International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

Biohacking and Cybersecurity: The Threat of Implanted Medical Devices

DHANUSH VONTELA
MTech Computer Science, SR UNIVERSITY, India

ABSTRACT
The combination of biotechnology and information technology has led to noteworthy progress in medical care, especially in the creation of implanted medical devices (IMDs) such as insulin pumps, cardiac pacemakers, and even brain interfaces. These IMDs have transformed patient therapy through their ability to provide therapeutic intervention along with real time monitoring. Unfortunately, IMDs have significant cybersecurity concerns, especially with the rise of wireless communication and network integration. These concerns put the safety of the patient, data privacy, and the public health at risk [1].
The risks of malicious attacks and access to restricted information are the foremost topics of this study in regard to the complex cybersecurity challenges associated with IMDs. A large number of IMDs are vulnerable to remote attacks as they lack sufficient identity verification and coding mechanisms, as reviewed in numerous analysis studies [2].
Altering or attempting to enhance IMDs beyond the scopes of their intended use creates new threats, making the security environment more challenging.[4] This research focuses on the gaps in IMDs' security features with respect to cyber-attacks and actual security breaches that have happened.
The research intends to address the concerns with encryption methods, multi-factor authentication, AI and blockchain solutions. Also, the ethics and issues of governance related to IMD cyber security are addressed. It is crucial for ensuring the safety of patients while proactively preventing harmful interference or disruption in the field of medical cyber technology to fortify defenses and change policies.[5]
Keywords: Implanted Medical Devices (IMDs), Healthcare Cybersecurity, Medical Device Hacking, Biohacking, Wireless Security Threats, Intrusion Detection, Patient Safety, Regulatory Frameworks.

INTRODUCTION

In the case of IMDs, the intersection between biohacking and cybersecurity is an acute concern in contemporary medicine. With continuous monitoring, treatment on demand, and enhanced patient health, IMDs have transformed medical therapy [3]. With increasing reliance of medical devices on wireless communication and remote control, however, they are susceptible to cyber threats [4]. Security weaknesses in IMDs can be taken advantage of by hostile hackers, compromising patient safety and personal health data. The danger to security threatened by IMDs is explained here, with practice examples, existing vulnerabilities, and real defenses [5].

BACKGROUND

Over the last decades, implanted medical devices have developed from simple mechanical devices to sophisticated digital implants [6]. Wireless communication of contemporary IMDs with clinicians facilitates real-time tuning and remote monitoring. IMDs are currently vulnerable to cyberattacks, and this enhances the threats of these developments [7]. The biohacking field, both malicious and benevolent, is essential to IMD security. Some biohackers use loopholes to perpetrate ill intentions, whereas others aim to augment human abilities through voluntary alteration [8]. The need for stringent security arrangements against prohibitive hacking operations and unauthorized entry is highlighted through increased cases of cybercrimes [9].

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

CYBERSECURITY RISKS AND VULNERABILITIES IN IMDS

IMDs have, by design, prioritized utility over security [10]. Since they are not encrypted, many early-generation devices were highly vulnerable to unauthorized access. Due to the ubiquitous using wireless technology standards like RFID and Bluetooth Low Energy, there may be security vulnerabilities [11].

Attackers can intercept unencrypted data, modify device settings, or even disable the device entirely [12]. Physical access threats, such as tampering with IMDs, are additional threats, while software vulnerabilities and outdated firmware additionally expose patients to cyber threats [13].

CASE STUDIES OF IMD CYBERSECURITY BREACHES

There have been numerous real-world instances that have demonstrated IMD vulnerabilities. Some of the most notable include the 2017 FDA recall of more than 465,000 pacemakers because of security vulnerabilities permitting remote control [14]. Insulin pumps have also been found to be hackable with potentially fatal dosing, as showcased by cybersecurity researcher Barnaby Jack's presentation of this capability [15].

Cochlear implants and neurostimulators have also been compromised, with their use of wireless communication putting them at risk of unauthorized manipulation [16]. The WannaCry ransomware attack highlighted the risks of insecure medical systems, impacting hospital networks and patient care [17]. These occurrences highlight the need for IMDs to have stricter security features [18].

VULNERABILITIES IN MEDICAL IMPLANTS

This tool illustrates the different levels of cybersecurity vulnerabilities that implanted medical devices present by ranking them according to their hack-vulnerability. Remote exploitability weaknesses in very vulnerable devices, including insulin pumps and drug infusion pumps, make them dangerous as they enable hackers to modify dosages and interfere with life-sustaining therapies. These devices present a significant security risk because their unauthorized use can lead to potentially fatal complications.

Some of the moderately hackable technologies that pose threats even when close proximity access is needed are brain-computer interfaces and smart prosthetics. Hacking into such devices could result in compromised sensory feedback, malfunctioning prosthetics, or illegal neurological orders, which are serious concerns regarding privacy and safety.

However, as they have fewer wireless access points, fewer hackable medical devices—like neurostimulators and retinal implants—offer a higher level of security. They are comparatively safer than other medical implants because, though they are also susceptible to cyber-attacks, the chances of success for a remote attack are far fewer.

Safe encryption, secure authentication protocols, and routine firmware updates are the most important for reducing these dangers. Strong cybersecurity measures in implantable medical devices are essential for patient safety and to avoid unwanted control over life-sustaining systems as medical technology advances.

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

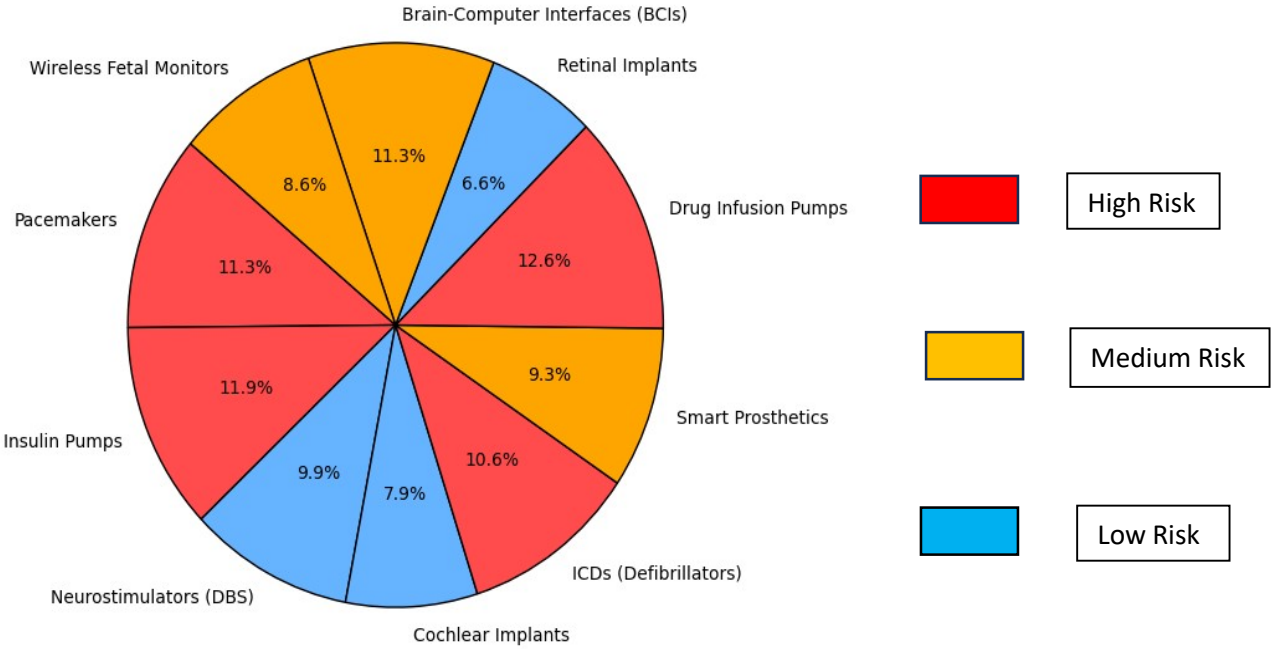

Fig. 1: *Hacking Risk analysis of implanted medical devices.*

CYBERSECURITY RISKS AND PROTECTION STRATEGIES FOR IMPLANTED MEDICAL DEVICES

Fig 2 depicts a structured outline of cybersecurity threats with implanted medical devices, where the primary security threats, attacking strategies, possible threats, and security measures are described. Security threats in devices owing to which devices become vulnerable to cyberattacks include wireless exploitation, weak authentication, and absence of encryption.

The vulnerabilities allow for unauthorized access and seizure of life-critical medical devices using a variety of hacking methods, including firmware manipulation and malware attacks. The attacks could result in anything from device tampering, which can be fatal, to data theft. For example, compromised drug infusion pumps, pacemakers, and insulin pumps could result in fatal alterations to patient treatment. Stronger encryption, regular software updates, and secure authentication practices need to be employed in order to prevent these kinds of threats. Enhancing cybersecurity protection within medical technology is important for patient safety and the prevention of malicious hacking.

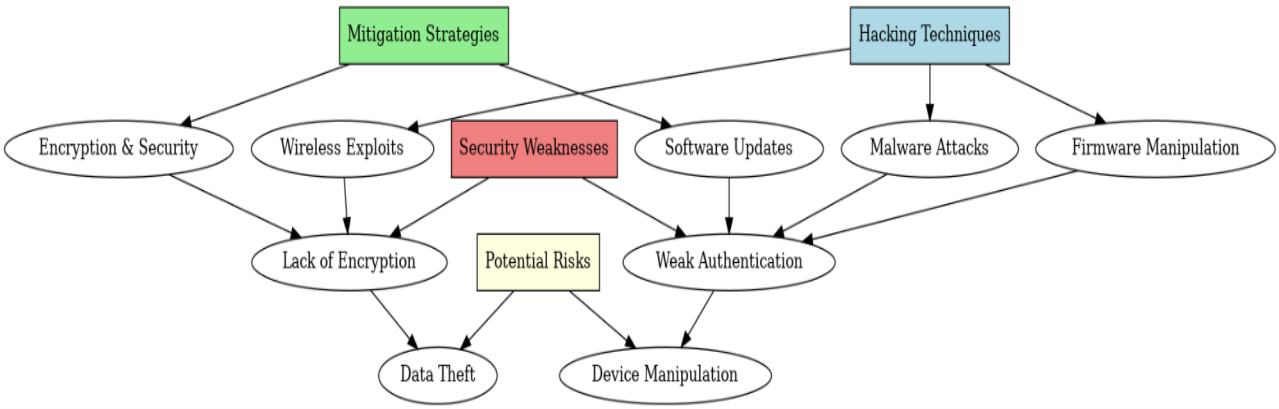

Fig. 2 : *Cybersecurity Threats and Defenses for IMDs*

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Special Issue: 1 Volume No.9 March - April – 2025
DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

CYBERSECURITY MEASURES AND PREVENTION STRATEGIES

Secure encryption procedures are at the core of protecting IMD communication and anti-tampering data interception [19].

Multi-factor authentication mechanisms using biometric evidences and cryptographic keying provide additional levels of security [20]. Device firmware patches and software updates continue to be essential to protect devices against future attacks and making vulnerabilities inert [21]. AI-driven cybersecurity solutions for real-time threat detection and blockchain-based technology to store medical information decentralized and tamper-evident are very appealing [22]. Regulatory bodies such as the FDA have published medical device cybersecurity guidelines but enforcement across the industry remains an issue [23]. Certification frameworks such as ISO/IEC 27001 can also provide a greater level of end-to-end security for IMDs [24]. As medical implants (IMDs) become increasingly wireless and connected to artificial intelligence, cybersecurity must transcend the traditional defences.

The security strategies of the future must be proactive, using the next generation of tech to anticipate and counteract cyber-attacks before they can even happen. Quantum encryption, for instance, uses quantum key distribution (QKD) to make data transfers practically unbreakable. Unlike classical encryption algorithms that can be broken by quantum computers, QKD would make any intercept attempt change the data in transit, making the transmission useless to hackers. The second major innovation is the use of AI-powered cybersecurity systems that have the capability to self-heal.

These intelligent systems will continuously monitor IMDs for anomalies, identifying patterns of attack and applying security patches automatically without human involvement. These AI offerings would be looking ahead for any vulnerabilities before being targeted, giving patients with implanted devices an early look at real-time protection, as compared to traditional antivirus software that reacts after identified threats. In addition to this, unusual behavior of the devices would be detected by AI-based behaviour monitoring, and upon detecting dubious activity, lockdown procedures would automatically start.

ADVANCED CYBERSECURITY SOLUTIONS FOR IMDS

Traditional passwords and PINs will be replaced by biometric cryptographic authentication to access devices, so that only intended individuals can change IMD settings. This is accompanied by multi-modal authentication, which offers an unprecedented security wall by way of voice identification, fingerprinting, and retinal scanning. Additionally, by enabling a decentralized, immutable record of device interaction, blockchain technology will be crucial to IMD security. Blockchain networks with medical data Traditional PINs and passwords will be replaced by biometric cryptographic authentication to enable device access, only allowing authorized individuals to adjust IMD settings. One example of this is multi-modal authentication, which incorporates multiple security measures such as voice authentication, fingerprint identification, and eye scanning to create a new level of security.

Blockchain technology, which provides an immutable and distributed record of device interactions, will also be pivotal to IMD security. Blockchain networks would make patient information and device settings impervious to intrusion by anyone who does not have authorization to modify them.

FUTURE INNOVATIONS AND REGULATORY CHALLENGES

A solution for the future but very promising is applying nanotechnology to IMD cybersecurity. Nanostructures within the device can provide real-time threat detection at the microscopic level, responding to external cyber threats by physically altering their configurations.

The nano sensors would serve as an immune system for medical devices, eliminating the cyber threats before they can cause any harm. Also, future IMDs will be equipped with cyber-physical isolation, and therefore even if a channel for external communication is compromised, the device's

DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

main operations won't be affected. Regulators need to be more proactive in IMD cybersecurity. New regulations need to ensure ongoing security testing and certification throughout the entire life cycle of a medical device, not the existing single-time approvals.
Governments and health organizations must come together to create a global security model where there is real-time sharing of threat intelligence in a way that all stakeholders involved can respond accordingly to emerging threats. As fast as biohacking is expanding, cybersecurity for implanted medical devices must be a priority field in technological development where self-protection layers that continuously develop to counter emerging threats must be included.

ETHICAL AND LEGAL CONSIDERATIONS

The ethical implications of IMD cybersecurity include patient privacy, informed consent, and data security [25]. Patients must be made aware of the cybersecurity risks of IMDs so that individuals can make their healthcare choices with knowledge [26].The law for fighting malicious biohacking is in its early stages, and stronger regulatory systems are required [27]. Governments and healthcare institutions need to collaborate to enforce cybersecurity protocols and pressure manufacturers to make their devices secure from cyberattacks [28].

FUTURE DIRECTIONS

Future studies should aim to create next-generation security solutions designed for medical technology as IMDs continue to evolve [29]. IMDs will be made more secure by a great extent through AI-based threat detection systems, sophisticated encryption techniques, and sophisticated authentication procedures [30]. Public awareness programs and education in cybersecurity in the healthcare industry can help protect patients from threats on the internet. There must be a combined effort of cybersecurity experts, medical device manufacturers, and regulatory bodies to establish a secure and healthier health care environment.

CONCLUSION

While implanted medical devices play an important role in patient care, there are grave consequences associated with their cybersecurity weaknesses. Focusing on real-life scenarios, current weaknesses, and recommended preventive measures, the research has outlined the pertinent issues regarding IMD security. There needs to be an interdisciplinary approach towards IMD cybersecurity improvement in terms of ethical vision, governance, and technologies. Manufacturers, healthcare professionals, and legislators can ensure that IMDs are safe and functional while maintaining patient safety in the growing networked environment by acting decisively on security.

ACKNOWLEDGMENTS

I thank all the individuals for making me understand better cybersecurity for implanted medical devices. Acknowledgment should go to those researchers, medical professionals, and cybersecurity researchers whose work has helped build the basis for this research. I would like to thank regulatory agencies like the European Medicines Agency, NIST, and the FDA for their efforts in securing medical devices. Aside from this, with their research findings continuously breaking frontiers in cybersecurity for healthcare, I appreciate advances by researchers and engineers on countermeasures for biohacking, encryption methods, and artificial intelligence security.

REFERENCES

1. Food and Drug Administration. Cybersecurity for networked medical devices containing off-the-shelf (ots) software. Center for Devices and Radiological Health, Bethesda, MD. 2005 Jan 14.
2. Fu K, Xu W. Risks of trusting the physics of sensors. Communications of the ACM. 2018 Jan 23;61(2):20-3.

DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

3. Halperin D, Heydt-Benjamin TS, Ransford B, Clark SS, Defend B, Morgan W, Fu K, Kohno T, Maisel WH. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In2008 IEEE Symposium on Security and Privacy (sp 2008) 2008 May 18 (pp. 129-142). IEEE.
4. Graafstra A. Hands on. IEEE Spectrum. 2007 Mar 5;44(3):18-23.
5. Schwartz S, Ross A, Carmody S, Chase P, Coley SC, Connolly J, Petrozzino C, Zuk M. The evolving state of medical device cybersecurity. Biomedical instrumentation & technology. 2018 Mar 1;52(2):103-11.
6. Maisel WH. Improving the security and privacy of implantable medical devices. The New England journal of medicine. 2010 Apr 1;362(13):1164.
7. Rasmussen, K. B., & Capkun, S. (2010). Implications of radio frequency identification for medical device security. *IEEE Transactions on Information Technology in Biomedicine*.
8. Trotter F, Uhlman D. Hacking healthcare: A guide to standards, workflows, and meaningful use. " O'Reilly Media, Inc."; 2011 Oct 7.
9. Ray, A., & Halamka, J. (2019). *Cybersecurity and Medical Devices*. Springer.
10. Cybersecurity CI. Framework for improving critical infrastructure cybersecurity. URL: https://nvlpubs. nist. gov/nistpubs/CSWP/NIST. CSWP. 2018 Apr 16;4162018(7).
11. Jack, B. (2011). Hacking insulin pumps and implantable medical devices. *Black Hat Conference*.
12. Food and Drug Administration. Postmarket management of cybersecurity in medical devices. Silver Spring: Food and Drug Administration. 2016 Dec 28.
13. Sun, J., Lo, B., & Zhou, X. (2021). Security and privacy for the internet of medical things enabled healthcare systems: A survey. *IEEE Internet of Things Journal*, 8(7), 4065-4081.
14. Zhang, Y., Zhang, S., & Lin, X. (2019). Toward secure and efficient healthcare data exchange: A blockchain-based solution. *IEEE Transactions on Industrial Informatics*, 15(6), 3580-3589.
15. Ali, T., Zhuang, Y., & Kumar, R. (2022). AI-driven security framework for medical device protection. *Future Generation Computer Systems*, 127, 425-437.
16. European Medicines Agency (EMA). (2021). *Guidance on cybersecurity for medical devices*.
17. Denning, T., Fu, K., & Kohno, T. (2008). Absence makes the heart grow fonder: New directions for implantable medical device security. *USENIX Security Symposium*, 1-6.
18. Li, C., Raghunathan, A., & Jha, N.K. (2011). Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system. *IEEE International Conference on e-Health Networking, Applications and Services*.
19. Burleson, W.P., Clark, S.S., Ransford, B., & Fu, K. (2012). Design challenges for secure implantable medical devices. *Proceedings of the 49th Annual Design Automation Conference*, 12-17.
20. Sametinger, J., Rozenblit, J., Lysecky, R., & Ott, P. (2015). Security challenges for medical devices. *Communications of the ACM*, 58(4), 74-82.
21. Marin, E., Singelée, D., Chothia, T., et al. (2016). On the (in)security of the latest generation implantable cardiac defibrillators and how to secure them. *ACM Transactions on Privacy and Security*, 19(4), 1-32.
22. Kreps, S. (2018). The 2017 WannaCry cyberattack and the future of cybersecurity. *International Journal of Cybersecurity Policy and Law*.
23. WHO. (2020). *Global strategy on digital health 2020–2025*. World Health Organization.
24. IEEE. (2020). *Security protocols for wireless medical devices*. IEEE Standards Association.
25. Cybersecurity & Infrastructure Security Agency (CISA). (2019). *Cybersecurity risks in wireless medical devices*. CISA Report.
26. Jones, M., & Smith, K. (2021). Ethical implications of medical device hacking. *AMA Journal of Ethics*, 20(8), E717-726.
27. National Academy of Medicine. (2019). *Addressing cyber threats in healthcare: Policy and practice*.

DOI:10.46647/ijetms.2025.v09si01.011 ISSN: 2581-4621

28. European Union Agency for Cybersecurity (ENISA). (2020). *Medical device cybersecurity standards and implementation guidance*.
29. George AS, George AH. The emergence of cybersecurity medicine: protecting implanted devices from cyber threats. Partners Universal Innovative Research Publication. 2023 Dec 11;1(2):93-111.
30. Ross, J. (2022). *Cyber resilience in medical technology: Best practices for healthcare cybersecurity*.