iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VI **Month of publication:** June 2025

DOI: https://doi.org/10.22214/ijraset.2025.72862

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

Security Risks in Internet-Connected Medical Devices (IoMT): A Threat Analysis and Mitigation Approach

Harikrishnan K V
Cybersecurity Researcher, Kerala, India

Abstract: ***The integration of Internet of Things (IoT) and related technologies into the healthcare sector has revolutionized through the Internet connected Medical Devices (IoMT). Even though these devices are enhancing the diagnostics and real time monitoring they also possess significant cybersecurity risks and challenges. This paper will cover the evolution of cybersecurity threats targeting IoMT assess the impact on patient safety and data integrity, and proposes layered security framework important discoveries indicate that weak authentication, outdated firmware versions and insecure communication channels are some of the most often exploited weaknesses. The paper ends by suggesting legislative and technical actions to strengthen IoMT ecosystems' security posture.***

I. INTRODUCTION

The Internet of Medical Things (IoMT) refers to a network of connected medical devices and applications that collect, transmit, and analyze health-related data through the internet or other communication networks. The security of these devices has become a major concern because to their expanding use in contemporary healthcare systems.

II. IOMT IN MODERN HEALTHCARE

The Internet of Medical Things (IoMT) is transforming modern healthcare by connecting medical devices, sensors, and software systems to collect and share real-time health data. It enables remote monitoring, early diagnosis, and personalized treatment, improving patient outcomes and reducing hospital workloads. From wearable fitness trackers to smart infusion pumps and remote patient monitoring tools, IoMT is making healthcare more efficient, accessible, and data-driven. However, it also introduces new challenges related to data privacy, cybersecurity, and regulatory compliance.

III. SECURITY THREATS IN IOMT DEVICES

The growing adoption of Internet of Medical Things (IoMT) devices is transforming healthcare by enabling real-time monitoring, remote care, and more accurate diagnostics. Devices like wearable health trackers, smart infusion pumps, and connected imaging systems are improving patient outcomes and streamlining clinical workflows. However, this increased connectivity also brings cybersecurity concerns. As more devices link to hospital networks, they expand the attack surface for threats such as unauthorized access, data breaches, denial-of-service attacks, remote code execution, and ransomware.

These threats often exploit common vulnerabilities like weak authentication, outdated firmware, and unsecured communication channels. Many IoMT devices lack built-in security, making them easy targets for attackers. The consequences can be serious which are ranging from disruption of medical services and altered device performance to exposure of sensitive patient data. While IoMT offers clear benefits, it also requires strong security measures to ensure the safety, reliability, and integrity of both healthcare systems and patient information.

A. Common IoMT Security Threats

1) Unauthorized Access: Unauthorized access occurs when attackers gain entry into IoMT devices or systems without valid credentials or approval. These intrusions can happen due to weak authentication, outdated software, or unpatched vulnerabilities. Once inside, attackers may take control of critical device functions**,** alter operational behavior**, or even** disable the device entirely**.**

©IJRASET: All Rights are Reserved

2) Data Theft: Data Theft Refers to the illegal access and extraction of sensitive health related data such as electronic health records (EHRs) and personally identifiable Information, this will lead to privacy breach or identity theft.
3) Denial of Service (DoS) Attacks: The attackers will flood the networks or devices with traffic which makes the systems unavailable for the genuine users. When DoS attacks are in health care industry will lead to the delay or blocking access to the essential medical services and that will affect the patient data.
4) Remote Code Execution (RCE): This allows the attackers to run the malicious code on the medical device or service remotely. Remote code execution in Internet connected medical devices can lead to the severe malfunction or hijacking of control systems in critical care environments and may lead to life threatening situations.
5) Ransomware: Ransomware in healthcare industry is really concerning as it is because of the attack nature like it will encrypt files or systems and will demand a ransom amount for the releasing or decryption of the same. If the ransomware is affected on the hospital networks it can cause shutdown in patient records, diagnostic equipment and even on communication systems.

IV. REAL-WORLD INCIDENTS AND CASE STUDIES

A. *WannaCry Attack on the NHS (2017)*

The WannaCry ransomware attack occurred on May 12, 2017, a Friday, at approximately 12:00 PM British Summer Time (BST). It caused a severe disruption to digital infrastructure across multiple sectors, with the United Kingdom's National Health Service (NHS) being among the most critically affected. WannaCry is a ransomware worm that exploited a vulnerability in the SMBv1 protocol (CVE-2017-0144) using the EternalBlue exploit. This vulnerability had been previously disclosed and patched by Microsoft in March 2017 (MS17-010), but many NHS systems remained unpatched due to outdated operating systems such as Windows XP and legacy dependencies. The malware spread via TCP port 445 and encrypted files using AES and RSA algorithms, locking systems and displaying a ransom demand.

The malware had spread widely across NHS networks, encrypted the files locked the users out of their critical systems as of result this action:

- More than third of NHS trusts were got affected
- Nearly 600 general practices experienced disruption
- Around 19, 000 appointments and surgeries were cancelled
- Operations of critical medical equipment such as MRI Scanners and Blood Refrigerators got affected
- Forced ambulance rerouting**,** delaying emergency treatment.

B. *Recovery and Restoration*

After the attack National Health Services (NHS) led the recovery efforts with the help of affected trusts. The infected systems were disconnected from the network to stop the further spreading. Recovery involved reimaging systems and restoring data from backups. For the systems where the backups were not there had begun to rebuilt. The security teams also applied the MS17-010 patch to uninfected machines and updated antivirus tools to remove the malware. During this time, critical services were run using manual, paper-based processes. It took several days to fully restore operations, and the attack led to new investments in cybersecurity, patch management, and system protection across the NHS.

C. *Medtronic Cardiac Device Vulnerability (2019)*

In March 21, 2019, two serious security problems were found in Medtronic's heart devices, such as pacemakers and defibrillators. These devices use a wireless system called the Conexus RF protocol to connect with bedside monitors and tools used by doctors. The problem was that this system did not have proper security. It did not check who was sending commands (CVE-2019-6540), and it did not protect the data with encryption (CVE-2019-6541). Because of this, someone standing nearby, within about 6 meters, could send dangerous commands to the device or listen to sensitive medical information without being noticed.

The identified weakness allowed for:

- Unauthorized read/write access to the device's memory
- Modifications to therapy settings**,** potentially altering pacing or defibrillation parameters
- Eavesdropping on patient health information transmitted over the air in plaintext
- Risk of disabling the device or causing unintended shocks**,** posing life-threatening consequences

Impact on Patient and healthcare:

- Around 750,000 devices in circulation were potentially affected
- Due to surgical risks, patients were cautioned against replacing devices right away
- Clinical use of Conexus-enabled telemetry was limited to secure settings
- Increased concern and anxiety about implant safety among cardiac patients
- Potential exploitation could cause therapy to be disrupted, which could cause death or severe harm.

D. Recovery and Risk Mitigation

The U.S. FDA and Medtronic jointly released safety communications after the disclosure. Medtronic advised putting in place physical access controls during programming and turning off wireless communication functions when not clinically required. Since firmware updates were delayed due to regulatory hurdles, clinicians were advised to use the affected devices with caution. Medtronic later released new devices with improved security features like encryption and authentication. In response, healthcare providers reviewed how telemetry was used and tightened environmental controls during device interactions. The incident also led to greater focus on regulatory oversight, secure-by-design practices, and long-term cybersecurity planning for IoMT devices.

Both the WannaCry ransomware attack and the Medtronic device vulnerabilities underscore the growing cybersecurity challenges facing the healthcare industry. While one disrupted critical operation at a network level, the other exposed life-threatening risks at the device level. Together, they reflect the complex and interconnected nature of IoMT threats, where both legacy IT systems and modern medical technologies are vulnerable without proactive security design and regulation.

V. KEY VULNERABILITIES IN IOMT SYSTEMS

As more hospitals and healthcare providers use interconnected medical devices new security issues are emerging. Most IoMT devices are built with a focus on medical function, bot cybersecurity due to this they often have the vulnerabilities that the hackers can able to exploit which can put the patient safety and hospital systems at risks.

Here are some of key vulnerabilities associated within the IoMT systems:

1) Outdated Firmware and Software: Many of the IoMT devices are running on the outdated or unsupported operating systems (OS), without having any prompt security patches which will definitely leave those systems or devices to vulnerable state or it will be exposed to known exploits or malware.
2) Weak or no Authentication: Mostly devices are coming with default or hardcoded credentials. In some cases, authentication is not enforced at all which allowing the attackers to have the unauthorized access and device misuse.
3) Lack of Data Encryption: In some cases the sensitive medical data is stored then after transmitted in plain text, such practices without any encryption those data can be easily intercepted or altered during the transmission.
4) Insecure Network Communication: There are some devices which are still using the unsecured communication protocols such as HTTP, FTP or Telnet these communication protocols will make the devices vulnerable to man-in-the-middle (MitM) attacks and session hijacking as well.
5) Poor Physical Security: Mostly the IoMT devices are placed in a public or semi-public environments without any physical safeguards this can allow the attackers to access the ports or interfaces to gather the data or to inject the malicious code.
6) Hardcoded Credentials and Backdoors: Some devices come with hidden backdoor access points or hardcoded login credentials, these are extremely vulnerable because they are typically undocumented and difficult to modify.
7) Lack of Logging and Monitoring: The majority of IoMT devices lack the ability to create logs or alarms, which makes it challenging to identify or address security concerns quickly.
8) Improper Device Lifecycle Management: Devices might be used again without properly deleting their data or may be kept in use over its support lifecycle. This gives opportunities for exploitation and raises concerns about data privacy.
9) Third-Party Component Vulnerabilities: Most of the IoMT devices include the third-party software, libraries, or APIs. Vulnerabilities in these components can compromise the security of the entire device or system.
10) Lack of Security by Design: The majority of devices frequently lack security features like hardware-based trust anchors, secure boot, and sandboxing. The risk of compromise is increased by this unsecure basis.

VI. THREAT ANALYSIS AND RISK ASSESSMENT

Threat Analysis and risk assessment help to identify what need in an IoMT environment need to be protected and how the different threats could affect the patient safety and the day-to-day operations of hospitals.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

In a hospital environment the assets such as patient data, medical devices, networks and communication channels need to be protected from the unauthorized access, tampering and service disruption.

When assessing risks, popular threat modeling techniques like the CIA Triad are helpful:

- Confidentiality: Protecting sensitive patient data from unauthorized access
- Integrity: Making sure that data and device behavior are not changed
- Availability: Making sure devices are operational when needed for patient care

The following table provides examples of common threats in IoMT environments, along with their estimated likelihood, potential impact, and overall risk level.

Each of the risk can be evaluated based on the two key factors, how likely it is to happen and what will be the impact if it does. For instance, a device with out-of-date firmware is more likely to be targeted, and this could have a serious effect on patient safety or data.

Threat	Likelihood	Impact	Risk Level
Unpatched device firmware	High	High	Critical
Default Credentials	High	Medium	High
Data transmitted without encryption	Medium	High	High
Bluetooth based man-in-the-middle	Low	High	Medium

The values in the table are derived from common cybersecurity evaluation techniques. While impact indicates a danger's possible influence on patient safety, data, or system availability, likelihood indicates how frequently a threat may occur in IoMT. Using a qualitative methodology influenced by the CIA triad and the CVSS framework, risk level is determined by combining the two. This makes it easier to rank the most important risks for quick response.

VII. MITIGATION STRATEGIES AND BEST PRACTICES

It is necessary to employ both technical and procedural approaches to tackle the increasing cybersecurity issues in internet connected medical devices. Reducing the risk and improving the security posture of IoMT systems require the following mitigation techniques:

- Secure Device Design: Ensure security is integrated during the design phase of medical devices by incorporating secure boot, hardware-based protection, and tamper resistance.
- Firmware and Software Updates: Update the software and firmware on your devices with the most recent security fixes. Turn on over-the-air (OTA) updates to reduce patching delays.
- Authentication and Access Controls: Make multi-factor authentication and strong passwords mandatory. To restrict administrative access, disable default credentials and use role-based access controls.
- Data Protection: Encrypt sensitive health data both in transit and at rest. Use secure communication protocols such as HTTPS and TLS.
- Network Segmentation and Monitoring: Use intrusion detection/prevention systems (IDS/IPS) to continually monitor traffic and segment IoMT devices on dedicated VLANs.
- Regular Security Audits: Conduct periodic vulnerability assessments and penetration testing to identify and fix security gaps.
- Physical Security: Limit who can physically access medical equipment. Unused ports and interfaces can be disabled or locked down.
- Incident Response and Reporting: Keep a medical-specific incident response plan up to date. Teach employees to recognize and quickly report security incidents.
- Compliance and Regulations: Following industry guidelines and standards like FDA cybersecurity recommendations, NIST 800-53/800-82, ISO/IEC 80001, and HIPAA is essential.

A layered and proactive security approach that includes the right technology, informed users, and clear policies is essential to protect IoMT systems from growing cyber threats and to keep patient data and safety secure.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VI June 2025- Available at www.ijraset.com

VIII. FUTURE-PROOFING IOMT SECURITY

Threats to Internet-connected medical devices are always changing along with them. IoMT security is a continuous process that needs to be adjusted to new cyberthreats and technology developments.

To ensure long-term protection of IoMT systems, the following strategies should be considered:

- Integrate AI and Machine Learning for Threat Detection: Utilize monitoring technologies driven by AI to identify anomalous activity in real time and address possible issues before they become more serious.
- Adopt Zero Trust Architecture: Move toward a zero-trust model where no user or device is trusted by default. This minimizes the risk of internal breaches and lateral attacks within hospital networks.
- Implement Software Bill of Materials (SBOM): Make a clear inventory of the software components included in all medical devices mandatory. This facilitates faster patching during zero-day threats and aids in identifying third-party code that is vulnerable.
- Regulatory Evolution and Global Standards: Promote international cooperation on IoMT-specific security certification and laws. As new technology and attack methods emerge, compliance should change accordingly.
- Lifecycle Security Management: It is important to plan for security updates, monitoring, and eventual decommissioning at every stage of a device's lifecycle, not only during deployment.
- Promoting Security-by-Design in Medical Device Development: Encourage creativity in the production of medical devices by making security a core component rather than an afterthought.
- Awareness and Training for the Workforce: Instruct biomedical engineers, IT workers, and medical staff on safe device handling practices, growing threats, and secure usage.

Building security into the design phase helps reduce future risks and ensures safer, more resilient medical devices. It’s a critical step toward protecting patient trust and healthcare integrity in an increasingly connected world. By addressing vulnerabilities early, manufacturers can avoid costly patches later and create devices that are better equipped to withstand evolving cyber threats. This proactive approach forms the foundation of secure-by-design principles in modern healthcare technology.

IX. INDIAN HEALTHCARE PERSPECTIVE

The use of Internet-connected medical equipment has increased due to India’s quickly growing digital healthcare environment, which is aided by the programs like the eSanjeevani telemedicine services and the Ayushman Bharat Digital Mission (ABDM). Although the efficiency and accessibility of healthcare are enhanced by this digital transformation, new cybersecurity threats are also brought about.

A. Key Considerations

- Absence of Cybersecurity Standards at the Device Level: There are presently no specific IoMT cybersecurity requirements in India. The majority of locally produced or imported devices are not put through rigorous security testing.
- Lack of a Unified Regulatory Framework: India still lacks a single, well-coordinated set of regulations specifically for protecting Internet of Medical Things (IoMT) devices, despite the fact that groups like the Central Drugs Standard Control Organization (CDSCO), National Health Authority (NHA), and Indian Computer Emergency Response Team (CERT-In) are active in cybersecurity and healthcare regulation.
- Rural Infrastructure Is More Vulnerable: Many smaller hospitals and rural health centers operate on outdated IT infrastructure, making them especially vulnerable to ransomware and data breaches.
- Healthcare Workers' Limited Cybersecurity Awareness: In many smaller cities and rural areas, doctors, nurses, and technicians often lack proper training and awareness about securing connected medical devices, which increases the risk of cybersecurity issues.
- Risks to Patient Privacy and Data Sensitivity: As more hospitals use digital health records, a data breach could leak sensitive patient information. However, clear laws to protect this kind of data are still being worked on.

B. Proposed Actions to Improve IoMT Security in India

- Create and implement national IoMT (Internet of Medical Things) security standards, possibly in collaboration with the Ministry of Electronics and Information Technology (MeitY), Central Drugs Standard Control Organization (CDSCO), and National Health Authority (NHA).

©IJRASET: All Rights are Reserved

- Require cybersecurity certifications for both local and foreign medical equipment.
- Offer funds and training to improve security awareness and infrastructure in public and private hospitals.
- Speed up the approval and use of the Digital Personal Data Protection Act (DPDPA) in the healthcare sector.

Securing IoMT infrastructure is crucial to the success of digital health initiatives and the large scale protection of patient safety as India moves toward a more connected healthcare future.

X. CONCLUSION

The growing use of internet-connected medical devices is improving healthcare by supporting faster diagnosis, remote monitoring, and better patient care. At the same time, it introduces serious cybersecurity risks. If these devices are not properly secured, attackers could take advantage of them, putting patient safety, data privacy, and hospital services at risk. This paper explained the main vulnerabilities in IoMT systems, shared real-world examples, and discussed practical ways to reduce these risks.

A strong security approach that includes secure device design, regular software updates, good access control, and clear rules can help healthcare providers stay protected. In the future, countries like India should work on improving laws, building awareness, and planning better for long-term digital safety. Keeping IoMT systems secure is important for protecting patients and building trust in digital healthcare.

REFERENCES

[1] U.S. Food and Drug Administration (FDA) (2023). Cybersecurity in Medical Devices: https://www.fda.gov
[2] Indian Computer Emergency Response Team (CERT-In) (2023). Cybersecurity Framework for Indian Healthcare: https://www.cert-in.org.in
[3] BBC News (2017). WannaCry Attack Impact on NHS: https://www.bbc.com/news
[4] Medtronic (2019). Advisory on Insulin Pump and Cardiac Device Vulnerabilities: https://www.medtronic.com/in-en/patients/important-safety-notice.html
[5] National Health Authority (NHA). (2023). Ayushman Bharat Digital Mission: https://abdm.gov.in

Appendix A - Hospital Security Checklist

To help hospitals improve their cybersecurity posture with the growing use of connected medical devices, the following checklist outlines key practices for securing Internet of Medical Things (IoMT) technologies. These devices play a critical role in patient care but can also introduce risks like unauthorized access and data breaches if not properly managed.

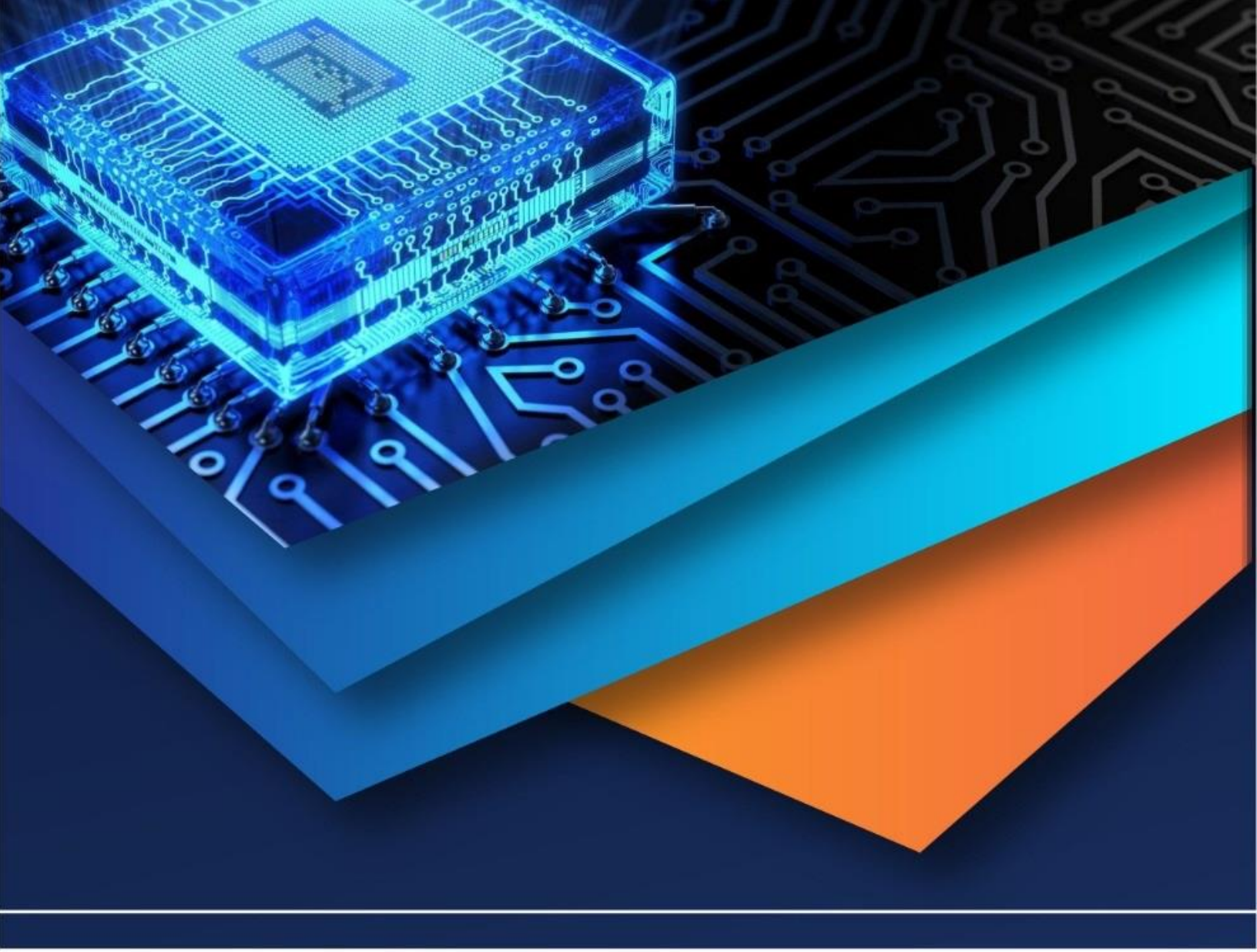
The checklist focuses on important areas such as device management, network security, access control, data protection, and incident response. It is designed to help healthcare teams assess their current practices and identify areas that need improvement.

While not a replacement for formal audits or regulatory compliance, this checklist provides a practical starting point for strengthening IoMT security, especially in hospitals with limited resources.

Security Domain	Evaluation Question	Status (Yes / No / In Progress)
Device Security	Are all connected medical devices tracked and regularly updated?	
Network Protection	Are IoMT devices placed on a separate, secured network segment?	
Access Control	Are user roles defined and protected with strong authentication?	
Data Privacy	Is patient data encrypted during transmission and while stored?	
Incident Response	Is there a defined procedure for responding to IoMT-related threats?	
Staff Training	Are healthcare staff trained in IoMT cybersecurity practices?	
Audit and review	Are periodic security audits conducted for connected medical systems?	
Vendor Management	Are medical device vendors assessed for their cybersecurity practices before onboarding?	
Patch Management	Are security patches applied to IoMT devices in a timely and documented manner?	
Backup and Recovery	Are critical device configurations and patient data regularly backed up and tested?	
Policy Enforcement	Are cybersecurity policies clearly defined and enforced across all departments?	
Remote Access Control	Is remote access to medical devices restricted, encrypted, and logged?	

As healthcare continues to adopt digital technologies and connected devices, securing Internet of Medical Things (IoMT) systems is more important than ever. This research has highlighted key vulnerabilities, real-world incidents, risk factors, and practical strategies to improve security. By using a layered approach that includes strong policies, regular audits, and improved awareness, healthcare organizations can better protect both patient safety and operational continuity. Moving forward, stronger collaboration between medical device manufacturers, cybersecurity professionals, and policymakers will be essential to build a secure and resilient digital health environment.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)