Understanding Cybersecurity Threats to Implantable Medical Devices: A Review

Austin James[1], Lucas Potter[2] and Xavier-Lewis Palmer[2]
[1]Independent Researcher
[2]BiosView Labs, Oswego, USA

Austinjamesigwe@gmail.com
Lpott005@odu.edu
Biosview@protonmail.com

Abstract: Implantable Medical Devices (IMDs) are wholly or partially introduced to the body permanently or temporarily to serve a medical purpose. These devices, including pacemakers, cardiac defibrillators, deep brain stimulators, and various drug delivery systems, offer significant medical benefits but pose unique security and privacy risks. The modern history of biomedical implantable devices dates to the 1950s. Since then, the demands for them have pushed the frontiers of medicine and engineering. With millions of these devices now equipped with advanced computing and networking capabilities, they are continually exposed to the same security threats the broader cyberspace faces. Current security approaches often rely on "security by obscurity," which is ineffective. Moreover, managing access for multiple stakeholders, such as doctors, patients, and manufacturers, while adhering to the principle of least privilege poses a significant challenge. These threats include data breaches, where sensitive patient information, such as medical history and treatment plans, could be compromised, and device hijacking, which could allow malicious actors to gain control of the device and potentially harm the patient. Furthermore, managing access for multiple stakeholders, including healthcare providers, patients, and manufacturers, while adhering to the principle of least privilege presents a significant challenge. This literature review examines the evolution of security research in IMDs from 2015 to 2025. The review also explores the potential of leveraging advancements in adjacent technology fields, such as cryptography, artificial intelligence, and blockchain, to enhance the security and privacy of IMDs. Key findings underscore the increasing significance of collaborative efforts among researchers, industry stakeholders, and regulatory bodies. Moreover, the review demonstrates a shift towards more holistic security approaches that consider the entire lifecycle of an IMD, from design and development to deployment and maintenance. This review aims to provide valuable insights for developing more secure and trustworthy IMDs, ultimately improving patient safety and confidence in these life-saving technologies.

Keywords: Implantable medical devices, Cyberbiosecurity, Biocybersecurity, Vulnerabilities, Healthcare, Access

1. Introduction

1.1 Overview of IMD and its Importance in Healthcare

IMDs represent therapeutic devices that are surgically implanted into a patient's body to manage chronic conditions. Some examples include cardiac pacemakers, implantable cardioverter-defibrillators (ICDs), and cochlear implants. For many years, IMDs have been able to communicate only in a relatively straightforward manner. The communication between the IMD and the programmer relies exclusively on a cable and a band placed over the patient's body (Camara et al., 2021). This setup uses an inductive channel, which has several limitations. The maximum separation between the two coils, one inside and the other outside the body, cannot exceed 6 cm (Islam and Yuce, 2016). As a result, the programmer's coil must stay in contact with the body throughout the communication. Additionally, the extremely low bandwidth of these devices forces the patient to remain in uncomfortable positions for extended periods.

In recent years, IMDs have undergone significant technological improvements. These have improved the remote monitoring of patient vitals and drastically reduced the need for invasive surgeries to reprogram or maintain the device. From a clinical perspective, remote monitoring can significantly reduce the time to detect clinical events, thereby improving disease management and survival rates in cases where adverse clinical incidents may arise (Parthiban *et al.*, 2015). This can range from simple electromechanical devices to those that allow telemetry transmission and a degree of computation and data processing. As IMDs continue to play a crucial role in modern healthcare, their integration with the Internet of Things (IoT) drives significant market growth. The healthcare IoT market is experiencing rapid growth, with an estimated value exceeding $44 billion by 2023. It is projected to maintain a compound annual growth rate (CAGR) of 21.2% over the next six years. Of these, the medical devices segment held the largest share, at 37.5%, in 2023. This is attributed to the large-scale adoption of medical devices, driven by the increasing need for efficient and cost-effective solutions to deliver healthcare services (Grand View Research, 2024).

1.2 Preview of Security Challenges

These improvements, while commendable, have also introduced a whole new subcategory to the ever-expanding attack surface in cyberspace. As IMDs gained remote capabilities, the ability to monitor and reprogram them became a crucial factor in advancing the technology. However, introducing wireless communication to IMD exposes them to the hostile world of wireless communication, where threat actors find ingenious ways to compromise a system. According to (Rathore et al., 2020), intruders can intercept an IMD's radio transmissions and frequently gather private data with minimal effort. An attack on an implantable cardioverter defibrillator (ICD) or a deep brain stimulator (DBS) can cause serious harm to a patient; insulin pumps can also deliver dangerous doses of insulin (Finkle, 2016). (Barnett et al., 2024) discussed the potential impacts of botnet-orchestrated attacks, such as DDoS, on IMDs like glucose monitors. In addition to these, according to Hassija et al. (2021), IMDs also carry numerous unintentional risks, including device failure, battery leakage, vulnerabilities in patches and updates, insecure data exchange and storage, and unexpected device-related infections.

2. Context and Importance

2.1 Integration in Healthcare

The integration of implantable medical devices (IMDs) into routine clinical workflows extends beyond therapeutic applications to enable continuous physiological monitoring and real-time data analysis (Kloosterman et al., 2019; Tarakji et al., 2021). This approach allows healthcare providers to make proactive treatment adjustments, contrasting sharply with traditional episodic care models, where interventions occur primarily during scheduled visits or emergencies (Parthiban et al., 2015). Remote monitoring of cardiac implantable electronic devices (CIEDs), for instance, can promptly detect arrhythmias or device malfunctions, enabling early intervention and reducing hospital visits (Kloosterman et al., 2019). Seamless IMD integration enhances patient engagement, improves health outcomes, and fosters safer, more efficient healthcare delivery (Affia et al., 2023; Camara et al., 2021).

2.2 Multi-Stakeholder Environment

Modern IMDs exhibit dynamic capabilities, enabled by advanced interoperability technologies such as wireless telemetry and near-field communication (Islam & Yuce, 2016; Camara et al., 2021). Devices can be accessed via sound, touch, or remote wireless networks, often over untrusted public channels (Zheng et al., 2017). Consequently, as more external entities access patient data remotely, the overall attack surface broadens, increasing cybersecurity risks (Bennouk et al., 2024; Yaqoob et al., 2019). Figure 1 illustrates the relationship between access modalities and vulnerability exposure.

3. Life-Critical Nature

Implantable medical devices (IMDs) perform critical functions essential for patient survival and quality of life, from preventing sudden cardiac arrest to restoring hearing in the profoundly deaf (Catuogno & Galdi, 2024). Drug delivery implants enable targeted medication administration, enhancing therapeutic efficacy while minimising side effects (Hassija et al., 2021). Given their essential role, IMD reliability is paramount; malfunctions from cyberattacks, battery failures, or software glitches can compromise patient safety and become life-threatening (Altawy & Youssef, 2016; FDA, 2023).

4. Resource Constraints

Three major factors limit the creation of robust security mechanisms like those found in smartphones. IMDs are severely constrained by their power, storage, and processing capabilities. For this reason, some authors have opted to delegate these tasks to mobile devices or bedside monitors (Tarakji *et al.*, 2021), which serve as controllers (Kar, Liu, and Li, 2024) for the user.

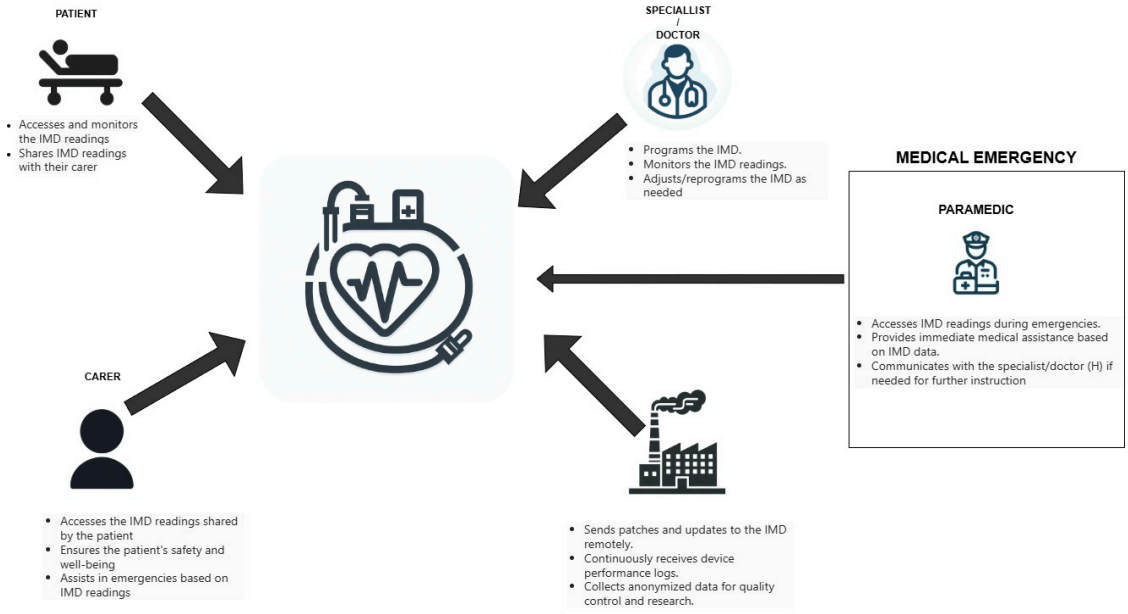

Figure 1: Diagram of IMD usage ecosystem

5. Threat Landscape for IMDs

5.1 Threat Model

Passive adversaries: These attackers eavesdrop on the communication between IMD and the programmer during configuration or an exchange with the bedside reader. This can lead to the disclosure and further weaponization of unencrypted communication containing confidential information, such as names, diagnoses, and medications (Potter et al., 2024).

Active adversaries: One common attack is the resource depletion attack. In this attack, an adversary can continually force the IMD to engage with it via wireless communication. They will continue to attempt to authenticate with the IMD via its security module. The aim is to terminate the communication cycle in the event of an authentication failure and restart it until the battery is depleted (Zheng *et al.*, 2017). An active adversary can intercept and tamper with messages and send unauthorised commands to the IMD, like changing the configurations and parameters of the device or delivering a drug overdose, which can pose a fatal threat to the patient (Wu *et al.*, 2017).

5.2 Attack Types

assive Attacks: In these types of attacks, the attacker is primarily interested in gathering as much information as possible, including the type of device, its manufacturer, serial number, version, status, and any other relevant information that may facilitate subsequent intrusions (Catuogno and Galdi, 2024). Three popular types of passive attacks are eavesdropping traffic analysis, and side-channel attacks.

Active attacks: The attacker actively tampers with the system. By doing this, they aim to trick the device into malfunctioning, thereby risking the patient's rights and safety. Examples of these are:

- Battery depletion attacks: Adversaries send continuous or frequent commands to the IMD, causing it to consume its battery power rapidly (Ellouze et al., 2018), potentially requiring invasive surgery for battery replacement.
- Command injection occurs when attackers inject arbitrary code into a device, causing it to malfunction. This can result in incorrect device operation, such as delivering inappropriate therapy or stopping the device altogether, which can be life-threatening.
- Replay attacks: Attackers capture legitimate communication between the IMD, which lacks a timestamp, and an external device and then replay it later (Zheng et al., 2017).

6. Emerging Security Challenges from Novel Healthcare Technologies

Emerging technologies are rapidly advancing, introducing new frontiers to the healthcare industry's capabilities and quality of service. 5G, IoT, AI, cloud computing, blockchain, quantum computing, and the conceptualisation of 6G, while offering significant benefits to healthcare, also introduce new vulnerabilities to IMDs. These technologies expand the attack surface, creating novel security challenges that can compromise patient safety and the integrity of healthcare systems. As IMDs become increasingly interconnected and reliant on these technologies, it is crucial to understand and address the potential threats they pose to ensure the security and reliability of these life-critical devices. (Bennouk et al., 2024) highlight the impact of emerging technologies on cybersecurity in general. For example, AI/ML enables continuous monitoring and proactive threat mitigation, particularly in fields such as IoT. They have also shown promise in disease diagnosis, discovery of new therapies, and aiding in decision-making (Affia et al., 2023). Cloud computing enables the seamless processing of vast amounts of data. Christo et al. (2021) propose using edge computing to cache medical data for quick access. Blockchain is a decentralised digital ledger that stores records cryptographically securely across a storage network in a transparent, immutable, and tamper-resistant form. Many writers have discussed the potential for blockchain to enhance the security of IMDs. For example, (Aslam et al., 2024) suggest storing patient information on blockchain ledgers and enforcing role-based access control through smart contracts. While quantum blockchain is still experimental, Qu et al. (2024) theorised one such environment for processing medical data. The use of quantum signatures, identity authentication, and homomorphic encryption aimed to address potential security risks posed by quantum computing to the classical blockchain environment. 5G and the proposed 6G are revolutionising industry connectivity with faster data transfer speeds, extremely low latency, and enhanced connectivity. This is good news for healthcare providers, as significantly higher throughput and ultra-low latency enable instantaneous data processing and decision-making, ultimately improving patient outcomes.

7. Literature Gaps

7.1 Previous Studies

Several papers, including (Zheng et al., 2017), have comprehensively explored the security of IMDS and proposed various solutions. (Rathore et al., 2020) examined multi-layer security, utilising ECG as a biometric signal for authentication. (Karimian et al., 2023) utilise the patient's ECG for key generation while authentication and further processing are performed on a private blockchain. However, it is worth noting that the ECG is a particularly random signal. The use of blockchain for authentication, encryption, and decentralised data storage has been studied and proposed by many authors, highlighting its potential to enhance the security and privacy of IMDs (Aslam *et al.*, 2024). Altawy and Youssef (2016) reviewed different solutions, analysing them based on their strengths and weaknesses.

7.2 Identified Limitations

Prior reviews lack a longitudinal analysis of threats and solutions across the 2015-2025 spectrum; hence, critical technological developments were not entirely factored in. Few studies anticipate emerging threats or address mitigation strategies for next-gen IMDs. While there is no shortage of papers addressing key generation, management, and sharing, there is no consensus on how these solutions address some of the core tenets of information security, namely, nonrepudiation. This review addresses these gaps and synthesises advancements from 2015 to 2025 while proposing solutions that align with the rapidly evolving technology landscape.

7.3 Need for an Updated Review

Between 2015 and 2025, significant advancements have occurred in technologies such as AI, blockchain, 5G, IoT, and quantum computing, which introduce new vulnerabilities and attack vectors and the latest security solutions. Recent studies have demonstrated the functionality of physically unclonable functions (PUFS), biometric key generation, and zero-knowledge proofs (ZKPS). An updated review is necessary to address these emerging threats and propose contemporary security solutions.

8. Discussion

The literature review reveals significant advancements in IMD security, particularly in cryptographic key management, emergency access protocols, and lightweight authentication mechanisms for resource-constrained devices. A recurring theme across studies is the tension between security and safety: robust

encryption and access control must coexist with emergency access mechanisms. Recent work has increasingly focused on batteryless IMDs, leveraging energy harvesting to address power limitations, though scalability and reliability under real-world conditions remain understudied. IMD threat models have evolved from conventional risks, such as eavesdropping, to sophisticated AI-driven and supply chain attacks (Barnett et al., n.d.). However, inconsistencies remain in threat prioritisation and validation practices (Bennouk et al., 2024). Frameworks like NIST's Cybersecurity Framework often overlook IMD-specific constraints, such as biocompatibility, latency tolerance, and regulatory mandates, including FDA post-market surveillance (FDA, 2023). Three persistent gaps are evident: (1) fragmented threat modelling limits reproducibility, (2) reliance on proprietary architectures hinders transparency and interoperability, and (3) the lack of real-world validation through physiological testing raises concerns about practical applicability (Siddiqi et al., 2020; Yaqoob et al., 2019).

Rapid innovation in adjacent fields outpaces IMD security literature, creating a knowledge lag. Improving regulatory guidance still lacks specificity for IMDs (Kar, Liu, and Li, 2024), leaving manufacturers to navigate security and safety trade-offs independently. These points are in Figure 3.

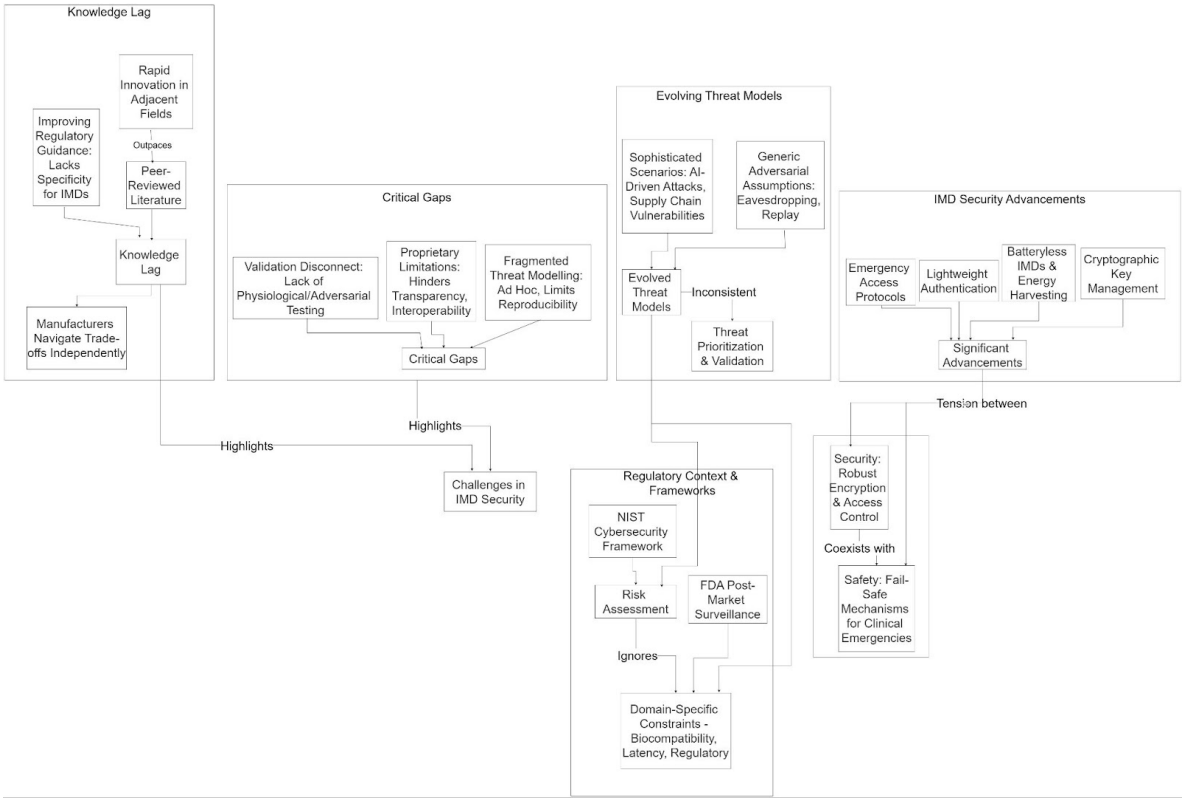

Figure 3: Overview of Key Themes and Relationships in IMD Security Literature within the scope of this paper

9. Objectives and Contributions

The primary objective of this paper is to analyse advancements in security mechanisms, particularly focusing on the Batteryless Implantable Medical Device (IMD) solutions. It aims to evaluate breakthroughs in key generation and management while proposing potential solutions and directions for future research.

9.1 Methodology

The literature review supporting this paper was conducted through a systematic search across several academic databases, including IEEE Xplore, ACM Digital Library, PubMed, and Google Scholar. The search strategy utilised a combination of targeted keywords such as "implantable medical device security," "IMD security," "batteryless IMD security," "key management IMD," "threat models IMD," and "emergency access IMD." Date filters focused on publications between 2015 and 2025, ensuring contemporary relevance. Inclusion criteria were restricted to peer-reviewed journal articles, conference proceedings, and reports from authoritative regulatory bodies, such as the U.S. Food and Drug Administration (FDA). Papers falling outside the specified date range or not addressing IMD security were excluded. It is acknowledged that some relevant

proprietary research may remain undisclosed due to concerns over trade secrecy, particularly regarding device-specific security implementations. The multi-stage selection process, illustrated in Figure 4, involved removing duplicate records, screening titles and abstracts, and prioritising based on gap alignment, topical relevance, and comprehensiveness. Although no formal threat modelling frameworks (e.g., STRIDE, DREAD) were explicitly applied during the initial screening, elements of threat identification and categorisation were inherently incorporated through comparisons of historical and contemporary models. Following article selection, a literature summary table (Table 1) was developed to extract and organise key study characteristics systematically. The table includes author names (citations), article titles, publication year, source, and key findings. This structured approach identified recurring themes, research trends, and notable gaps across the reviewed body of work. A limitation of this methodology is that the rapid pace of technological innovation in the IMD field may have led to the under-representation of the most recent advancements not yet reflected in peer-reviewed literature.

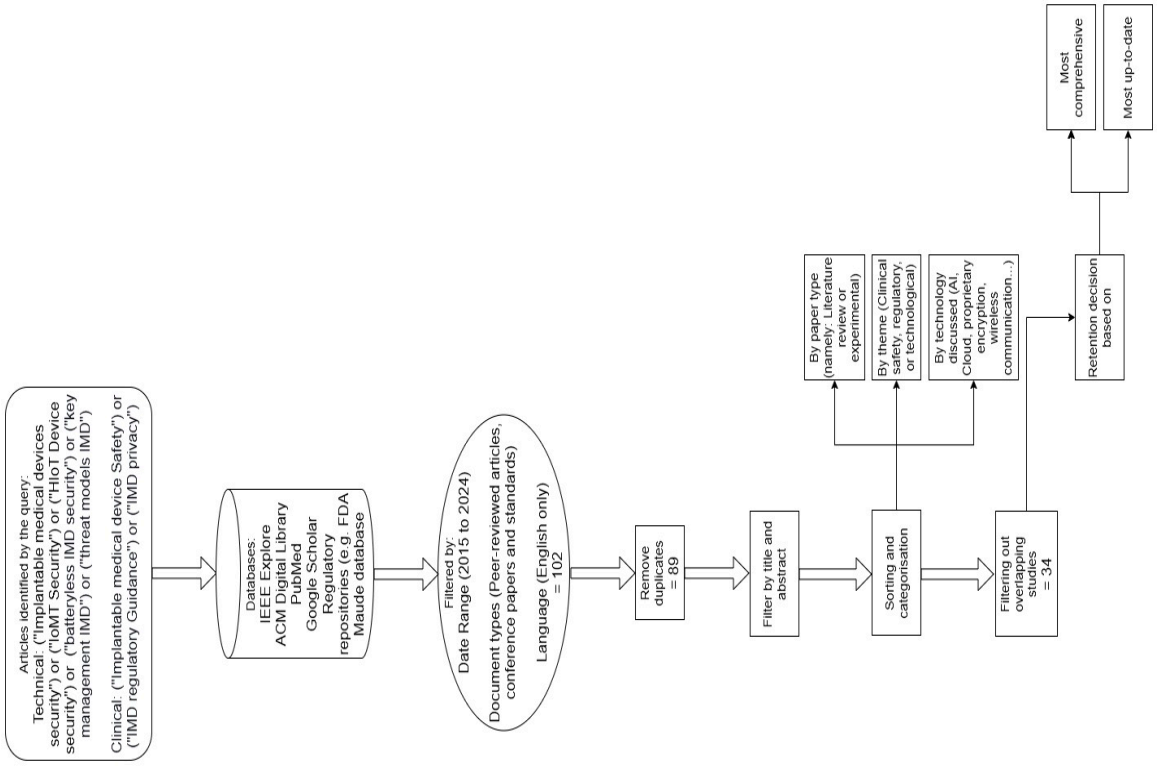

Figure 4: Systematic Literature Selection and Pruning Process for IMD Security Studies

9.2 Key Contributions

Between 2015 and 2025, awareness and research efforts dedicated to enhancing the security of implantable medical devices (IMDs) grew substantially (Yaqoob et al., 2019; Bennouk et al., 2024). Threats and vulnerabilities, once theoretical, materialised into real-world incidents. Notable examples include the vulnerability disclosure involving Johnson & Johnson's Animas insulin pumps (Finkle, 2016) and the cybersecurity advisory concerning Smiths Medical's Medfusion 4000 wireless infusion pumps (CISA, 2017). These incidents underscored the tangible risks of connected medical devices and catalysed broader security initiatives. Manufacturers proactively addressed these challenges, issuing public warnings and initiating efforts to remediate identified vulnerabilities (Yaqoob et al., 2019; FDA, 2023). A fundamental evolution during this period was the shift toward structured cybersecurity practices within the medical device industry, emphasising critical activities such as digital asset protection, threat modelling, vulnerability analysis, and implementation of layered risk controls (Altawy & Youssef, 2016; Barnett et al., n.d.). Regulatory bodies reinforced this shift, notably by transforming the FDA's guidance documents. The original 2014 guidance on *the Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* was succeeded by the more comprehensive 2023 update, reflecting a shift from demonstrating basic security measures to embedding "security by design" principles throughout the device development lifecycle (FDA, 2023; Catuogno & Galdi, 2024).

The 2023 guidance includes recommendations for post-market cybersecurity management. This involves continuous monitoring, vulnerability management, and timely updates to address emerging threats. This period also saw a growing recognition that traditional information security mechanisms often prove inadequate or inappropriate for medical technologies' unique constraints and complexities. Within this broader context, notable progress has been made in the security of IMD through the many proposed batteryless IMD solutions. Since IMDs are typically used for long-term purposes, it is essential that their batteries also provide a reliable and long-term source of power. Non-rechargeable and non-replaceable batteries usually are expected to last 5-10 years (Zheng et al., 2017).

Table 1: A detailed overview of the key characteristics of the studies included in this analysis

Author(s)	Year	Title	Key Findings	Source
Affia et al.	2023	IoT health devices: Security risks	Notes weak authentication in IoT devices; suggests secure protocols.	IoT
Altawy et al.	2016	Security tradeoffs in IMDs	Highlights unauthorized access and battery drain risks in IMDs.	IEEE Access
Aslam et al.	2024	Blockchain-based IoMT authentication	Proposes role-based access control for IoMT security.	PLoS ONE
Barnett et al.	2023	Botnets in healthcare	Examines botnet threats; recommends network monitoring.	ECCWS
Bennouk et al.	2024	Cybersecurity vulnerability detection	Reviews scanning and testing for IMD vulnerabilities.	J. Cybersecurity
Camara et al.	2021	Access control for IMDs	Suggests lightweight access control for IMDs.	IEEE TETC
Catuogno et al.	2024	IMD security	Focuses on cryptographic key management for IMDs.	Cryptography
Christo et al.	2021	ECC and blockchain for medical data	Proposes ECC-blockchain for secure IoMT data.	Security & Comm.
CISA	2017	Medfusion 4000 vulnerabilities	Reports unencrypted data in infusion pumps; urges updates.	CISA
Ellouze et al.	2018	Powerless security for cardiac IMDs	Uses wireless sensing for cardiac IMD security.	J. Network Apps
FDA	2023	Cybersecurity in medical devices	Guides cybersecurity in device design.	FDA
Finkle	2016	Insulin pump hacking risk	Notes insulin pump vulnerabilities; prompts patches.	Reuters
Gao et al.	2024	Energy harvesters for IMDs	Links power constraints to IMD security.	Advanced Materials
Grand View Research	2024	IoT in healthcare market	Notes growing attack surface in IoT healthcare.	Grand View
Hassija et al.	2021	IMD security: Fact or fiction?	Stresses robust encryption for IMDs.	Sustainable Cities
Islam et al.	2016	MICS band for IMDs	Notes wireless protocol vulnerabilities in MICS.	ICT Express
Kar et al.	2024	Lightweight IMD authentication	Uses smart contracts for IMD security.	IEEE Access
Karimian et al.	2023	ECG-based IMD authentication	Proposes ECG for secure IMD key generation.	IEEE Access
Kloosterman et al.	2019	Remote control of cardiac IMDs	Highlights security issues in remote IMD access.	J. Cardiac Rhythm
Ortiz-Martin et al.	2018	Heartbeats for random numbers	Finds heartbeats unsuitable for IMD cryptography.	Entropy
Parthiban et al.	2015	Remote monitoring of ICDs	Notes cybersecurity risks in ICD data transmission.	EP Europace
Potter et al.	2024	Biocybersecurity modeling	Uses predictive modeling for IMD security.	IJSSE
Qu et al.	2023	Quantum blockchain for IoMT	Proposes quantum blockchain for IoMT privacy.	IEEE IoT Journal
Radziemski et al.	2016	Ultrasound power for IMDs	Notes security risks in ultrasound power delivery.	Ultrasonics
Rathore et al.	2020	Multi-layer IMD security	Combines encryption and access control for IMDs.	Neural Computing
Rosa et al.	2023	NFC-powered IMD monitoring	Uses blockchain for secure NFC IMD data.	IEEE Cybernetics
Siddiqi et al.	2020	IMDfence protocol	Prevents IMD eavesdropping with secure protocol.	IEEE Access
Tarakji et al.	2021	Pacemaker app monitoring	Notes cybersecurity needs for app-based pacemakers.	Heart Rhythm O2
Velarde et al.	2023	Virtual surgical planning	Notes cybersecurity risks in surgical networks.	Computer Surgery
Wazid et al.	2018	IMD authentication scheme	Ensures secure IMD deployment with authentication.	IEEE JBHI
Wu et al.	2017	Access control for IMDs	Surveys lightweight access control for IMDs.	IEEE IoT Journal
Yang et al.	2024	Optical charging for pacemakers	Notes security risks in pacemaker charging.	Sensors & Materials
Yaqoob et al.	2019	IMD vulnerabilities review	Reviews IMD attacks and regulatory countermeasures.	IEEE Comm. Surveys
Zheng et al.	2017	Securing wireless IMDs	Proposes encryption for wireless IMD security.	IEEE Sensors

Traditional IMD batteries necessitate surgical replacement upon depletion, prompting research into non-invasive charging methods. (Radziemski and Makin 2016) demonstrated ultrasound-based transcutaneous energy transfer, while (Yang et al. 2024) applied optical energy to cardiac pacemakers. Batteryless energy harvesting technologies provide an additional avenue for enhancing miniaturisation and mitigating battery depletion attacks (Gao et al., 2024). NFC-powered IMDs also show promise, enabling secure in-situ encryption and over-the-air data transfer (Rosa, Anastasova & Yang, 2023). Rosa et al. integrate private blockchain storage to securely manage patient data. Furthermore, zero-power security devices, such as those proposed by (Ellouze et al., 2018), employ RF energy harvesting via wireless identification sensing platforms (WISP) to enable authentication without draining IMD batteries.

Furthermore, research has explored NFC-powered IMDs that incorporate in-situ encryption of acquired physiological signals. These batteryless devices employ lightweight symmetric-key distribution schemes with data stream hopping to ensure secure over-the-air data transfer between the patient and trusted entities. (Rosa, Anastasova and Yang, 2023) explore the safe design of IMDs by implementing a batteryless IMD with near-field communication (NFC) as a link between the device and a mobile phone. The NFC will serve as a communication medium between both devices and as a source of RF charging for the IMD. After the data is transmitted to the mobile phone, it is stored in central storage on a private blockchain with necessary access

controls, and the patient data will be available to authenticated and permissioned users. The concept of zero-power security devices that assist IMDs with authentication and key exchange without drawing power from the implant's battery has also been investigated. According to (Ellouze et al., 2018), the system is designed to integrate a wireless identification sensing protocol (WISP) to harvest RF energy from incoming signals delivered by an ultra-high-frequency RFID reader.

9.3 Evaluation of Breakthroughs in key Generation and Management Techniques

Effective cryptographic key management is crucial for secure communication systems, particularly for implantable medical devices (IMDs), where breaches may lead to life-threatening outcomes (Catuogno & Galdi, 2024; Hassija et al., 2021). Symmetric key encryption, using the same key for encryption and decryption, typically offers faster processing speeds and lower resource consumption, making it suitable for continuous IMD data transmission (Altawy & Youssef, 2016). However, secure key distribution poses a significant challenge, as communication channels often cannot be presumed secure (Wu et al., 2017). A commonly implemented yet problematic solution involves hardcoded keys, which attackers can recover through known plaintext attacks, subsequently allowing key recomputation (FDA, 2023; Yaqoob et al., 2019). Moreover, achieving forward secrecy is notably difficult with hardcoded keys (Zheng et al., 2017). In contrast, asymmetric encryption, which employs a public-private key pair, effectively addresses these key distribution challenges. It excels in authentication scenarios, often supported by digital certificates that verify identities (Camara et al., 2021). Although computationally intensive, the strategic integration of asymmetric and symmetric methods enhances overall IMD security (Christo et al., 2021; Rathore et al., 2020). (Wazid et al., 2018) demonstrated an effective elliptic curve cryptography (ECC) implementation using asymmetric methods for authentication and secure symmetric key exchange. ECC is advantageous due to its shorter key lengths, providing strong encryption well-suited for resource-constrained environments (Christo et al., 2021; Wazid et al., 2018). Another innovative approach involves using patients' physiological data, such as ECG and PPG signals, as inherent sources of entropy for cryptographic key generation, eliminating the need for traditional key distribution protocols (Karimian et al., 2023). A challenge with physiological data for key generation lies in managing signal noise while preserving adequate entropy (Ortiz-Martin et al., 2018). Although using ECG-derived inter-pulse intervals (IPIs) showed limitations in long-term reliability (Ortiz-Martin et al., 2018), Karimian et al. (2023) proposed temporal fiducial features from ECG signals, particularly peak amplitude differences, as a robust alternative for generating secure cryptographic keys.

9.4 Role of Blockchain Technology in Securing IMDs

Blockchain technology offers significant opportunities to enhance IMD security, particularly in secure data logging, firmware integrity, and access control. Its inherent immutability supports the creation of tamper-proof audit trails for device data, production details, usage logs, and maintenance records, improving traceability and accountability (Qu et al., 2024; Catuogno & Galdi, 2024). Verifiable histories of device operations are critical for ensuring the authenticity and trustworthiness of health data (Barnett et al., n.d.). Beyond audit trails, blockchain can establish decentralised healthcare data marketplaces, empowering patients to have greater control over who accesses their medical information (Aslam et al., 2024; Affia et al., 2023). For instance, smart contract–based systems enable patients to dynamically grant or revoke data access rights, thereby maintaining ownership over their information (Aslam et al., 2024). Secure firmware distribution remains another critical application. Blockchain-based mechanisms can ensure the integrity and authenticity of over-the-air (OTA) firmware updates, mitigating risks associated with unauthorized modifications (Catuogno & Galdi, 2024; Yaqoob et al., 2019). Such systems provide an auditable, tamper-resistant method for verifying updates throughout the device lifecycle.

9.5 Evolution of Emergency Access Design for IMDs

A central theme in the design of emergency access has been the continuous effort to reconcile robust security protocols with the necessity for immediate access to device functionalities and patient data when life is at risk. Scenarios, where the patient might be unconscious or otherwise unable to provide access credentials, necessitate the development of alternative methods for authorised personnel to gain control of the device. (Altawy and Youssef 2016) discuss extensively different emergency access techniques, categorising them accordingly. One of the observations of this work is the lack of formal verification techniques for the IMD authentication protocols that provide emergency access. Since the publication of that paper, notable changes have been proposed blocking emergency access protocols and standards. These have facilitated the integration of new technologies to provide more secure and timely emergency access to IMDS. The use of blockchain for authenticating healthcare professionals, as seen in (Rosa, Anastasova, and Yang, 2023), is

proposed by (Karimian et al., 2023) as a similar approach, albeit with a public key infrastructure featuring a single root CA. Proposed efforts aim to establish manufacturer-independent standards for secure communication between emergency responders' readers and IMDS, ensuring paramedics can interact with any device, regardless of its manufacturer. (Siddiqi, Doerr and Strydis, 2020) proposed an Out-Of-Band (OOB) channel-based version of their IMDfence solution for offline or emergency access. However, they also agree that to facilitate the multi-manufacturer environment necessary for emergency access; there must be a single agreed-upon root CA that grants certificates to the manufacturers, who can then act as intermediate CAs that sign public keys, enabling offline or emergency access.

10. Limitations of Current Research and Its Implications for Future Works

While the current body of research on IMD security is substantial and growing, it still exhibits certain limitations. One notable gap is the relative lack of comprehensive real-world attack data. While numerous vulnerabilities have been identified and theoretical attacks demonstrated, publicly documented instances of successful malicious attacks on implanted medical devices remain relatively scarce. One possible explanation is that these devices are not yet widely targeted in the wild. Most of the papers reviewed have based their research on observed system vulnerabilities rather than actual attacks or threats. This lack of empirical data makes it challenging to assess the threat landscape and prioritise security efforts effectively and thoroughly. That said, there is a consensus on the key challenges and directions for addressing IMD security, as most authors have identified similar problems, even though their proposed solutions vary greatly. This highlights the need for more stakeholder collaboration and openness. It is also a significant challenge, as evidenced by stakeholders' continued disregard for security protocols. This lack of transparency is indicative of the foregoing. This limited collaboration hampers the ability to create standardised, long-term security measures essential for the safety and reliability of IMDs, which remain in patients' bodies for extended periods.

11. Conclusion

This review highlights significant advancements in addressing the growing cybersecurity risks associated with these increasingly connected and sophisticated medical technologies (Affia et al., 2023; Velarde et al., 2024). It also demonstrates how these emerging technologies can enhance security and address existing challenges. There is key progress in developing batteryless IMD solutions, such as transcutaneous energy transfer via optics or RF signals and using energy harvesting methods to generate power in complex security computations. The importance of these findings lies in their contribution to a deeper understanding of the current state of IMD security and the identification of critical areas for future research and development. This review provides a comprehensive overview of the advancements, challenges, and future directions in this vital field, offering valuable insights for researchers, medical device manufacturers, healthcare professionals, and policymakers who strive to ensure the security and safety of implantable medical devices (IMDS).

Ethics Declaration: This research did not require ethical clearance as it did not involve human participants, animals, or sensitive data.

AI Declaration: This paper was created with the assistance of AI tools. The AI tools were used for grammar and style checking, generation of icons, and table formatting. The authors reviewed and validated all AI-generated content to ensure accuracy and integrity.

References

Affia, A.A.O., Finch, H., Jung, W., Samori, I.A., Potter, L. and Palmer, X.L. (2023) 'IoT health devices: Exploring security risks in the connected landscape', *IoT*, 4(2), pp. 150–182. Available at: https://doi.org/10.3390/iot4020009.

Altawy, R. and Youssef, A.M. (2016) 'Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices', *IEEE Access*, 4, pp. 959–979. Available at: https://doi.org/10.1109/ACCESS.2016.2521727.

Aslam, M.S., Altaf, A., Iqbal, F., Nigar, N., Galán, J.C., Aray, D.G., de la Torre Díez, I. and Ashraf, I. (2024) 'Novel model to authenticate role-based medical users for blockchain-based IoMT devices', *PLoS ONE*, 19(7). Available at: https://doi.org/10.1371/journal.pone.0304774.

Barnett, M., Womack, J., Brito, C.E., Miller, K., Potter, L. and Palmer, X.L. (2023) 'Botnets in healthcare: Threats, vulnerabilities, and mitigation strategies', *European Conference on Cyber Warfare and Security*, 23(1), pp. 2345–2354. Available at: https://doi.org/10.34190/eccws.23.1.2345.

Bennouk, K., Ait Aali, N., El Bouzekri El Idrissi, Y., Sebai, B., Faroukhi, A.Z. and Mahouachi, D. (2024) 'A comprehensive review and assessment of cybersecurity vulnerability detection methodologies', *Journal of Cybersecurity and Privacy*, 4(4), pp. 853–908. Available at: https://doi.org/10.3390/jcp4040040.

Camara, C., Peris-Lopez, P., De Fuentes, J.M. and Marchal, S. (2021) 'Access control for implantable medical devices', *IEEE Transactions on Emerging Topics in Computing*, 9(3), pp. 1126–1138. Available at: https://doi.org/10.1109/TETC.2020.2982461.

Catuogno, L. and Galdi, C. (2024) 'Implantable medical device security', *Cryptography*, 8(4). Available at: https://doi.org/10.3390/cryptography8040053.

Christo, M.S., Jesi, V.E., Priyadarsini, U., Anbarasu, V., Venugopal, H. and Karuppiah, M. (2021) 'Ensuring improved security in medical data using ECC and blockchain technology with edge devices', *Security and Communication Networks*, 2021. Available at: https://doi.org/10.1155/2021/6966206.

CISA (2017) 'Smiths Medical Medfusion 4000 wireless syringe infusion pump vulnerabilities'. Available at: https://www.cisa.gov/news-events/ics-medical-advisories/icsma-17-250-02a.

Ellouze, N., Rekhis, S., Boudriga, N. and Allouche, M. (2018) 'Powerless security for cardiac implantable medical devices: Use of wireless identification and sensing platform', *Journal of Network and Computer Applications*, 107, pp. 1–21. Available at: https://doi.org/10.1016/j.jnca.2018.01.009.

FDA (2023) 'Cybersecurity in medical devices: Quality system considerations and content of premarket submissions guidance for industry and Food and Drug Administration staff'. Available at: https://www.fda.gov/media/171719/download.

Finkle, J. (2016) 'J&J warns diabetic patients: Insulin pump vulnerable to hacking'. Available at: https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e-idUSKCN12411L/.

Gao, Z., Zhou, Y., Zhang, J., Foroughi, J., Peng, S., Baughman, R.H., Wang, Z.L. and Wang, C.H. (2024) 'Advanced energy harvesters and energy storage for powering wearable and implantable medical devices', *Advanced Materials*. Available at: https://doi.org/10.1002/adma.202404492.

Grand View Research (2024) 'Internet of things in healthcare market size'. Available at: https://www.grandviewresearch.com/industry-analysis/internet-of-things-iot-healthcare-market.

Hassija, V., Chamola, V., Bajpai, B.C., Naren and Zeadally, S. (2021) 'Security issues in implantable medical devices: Fact or fiction?', *Sustainable Cities and Society*, 66, 102552. Available at: https://doi.org/10.1016/j.scs.2020.102552.

Islam, M.N. and Yuce, M.R. (2016) 'Review of medical implant communication system (MICS) band and network', *ICT Express*, 2(4), pp. 188–194. Available at: https://doi.org/10.1016/j.icte.2016.08.010.

Kar, J., Liu, X. and Li, F. (2024) 'LA-IMDCN: A lightweight authentication scheme with smart contract in implantable medical device communication networks', *IEEE Access*, 12, pp. 99694–99703. Available at: https://doi.org/10.1109/ACCESS.2024.3429137.

Karimian, N., Saldamli, G., Park, Y. and Lui, V. (2023) 'Never lose your ECG: A novel key generation and authentication scheme for implantable medical devices', *IEEE Access*, 11, pp. 81815–81827. Available at: https://doi.org/10.1109/ACCESS.2023.3302175.

Kloosterman, E., Rosenbaum, M., La Starza, B., Wilcox, J. and Rosman, J. (2019) 'Remote control of cardiac implantable electronic devices: Exploring the new frontier—First clinical application of real-time remote-control management of cardiac devices before and after magnetic resonance imaging', *Journal of Innovations in Cardiac Rhythm Management*, 10(1), pp. 3477–3484. Available at: https://doi.org/10.19102/icrm.2019.100102.

Ortiz-Martin, L., Picazo-Sanchez, P., Peris-Lopez, P. and Tapiador, J. (2018) 'Heartbeats do not make good pseudo-random number generators: An analysis of the randomness of inter-pulse intervals', *Entropy*, 20(2), 94. Available at: https://doi.org/10.3390/e20020094.

Parthiban, N., Esterman, A., Mahajan, R., Twomey, D.J., Pathak, R.K., Lau, D.H., Roberts-Thomson, K.C., Young, G.D., Sanders, P. and Ganesan, A.N. (2015) 'Remote monitoring of implantable cardioverter-defibrillators: A systematic review and meta-analysis of clinical outcomes', *EP Europace*, 17(3), pp. 369–376. Available at: https://doi.org/10.1093/europace/euu327.

Potter, L., Shetty, S., Karahan, S. and Palmer, X.L. (2024) 'Biocybersecurity and applications of predictive physiological modelling', *International Journal of System of Systems Engineering*, 14(4), pp. 349–361. Available at: http://dx.doi.org/10.1504/IJSSE.2024.10056103.

Qu, Z., Meng, Y., Liu, B., Muhammad, G. and Tiwari, P. (2023) 'QB-IMD: A secure medical data processing system with privacy protection based on quantum blockchain for IoMT', *IEEE Internet of Things Journal*, 11(1), pp. 40–49. Available at: https://doi.org/10.1109/JIOT.2023.3285388.

Radziemski, L. and Makin, I.R.S. (2016) 'In vivo demonstration of ultrasound power delivery to charge implanted medical devices via acute and survival porcine studies', *Ultrasonics*, 64, pp. 1–9. Available at: https://doi.org/10.1016/j.ultras.2015.07.012.

Rathore, H., Fu, C., Mohamed, A., Al-Ali, A., Du, X., Guizani, M. and Yu, Z. (2020) 'Multi-layer security scheme for implantable medical devices', *Neural Computing and Applications*, 32(9), pp. 4347–4360. Available at: https://doi.org/10.1007/s00521-018-3819-0.

Rosa, B.M.G., Anastasova, S. and Yang, G.Z. (2023) 'NFC-powered implantable device for on-body parameters monitoring with secure data exchange link to a medical blockchain type of network', *IEEE Transactions on Cybernetics*, 53(1), pp. 31–43. Available at: https://doi.org/10.1109/TCYB.2021.3088711.

Siddiqi, M.A., Doerr, C. and Strydis, C. (2020) 'IMDfence: Architecting a secure protocol for implantable medical devices', *IEEE Access*, 8, pp. 147948–147964. Available at: https://doi.org/10.1109/ACCESS.2020.3015686.

Tarakji, K.G., Zaidi, A.M., Zweibel, S.L., Varma, N., Sears, S.F., Allred, J., et al. (2021) 'Performance of first pacemaker to use smart device app for remote monitoring', *Heart Rhythm O2*, 2(5), pp. 463–471. Available at: https://doi.org/10.1016/j.hroo.2021.07.008.

Velarde, K., Cafino, R., Isla, A., Ty, K.M., Palmer, X.L., Potter, L., Nadorra, L., Pueblos, L.V. and Velasco, L.C. (2023) 'Virtual surgical planning in craniomaxillofacial surgery: A structured review', *Computer Assisted Surgery*, 28(1), p. 2271160. Available at: https://doi.org/10.1080/24699322.2023.2271160.

Wazid, M., Das, A.K., Kumar, N., Conti, M. and Vasilakos, A.V. (2018) 'A novel authentication and key agreement scheme for implantable medical devices deployment', *IEEE Journal of Biomedical and Health Informatics*, 22(4), pp. 1299–1300. Available at: https://doi.org/10.1109/JBHI.2017.2721545.

Wu, L., Du, X., Guizani, M. and Mohamed, A. (2017) 'Access control schemes for implantable medical devices: A survey', *IEEE Internet of Things Journal*, 4(5), pp. 1272–1283. Available at: https://doi.org/10.1109/JIOT.2017.2708042.

Yang, S.K., Chen, C.H., Zhu, Y.J. and Chen, K.J. (2024) 'Remote charging for cardiac pacemakers using transcutaneous optical energy transmission system', *Sensors and Materials*, 36(8), pp. 3335–3350. Available at: https://doi.org/10.18494/SAM5039.

Yaqoob, T., Abbas, H. and Atiquzzaman, M. (2019) 'Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review', *IEEE Communications Surveys & Tutorials*, 21(4), pp. 3723–3768. Available at: https://doi.org/10.1109/COMST.2019.2911575.

Zheng, G., Shankaran, R., Orgun, M.A., Qiao, L. and Saleem, K. (2017) 'Ideas and challenges for securing wireless implantable medical devices: A review', *IEEE Sensors Journal*, 17(3), pp. 562–576. Available at: https://doi.org/10.1109/JSEN.2016.2633973.