International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. #, No.# (Mon-20..)

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, Saudi Arabia

m.aldalaien@psut.edu.jo, halbazar@arabou.edu.sa, habdeljaber@arabou.edu.sa

Abstract: Implantable Medical Devices (IMDs) have gained significant popularity due to their telemetry capabilities, making them a preferred choice for patients and medical professionals alike. However, like any networked device, IMDs are vulnerable to security breaches, which can pose serious risks to human life. Consequently, ensuring robust security measures for these devices is of utmost importance. While researchers have made efforts to address these vulnerabilities, many proposed solutions are impractical due to the inherent constraints associated with IMDs, particularly their limited battery life. This paper presents a comprehensive review of battery-efficient security solutions for IMDs by surveying extensive research literature in the field. By exploring innovative approaches that provide both strong security and optimized energy consumption, this study aims to strike a balance between safeguarding IMDs and prolonging their operational lifespan. The paper consolidates existing research, highlighting promising avenues for practical and effective security solutions in the face of evolving threats. Serving as a valuable reference for future research endeavors, this work emphasizes the criticality of continuous advancements in this field to ensure the well-being of patients who rely on these life-saving devices. Ultimately, it underscores the need to overcome the unique challenges posed by limited battery life in order to enhance the security of IMDs and mitigate potential risks to human health.

Keywords: : Implantable Medical Devices, Security, Privacy, battery-efficient.

1. INTRODUCTION

We are living in a cyber age. Technology is all around us. From kitchen chores to defense hallmarks, technology has to play a 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].

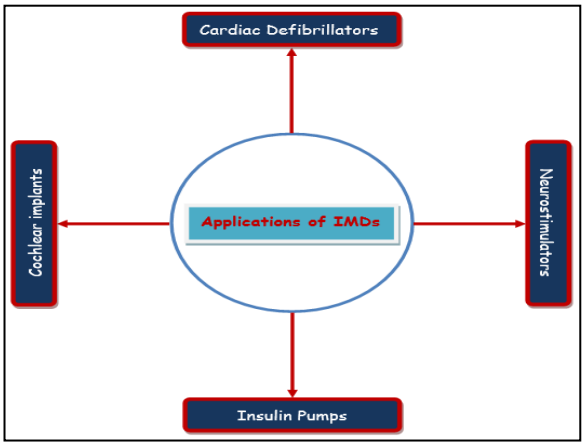

Figure 1. Common applications of IMDs

E-mail:author's email

IMDs are coming in to assist both doctors and patients. For the doctor, it is easier to examine the patient with less 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 IMDs market is valued at US$ 115 billion; in 2027, it is envisaged to reach US$ 155 billion by 2027 as shown in Figure 2 [28]. 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, mostly in the case of cardiac IMDs [31], [32], [33].

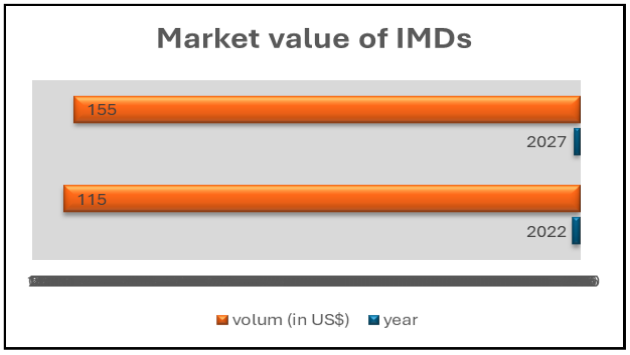

Figure 2. IMDs market in 2022 vs 2027

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]. This research has also been reviewed by other researchers. On the other hand, many researchers have put efforts to combat these challenges [39], [40], [41]. There is, so far, very little 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.

The rest of the paper is organized as section 2 covers the working mechanism of IMDs; section 3 discusses the main components of the security architecture of these devices; in section 4, some common security threats to IMDs have been discussed; section 5 discusses the methodology of research; section 6 reviews the literature; section 6 is the discussion section of the reviewed literature; section 7 concludes the paper.

2. WORKING OF IMDS

There are several components involved in the working of an IMD, the sensor, the stimulator, 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 explanation is as below.

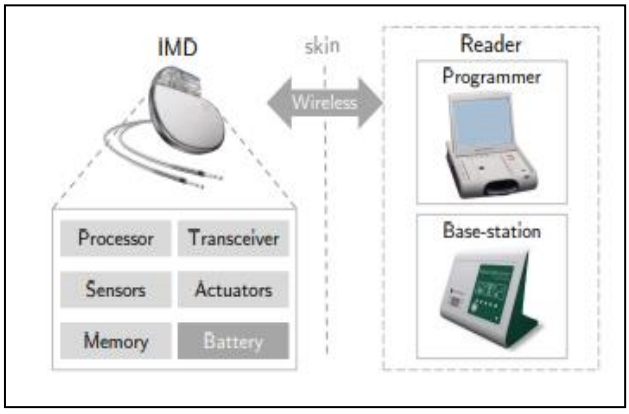

Figure 3. Working of IMDs [42]

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

3. SECURITY ARCHITECTURE OF IMDS

Since IMDs are mostly attached to life-critical body parts, that is why their security is of utmost importance

[45]. Most of the IMDs today have multi-layer security approaches [46]. Some of the common security layers in IMDs are discussed below.

- **Authentication:** This process should ensure that the IMD is being accessed by an authorized person. This is usually ensured through a password or some biometric verification [47].
- **Secure Communication:** Since IMDs transmit very critical information through a wireless channel, it is therefore necessary that the communication be secure. For doing so, the communication is encrypted using different techniques [48], [49].
- **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.
- **Securing the device physically:** It is also equally important that the IMD must be secured from any physical harm. It is ensured as part of human personal security.
- **Updating the firmware:** The firmware of the IMD should be able to install the updates offered by the manufacturer.

4. COMMON THREATS TO IMDS

There are some prevalent threats to IMDs based on the security features that can be exploited. These vulnerabilities can be in the network or even in the IMD itself [37], [50], [51]. Some of these threats are discussed as follows and shown in Table I.

- **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 [52].
- **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 in some illegitimate manner, it is unauthorized access. This can even endanger the life of the patient in the worst-case scenario [53].
- **Battery drain:** Some of the 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 few cases) to replace the battery. So, these attacks, in fact, intend to physically harm the patient. Attacks like Denial-of-Service (DoS) are carried out to sting this harm to the patient [54].
- **Manipulating the firmware:** There are attackers who try to change the firmware settings of the IMD. This helps them take control of the device [41].
- **Man-in-the-middle**: An IMD can be easily exploited if another programmer is brought near it. It can communicate with any programmer having a similar configuration to the one it initially was connected to [55].
- **Stealing data**: Attackers can also succeed in stealing the data generated by the IMD. This data is normally stored in an IMD or some server of the hospital. This type of attack normally happens when there is no proper data encryption in place.
- **Malware**: Like every other modern device, IMD is also on the verge of malware attacks. Different malware attack it. From viruses and spyware to trojans are being injected into the IMDs. This malware can steal data from the IMD as well as they can tamper it [56].
- **Physical Attack:** An IMD can also face physical attacks. These attacks can be stealing the IMD, tampering with the IMD, or even damaging its part (lead, circuit, etc.).

TABLE I. The main functions of the proposed solution.

Security Threat	Against Vulnerability
Eavesdropping	Network protocols
Unauthorized Access	Authentication
Battery Drain	Network and device security
Manipulating the Firmware	Penetrating through the 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]. Many keywords searched on Google Scholar search engine are 'zero-power solutions to IMDs', 'Powerless security solutions to IMDs', 'Enhancing 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'. Many researches were returned among which the most relevant to the real-world implementation were selected. Literature has been reviewed in reverse chronological order. All the relevant proposed solutions were reviewed for their advantages and shortcomings.

6. LITERATURE REVIEW

In this section, the most important works regarding IMD security are being reviewed. The focus of this review is on covering those techniques that have considered power-efficiency, although, some of the reviewed techniques are those which does not consider power efficiency so that a comparison can be drawn. An overview of all the reviewed literature has been presented in Table II.

A. Solutions With No Focus on Power-Efficiency

According to research conducted by I. Almazyad et al. Data security has been brought under experiment in this research. The authors have proposed three modes of data transmission from IMD to the doctor. The modes are mode 0, mode 1, and mode 2 where mode 0 has the most critical data. For selecting an appropriate mode for data transmission, the Adaptive Mode Selection (AMS) mechanism is proposed. A Priority-Queue-based (PQ-based) mechanism has been used to stop dangerous data from spreading to the rest of the system. To choose a transmission mechanism, the Adaptive Protocol Selection (APS) is employed. Experiments have shown that the three methods combined deliver very efficient performance while securing the data [57].

In their research, G. Zheng et al. 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 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% [58].

In their paper, L. Pycroft et al. have proposed a theoretical framework for securing the IMD. Four steps 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, this has been called to as ‘auditing’. The second step in this direction is the reporting of any bug that arises in the IMD. Another very important recommendation is the include multi-factor authentication in the IMD design. Last but not least point is that there is dire need to increase IMD security awareness among the manufacturers and clinicians [30].

According to the research conducted by M Zhang et al., the authors have uncovered some common security challenges in IMDs and then have proposed respective solutions to these challenges. The first challenge they have discussed is the possible software or hardware failure, while common solutions presented to it are 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 to 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 like intrusion detection needs to be implemented. An intimidating security breach is a side-channel attack. System-level countermeasures have been proposed to combat it [59].

C. Li et al., have first sought security bugs in an IMD and then presented a two-step defense against these vulnerabilities. The authors performed experiments on glucose monitoring and insulin delivery pumps. The vulnerabilities that have been unearthed are eavesdropping and tampering with the information stored on the IMD. The possible solutions presented are cryptographic protection and body-coupled communication. As part of cryptographic protection, a rolling code mechanism has been used. Body-coupled communication needs the insulin meter to be very close to the body of the patient. It can thwart any remote attack. Both combined have demonstrated that they can significantly secure an IMD against security threats [60].

In research conducted by F. Xu et al. A proposed method in this research has been called to as IMDGuard. In the said model, an external wearable device called ‘Guardian’ has been deployed. This external device has been deployed for authentication between IMD and the programmer based on ECG of the patient. The main aim of the Guardian is to utilize the randomness of the ECG. Randomness of the authentication would come to aid in overcoming the drawbacks of pre-shared non-rewritable keys. In case of emergency, the doctor has to physically remove the Guardian from the patient. To avoid spoofing, a mechanism has also been implemented in the proposed model. The authors have performed experiments on TelosB and TinyOS 2.1. Results show that the proposed model does not need any additional hardware to run which makes it very viable. [61]

B. Power-efficient solutions

M. Prematilake et al. proposed a hardware and software-based security solution in their research. The

proposed method monitors the readings of the sensor as well as 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 to see if the rules are abided by or not. 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 the insulin pump was 253 ms which is considered as quite low [62].

The focus of research conducted by M. A. Siddiqi et al. is to provide 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 battery of the device. The authors have come up with a zero-power defense based on the 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 [63].

In research conducted by N. Ellouze et al., the authors proposed a zero-power solution to IMDs security. Th primary contribution of this research is ECG-based key authentication that has to be backed by the power harvested from RFID system. The ECG-based key needs to be matched at IMD as well as at the programmer for authorization. This research has specifically been aimed at Cardiac IMDs. In their approach, the first thing that the authors have done is to add extra hardware in the IMD. This additional hardware is called to as Wireless Identification and Sensing Platform (WISP). The fundamental purpose of deploying WISP is that it will decode the ECG signal for mutual authentication. WISP does not come with extra power overhead rather it uses the energy of RFID. On the part of the programmer, an RFID reader has been deployed along with a set of cardiac sensors. There are separate mechanisms 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 [64].

An energy-efficient key exchange solution has been proposed by W. Choi et al. The key is generated using inter-pulse intervals. In the proposed solution, the heartbeat rate is measured at IMD as well as at 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 any communication overhead for error correction. To verify the proposed model. The authors have carried experiments on the ECG signals dataset named PhysioBank (reference). For security analysis, the Secure Sketch (reference) mechanism was used. It was proven that the proposed model satisfies many security parameters like entropy etc. Further, the energy that this model required for transmitting a single bit 3.79 mJ, while for receiving a single bit required 1.83 mJ [65].

M. Yasin et al. have combined two separately proposed solutions. The two separately proposed solutions are security solutions and overcoming power issues. In this study, a power-efficient secure mechanism has been proposed for predicting ventricular arrhythmia almost three hours before the attack. On the aspect of prediction, Naïve Bayes classifier has been used. The prediction has achieved an accuracy of 86%. On the security side, ECG-based random key extraction technique has been employed. It has a multi-layer security approach. Overall, the proposed chip consumes 62.2% less power and occupies 16% less space [66].

In this research, Y. Kim et al. have sought to establish a secure communication channel and a viable key exchange model. The proposed channel is a vibration-based side channel and key exchange mechanism called SecureVibe. The advantage of a vibration-based has been used is its short-range and is easily perceptible by the host. For exchanging (AES) key with a faster bitrate, the On-Off Keying (OOK) demodulation scheme has been used. These techniques combined (especially vibration-based channels) make the communication power-efficient and resistant against any battery drain attack. Key exchange ensures authorized connection establishment only, while a vibration-based channel awakens the host-patient against any infiltration. For carrying out the experiment, nRF51822 RF SoC IMD was used; a Nexus 5 smartphone was used as an external device [67].

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 is deployed to facilitate 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 accessing the IMD. For data encoding, amplitude shift keying with pulse width modulation (ASK-PWM) is used. This ensures low power consumption. For security, SHA-1 algorithm is used. Experiments have shown that the system transmitted data with a speed of 500Kbps [68].

According to research conducted by T. Xu et al., A physical unclonable functions (PUFs) based approach has been put forward by the authors in this research. PUFs work on complex, unpredictable mathematical functions. This research uses two PUFs based circuits, one is to be deployed inside the body of the patient 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 [69].

In this research, M. Zhang et al. have proposed a strategy for wireless channel monitoring and detection of malicious traffic. According to the authors, the existing security solutions for IMDs are power-expensive. For this, they have proposed a general security framework called MedMon (Medical security monitor). MedMon can be a dedicated device or can be 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 detect anomalous traffic. It has two-staged mechanisms in responding to the attack: the first one 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 performed the experiment on glucose monitoring and insulin delivery IMD [70].

D. Halperin et al. have first exploited a few vulnerabilities in IMDs, and then have proposed defenses to these loopholes. The vulnerabilities that they have found include intercepting communication and inferring critical personal information of the patient as well as 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 any 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 zero power defense which means that it does not further power. The experiment was performed on "Medtronic Maximo DR VVEDDDR (7278)" model cardiac defibrillator [71].

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 mechanisms 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	Does not consider design and resources 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 does 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 the effectiveness of cryptographic and body-coupled communication	These techniques, especially the cryptographic technique may increase power overhead as well may not be applicable to every IMD
D. Halperin et al. (2008)	Zero-power defense against interception and unauthorized access	Does not consider a data integrity breach as well as the experiment was performed on a single ICD

TABLE II. An overview of the literature review.

Paper	Advantages	Shortcomings
M. Prematilake et al. (2021)	Classifying safe and unsafe activities	Increasing computational and power overhead

7. DISCUSSION AND FUTURE WORK

Looking at the proposed solutions, some results can be inferred regarding the security of IMDs as shown in Table 3. The foremost thing among these is that there are two

fundamental issues in IMDs Security, unencrypted data communication and weak authentication mechanisms.

Most of the experiments have been performed on simulators and emulators which don't wholly cover the issues raised in the real-world scenarios. Therefore, the focus must be on performing experiments using real environments.

On the security enhancement side, most of the researchers tend to propose solutions based on biometric mechanisms Like ECG etc. One of the thoughts behind doing so is the real and natural randomness of the biometric processes.

Looking at the proposed solutions, zero-power authentication sounds like the best and most viable approach. It needs further improvements in future.

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

TABLE III. 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 the spreading of malicious data	Computationally costly, and complex in design
Cryptographic techniques	Securing the communication	Not well-suited for the special usage model of IMDs having extreme power and size issues
Traffic Monitoring	Anomaly detection becomes easier	Continuous monitoring of traffic is required
Strengthening authorization mechanism	Saves the device from unauthorized access and hence any unwanted change	Increases overheads
External Hardware-based solutions	Averts the danger of any malicious intrusion	Mostly increases the size of IMD or an additional device needs to be implanted along with the IMD

8. CONCLUSION

The use of IMDs on the boom for so many reasons, it offer remote monitoring, instant therapy, and the least physical contact. It can be very helpful in certain attacks like cardiac arrest that aren't very easy for a doctor. Nevertheless, IMDs possess 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 are more feasible which consider these constraints of the IMDs. These constraints make the battery the most scarce 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] Q. D. A. T. K. Z. k. Khalilova Barnogul Abdulazizovna, "INFORMATION TECHNOLOGIES AS A STEP TO THE DEVELOPMENT OF SOCIETY," *IJRCIESS*, vol. 16, no. 3, pp. 73-77, 2022.

[2] M. B. D. L. M. R. Sarah Pink, Everyday Automation Experiencing and Anticipating Emerging Technologies, Taylor & Francis, 2022, p. 250.

[3] B. R. H. D. S. A. M. Andrew Sixsmith, "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] F. G. Mustafa Ali Sezal, "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," *QALAAI ZANIST JOURNAL*, vol. 7, no. 2, pp. 869-895, 2022.

[6] C. I. N. G. C. A. D.-S. K. Judith Nkechinyere Njoku, "Prospects and challenges of Metaverse application in data-drivenintelligent transportation systems," *IET Intelligent Transport Systems*, vol. 17, no. 1, pp. 1-21, 2023.

[7] R. S. A. G. S. K. A. J. A. S. V. A. Daman Kumar Shah, "Smart Kitchen: Real Time Monitoring of Kitchen through IoT," in *2022 3rd International Conference on Intelligent Engineering and Management (ICIEM)*, London, United Kingdom, 2022.

[8] K. Graf, "Cooking with(out) others? Changing kitchen technologies and family values in Marrakech," *The Journal of North African Studies*, pp. 1-26, 2022.

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

[10] J. B. G. G. B. M. Elliot Mbunge, "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] C. S. L. F. S. B. C. S. T. K. W. G. S. F. Y. M. J. L. Z. H. K. S. L. A. C. I. L. C. M. Deepa Elangovan, "The Use of Blockchain Technology in the Health Care Sector: Systematic Review," *JMIR Medical Informatics*, vol. 10, no. 1, 2022.

[12] A. Ś. Kornelia Batko, "The use of Big Data Analytics in healthcare," *Journal of Big Data*, vol. 9, no. 2022, 2022.

[13] M. H. A. A. A. P. J. M. K. A. Z. I. M. A. M. Dipak Kumar Gupta, "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, 2021.

[14] B. B. M. L. C. M. P. B. M. I. M. M. P. Scott J. Adams MD a, "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] C. L. S. M. L. T. L. C. G. L. J. C. Keshia R. De Guzman, "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. M. A. T. M.-È. D. F. L. B. L. N. T. L. N. C. V. F. L.-P. P. Khayreddine Bouabida, "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, 2022.

[17] R. D. J. Z. N. M. J. M. H. H. Jungang Zhang, "Battery-Free and Wireless Technologies for Cardiovascular Implantable Medical Devices," *ADVANCED MATERIALS TECHNOLOGIES*, vol. 7, no. 6, pp. 1-26, 2022.

[18] D. E. A. Caroline Billings, "Role of Implantable Drug Delivery Devices with Dual Platform Capabilities in the Prevention and Treatment of Bacterial Osteomyelitis," *bioengineering*, vol. 9, no. 2, 2022.

[19] S. R. S. M. M. D. Brendan Turner, "Resorbable elastomers for implantable medical devices: highlights and applications," *Polymer International*, vol. 71, no. 5, pp. 552-561, 2021.

[20] H. T. Amit Degada, "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, "Insight into Implantable Medical Devices," 30 June 2022. [Online]. Available: https://www.news-medical.net/health/Insight-into-Implantable-Medical-Devices.aspx#:~:text=The%20most%20common%20examples%20of,implants%2C%20and%20intrauterine%20contraceptive%20devices.. [Accessed 7 April 2023].

[22] A. C. T. A. J. S. S. W. M. D. R. A. T. T. M. M. Carly Daley, "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] R. P. S. B. B. K. J. M. G. G. C. D. D. E. M. A. A. S. B. Stefan Simovic, "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] S. T. S. Md Oqail Ahmad, "The Internet of Things for Healthcare: Benefits, Applications, Challenges, Use Cases and Future Directions," in *Advances in Data and Information Sciences*, Singapore, 2022.

[25] M.-R. C. M. S. G. S. L.-M. M. A.-M. A. S. A. B. I. D. K. G. G. S. N. F. C. D. M. Liviu-Nicolae Ghilencea, "Telemedicine: Benefits for Cardiovascular Patients in the COVID-19 Era," *Frontiers in Cardiovascular Medicine*, vol. 9, pp. 1-12, 2022.

[26] S. K. C. S. R. B. M. A. Shivam Singh, "5G Revolution Transforming the Delivery in Healthcare," Singapore, 2022.

[27] T. M. G. R. A. S. B. P. H. G. A. A. E. S. A.-K. H. M. A. Mohammad Kamrul Hasan, "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, 2021.

[28] Fact.MR, "increasing demand for implanted medical devices," Fact.MR, 2022. [Online]. Available: https://www.factmr.com/report/implantable-medical-devices-market#:~:text=The%20implantable%20medical%20devices%20market%20is%20predicted%20to%20increase%20at,6.1%25%20from%202022%20to%202027.. [Accessed 10 April 2023].

[29] M. A. Siddiqi, A.-A. Tsintzira, G. Digkas, M. Siavvas and C. Strydis, "Adding Security to Implantable Medical Devices: Can We Afford It?," in *International Conference on Embedded Wireless Systems and Networks (EWSN)*, Delft, The Netherlands, 2021.

[30] T. Z. A. Laurie Pycroft, "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] H.-B. T. R. B. C. S. D. B. M. W. F. K. K. T. M. W. Halperin D, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," in *IEEE Symposium on Security and Privacy (sp 2008)*, 2008.

[32] R. J, "Hacker shows off lethal attack by controlling wireless medical device," Bloomberg.com, 2012. [Online]. Available: http://go.bloomberg.com/tech-blog/2012-02-29-hacker-shows-off-lethal-attack-by-controlling-wireless-medical-device/. [Accessed 11 April 2023].

[33] S. D. G. F. D. C. T. W. R. P. B. Marin E., "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.

[34] R. R. M. A. M. V. K. R. Karthick, "Overcome the challenges in bio-medical instruments using IOT – A review," *Materials Today*, vol. 45, no. 2, pp. 1614-1619, 2021.

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

[36] V. C. B. C. B. N. S. Z. Vikas Hassija, "Security issues in implantable medical devices: Fact or fiction?," *Sustainable Cities and Society*, vol. 66, no. March 2021, 2021.

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

[38] J. B. &. S. Pournouri, "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions," *Blockchain and Clinical Trial*, pp. 249-267, 2019.

[39] R. H. B. P. K. C. I. D. Z. C. S. Siddiqi Muhammad Ali, "Securing implantable medical devices using ultrasound waves," *IEEE Access*, vol. 9, no. 2021, pp. 80170-80182, 2021.

[40] J.-Y. C. K.-H. H. Kim Dong-Won, "Medical device safety management using cybersecurity risk analysis," *IEEE Access*, vol. 8, no. 2020, pp. 115370-115382, 2020.

[41] N. M. Easttom Chuek, "Mitigating implanted medical device cybersecurity risks," in *In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 2019.

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

[43] S. S. K. Y. W. K. G. O. Bradley D. Nelson, "Wireless Technologies for Implantable Devices," *Sensors*, vol. 20, no. 16, 2020.

[44] W. L. A. R. V. R. N. K. J. Younghyun Kim, "Reliability and security of implantable and wearable medical devices," in *Implantable Biomedical Microsystems*, ScienceDirect, 2015, pp. 167-199.

[45] "Implantable Medical Device," Definitive Healthcare, 2023. [Online]. Available: https://www.definitivehc.com/resources/glossary/implantable-medical-devices#:~:text=Since%20many%20implantable%20medical%20devices,direct%20individuals%20to%20appropriate%20care.. [Accessed 12 April 2023].

[46] C. F. A. M. A. A.-A. X. D. M. G. Z. Y. Heena Rathore, "Multi-layer security scheme for implantable medical devices," *Neural Computing and Applications*, vol. 32, no. 9, pp. 4347-4360, 2020.

[47] 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, 2018.

[48] M. G. K. M. A. K. Lake Bu, "Bulwark: Securing implantable medical devices communication channels," *Computers & Security*, vol. 86, no. 2019, pp. 498-511, 2019.

[49] F. H. Q. Hao and M. Lukowiak, "Implantable Medical Device Communication Security: Pattern vs. Signal Encryption," in *2nd USENIX Workshop on Health Security and Privacy*, San Francisco, CA, 2011.

[50] 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.

[51] B. Alexander and S. Haseeb, "Are implanted electronic devices hackable?," *Trends in Cardiovascular Medicine*, vol. 29, no. 8, pp. 476-480, 2019.

[52] M. F. Awan and K. Kansanen, "Estimating Eavesdropping Risk for Next Generation Implants," in *Advances in Body Area Networks*, 2019.

[53] V. H. Tutari, B. Das and D. R. Chowdhury, "A Continuous Role-Based Authentication Scheme and Data Transmission Protocol for Implantable Medical Devices," in *Second International Conference on Advanced Computational and Communication Paradigms (ICACCP)*, Gangtok, India, 2019.

[54] A. Alsuwaidi, A. Hassan, F. Alkhatri, H. Ali, M. Qbea'H and S. Alrabaee, "Security Vulnerabilities Detected in Medical Devices," in *2020 12th Annual Undergraduate Research Conference on Applied Computing (URC)*, Dubai, United Arab Emirates, 2020.

[55] 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.

[56] J. Beavers and S. Pournouri, "Recent Cyber Attacks and Vulnerabilities in Medical Devices and Healthcare Institutions," in *Blockchain and Clinical Trial*, Springer, Cham, 2019, pp. 249-267.

[57] I. Almazyad, A. Rao and J. Rozenblit, "A Framework for Secure Data Management for Medical Devices," in *2020 Spring Simulation Conference (SpringSim)*, Fairfax, VA, USA, 2020.

[58] 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, 2019.

[59] 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.

[60] 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*, 2011.

[61] F. Xu, Z. Qin, C. C. Tan, B. Wang and Q. Li, "IMDGuard: Securing Implantable Medical Devices with the External Wearable Guardian," in *IEEE INFOCOM 2011*, 2011.

[62] Y. K. V. R. A. R. N. J. Malin Prematilake, "HW/SW Framework for Improving the Safety of Implantable and Wearable Medical Devices," pp. 1-26, 2021.

[63] 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*, Alghero, Italy, 2019.

[64] 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, no. 1 April 2018, pp. 1-21, 2018.

[65] 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, pp. 1-16, 2018.

[66] M. Yasin, T. Tekeste, H. Saleh, B. Mohammad, O. Sinanoglu and M. Ismail, "ltra-Low Power, Secure IoT Platform for Predicting Cardiovascular Diseases," *IEEE Transactions on Circuits and Systems I: Regular Papers (Volume: 64, Issue: 9, September 2017)*, vol. 64, no. 9, pp. 2624 - 2637, 2017.

[67] 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*, San Francisco, California, 2015.

[68] 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)*, College Station, TX, USA, 2014.

[69] 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*, Verona, Italy, 2014.

[70] 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.

[71] 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)*, Oakland, CA, USA, 2008.

[72] A. Longras, H. Oliveira and S. Paiva, "Security Vulnerabilities on Implantable Medical Devices," in *15th Iberian Conference on Information Systems and Technologies (CISTI)*, Seville, Spain, 2020.

Dr. Mu'awya Al-Dala'ien earned his PhD in network security from University Science Malaysia USM in 2011, and M.Sc. in Computer Science from USM in 2007. His research interests include network security and its applications cryptography and cyber laws , and he teaches networks security , Secure software developments and cyber Laws.

Dr. Hussein Al Bazar received his PhD Degree in computer networks especially in network security and monitoring from Universiti Sains Malaysia (USM) in 2010. He has published more than 18 research papers in International Journals and Conferences with high reputation. His research interests lie in advanced Internet security, Network monitoring, information security, IoT, E-learning. Currently, Dr. Al-Bazar is an Assistant Professor at Faculty of Computer Studies, Arab Open University, Dammam, Saudi Arabia.

Dr. Hussein Abdel-Jaber received his PhD in Computing from University of Bradford in 2009, and from the same university, he received his MSc in Mobile Computing in 2004. His research interests are in congestion control of networks (i.e. internet), queueing networks analysis using discrete-time queues or continuous-time queues, networks performance modelling and evaluation, fuzzy logic control, machine learning, data mining, computer security and e-learning. He has several published research papers in the previous research interests.