system's limitation is its reliance on a private blockchain for doctor and device programmer communication. It could introduce complexity in managing and maintaining access control in large-scale deployments [81].

A Almukhlifi and SM Almutairi
In this paper, the authors propose an efficient palm vein authentication encryption technique for wireless IMDs. The system leverages a combination of palm vein authentication and zero-watermarking to generate encrypted credential data for IMDs. This ensures secure access control, particularly in emergencies where the patient may be unconscious. The proposed scheme enhances the security of IMDs while balancing accessibility needs during emergencies. Key advantages include improved image quality, efficiency, and lower computational cost, as quantitative assessments such as PSNR, SSIM, and MSE demonstrate. These metrics highlight the scheme's superior performance compared to existing methods. However, computational complexity in some prior approaches remains a challenge, which the authors aim to address in future work using techniques like Fourier transforms and deep learning-based encryption [82].

S Maji's
Saurav Maji's thesis focuses on developing energy-efficient security solutions specifically for IMDs within next-generation embedded systems and the Internet of Things (IoT), addressing the growing security vulnerabilities in resource-constrained environments [83]. The research introduces a dual-factor authentication system that enhances the security of medical devices by integrating human responses with cryptographic measures. This solution prioritizes low resource overhead, making it suitable for devices with limited power and area budgets. While the approach shows promise, challenges such as potential difficulties in extremely low-power scenarios and complexities in implementation must be considered. Overall, Maji's work contributes significantly to embedded systems security by providing innovative and efficient solutions tailored to implantable medical devices' unique challenges [83].

7. Discussion and Future Work

Looking at the proposed solutions, Table 4 shows some results regarding the security of IMDs.

Most of the literature proposes solutions based on the following techniques, summarized in the trailing table.

- ECG-based key generation
- Data protection at the device's end
- Cryptographic techniques
- Traffic monitoring
- Strengthening authorization mechanisms
- External hardware-based solutions

In summarizing the reviewed literature, two fundamental issues in IMD security are unencrypted data communication and weak authentication mechanisms. The majority of the security issues in these devices stem from these two aspects, so research must focus on these issues.

In addition, in the current research arena, most experiments have been performed on simulators and emulators, which don't wholly cover the issues raised in real-world scenarios. Significant differences can often exist between the ideal environment provided by emulators and simulators vis-à-vis real-world scenarios. Therefore, the focus must be on performing experiments using real environments.

On the security enhancement side, most researchers tend to propose solutions based on biometric mechanisms like ECG, etc. One reason for doing so is the real and natural randomness of the biometric processes. This is very helpful in stopping the big issue of decoding the patterns in artificial random number generators.

While a handful of research has been reviewed, looking at the proposed solutions, there are many possible solutions. Zero-power authentication sounds like the best and most viable approach. But it needs further improvements in the future. If achieved in its true letter and spirit, over half of the IMD security issues can be resolved. So, there is a dire need to focus on it in academia and industry.

The implications of the research findings are provided as follows: leftmargin=2em

- The overheads for power and computations have increased.
- The cost of computations and hardware has increased.

- Some previous works, such as eavesdropping, data integrity, etc., do not consider some features.
- Some relevant works are used for specific IMDs such as cardiac IMDs, ventricular arrhythmia, or any other IMD.
- Some works do not consider the design and the issues of resources for IMDs.
- Some solutions to security problems for IMDs require more hardware.
- The difficulty of IMD circuits should be considered.

The significance of the research findings is presented as follows:

- IMDs are employed to monitor vital functions in the human body, such as the level of blood pressure and the rate of heartbeat.
- IMDs provide indications to doctors about the patient's health.
- Addressing the security problems of IMDs can help in offering better treatment for patients and reduce the risk of life-threatening situations.

The limitations of this research suggest several areas for future work. There is a need to explore more solutions to reduce the costs associated with computations, hardware, and power consumption in IMDs. Additionally, future studies should focus on developing more comprehensive approaches that address key security characteristics, such as eavesdropping and data integrity, which have been overlooked in some existing works. Furthermore, identifying and presenting a broader range of potential threats to IMDs will enhance their security and ensure better patient protection.

TABLE III. An overview of the literature review

Paper	Advantages	Shortcomings
M. Prematilake et al. (2021)	Classifying safe and unsafe activities	Increasing computational and power overhead
I. Almazyad et al. (Sep 2020)	Secure data	Increased computational cost
M. A. Siddiqi et al. (Apr 2019)	Zero-power defense against battery-DoS attacks	Does not consider other aspects like data integrity and eavesdropping, etc.
G. Zheng et al. (Feb 2019)	Ensuring real randomness in key generation	Applicable to defibrillators only
N. Ellouze et al. (2018)	Powerless and biometric authentication mechanism introduced	Besides extra hardware overhead, it is limited in scope where the solution is valid only for Cardiac IMDs and not for IMDs without ECG signals
L. Pycrof et al. (2018)	Theoretically very viable recommendations	Do not consider the design and resource issues of the IMD
W. Choi et al. (2018)	Energy-aware secure key exchange for secure data transmission	The IMD and programmer must be able to measure the ECG
M. Yasin et al. (2017)	Trade-off of energy efficiency and security enhancement	Very limited in scope as it can be applied to ventricular arrhythmia only
Y. Kim et al. (Jun 2015)	Secured communication and power-efficient	Tested on a model rather than in real environment
Q. Yang et al. (2014)	Zero-power authentication and real implementation on chip	Needs a security guard device
T. Xu et al. (2014)	Unpredictable output function is used as well as ultra-low power is needed	Additional hardware is needed
M. Zhang et al. (2013)	Embedding security solution into the existing system with zero power overhead	Rigorous monitoring of the traffic entails a lot of computational complexities
M. Zhang et al. (2013)	A comprehensive survey of common threats faced by IMDs	Solutions do not consider the complexities of IMD circuit
F. Xu et al. (2011)	Authentication based on ECG with no additional hardware overhead	Applicable only to Cardiac IMDs
C. Li et al. (2009)	Unearthing security vulnerabilities and demonstrating effectiveness of cryptographic and body-coupled communication	These techniques, especially the cryptographic technique, may increase power overhead and may not apply to every IMD
D. Halperin et al. (2008)	Zero-power defense against interception and unauthorized access	Does not consider data integrity breach, and the experiment was performed on a single ICD
S Duttagupta et al. (2023)	Low energy and memory overhead, ensures robust security with cryptographic token-based authentication and supports flexible access management	he system relies on an external device, introducing a single point of failure, frequent session key renewals may increase the IMD's energy demands over time

TABLE III. (Continued)

Paper	Advantages	Shortcomings
N Karimian, et al. (2023)	Efficient key generation, improved randomness as verified by statistical tests and secure communication through dynamic key updates	Its reliance on a private blockchain for doctor and device programmer communication may complicate access control management in large-scale deployments
L. Wu et al. (2024)	Reduced power consumption and computational overhead	Decryption takes the longest time, but both encryption and decryption times are acceptable
M. Zhang et al. (2024)	The IMD key exchange can be done using bodily motion	IMD patients were excluded from the experiments due to institutional ethical restrictions
B. Wan et al. (2024)	The study's attributes significantly shape respondents' choices for IMDs. Respondents are willing to invest in high-cost devices if they improve clinical safety, effectiveness, and access to medications for severe conditions through innovative technology without requiring replacements.	The conclusion may not reflect the broader population, as respondents had specific criteria, and the questionnaire contained professional jargon unfamiliar to the general public, limiting accessibility to educated patients. The study focused on patients from a tertiary medical center in China, excluding local doctors, which may restrict the findings' applicability. HTA experts recommended incorporating incidence rates to better capture the impact of medical devices. Since patients are key stakeholders, they must understand the study's attributes; thus, the definition of disease incidence was simplified for clarity.

TABLE IV. Generalization of security techniques used

Technique	Pros	Cons
ECG-based key generation	Enhanced security	Applicable only for cardiac implants
Data protection on the end of the device	Secures the device from spreading malicious data	is Computationally costly and complex in design
Cryptographic techniques	secure communication	are Not well-suited for the special usage model of IMDs due to extreme power and size issues
Traffic Monitoring	Anomaly detection becomes easier	Continuous monitoring of traffic is required
Strengthening authorization mechanism	Protects the device from unauthorized access and unwanted changes	Increases overheads
External Hardware-based solutions	avert the danger of malicious intrusion	Often increase the size of IMD or require an additional device to be implanted

Wireless charging is seen as a panacea for IMDs' security problems. It would free them from the never-ending problem of invasive battery drainage. Recharging the battery would not require critical measures like surgery. So, the focus must be shifted toward wireless charging of IMDs.

8. Recommendations

As technology always has room for improvement, some recommendations can be made as a future direction for research in IMD security.

- While conducting experiments in the field, the discovered or proposed solutions should not introduce significant computational complexity.
- Recommended solutions must be tested under real conditions in actual devices to avoid drawbacks associated with tests conducted under ideal conditions (e.g., emulators and simulators).
- A more holistic system is preferable; it should cover multiple aspects (such as data integrity and secure communication) and apply to various devices (like defibrillators and insulin pumps). Focusing on one aspect may compromise others.
- The device's size is crucial, as many IMDs are implanted in critical body parts; increases in size can be unaffordable.
- Weak authentication mechanisms are significant vulnerabilities in IMDs, making developing models that address these issues essential. Biometric random number generators may serve as a viable solution.
- Low-cost and low-energy solutions should be developed to be incorporated into existing devices, allowing them to operate according to a new algorithm after a simple firmware upgrade. Item While external devices can enhance the functionality of internally implanted devices, they may only sometimes be practical, especially for patients with limited mobility.
- The real technical capabilities of patients and programmers must be considered during innovation. They may not be familiar with medical terminologies and measurements, such as decoding ECG reports; hence, the system should not assume non-technical users possess this knowledge.
- Data within the IMD or connected devices may be secure, but interception during communication is a concern; therefore, data transmission must be secure.

9. Conclusion

IMDs are on the boom for so many reasons; they offer remote monitoring, instant therapy, and the least physical contact. It can be very helpful in specific attacks like cardiac arrest that aren't very easy for a doctor. Nevertheless, IMDs also pose many challenges. Among these challenges, security issues are at the top. Researchers continue to combat these issues. Because of the small size and complex design of IMDs, every proposed solution may not be practically feasible for these devices. Only those solutions that consider these constraints of the IMDs are more feasible. These constraints make batteries the scarcest resource. This paper is an effort to combine power-efficient solutions to the security of IMDs. These solutions have also been compared with other non-power-based solutions. This paper would serve as a reference for future research on battery-efficient solutions.

Acknowledgment

The authors extend their appreciation to the Arab Open University for funding this work through AOU research fund No. (AOURG-2023-011).

References

[1] K. B. Abdulazizovna, Q. D. Abdunabiyvna *et al.*, "Information technologies as a step to the development of society," *INTERNATIONAL JOURNAL OF RESEARCH IN COMMERCE, IT, ENGINEERING AND SOCIAL SCIENCES ISSN: 2349-7793 Impact Factor: 6.876*, vol. 16, no. 3, pp. 73–77, 2022.

[2] S. Pink, M. Berg, D. Lupton, and M. Ruckenstein, *Everyday automation: Experiencing and anticipating emerging technologies*. Taylor & Francis, 2022.

[3] A. Sixsmith, B. R. Horst, D. Simeonov, and A. Mihailidis, "Older people's use of digital technology during the covid-19 pandemic," *Bulletin of Science, Technology & Society*, vol. 42, no. 1-2, pp. 19–24, 2022.

[4] M. A. Sezal and F. Giumelli, "Technology transfer and defence sector dynamics: the case of the netherlands," *European Security*, vol. 31, no. 4, pp. 558–575, 2022.

[5] Y. A. Ali, "The role of quantitative techniques and devices in military geography: Political geography study," *QALAAI ZANIST JOURNAL*, vol. 7, no. 2, pp. 869–895, 2022.

[6] J. N. Njoku, C. I. Nwakanma, G. C. Amaizu, and D.-S. Kim, "Prospects and challenges of metaverse application in data-driven intelligent transportation systems," *IET Intelligent Transport Systems*, vol. 17, no. 1, pp. 1–21, 2023.

[7] D. K. Shah, R. Singh, A. Gehlot, S. Khantwal, A. J. Ahmad, and S. V. Akram, "Smart kitchen: real time monitoring of kitchen through iot," in *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*. IEEE, 2022, pp. 718–722.

[8] K. Graf, "Cooking with (out) others? changing kitchen technologies and family values in marrakech," *The Journal of North African Studies*, vol. 29, no. 4, pp. 575–600, 2024.

[9] M. Attaran, "Blockchain technology in healthcare: Challenges and opportunities," *International Journal of Healthcare Management*, vol. 15, no. 1, pp. 70–83, 2022.

[10] E. Mbunge, J. Batani, G. Gaobotse, and B. Muchemwa, "Virtual healthcare services and digital health technologies deployed during coronavirus disease 2019 (covid-19) pandemic in south africa: a systematic review," *Global health journal*, vol. 6, no. 2, pp. 102–113, 2022.

[11] D. Elangovan, C. S. Long, F. S. Bakrin, C. S. Tan, K. W. Goh, S. F. Yeoh, M. J. Loy, Z. Hussain, K. S. Lee, A. C. Idris *et al.*, "The use of blockchain technology in the health care sector: systematic review," *JMIR medical informatics*, vol. 10, no. 1, p. e17278, 2022.

[12] K. Batko and A. Ślezak, "The use of big data analytics in healthcare," *Journal of big Data*, vol. 9, no. 1, p. 3, 2022.

[13] D. Kumar Gupta, M. H. Ali, A. Ali, P. Jain, M. K. Anwer, Z. Iqbal, and M. A. Mirza, "3d printing technology in healthcare: applications, regulatory understanding, ip repository and clinical trial status," *Journal of Drug Targeting*, vol. 30, no. 2, pp. 131–150, 2022.

[14] S. J. Adams, B. Burbridge, L. Chatterson, P. Babyn, and I. Mendez, "A telerobotic ultrasound clinic model of ultrasound service delivery to improve access to imaging in rural and remote communities," *Journal of the American College of Radiology*, vol. 19, no. 1, pp. 162–171, 2022.

[15] K. R. De Guzman, C. L. Snoswell, M. L. Taylor, L. C. Gray, and L. J. Caffery, "Economic evaluations of remote patient monitoring for chronic disease: a systematic review," *Value in Health*, vol. 25, no. 6, pp. 897–913, 2022.

[16] K. Bouabida, K. Malas, A. Talbot, M.-È. Desrosiers, F. Lavoie, B. Lebouché, N. Taghizadeh, L. Normandin, C. Vialaron, O. Fortin *et al.*, "Healthcare professional perspectives on the use of remote patient-monitoring platforms during the covid-19 pandemic: a cross-sectional study," *Journal of Personalized Medicine*, vol. 12, no. 4, p. 529, 2022.

[17] J. Zhang, R. Das, J. Zhao, N. Mirzai, J. Mercer, and H. Heidari, "Battery-free and wireless technologies for cardiovascular implantable medical devices," *Advanced Materials Technologies*, vol. 7, no. 6, p. 2101086, 2022.

[18] C. Billings and D. E. Anderson, "Role of implantable drug delivery devices with dual platform capabilities in the prevention and treatment of bacterial osteomyelitis," *Bioengineering*, vol. 9, no. 2, p. 65, 2022.

[19] B. Turner, S. Ramesh, S. Menegatti, and M. Daniele, "Resorbable elastomers for implantable medical devices: highlights and applications," *Polymer International*, vol. 71, no. 5, pp. 552–561, 2022.

[20] A. Degada and H. Thapliyal, "2-phase adiabatic logic for low-energy and cpa-resistant implantable medical devices," *IEEE Transactions on Consumer Electronics*, vol. 68, no. 1, pp. 47–56, 2022.

[21] D. S. S. Dutta. (2022, June 30) Insight into implantable medical devices. [Online]. Available: https://www.news-medical.net/health/Insight-into-Implantable-Medical-Devices.aspx. [Accessed: Apr. 7, 2023]. [Online]. Available: https://www.news-medical.net/health/Insight-into-Implantable-Medical-Devices.aspx

[22] C. Daley, A. Coupe, T. Allmandinger, J. Shirazi, S. Wagner, M. Drouin, R. Ahmed, T. Toscos, and M. Mirro, "Clinician use of data elements from cardiovascular implantable electronic devices in clinical practice," *Cardiovascular Digital Health Journal*, vol. 4, no. 1, pp. 29–38, 2023.

[23] S. Simovic, R. Providencia, S. Barra, B. Kircanski, J. M. Guerra, G. Conte, D. Duncker, E. Marijon, A. Anic, and S. Boveda, "The use of remote monitoring of cardiac implantable devices during the covid-19 pandemic: an ehra physician survey," *EP Europace*, vol. 24, no. 3, pp. 473–480, 2022.

[24] M. O. Ahmad and S. T. Siddiqui, "The internet of things for healthcare: benefits, applications, challenges, use cases and future directions," in *Advances in Data and Information Sciences: Proceedings of ICDIS 2021*. Springer, 2022, pp. 527–537.

[25] L.-N. Ghilencea, M.-R. Chiru, M. Stolcova, G. Spiridon, L.-M. Manea, A.-M. A. Stănescu, A. Bokhari, I. D. Kilic, G. G. Secco, N. Foin *et al.*, "Telemedicine: benefits for cardiovascular patients in the covid-19 era," *Frontiers in cardiovascular medicine*, vol. 9, p. 868635, 2022.

[26] S. Singh, S. K. Chowdhary, S. Rawat, and B. M. Acharya, "5g revolution transforming the delivery in healthcare," in *Ambient Intelligence in Health Care: Proceedings of ICAIHC 2022*. Springer, 2022, pp. 179–188.

[27] M. K. Hasan, T. M. Ghazal, R. A. Saeed, B. Pandey, H. Gohel, A. Eshmawi, S. Abdel-Khalek, and H. M. Alkhassawneh, "A review on security threats, vulnerabilities, and counter measures of 5g enabled internet-of-medical-things," *IET communications*, vol. 16, no. 5, pp. 421–432, 2022.

[28] Fact.MR. (2022) Increasing demand for implanted medical devices. [Online]. Available: https://www.factmr.com/report/implantable-medical-devices-market. [Accessed: Apr. 10, 2023]. [Online]. Available: https://www.factmr.com/report/implantable-medical-devices-market

[29] M. A. Siddiqi, A.-A. Tsintzira, G. Digkas, M. G. Siavvas, and C. Strydis, "Adding security to implantable medical devices: Can we afford it?" in *EWSN*, 2021, pp. 67–78.

[30] L. Pycroft and T. Z. Aziz, "Security of implantable medical devices with wireless connections: The dangers of cyber-attacks," *Expert Review of Medical Devices*, vol. 15, no. 6, pp. 403–406, 2018.

[31] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *2008 IEEE Symposium on Security and Privacy (sp 2008)*. IEEE, 2008, pp. 129–142.

[32] R. J. (2012) Hacker shows off lethal attack by controlling wireless medical device. [Online]. Available: http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off lethal-attack-by-controlling-wireless-medical-device/. [Accessed: Apr. 11, 2023]. [Online]. Available: http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off\protect\let\reserved@d=[\def{\@@par}

[33] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems, and B. Preneel, "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*, 2016, pp. 226–236.

[34] R. Karthick, R. Ramkumar, M. Akram, and M. V. Kumar, "Overcome the challenges in bio-medical instruments using iot–a review," *Materials Today: Proceedings*, vol. 45, pp. 1614–1619, 2021.

[35] R. Somasundaram and M. Thirugnanam, "Review of security challenges in healthcare internet of things," *Wireless Networks*, vol. 27, no. 8, pp. 5503–5509, 2021.

[36] V. Hassija, V. Chamola, B. C. Bajpai, S. Zeadally *et al.*, "Security issues in implantable medical devices: Fact or fiction?" *Sustainable Cities and Society*, vol. 66, p. 102552, 2021.

[37] A. Longras, H. Oliveira, and S. Paiva, "Security vulnerabilities on implantable medical devices," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*. IEEE, 2020, pp. 1–4.

[38] J. Beavers and S. Pournouri, "Recent cyber attacks and vulnerabilities in medical devices and healthcare institutions," *Blockchain and clinical trial: Securing patient data*, pp. 249–267, 2019.

[39] M. A. Siddiqi, R. H. Beurskens, P. Kruizinga, C. I. De Zeeuw, and C. Strydis, "Securing implantable medical devices using ultrasound waves," *IEEE Access*, vol. 9, pp. 80 170–80 182, 2021.

[40] D.-W. Kim, J.-Y. Choi, and K.-H. Han, "Medical device safety management using cybersecurity risk analysis," *IEEE Access*, vol. 8, pp. 115 370–115 382, 2020.

[41] C. Easttom and N. Mei, "Mitigating implanted medical device cybersecurity risks," in *2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*. IEEE, 2019, pp. 0145–0148.

[42] K. H. John and X. J. Zhang, *Chapter 7 - Implantable Sensors*. ScienceDirect, 2014, pp. 415–465.

[43] B. D. Nelson, S. S. Karipott, Y. Wang, and K. G. Ong, "Wireless technologies for implantable devices," *Sensors*, vol. 20, no. 16, p. 4604, 2020.

[44] Y. Kim, W. Lee, A. Raghunathan, V. Raghunathan, and N. K. Jha, "Reliability and security of implantable and wearable medical devices," in *implantable biomedical microsystems*. Elsevier, 2015, pp. 167–199.

[45] M. A. Siddiqi and C. Strydis, "Towards realistic battery-dos protection of implantable medical devices," in *Proceedings of the 16th ACM international conference on computing frontiers*, 2019, pp. 42–49.

[46] D. Healthcare. (2023) Implantable medical device. [Online]. Available: https://www.definitivehc.com/resources/glossary/implantable-medical-devices. [Accessed: Apr. 12, 2023]. [Online]. Available: https://www.definitivehc.com/resources/glossary/implantable-medical-devices

[47] H. Rathore, C. Fu, A. Mohamed, A. Al-Ali, X. Du, M. Guizani, and Z. Yu, "Multi-layer security scheme for implantable medical devices," *Neural Computing and Applications*, vol. 32, pp. 4347–4360, 2020.

[48] S. Challa, M. Wazid, A. K. Das, and M. K. Khan, "Authentication protocols for implantable medical devices: Taxonomy, analysis and future directions," *IEEE Consumer Electronics Magazine*, vol. 7, no. 1, pp. 57–65, 2017.

[49] L. Bu, M. G. Karpovsky, and M. A. Kinsy, "Bulwark: Securing implantable medical devices communication channels," *Computers & Security*, vol. 86, pp. 498–511, 2019.

[50] F. Hu, Q. Hao, and M. Lukowiak, "Implantable medical device communication security: pattern vs. signal encryption," in *2nd USENIX Workshop on Health Security and Privacy (HealthSec 11)*, 2011.

[51] T. Yaqoob, H. Abbas, and M. Atiquzzaman, "Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—a review," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 4, pp. 3723–3768, 2019.

[52] B. Alexander, S. Haseeb, and A. Baranchuk, "Are implanted electronic devices hackable?" *Trends in cardiovascular medicine*, vol. 29, no. 8, pp. 476–480, 2019.

[53] M. F. Awan and K. Kansanen, "Estimating eavesdropping risk for next generation implants," in *Advances in Body Area Networks I: Post-Conference Proceedings of BodyNets 2017*. Springer, 2019, pp. 387–398.

[54] V. H. Tutari, B. Das, and D. R. Chowdhury, "A continuous role-based authentication scheme and data transmission protocol for implantable medical devices," in *2019 Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*. IEEE, 2019, pp. 1–6.

[55] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, Q. Mohammad, and S. Alrabaee, "Security vulnerabilities detected in medical devices," in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*. IEEE, 2020, pp. 1–6.

[56] M. M. U. Rehman, H. Z. U. Rehman, and Z. H. Khan, "Cyber-attacks on medical implants: A case study of cardiac pacemaker vulnerability," *International Journal of Computing and Digital Systems*, vol. 9, no. 6, pp. 1229–1235, 2020.

[57] MDPI Open Access Journals. (2023, May 1) MDPI Open Access Journals. [Online]. Available: https://www.mdpi.com/. [Accessed: May 1, 2023]. [Online]. Available: https://www.mdpi.com/

[58] IEEE Xplore. (2023, May 1) IEEE Xplore. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp. [Accessed: May 1, 2023]. [Online]. Available: https://ieeexplore.ieee.org/Xplore/home.jsp

[59] ACM Digital Library. (2023, May 1) ACM Digital Library. [Online]. Available: https://www.acm.org/. [Accessed: May 1, 2023]. [Online]. Available: https://www.acm.org/

[60] Science Direct. (2023, May 1) Science Direct. [Online]. Available: https://www.sciencedirect.com/. [Accessed: May 1, 2023]. [Online]. Available: https://www.sciencedirect.com/

[61] I. Almazyad, A. Rao, and J. Rozenblit, "A framework for secure data management for medical devices," in *2020 Spring Simulation Conference (SpringSim)*. IEEE, 2020, pp. 1–12.

[62] G. Zheng, R. Shankaran, W. Yang, C. Valli, L. Qiao, M. A. Orgun, and S. C. Mukhopadhyay, "A critical analysis of ecg-based key distribution for securing wearable and implantable medical devices," *IEEE Sensors Journal*, vol. 19, no. 3, pp. 1186–1198, 2018.

[63] M. Zhang, A. Raghunathan, and N. K. Jha, "Towards trustworthy medical devices and body area networks," in *Proceedings of the 50th Annual Design Automation Conference*, 2013, pp. 1–6.

[64] C. Li, A. Raghunathan, and N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," in *2011 IEEE 13th international conference on e-health networking, applications and services*. IEEE, 2011, pp. 150–156.

[65] F. Xu, Z. Qin, C. C. Tan, B. Wang, and Q. Li, "Imdguard: Securing

implantable medical devices with the external wearable guardian," in *2011 Proceedings IEEE INFOCOM*. IEEE, 2011, pp. 1862–1870.

[66] L. Wu and J. Du, "Designing novel proxy-based access control scheme for implantable medical devices," *Computer Standards & Interfaces*, vol. 87, p. 103754, 2024.

[67] M. Zhang, E. Marin, M. Ryan, V. Kostakos, T. Murray, B. Tag, and D. Oswald, "Oobkey: Key exchange with implantable medical devices using out-of-band channels," in *Proceedings of the 19th International Conference on Availability, Reliability and Security*, 2024, pp. 1–13.

[68] B. Wan, J. Shen, J. Chen, L. Weng, P. Zhao, Y. Deng, L. Zhang, F. Zhang, Y. Wang, X. Li *et al.*, "Quantifying stakeholders' preference for implantable medical devices in china: a discrete choice experiment," *International Journal of Technology Assessment in Health Care*, vol. 40, no. 1, p. e8, 2024.

[69] D. Bhavani and K. Venkata Raju, "A panoptic of vulnerabilities in implantable medical devices," in *4th International Conference on Communication & Information Processing (ICCIP)*, 2022.

[70] M. Prematilake, Y. Kim, V. Raghunathan, A. Raghunathan, and N. K. Jha, "Hw/sw framework for improving the safety of implantable and wearable medical devices," *arXiv preprint arXiv:2103.01781*, 2021.

[71] N. Ellouze, S. Rekhis, N. Boudriga, and M. Allouche, "Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform," *Journal of Network and Computer Applications*, vol. 107, pp. 1–21, 2018.

[72] PhysioNet. (2024) PhysioNet. [Online]. Available: https://physionet.org/. [Accessed: Sept. 6, 2024].

[73] Secure Sketch. (2024) Secure Sketch. [Online]. Available: https://www.secure-sketch.com/en/knowledge/secure-sketch-security-guide. [Accessed: Sept. 6, 2024].

[74] W. Choi, Y. Lee, D. Lee, H. Kim, J. H. Park, I. S. Kim, and D. H. Lee, "Energy-aware key exchange for securing implantable medical devices," *Security and Communication Networks*, vol. 2018, no. 1, p. 1809302, 2018.

[75] M. Yasin, T. Tekeste, H. Saleh, B. Mohammad, O. Sinanoglu, and M. Ismail, "Ultra-low power, secure iot platform for predicting cardiovascular diseases," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 64, no. 9, pp. 2624–2637, 2017.

[76] Y. Kim, W. S. Lee, V. Raghunathan, N. K. Jha, and A. Raghunathan, "Vibration-based secure side channel for medical devices," in *Proceedings of the 52nd Annual Design Automation Conference*, 2015, pp. 1–6.

[77] Q. Yang, S. Mai, Y. Zhao, Z. Wang, C. Zhang, and Z. Wang, "An on-chip security guard based on zero-power authentication for implantable medical devices," in *2014 IEEE 57th international midwest symposium on circuits and systems (MWSCAS)*. IEEE, 2014, pp. 531–534.

[78] T. Xu, J. B. Wendt, and M. Potkonjak, "Matched digital pufs for low power security in implantable medical devices," in *2014 IEEE international conference on healthcare informatics*. IEEE, 2014, pp. 33–38.

[79] M. Zhang, A. Raghunathan, and N. K. Jha, "Medmon: Securing medical devices through wireless monitoring and anomaly detection," *IEEE Transactions on Biomedical circuits and Systems*, vol. 7, no. 6, pp. 871–881, 2013.

[80] S. Duttagupta, E. Marin, D. Singelée, and B. Preneel, "Hat: Secure and practical key establishment for implantable medical devices," in *Proceedings of the Thirteenth ACM Conference on Data and Application Security and Privacy*, 2023, pp. 213–224.

[81] N. Karimian, G. Saldamli, Y. Park, and V. Lui, "Never lose your ecg: A novel key generation and authentication scheme for implantable medical devices," *IEEE Access*, 2023.

[82] A. Almukhlifi and S. M. Almutairi, "Efficient palm vein authentication encryption technique in wireless implantable medical devices," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 30, no. 3, pp. 1651–1658, 2023.

[83] S. Maji, "Energy-efficient security solutions for next-generation embedded systems," Ph.D. dissertation, Massachusetts Institute of Technology, 2023.