Sudarshan Research Journal
Volume – 2, Issue - 3, March-2024
ISSN No: 2583-8792
Impact Factor: 3.179 (SJIF)

EXPLORING SECURITY RISKS AND PRIVACY THREATS IN THE INTERNET OF MEDICAL THINGS (IOMT)

Preeti
Research Scholar, Department of Computer Science and Applications,
Kurukshetra University Kurukshetra

ABSTRACT

Pervasive healthcare arises as a technology solution to solve global health challenges, given the rising prices and the rising demands for high-quality healthcare. Notably, the Internet of Medical Things (IoMT) has emerged because of recent breakthroughs in the Internet of Things. Although the shift from reactive to preventative care might benefit from these widely available and reasonably priced sensing devices, their security and privacy issues are frequently overlooked. Strong security measures for medical devices and associated communication channels are essential to protect user privacy since these devices manage and record extremely sensitive personal health data. The installation of extensive security measures is limited by the processing power limits imposed by the small size of IoMT devices. Moreover, the extensive use of IoMT devices presents serious difficulties for maintaining and guaranteeing the security of IoMT systems, which hinders the use of IoMT devices for therapeutic purposes. This article provides a thorough overview of state-of-the-art methods while reviewing the security and privacy requirements, dangers, problems, and future research objectives within the IoMT sector.

KEYWORDS: IoMT, Security and Privacy, Threats.

I. INTRODUCTION

The term "Internet of Medical Things" (IoMT) describes a network of medical applications and devices that are linked to internet computer networks and healthcare IT systems. The real-time collection, transmission, and analysis of patient data is made possible by these networked devices, which include wearable sensors, medical monitoring devices, implantable devices, and medical imaging equipment. This allows healthcare providers to make data-driven decisions and monitor patients remotely. IoMT has a great deal of relevance in contemporary healthcare, in many ways.

- **Remote Patient Monitoring:** Outside of conventional clinical settings, IoMT devices enable healthcare practitioners to remotely monitor patients' vital signs, health data, and adherence to treatment recommendations. This capacity is especially helpful in the management of chronic illnesses, early detection of deterioration, and prompt action facilitation, all of which improve patient outcomes and lower healthcare costs.
- **Personalised medicine:** IoMT makes it possible to gather ongoing, high-resolution data on the health and habits of specific patients. This data can then be processed to create treatment plans and treatments that are specifically tailored to the requirements, preferences, and therapeutic response of each patient. IoMT has the potential to maximise therapy efficacy, reduce side effects, and improve patient satisfaction by enabling personalised medicine methods.
- **Effective Healthcare Delivery:** By automating data collection, transmission, and analysis, IoMT devices reduce the need for manual intervention, allow healthcare practitioners to make decisions in real time, and streamline healthcare delivery procedures. Shorter wait times, better use of available resources, and an improvement in the general standard of patient care are all results of these efficiency gains.
- **Early illness diagnosis and Prevention:** By continually monitoring physiological parameters and identifying variations from baseline patterns suggestive of possible health risks or anomalies, IoMT devices help in the early diagnosis of health concerns and the start of illness. To slow the course of a disease and improve health outcomes, early identification makes it possible to implement timely therapies, preventative measures, and lifestyle changes.
- **Improved Patient Empowerment and Engagement:** IoMT gives patients the ability to take an active role in managing their own health by giving them access to their data, encouraging self-care and self-monitoring practices, and facilitating communication between patients and healthcare professionals via digital health platforms and remote consultations. IoMT promotes a sense of ownership and accountability for health outcomes, enhances treatment adherence, and facilitates shared decision-making by encouraging patient participation.
- **Healthcare System Optimisation:** By providing insightful information about population health trends, healthcare utilisation patterns, and resource allocation requirements, IoMT data

analytics and predictive modelling capabilities help policymakers and healthcare organisations optimize healthcare delivery, allocate resources effectively, and carry out focused interventions to address common health issues and disparities in communities.

All things considered, IoMT is a revolutionary paradigm shift in the delivery of healthcare, presenting hitherto unseen chances to advance population health management, boost healthcare efficiency, and improve patient outcomes through the smooth integration of digital technologies, data analytics, and medical devices. Its potential to completely transform how healthcare is provided, experienced, and viewed in the contemporary day makes it significant. The desire for remote patient monitoring, the push for healthcare digitalization, and advances in medical technology are driving a rapid expansion in the deployment of Internet of Medical Things (IoMT) devices. This growth is noticeable in several healthcare environments, including as clinics, nursing homes, hospitals, and even patients' homes. The goal for better patient outcomes and care is a major factor driving the introduction of IoMT.

IoMT devices give medical professionals the ability to remotely check on their patients' health in real time, which makes it easier to identify health problems early on, create individualised treatment programmes, and take prompt action. Furthermore, IoMT devices encourage higher engagement and adherence to treatment plans by enabling patients to actively manage their health. Adoption of IoMT brings advantages, but it also presents serious security risks. IoMT devices are becoming more and more appealing targets for cyberattacks and privacy violations as they gather, transfer, and retain sensitive patient data. The increasing number of devices that are networked together, the variety of communication protocols, and the sometimes-inadequate security safeguards that are included into medical device design all contribute to these security concerns. The following are a few of the major security issues with IoMT devices:

- **Data Privacy and Confidentiality:** Medical records, vital signs, and personal identifiers are just a few of the sensitive patient data that IoMT devices gather. Maintaining patient trust and adhering to legal obligations, such as the GDPR (General Data Protection Regulation) in the European Union and the HIPAA (Health Insurance Portability and Accountability Act) in the United States, depends critically on protecting the privacy and confidentiality of this data.
- **Unauthorised Access and Data Breaches:** IoMT devices that have weak authentication procedures or other security flaws may be vulnerable to malevolent actors gaining unauthorised access. Serious dangers to patient safety and healthcare operations can result

from unauthorized access, which can also lead to data breaches, the manipulation of medical records, and even the interruption of medical device performance.

- **Malware and Ransomware Attacks:** IoMT devices are susceptible to ransomware and malware attacks, which can extort sensitive patient data, interrupt healthcare services, and jeopardise device integrity. The reputation and financial viability of healthcare organisations, as well as patient treatment, may suffer greatly because of these attacks.
- **Supply Chain Risks:** Because IoMT devices frequently depend on intricate supply chains with several suppliers and componentry, there is a higher chance that security flaws will be introduced at different points during the device's lifetime. Risks associated with the supply chain, including as phoney parts, faulty firmware, and inadequate security testing, might weaken IoMT devices' overall security posture and jeopardise patient safety.
- **Regulatory Compliance:** When implementing IoMT devices, healthcare institutions have to go by a number of regulations pertaining to patient privacy, data security, and medical device safety. Ensuring IoMT security and regulatory compliance is highly challenging when navigating these regulatory frameworks, such as FDA (Food and Drug Administration) rules for medical devices and industry-specific standards like ISO 27001 for information security management.

A comprehensive strategy that includes organisational rules and procedures, technical protections, continuous security monitoring, and risk management initiatives is needed to address these security issues. To protect patient data and guarantee the integrity and dependability of IoMT devices in the delivery of healthcare, healthcare stakeholders must work together to create strong security plans, put in place efficient security measures, and be alert against new cyber threats. The Internet of Medical Things (IoMT) is introduced in this paper's Section I, which also highlights the technology's importance and uses in contemporary healthcare. A thorough assessment of the literature is provided in Section II, which summarizes recent findings and advancements in the fields of IoMT technology, security issues, and mitigation techniques.

In-depth treatment of security concerns unique to IoMT installations is covered in Section III, which also looks at risks, vulnerabilities, and threats present in IoMT ecosystems. Section IV is devoted to exploring potential avenues for further investigation. The report concludes with a final part that summarises the main conclusions and insights, identifies future research paths and difficulties, and advances IoMT security and resilience in hospital settings.

II. BACKGROUND

Examine existing studies on IoMT security and privacy to understand current knowledge gaps. Gather qualitative insights through interviews and quantitative data from incident reports and surveys. Use thematic analysis to identify patterns and trends in IoMT security and privacy issues. Evaluate potential vulnerabilities and threats to IoMT systems, prioritizing for mitigation. Assess compliance with privacy regulations and analyse implications of IoMT data handling. Assess effectiveness of current security measures and propose enhancements. Summarize findings, offer recommendations for stakeholders, and suggest future research directions. This section presents an overview of the survey conducted in previous years regarding security in the realm of Internet of Medical Things (IoMT).

Year	Author	Security Issues	Suggested Solution
2023	Bhushan	Privacy concerns	Various techniques for Secure data transmission
2023	Ksibi	Cyber Attacks	ML for detecting abnormalities & intrusions
2022	Md. Nazmul Hossen	Data Security in healthcare system	CNN Algorithms and Federated learning
2021	Alexan	User Authentication and Confidentiality	Info security schemes AES-256, RSA, SHA-3
2020	Mohmad. Ayub khan	Cyber-attacks and malware attacks	DNN with Machine learning
2019	Senthil Kumar Mohan	Cloud Security	Security Assessment frameworks
2016	Gope	Real time Security	body sensor network (BSN) technology
2015	S.M. Razaul Islam	Patient data privacy	RSA based authentication protocols
2015	Schurgot	Attacks	Two factor Protocols

Table1. Security Issues in IoMT

III. SECURITY THREATS AND CHALLENGES

The confidentiality, integrity, availability, and safety of patient data as well as device operation are all at danger from a variety of security vulnerabilities that are specific to Internet of Medical Things (IoMT) devices. These dangers fall into several important areas, including:

- **Data Breaches:** When sensitive patient data is stored or sent by IoMT devices, there is an unauthorized access to such data. Vulnerabilities in cloud storage systems, backend servers, or device connection protocols may be exploited by attackers to get personally identifiable information (PII) or medical data. Identity theft, financial fraud, and reputational harm to healthcare organisations are all possible outcomes of data breaches.
- **Unauthorized Access:** When someone enters an IoMT device, network, or data without the required authorization or authentication, it is referred to as unauthorized access. Weak passwords, default credentials, or unprotected network connections may be used to cause this. Unauthorized access puts patient privacy and safety at risk since it can result in unauthorized device control, patient data tampering, and device malfunction.
- **Malware Attacks:** These occur when malicious software is installed on Internet of Medical Things (IoMT) devices with the goal of compromising device integrity, stealing confidential information, or impairing device operation. Via hacked network connections, malicious email attachments, or contaminated software upgrades, malware can enter a system. Ransomware, which encrypts device data for extortion, and botnets, which take over devices for coordinated assaults, are common malware kinds that target IoMT devices.
- **Device Tampering:** This is the act of physically or virtually manipulating Internet of Medical Things (IoMT) devices to change their configurations, change how they behave, or obtain unauthorized access to their functionalities. Attackers can circumvent security measures or insert malicious code by tampering with the firmware of the device, hardware parts, or communication connections [14]. The safety of patients, the accuracy of medical data, and the dependability of device operations can all be jeopardised by device manipulation.
- **Denial of Service (DoS) Attacks:** The goal of DoS attacks is to interfere with or impair the performance of IoMT devices, networks, or services, making them unavailable to authorised users. Devices become unresponsive or inaccessible because of DoS assaults overloading device resources, network bandwidth, or communication channels with excessive traffic or requests. DoS attacks can affect healthcare operations, postpone the administration of

treatment, and interfere with patient monitoring.

- **Privacy Violations:** These occur when private patient data that IoMT devices gather or retain is exposed to third parties without authorization. Insufficient data encryption, unsafe data storage, or unsanctioned data sharing activities can all lead to this. Infractions of privacy regulations may result in penalties for regulatory non-compliance under data protection laws like HIPAA and GDPR, patient humiliation, and diminished patient trust in healthcare providers.
- **Supply Chain Risks:** These risks are related to security flaws that might arise throughout the production, distribution, deployment, and maintenance phases of an IoMT device's lifespan. Attackers may damage the security and integrity of devices by taking advantage of flaws in the supply chain, such as phoney parts, unsecured firmware upgrades, or unreliable suppliers. Risks associated with the supply chain can compromise the IoMT devices' overall security posture and jeopardise patient safety and privacy.
- To handle these security risks and preserve IoMT devices as well as patient information and privacy in healthcare settings, a thorough strategy including technological controls, security best practices, and regulatory compliance procedures is needed. Because of their vital role in the delivery of healthcare and the sensitive nature of the data they manage, Internet of Medical Things (IoMT) devices pose distinct security issues from other IoT devices. Among these difficulties are:
- **Limited Computational Resources:** The processing power, memory, and energy efficiency of many IoMT devices—especially wearable sensors and implanted medical devices—are constrained. Due to these limitations, implementing strong security features like intrusion detection, authentication, and encryption without affecting device performance or battery life is difficult. IoMT devices might therefore be more vulnerable to resource-constrained assaults and security flaws.
- **Various Communication Protocols:** To send health data to electronic health record (EHR) systems, healthcare providers, and other linked devices, IoMT devices frequently rely on a variety of communication protocols and standards. Cellular networks, Bluetooth, Wi-Fi, Zigbee, and specialised communication protocols unique to medical equipment are a few examples of these protocols. Handling the security of several communication channels becomes more complicated and expands the attack surface since every protocol could have different security flaws and setup needs.

- **Regulatory Compliance Issues:** Tight regulations and standards pertaining to patient privacy, data security, and medical device safety apply to IoMT devices. Protecting patient rights and reducing legal and financial risks for healthcare providers require adherence to laws like the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Ensuring regulatory compliance complicates IoMT security initiatives and can need for more funding and knowledge.
- **Heterogeneous Device Ecosystem:** There are many different types of IoMT devices from various manufacturers, and each one has its own security architecture, software, and hardware. It is difficult to standardise security procedures and guarantee device compatibility and interoperability because of this variety. Furthermore, it's possible that outdated IoMT devices have fewer software updates and support or no built-in security protections, which makes them more vulnerable to security flaws and exploits.
- **Interconnectivity and Integration Challenges:** Internet of Medical Things (IoMT) devices frequently communicate with other medical infrastructure and systems, such as hospital networks, electronic health records (EHRs), and outside health apps. To prevent data breaches, data loss, or unauthorised access, integrating IoMT devices into current healthcare IT ecosystems necessitates careful consideration of interoperability, data exchange standards, and security policies. For healthcare organisations, ensuring the safe and smooth integration of IoMT devices with systems presents both logistical and technological obstacles.

A complex strategy that includes technical solutions, legislative frameworks, and stakeholder collaboration is needed to address these particular security concerns. To reduce the risks associated with IoMT devices and protect patient data and privacy, healthcare organisations need to prioritise security from the outset, implement strong encryption and authentication mechanisms, perform regular security assessments and audits, and fund staff training and awareness initiatives. In addition, industry standards organisations and regulatory organisations are essential in developing policies, guidelines, and best practices that support the safe implementation and use of IoMT devices in healthcare environments.

IV. RESEARCH CHALLENGES AND FUTURE DIRECTIONS

The dynamic threat landscape and growing complexity of Internet of Medical Things (IoMT) installations are driving the constant evolution of emerging trends and research initiatives in IoMT security. Key developments and areas for further research include:

- **Machine Learning (ML) and Artificial Intelligence (AI) for Threat Detection and Response**: In IoMT security, threat detection, anomaly detection, and predictive analytics are utilising AI and ML approaches more and more. AI/ML algorithms can proactively identify possible security risks and vulnerabilities by evaluating vast amounts of IoMT data to spot trends, detect irregularities, and make informed decisions. The main goals of this field of research are to create sophisticated AI/ML models specifically for IoMT security, increase threat detection efficiency and accuracy, and incorporate AI/ML-based solutions into IoMT security frameworks.
- **Blockchain Technology for Data Integrity and Access Control:** In IoMT implementations, blockchain technology presents potential ways to improve data integrity, transparency, and access control. Blockchain technology can assist in ensuring the integrity and provenance of medical data gathered and exchanged by Internet of Medical Things (IoMT) devices by offering a distributed, immutable ledger for documenting transactions and data transfers. Blockchain technology is being investigated for its potential use in IoMT ecosystems for patient consent management, secure health data exchange, and auditability.
- **Methods for Preserving Health Data Privacy:** In IoMT security research, privacy-preserving methods including federated learning, homomorphic encryption, and differential privacy are becoming more popular to solve privacy issues related to the gathering, storing, and sharing of private health information. By using these methods, healthcare institutions may study and gain knowledge from IoMT data while protecting patient confidentiality and privacy. The main goals of research are to create scalable and effective privacy-preserving systems that are suited for Internet of Medical Things applications and regulatory compliance.
- **Secure Device Authentication and Access Control:** To stop illegal access to IoMT devices and networks, secure device authentication and access control techniques are crucial. Researchers are investigating new authentication techniques including biometrics, multifactor authentication, and physical unclonable functionalities (PUFs) to improve IoMT device security and reduce the possibility of stolen credentials and unapproved device modification.

Furthermore, studies are concentrating on dynamic privilege management and adaptive access control policies to impose fine-grained access controls according to user roles and contextual variables.

- **Threat information Sharing and Collaboration:** To help manufacturers, cybersecurity researchers, and healthcare organisations work together to discover, analyse, and mitigate IoMT security threats, collaborative threat information sharing initiatives are starting to take shape. The goal of research is to provide standardised frameworks, protocols, and platforms that will allow information sharing, facilitate collective protection against cyber-attacks targeting IoMT installations, and share threat intelligence related to IoMT.
- **Regulatory Compliance and Certification Programmes:** As cybersecurity in healthcare becomes more and more scrutinised by regulators, there is an increased focus on IoMT security-specific regulatory compliance and certification programmes. To evaluate and verify IoMT device security postures and guarantee regulatory compliance, research is investigating the creation of uniform security frameworks, guidelines, and certification standards. Through encouraging interoperability and innovation, these projects seek to improve IoMT ecosystems' openness, accountability, and trustworthiness.

IoMT security research is generally progressing quickly due to the necessity of addressing new and emerging cyber threats, protecting patient privacy and data integrity, and encouraging the broad use of IoMT technology in healthcare. Researchers are working to provide scalable and reliable security solutions that are specific to the difficulties encountered in IoMT deployments. By doing so, they want to improve the dependability and resilience of IoMT ecosystems. They do this by using cutting-edge technology and cooperative methods.

V. CONCLUSION

IoMT devices manage sensitive patient health data and are integrated into vital healthcare systems, security issues present serious concerns. Data breaches, illegal access, malware attacks, Internet of Things botnets, physical security concerns, obsolete software vulnerabilities, and interoperability issues are some of these hazards. Robust authentication, encryption, software upgrades, network segmentation, intrusion detection, and compliance with industry rules are all necessary to mitigate these dangers. To protect patient privacy and data integrity and encourage the wider deployment of IoMT devices, security problems must be addressed. Establishing trust among stakeholders, guaranteeing adherence to rules, safeguarding patient confidentiality, upholding data correctness, and facilitating continuous care delivery are all dependent on this, and they eventually contribute to better healthcare results.

VI. REFERENCES

I. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. -S. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey," IEEE Access, vol. 3, pp. 678-708, 2015.

II. G. Zachos, G. Mantas, I. Essop, K. Porfyrakis, J. M. C. S. Bastos and J. Rodriguez, "An IoT/IoMT Security Testbed for Anomaly-based Intrusion Detection Systems," 2023 IFIP Networking Conference (IFIP Networking), Barcelona, Spain, pp. 1-6, 2023.

III. H. Tao, M. Z. A. Bhuiyan, A. N. Abdalla, M. M. Hassan, J. M. Zain and T. Hayajneh, "Secured Data Collection with Hardware-Based Ciphers for IoT-Based Healthcare," IEEE Internet of Things Journal, vol. 6, no. 1, pp. 410-420, Feb. 2019.

IV. Bhushan, B.; Kumar, A.; Agarwal, A.K.; Kumar, A.; Bhattacharya, P.; Kumar, A. "Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends". Sustainability, 15, 617, 2015.

V. S. Ksibi, F. Jaidi and A. Bouhoula, "IoMT Security Model based on Machine Learning and Risk Assessment Techniques," 2023 International Wireless Communications and Mobile Computing (IWCMC), Marrakesh, Morocco, pp. 614-619, 2023.

VI. M. N. Hossen, K. Ahmed, F. M. Bui and L. Chen, "FedRSMax: An Effective Aggregation Technique for Federated Learning with Medical Images," 2023 IEEE Canadian Conference on Electrical and Computer Engineering (CCECE), Regina, SK, Canada, pp. 229-234, 2023.

VII. W. Alexan, A. Ashraf, E. Mamdouh, S. Mohamed and M. Moustafa, "IoMT Security: SHA3-512, AES-256, RSA and LSB Steganography," 2021 8th NAFOSTED Conference on Information and Computer Science (NICS), Hanoi, Vietnam, pp. 177-181, 2021.

VIII. M. A. Khan, "An IoT Framework for Heart Disease Prediction Based on MDCNN Classifier," IEEE Access, vol. 8, pp. 34717-34727, 2020.

IX. Bharati, S., Podder, P., Mondal, M.R.H., Paul, P.K. "Applications and Challenges of Cloud Integrated IoMT". In: Hassanien, A.E., Khamparia, A., Gupta, D., Shankar, K., Slowik, A. (eds) "Cognitive Internet of Medical Things for Smart Healthcare. Studies in Systems, Decision and Control", vol 311. Springer, 2021.

X. G. Hatzivasilis, O. Soultatos, S. Ioannidis, C. Verikoukis, G. Demetriou and C. Tsatsoulis, "Review of Security and Privacy for the Internet of Medical Things (IoMT)," 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), Santorini, Greece, pp. 457-464, 2019.

XI. M. R. Schurgot, D. A. Shinberg and L. G. Greenwald, "Experiments with security and privacy in IoT networks," IEEE 16th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Boston, MA, USA, pp. 1-6, 2015.

XII. Jean-Paul A. Yaacoub, Mohamad Noura, Hassan N. Noura, Ola Salman, Elias Yaacoub, Raphaël Couturier, Ali Chehab, Securing internet of medical things systems: Limitations, issues and recommendations, Future Generation Computer Systems, Volume 105, Pages 581-606, 2020.

XIII. Mireya Lucia Hernandez-Jaimes, Alfonso Martinez-Cruz, Kelsey Alejandra Ramírez-Gutiérrez, Claudia Feregrino-Uribe, "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets, and Cloud–Fog–Edge architectures",Internet of Things, Volume 23, 2023, 100887.

XIV. R. Tikkha and S. Sharma, "Cryptographic Measures in IoMT: Security Threats and Measurement," 13th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, pp. 1-8, 2022.

XVI. Nayak, J., Meher, S.K., Souri, A. et al. "Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection." J Supercomput 78, 14866–14891, 2022.

XVII. Yousefi and S. M. Jameii, "Improving the security of internet of things using encryption algorithms," 2017 International Conference on IoT and Application (ICIOT), Nagapattinam, India, pp. 1-5, 2015.

XVI. Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1636-1675, 2019.

XVIII. Alsemmeari, R.A.; Dahab, M.Y.; Alsulami, A.A.; Alturki, B.; Algarni, S. "Resilient Security Framework Using TNN and Blockchain for IoMT". Electronics, 12, 2252, 2023.