International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2024: 7.101

The Security and Privacy Paradox of IoT-Enabled Implantable Medical Devices: A Systematic Review

Divya G

Bangalore, India
Email: *divyagkn488[at]gmail.com*

Abstract: ***IoT implantable devices in healthcare are small, surgically implanted devices with sensors that monitor vital signs, deliver treatments, and provide diagnostic information in real time. They wirelessly transmit data to healthcare providers, allowing for remote patient monitoring and proactive care. Examples include pacemakers, implantable cardioverter defibrillators (ICDs), and neurostimulators. Cybersecurity risks associated with connected medical devices have attracted some attention over the past decade. Hacking implantable devices in the human body may become the next significant security concern. This paper presents a comprehensive overview of widely used implantable devices in the human body, along with an analysis of the ethical considerations related to their usage. This paper aims to explore the key aspects of implantable medical devices and the significant security challenges they present. Understanding its capabilities and vulnerabilities is essential. The suggestions offered are intended to assist in avoiding or managing vulnerabilities.***

Keywords: Internet of Things (IoT), IoT devices, Internet of Medical Things (IoMT), Patient Safety, Healthcare, Privacy, Cyber Security, Ethical Hacking, Implantable Medical Devices (IMD)

1. Introduction

The Internet of Things (IoT) refers to a network of physical objects that can connect to and exchange data with other devices and systems via the Internet. These devices include sensors and various technologies that enable them to communicate with one another. IoT devices can connect via networks such as Wi-Fi, Bluetooth, or Ethernet. They may utilize cloud computing to store and process the data they gather. Prior to the Internet of Things in healthcare, patients could only interact with doctors during visits, as well as through telecommunication and text messages. There was no way for doctors or hospitals to continuously monitor patients' health and provide recommendations based on that data. The Internet of Things (IoT) in healthcare, also known as the Internet of Medical Things (IoMT), connects devices and systems to share patient data. This enables remote monitoring, proactive healthcare interventions, and improved patient management, often through applications like telemedicine, and enhances hospital efficiency. Although there are different types of IoT healthcare devices(shown in Fig. 1), this paper focuses on implantable medical devices, their functioning, threats, and related security concerns.

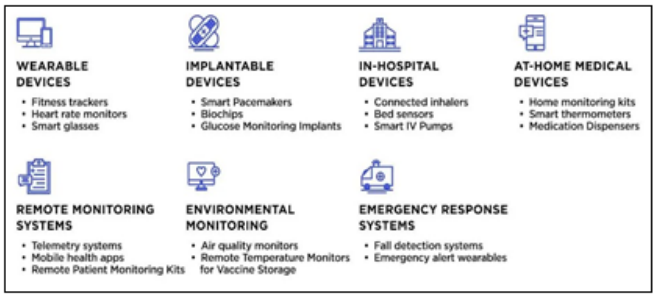

Figure 1: Different types of IoT Healthcare Devices [11].

"IoT implantable medical devices(IMD)" refers to medical devices, like pacemakers or neurostimulators, that are surgically implanted inside the human body and can connect to the internet through wireless technology(shown in Fig. 2), allowing for remote monitoring and control of the device by healthcare professionals via an IoT network; essentially, It's a medical implant that belongs to the "Internet of Things" ecosystem, facilitating data transmission and interaction with other devices. These devices can collect essential health data from within the body, such as heart rhythm or brain activity, and transmit it wirelessly to a healthcare provider for analysis and treatment modifications. Implantable IoT devices are critically important systems for many individuals who face challenges such as vision and hearing impairments, severe pain, or cardiac disorders. Therefore, it is essential to closely monitor their functionality. These devices are either permanently or temporarily placed in the human body to support the functions of specific organs or tissues, monitor physiological activities, or deliver medications. Some implants serve as prosthetics, designed to replace damaged body parts. These devices can be made from either human tissues or synthetic materials, including metals, plastics, and ceramics. The operation of active IMD relies on an external electrical energy source that is not generated directly by the human body or by gravity. These battery-powered devices commonly support cardiac functions and are intended to remain inside the body after the surgical or medical implantation procedure.

In the USA, the FDA (Food and Drug Administration) provides guidance on how to build cybersecurity into medical devices. This includes things like having a pre-market submission for devices to outline potential risks and mitigation strategies. In September 2023, the FDA issued final guidance [9] that expects manufacturers to include features such as data encryption, user authentication, resiliency, and software updates in the design of medical devices. It focuses on managing cybersecurity risks by requiring manufacturers to submit a cybersecurity risk management plan. This plan should cover things like how the device will handle vulnerabilities and protect patient data. It's a kind of disaster recovery plan before the disaster strikes. Without this, getting FDA approval is a tough undertaking.

A report from the U.S. Health Sector Cybersecurity Coordination Center and the Office of Information Security reveal that the frequency of healthcare data breaches has been increasing since 2012. The number of breaches more than doubled between 2018 and 2021, highlighting a concerning trend and suggesting that this issue is likely to continue worsening. Threat actors exploit files to steal identities, profit on the dark web, or prepare for cyberattacks. Recently, they have adopted a risky new tactic that undeniably puts patients at serious risk. Ransomware, account takeovers, and DDoS (Distributed Denial of Service) attacks can lock healthcare providers out of their systems, disrupt critical equipment, and force hospitals to comply with attackers to protect patients. This threat also extends to implantable medical devices, where the risk of harm motivates criminals.

Implantable cardiac devices such as pacemakers rank among the most hackable medical devices, along with smart pens, drug infusion and insulin pumps, and wearable vital sign monitors. To date, there's no evidence of a hacker harming a patient through a connected medical device, but vulnerabilities in implantable devices should be taken seriously. In 2023, the Cybersecurity and Infrastructure Security Agency (CISA) warned of a severe vulnerability in a device from a company called Medtronic — issue CVE-2023-31222. Its severity score is 9.8 out of 10 [7], according to the Common Vulnerability Scoring System. Also in June 2024, OneBlood, a blood donation center [8], was hit with ransomware, and the patients' sensitive health information was compromised. This took away normal functionality and highlighted the security of the healthcare data. These cases remind healthcare organizations to consider using early warning systems to protect important patient data.

As medical devices become increasingly interconnected with the human body, new cybersecurity threats arise that can jeopardize patient safety. Recent studies show that medical devices, such as pacemakers, insulin pumps, and neural implants, are at risk of being hacked or compromised by malware. This vulnerability emphasizes the urgent need to enhance their security in order to protect the health and safety of patients.

2. Research Methodology

The information for this paper is sourced from secondary sources, including the Internet, articles, and public journals.

a) Overview

This section describes a general overview of Implantable Medical Devices(IMD) and the security threats associated with them.

IMD works by using tiny sensors implanted within the body to collect physiological data like heart rate, blood pressure, or glucose levels, which is then transmitted wirelessly to a receiver outside the body, allowing healthcare providers to monitor a patient's health remotely and adjust treatment plans in real-time through a cloud-based system as depicted in Fig. 2; essentially acting as a "connected" medical implant that can send vital information to doctors without the need for constant physical examinations.

Various communication protocols are utilized for this type of communication, including BLE, Wi-Fi, Zigbee, and Z-Wave. Additionally, there are implantable medical devices (IMDs) that operate on a designated radio band known as the Wireless Medical Telemetry Service[10] (WMTS). The Federal Communications Commission (FCC) established this service by allocating specific frequency bands exclusively for wireless medical devices.

b) Key components of IMD

- *Sensors:* Tiny microchips embedded within the device that detect specific physiological parameters.
- *Transmitter:* A small component that wirelessly transmits the collected data from the sensors.
- *Receiver:* A device worn by the patient or placed nearby that receives the transmitted data.
- *Cloud platform:* A secure online server where healthcare providers store and analyse data.

c) How IMD Works

- *Data Collection:* The implanted sensors continuously monitor relevant physiological data within the body.
- *Transmission:* The collected data is transmitted wirelessly through the body tissues to the external receiver.
- *Data Processing:* The receiver processes the incoming data and transfers it to a cloud-based platform.
- *Analysis and Action:* Healthcare providers utilize the cloud platform to access data, analyse it for abnormalities, and adjust the patient's treatment plan as necessary.

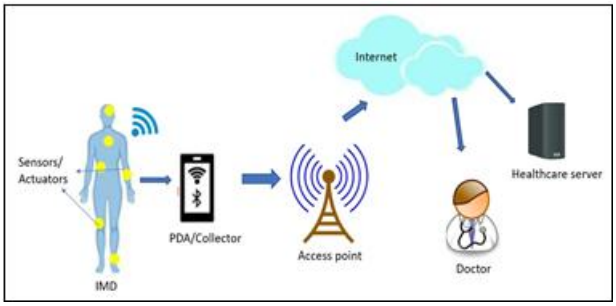

Figure 2: Working overview of IMD

d) Implantable Medical Devices(IMD)

Fig. 3 provides a general overview of typical implantable medical devices.

- *Pacemaker:* These compact battery-operated devices are surgically implanted in the chest to regulate abnormal heartbeat rhythms through electrical impulses. In addition to this primary function, smart pacemakers come with sensors that monitor and record the heart's electrical activity, wirelessly transmitting this data to physicians. They can be beneficial after a heart attack when a patient's cardiac rhythm is too slow, too fast, or irregular, helping to stabilize it[11].
- *Cardioverter Defibrillator:* An implantable cardioverter defibrillator (ICD) resembles a pacemaker, although it is slightly larger. It works very much like a pacemaker. It is a battery-powered medical device implanted in the heart tissue. The device is utilized to monitor heart rate rhythms and deliver electrical shocks to stimulate the heart muscle.

In patients experiencing recurrent and sustained ventricular tachycardia, the device is implanted to restore normal heart rhythms and prevent sudden cardiac death. Many devices integrate a pacemaker and ICD into a single unit for individuals who require both functions[12].

- *Left Ventricular Assist Device(LVAD):* The left ventricle is a large chamber of the heart that pumps blood out to circulate throughout the body. A left ventricular assist device is a battery-powered mechanical pump surgically implanted to support the pumping function of the left ventricle. This device is especially beneficial for patients with end-stage heart failure who are not candidates for heart transplantation. It utilizes a tube to transfer blood from the left ventricle to a pump, which is positioned in the upper abdomen. The pump then propels the blood into circulation via the aorta. The battery and control system, located outside the body, connect to the implanted pump through another tube inserted into the abdominal wall.
- *Breast implants:* Breast implants are positioned beneath the breast tissue or chest muscle for purposes of augmentation or reconstruction. Typically, the implants consist of a silicone outer shell filled with either saline or silicone gel. A variety of implants with differing sizes, thicknesses, textures, and shapes are available on the market[2].
- *Cochlear implants:* Cochlear implants are electronic hearing devices that contain an external microphone, sound processor, transmitter system, and an internally implanted receiver and electrode system. The internal system employs electronic circuits to receive signals from the external system and deliver electrical currents to the inner ear[2].
- *Biochips:* These tiny devices, are implanted under the skin to monitor various patients' physiological functions. Doctors can scan these biochips to instantly retrieve patients' health records. They can also depend on these micro healthcare IoT devices to report real-time changes in patients' physical well-being, diagnose, and detect medical conditions. For instance, biochips can track multiple biomarkers, such as glucose levels and the presence of specific proteins linked to disease states[11].
- *Implantable insulin pump:* The implantable insulin pump is surgically placed in the abdominal wall with the catheter inserted in the peritoneal cavity. Insulin delivery is programmable via a wireless transmitter. It's an alternative treatment for diabetes.
- *Neurostimulator:* a small device that sends electrical pulses to nerves in the body to treat chronic pain and other conditions. This pain management device helps mask chronic pain by blocking pain's nerve signals before they reach the brain. The electrodes are positioned between the spinal cord and the vertebrae (in the epidural space), while the generator is implanted beneath the skin, typically near the buttocks or abdomen. Spinal cord stimulators enable patients to transmit electrical impulses via a remote control when they experience pain.

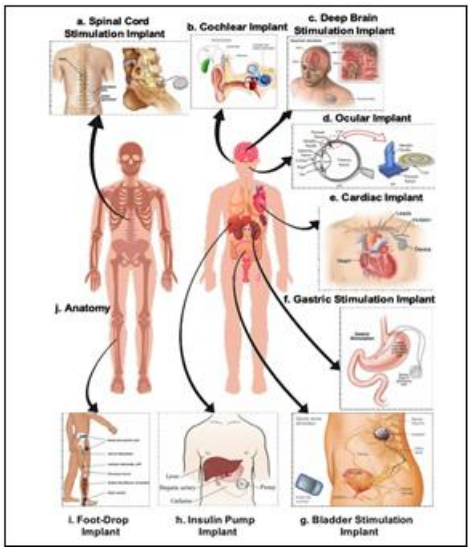

Figure 3: Implantable Medical Devices [10]

- *Brain implants:* The latest implantable device in humans is a brain-computer interface (BCI) implant from Neuralink. The implant is intended to help people with paralysis and other neurological conditions, improve cognitive abilities, and restore movement and speech. They can also be used to help people communicate with external devices. BCI connects the brain to external technology. They can translate neural signals into commands that can control devices.

e) Security Challenges and Concerns with IMD

This section highlights the security challenges of implantable medical devices (IMDs). The primary concern is the risk of hackers exploiting vulnerabilities in the device's communication network, which could lead to dangerous manipulation of settings or functionality. Key issues include outdated software, weak encryption, inadequate authentication protocols, and the potential for data breaches from insecure transmission of sensitive medical information. The major threats encompass:

- *Data Privacy and Security:* The collection and exchange of sensitive patient data naturally raise concerns about information security and privacy. If the sensitive patient data sent from the implant is not properly encrypted, it could be intercepted by unauthorized individuals. Therefore, strong data encryption and strict access controls are essential for safeguarding patient confidentiality.
- *Interoperability Issues:* The absence of standardization frequently results in compatibility challenges, obstructing the smooth operation of a network of IoT devices and, ultimately, data exchange[11].
- *Remote manipulation:* Hackers could potentially access and modify device settings like dosage levels or stimulation parameters, leading to serious health complications.
- *Denial-of-service attacks:* Malicious actors could disrupt the device's communication, preventing it from functioning properly and potentially causing medical emergencies.
- *Outdated software:* Many medical devices lack regular software updates, leaving them vulnerable to known exploits.

- *Weak authentication protocols:* Insufficient user authentication mechanisms could allow unauthorized access to device controls.
- *Unsecured communication channels:* If the communication channel between the implant and the external device is not properly secured, data could be intercepted.
- *Lack of network segmentation:* Improper network segmentation can allow attackers to access sensitive medical data from other devices on the network.

3. Mitigation of Security Risks

This section proposes some key recommendations to alleviate IMD security.

- *Strong encryption:* Data could be intercepted if the communication channel between the implant and the external device is not properly secured.
- *Regular software/firmware updates and implement patches:* Manufacturers should provide timely software updates to address vulnerabilities. The threat landscape evolves rapidly, and systems must stay ahead of hackers to protect against the latest malware and other threats.
- *Robust authentication protocols:* Implement strong authentication mechanisms for user access and adopt multi-layered authentication methods, such as biometrics (fingerprints or retinal scans).
- *Secure communication channels:* Utilizing secure communication protocols for data transmission.
- *Network segmentation:* Isolating medical devices on dedicated networks to prevent lateral movement of attacks.
- *Device design considerations:* Security features should be incorporated into device design from the outset, and manufacturers must follow proper guidelines. Manufacturers of implantable medical devices must integrate security measures during the design phase and throughout the device's lifecycle to protect against cyberattacks and ensure patient safety. Safeguarding the sensors and actuators, which are essential for monitoring vital functions and delivering therapy, is critical for patient safety.
- *Educate and spread awareness to healthcare providers:* Medical professionals, including doctors, nurses, and personnel handling medical data, must receive training in cybersecurity best practices. Regular training sessions should address topics such as data breaches, phishing, the risks of sharing medical information over unsecured networks, latest security threat information, and the importance of regularly changing passwords.

4. Conclusion

Transitioning to the digital landscape presents numerous advantages for the medical industry; however, there are also risks linked to IoT healthcare devices that everyone should recognize. It is crucial for all stakeholders—medical device manufacturers, federal regulatory authorities, physicians, and patient advocacy groups—to unite on a common platform to tackle cybersecurity concerns. Security must be taken into account during the design phase and continued through the implementation and post-marketing survey phases. The FDA plays a critical role in ensuring the safety and effectiveness of implantable medical devices by regulating their development, manufacturing, and marketing, through processes like premarket submissions and post-market surveillance.

This paper discusses the currently available IMD and the associated threats, anticipating that more will emerge in the future with advancements in technology. As per the analysis, neural implants are set to revolutionize our lives in the future. Imagine controlling devices simply by thinking, without the need for remotes or touch screens. As new implants like Neuralink's BCI, which could treat neurological disorders, emerge, new threats are also expected. By implanting a tiny chip in the brain, you can control your computer, mobile, and other electronic devices, even merging your mind with AI. This incredible potential will lead to serious risks. Imagine hackers accessing thoughts, and corporations invading our mental privacy. Also, constant data streams might overwhelm our brains.

In conclusion, an urgent need for robust ethical frameworks and regulatory oversight is essential for implantable medical devices. The future demands a careful consideration of the boundaries between technological advancement and the fundamental right to cognitive privacy. The future of implantable devices is exciting. But we must ask ourselves if we will truly remain in control.

References

[1] Dr.A.Shaji George, & A.S.Hovan George. (2023). Safeguarding the Cyborg: The Emerging Role of Cybersecurity Doctors in Protecting Human-Implantable Devices. Partners Universal International Research Journal (PUIRJ), 2(4), 1–12. https://doi.org/10.5281/zenodo.10397574.

[2] Dr. Dutta, S.(2022). Insight into Implantable Medical Devices. News Medical Life Sciences. Available at: https://www.news-medical.net/health/Insight-into-Implantable-Medical-Devices (last accessed: March 2025).

[3] Browning, John G. and Tuma, Shawn (2016) "If Your Heart Skips a Beat, It May Have Been Hacked: Cybersecurity Concerns with Implanted Medical Devices," South Carolina Law Review: Vol. 67: Iss. 3, Article 8. Available at: https://scholarcommons.sc.edu/sclr/vol67/iss3/8

[4] Gargan, R.(2024). Cybersecurity for Medical Devices: Risks & Defense Tools. Netmaker. Available at: https://www.netmaker.io/resources/medical-device-cybersecurity (last accessed: March 2025).

[5] Hassija et al.(2021). Security issues in implantable medical devices: Fact or fiction?. ScienceDirect, 66. https://doi.org/10.1016/j.scs.2020.102552

[6] Pycroft, Laurie, & Aziz, Tipu.(2018). Security of implantable medical devices with wireless connections: The dangers of cyber-attacks. Taylor&Francis Online. 15(6), 403-406, Available at: https://doi.org/10.1080/17434440.2018.1483235 (last accessed: March 2025).

[7] Greig, J.(2023). CISA issues warning for cardiac device system vulnerability. The Record from Recorded Future News. Available at:

https://therecord.media/cisa-warning-for-cardiac-device-system-vulnerability (last accessed: March 2025).

[8] McGee, M.(2025). OneBlood Notifying Donors Affected by 2024 Ransomware Hack**.** Bank Info Security. Available at: OneBlood Notifying Donors Affected by 2024 Ransomware Hack (last accessed: March 2025).

[9] U.S. Food and Drug Administration. Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions. Technical Report. Guidance for Industry and Food and Drug Administration Staff. 2023. Available at: Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions | FDA (last accessed: March 2025).

[10] Kwarteng, E, and Cebe, Mumin, "A Survey on Security Issues in Modern Implantable Devices: Solutions and Future Issues", Research Gate, 2022, DOI: 10.48550/arXiv.2205.00893.

[11] Dziuba, A.(2023). Guide to Different Types of IoT Healthcare Devices. Relevant Software. Available at: https://relevant.software/blog/iot-healthcare-devices/ (last accessed: March 2025).

[12] Overview of Pacemakers and Implantable Cardioverter Defibrillators (ICDs). Stanford Medicine Children's Health. Available at: https://www.stanfordchildrens.org/en/topic/default?id=overview-of-pacemakers-and-implantable-cardioverter-defibrillators-icds-85-P00234 (last accessed: March 2025).