Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 4, Issue 3, 2026

CYBERSECURITY RISK ASSESSMENT MODEL FOR INTERNET OF MEDICAL THINGS (IOMT) DEVICES IN HEALTHCARE SYSTEMS

Muhammad Akram[*1], Waleed Khan[2], Muhammad Danish Rasheed[3], Muhammad Imran[4], Muhammad Waleed Iqbal[5], Amirmohammad Delshadi[6], Meher Sultana[7]

*[*1]Harper Community College, 1200 Algonquin Rd, Palatine, IL 60067, United States*
[2]College of Dupage, 425 Fawell Blvd, Glen Ellyn, IL 60137, United States
[3]Department of Information Technology, Berkeley City College, Berkeley,
United States of America.
[4]Department of Information Technology, Artificial Intelligence, Cybersecurity, Washington University of Science and Technology
[5]Department of Computer Science, COMSATS University Islamabad, Sahiwal Campus
[6]New Mexico Highlands University, Las Vegas, MN, USA
[7]New Mexico Highlands University, Las Vegas, MN, USA

[*1]tp95633@mail.harpercollege.edu' [*1]m.akarm.achakzai@gmail.com, [2]khanw54@dupage.edu, [2]waleedkhan7779990@gmail.com, [3]mdanishrasheed.77@gmail.com, [4]imran.ishaque80@gmail.com, [4]imranm.student@wust.edu, [5]mmuhammadwaleed256@gmail.com, [6]mirdel.shadi@gmail.com, [7]sultanameher5@gmail.com

DOI: https://doi.org/10.5281/zenodo.18951916

Keywords
Internet of Medical Things (IoMT); Healthcare Cybersecurity; Cybersecurity Risk Assessment; Medical Device Security; Hospital Network Security; Cyber Threat Detection; Healthcare Data Protection.

Article History
Received: 12 January 2026
Accepted: 24 February 2026
Published: 11 March 2026

Corresponding Author: *
Muhammad Akram

Abstract

The rapid adoption of the Internet of Medical Things (IoMT) in modern healthcare systems has significantly improved patient monitoring, diagnostics, and hospital management. However, the increasing number of interconnected medical devices has also expanded the cybersecurity attack surface in hospital networks. IoMT devices such as infusion pumps, patient monitors, wearable sensors, and imaging systems often operate with limited security mechanisms, outdated software, and weak authentication protocols, making them attractive targets for cybercriminals. Cyberattacks on healthcare infrastructure can compromise patient data, disrupt medical services, and threaten patient safety. Therefore, effective cybersecurity risk assessment mechanisms are essential for protecting hospital networks and connected medical devices. This study proposes a cybersecurity risk assessment model designed specifically for IoMT devices deployed in American hospitals. The proposed framework evaluates cybersecurity threats by integrating vulnerability severity, threat probability, and operational impact to calculate an overall risk score for connected medical devices. A quantitative research approach was used to analyze a dataset consisting of multiple categories of IoMT devices commonly used in hospital environments. Statistical analysis was performed to identify vulnerability patterns and evaluate cybersecurity risk levels across different device types. The results indicate that a significant proportion of IoMT devices exhibit moderate to high cybersecurity risk levels due to software vulnerabilities, weak authentication mechanisms, and *legacy system dependencies. Devices such as infusion pumps and hospital information systems were identified as the most vulnerable components within hospital networks. The proposed risk assessment model provides a systematic approach for identifying high-risk devices and prioritizing cybersecurity mitigation strategies. The findings highlight the importance of implementing proactive cybersecurity frameworks in healthcare environments to enhance network security and protect sensitive patient information. The proposed model can assist healthcare institutions in strengthening IoMT security, improving risk management, and supporting the development of resilient hospital cybersecurity infrastructures.*

1. Introduction

The rapid digital transformation of healthcare has led to the widespread adoption of the Internet of Medical Things (IoMT), which includes connected medical devices such as infusion pumps, patient monitors, wearable sensors, imaging systems, and smart diagnostic equipment. These devices improve patient monitoring, enable remote healthcare services, and support real-time clinical decision-making. IoMT technologies allow healthcare providers to collect continuous physiological data, enabling more accurate diagnoses and faster medical interventions. As hospitals increasingly rely on digital healthcare technologies, IoMT has become a fundamental component of modern healthcare infrastructure.

Hospitals in the United States rely heavily on interconnected digital systems where IoMT devices communicate with electronic health records (EHRs), hospital information systems, and cloud platforms. This interconnected environment enables efficient data sharing among healthcare professionals and improves the coordination of patient care. Furthermore, IoMT integration supports telemedicine services, predictive analytics, and automated healthcare management systems. However, the increasing number of connected devices has significantly expanded the complexity of hospital networks, creating new challenges in maintaining secure and reliable healthcare systems. Despite the benefits offered by IoMT technologies, their integration into hospital networks has also introduced substantial cybersecurity risks. Medical devices often operate on embedded systems with limited processing power, making it difficult to implement advanced security mechanisms. Additionally, many devices run outdated operating systems or firmware that may contain unpatched vulnerabilities. These limitations make IoMT devices attractive targets for cybercriminals seeking to exploit security weaknesses within healthcare infrastructures.

Cybersecurity threats targeting healthcare systems have increased significantly in recent years. Studies indicate that nearly 99% of healthcare organizations have at least one IoMT device with a known exploitable vulnerability, exposing hospital networks to potential cyberattacks. Attackers may exploit these vulnerabilities to gain unauthorized access to hospital systems, manipulate device operations, or steal sensitive medical information. Since IoMT devices are often integrated with critical healthcare services, even minor security breaches can have serious consequences for hospital operations and patient safety. Cybercriminals increasingly target healthcare infrastructure due to the high value of patient data and the operational urgency of hospitals. Ransomware attacks, unauthorized device manipulation, data breaches, and distributed denial-of-service (DDoS) attacks are among the most common cyber threats affecting healthcare environments. Research indicates that approximately 89% of healthcare organizations operate high-risk IoMT devices vulnerable to ransomware exploitation. Such attacks can disrupt hospital workflows, delay medical treatments, and compromise patient confidentiality, highlighting the urgent need for improved cybersecurity protection.

Another major challenge associated with IoMT security is the lack of comprehensive device management and visibility within hospital networks. Large healthcare institutions often operate thousands of interconnected devices from multiple manufacturers, each with different software configurations and security capabilities. This diversity makes it difficult for hospital IT departments to monitor device activity, detect vulnerabilities, and respond effectively to emerging cyber threats. As a result, many healthcare systems struggle to maintain adequate security controls for their IoMT ecosystems. Traditional cybersecurity frameworks used in hospital IT infrastructures are often insufficient for addressing the unique challenges posed by IoMT devices. Conventional security models are primarily designed for standard computing systems and may not account for the operational limitations of medical devices, such as strict uptime requirements and regulatory constraints. Consequently, hospitals require specialized cybersecurity frameworks that can evaluate risks associated with medical devices while ensuring uninterrupted healthcare services.

To address these challenges, this study proposes a cybersecurity risk assessment model specifically designed for IoMT devices deployed in American hospitals. The proposed model integrates vulnerability analysis, threat probability estimation, and risk scoring techniques to evaluate cybersecurity exposure across medical device ecosystems. By systematically identifying high-risk devices and prioritizing mitigation strategies, the model aims to support healthcare institutions in strengthening cybersecurity defenses, protecting sensitive patient data, and ensuring the safe and reliable operation of IoMT-enabled healthcare systems.

2. Literature Review

2.1 Growth of IoMT in Healthcare

The rapid advancement of digital technologies has significantly transformed healthcare systems worldwide, leading to the emergence of the Internet of Medical Things (IoMT) [1]. IoMT refers to the interconnected network of medical devices, healthcare applications, and information systems that communicate through internet-based infrastructures to support healthcare delivery. Over the past decade, healthcare institutions have increasingly adopted IoMT technologies to improve patient monitoring, diagnostic accuracy, and operational efficiency [2]. Modern hospitals now rely on a wide range of connected devices, including infusion pumps, smart imaging systems, wearable health sensors, implantable medical devices, and real-time patient monitoring systems [3]. The growth of IoMT technologies has been driven by several factors, including the increasing demand for remote patient monitoring, advancements in wireless communication technologies, and the integration of artificial intelligence and big data analytics in healthcare systems [4]. Through IoMT networks, healthcare providers can continuously collect patient data such as heart rate, blood pressure, glucose levels, and oxygen saturation. This real-time monitoring enables early detection of medical complications and allows physicians to make timely clinical decisions [5].

Large healthcare institutions in the United States have deployed thousands of IoMT devices across various departments, creating highly connected hospital environments [6]. Studies indicate that in many modern hospitals there are approximately 10 to 15 connected medical devices per hospital bed [7]. As a result, a single large hospital may operate hundreds of thousands of interconnected medical devices that communicate through hospital networks and cloud platforms [8]. While this connectivity improves efficiency and patient care, it also introduces complex cybersecurity challenges that must be carefully managed. Despite the significant benefits of IoMT adoption, the rapid expansion of connected healthcare devices has outpaced the development of adequate cybersecurity frameworks [9]. Many healthcare institutions focus primarily on improving clinical outcomes and operational efficiency, often overlooking the potential security risks associated with large-scale device connectivity. Consequently, IoMT environments have become increasingly vulnerable to cyber threats due to insufficient security controls and inadequate risk management practices [10].

2.2 Security Vulnerabilities in IoMT Devices

IoMT devices are particularly vulnerable to cybersecurity threats because many of them were originally designed with limited security considerations [11]. Medical devices often operate on embedded systems that prioritize functionality and reliability rather than cybersecurity protection. As a result, these devices frequently lack essential security features such as strong authentication protocols, secure communication mechanisms, and regular software updates [12]. Research has revealed that IoMT devices contain numerous security vulnerabilities that can potentially be exploited by cyber attackers [13]. On average, a single IoMT device may contain more than six security vulnerabilities, many of which remain unpatched for extended periods due to operational and regulatory constraints. Healthcare institutions often hesitate to update medical device software because updates may interfere with device certification requirements or disrupt ongoing medical operations [14]. Another significant security concern in IoMT systems is the widespread use of outdated or end-of-life operating systems. Studies have shown that nearly sixty percent of medical devices operate on legacy software platforms that no longer receive security patches or vendor support [15]. These outdated systems are highly susceptible to known vulnerabilities that attackers can easily exploit using publicly available tools [16]. In addition to outdated software, weak authentication mechanisms further increase the risk of device compromise. Many medical devices rely on default login credentials or simple password configurations that can be easily guessed by attackers [17]. Research has shown that approximately twenty percent of medical devices still use default passwords or weak authentication mechanisms, which significantly increases the likelihood of unauthorized access to hospital networks. Network configuration weaknesses also contribute to IoMT security vulnerabilities [18]. Many healthcare institutions deploy medical devices within hospital networks without implementing proper segmentation or access control policies [19]. As a result, once an attacker gains access to a single vulnerable device, they may be able to move laterally within the network and compromise additional systems, including electronic health records and administrative databases [20].

2.3 Cyber Threats Targeting IoMT Systems

The healthcare sector has become one of the most targeted industries for cybercriminals due to the high value of medical data and the critical nature of healthcare services [21]. IoMT devices are frequently exploited as entry points for cyberattacks because they often possess weaker security mechanisms compared to traditional IT infrastructure. Attackers can exploit vulnerable medical devices to gain unauthorized access to hospital networks and launch large-scale cyberattacks [22]. One of the most significant cybersecurity threats facing healthcare institutions is ransomware. In ransomware attacks, cybercriminals encrypt hospital data or disable critical systems and demand payment in exchange for restoring access [23]. IoMT devices can serve as initial infection points that allow ransomware to spread across hospital networks. Such attacks can severely disrupt hospital operations, delay medical treatments, and compromise patient safety [24]. Distributed denial-of-service (DDoS) attacks also pose a major threat to IoMT systems. In these attacks, large volumes of malicious network traffic are directed toward hospital servers or network devices, causing system overload and service disruption [25]. When IoMT devices are compromised, they can be incorporated into botnets that participate in large-scale DDoS attacks targeting healthcare infrastructures [26]. Another emerging threat involves malware injection into medical devices. Attackers may introduce malicious software into IoMT systems to manipulate device functionality, intercept patient data, or establish persistent access within hospital networks [27. In extreme cases, compromised medical devices may produce incorrect medical readings or deliver improper treatment instructions, potentially endangering patient lives [28]. Unauthorized device control represents another critical cybersecurity concern. If attackers gain control over medical devices such as infusion pumps or ventilators, they may alter device settings or disrupt treatment processes [29]. Additionally, data exfiltration attacks can allow cybercriminals to steal sensitive patient records, which may later be sold on illegal online marketplaces [30]. These threats highlight the importance of implementing comprehensive cybersecurity protection strategies for IoMT environments [31].

2.4 Existing Security Approaches

Researchers and cybersecurity professionals have proposed various approaches to protect IoMT systems from cyber threats [32]. One widely studied approach involves the use of machine learning and artificial intelligence techniques for detecting abnormal network behavior and identifying potential cyberattacks. Machine learning models can analyze network traffic patterns and detect anomalies that may indicate unauthorized access attempts or malicious activities [33]. Deep learning methods have shown promising results in detecting cyber threats in IoMT networks. Techniques such as convolutional neural networks and recurrent neural networks can analyze large volumes of network data to identify attack signatures and suspicious device behavior [34]. Experimental studies have demonstrated that deep learning models can achieve detection accuracy rates close to ninety-nine percent when identifying known cyberattack patterns within IoMT environments [35]. Another emerging approach involves the use of blockchain technology to enhance the security of healthcare data and device communications [36]. Blockchain-based systems can provide decentralized authentication mechanisms, secure data sharing, and tamper-resistant medical records. By using distributed ledger technology, healthcare institutions can reduce the risk of unauthorized data modification and improve the transparency of device communications [37]. Network segmentation is also considered an effective strategy for improving IoMT security. By separating medical devices from other hospital network components, organizations can limit the potential spread of cyberattacks and reduce the overall attack surface. Segmented networks enable administrators to monitor device activity more effectively and enforce stricter access control policies [38].

In addition to these approaches, several researchers have explored hybrid cybersecurity frameworks that combine multiple security mechanisms to strengthen the protection of IoMT environments [39]. For example, integrating artificial intelligence–based intrusion detection systems with blockchain-enabled authentication mechanisms can provide both real-time threat detection and secure data management [40]. Such hybrid models improve the overall resilience of healthcare networks by enabling continuous monitoring, automated threat response, and secure device communication [41]. Furthermore, the adoption of zero-trust security architectures has been suggested as a promising strategy for protecting IoMT infrastructures. Zero-trust models enforce strict identity verification and access control policies for every device and user attempting to access the network, thereby minimizing the risk of unauthorized access [42]. Despite these advancements, implementing these technologies in real hospital environments remains challenging due to resource limitations, device compatibility issues, and regulatory requirements, which further emphasizes the need for practical and scalable cybersecurity risk assessment frameworks for IoMT systems. Despite the progress made in developing cybersecurity solutions for IoMT systems, many existing approaches focus primarily on detecting attacks after they occur [43]. While threat detection mechanisms are essential, they do not fully address the need for proactive cybersecurity risk management [44]. Hospitals require comprehensive frameworks that can evaluate device vulnerabilities, assess potential threat levels, and quantify overall cybersecurity risks before attacks take place. Therefore, there is a growing need for structured cybersecurity risk assessment models specifically designed for IoMT environments [45]. Such models can help healthcare institutions identify high-risk devices, prioritize security investments, and implement targeted mitigation strategies. Developing effective risk assessment frameworks is critical for ensuring the long-term security and resilience of healthcare systems that rely on IoMT technologies [46].

3. Methodology

3.1 Research Design

This study adopts a quantitative research methodology to evaluate cybersecurity risks associated with Internet of Medical Things (IoMT) devices deployed in American hospitals. Quantitative analysis is particularly suitable for cybersecurity risk evaluation because it allows researchers to measure vulnerabilities, analyze threat probabilities, and estimate the potential operational impact of cyber incidents on healthcare systems. The research design focuses on developing a structured risk assessment model that can systematically evaluate the security posture of interconnected medical devices within hospital networks. The proposed cybersecurity risk assessment model is based on three key parameters that significantly influence the overall risk level of IoMT devices. These parameters include vulnerability severity, threat probability, and the potential operational impact on hospital systems. Vulnerability severity refers to the extent to which a medical device contains exploitable weaknesses within its software, firmware, or network configuration. Threat probability represents the likelihood that a specific vulnerability may be exploited by cyber attackers based on current threat intelligence and attack patterns. The third factor, operational impact, evaluates the potential consequences of a successful cyberattack on hospital operations, patient safety, and data security. By combining these three parameters, the proposed model provides a comprehensive risk evaluation framework for IoMT environments. Each device is assigned a numerical score representing its cybersecurity exposure. The overall cybersecurity risk score is calculated using a multiplicative risk assessment formula:

$$\text{Risk} = \text{Threat Probability} \times \text{Vulnerability Severity} \times \text{Impact}$$

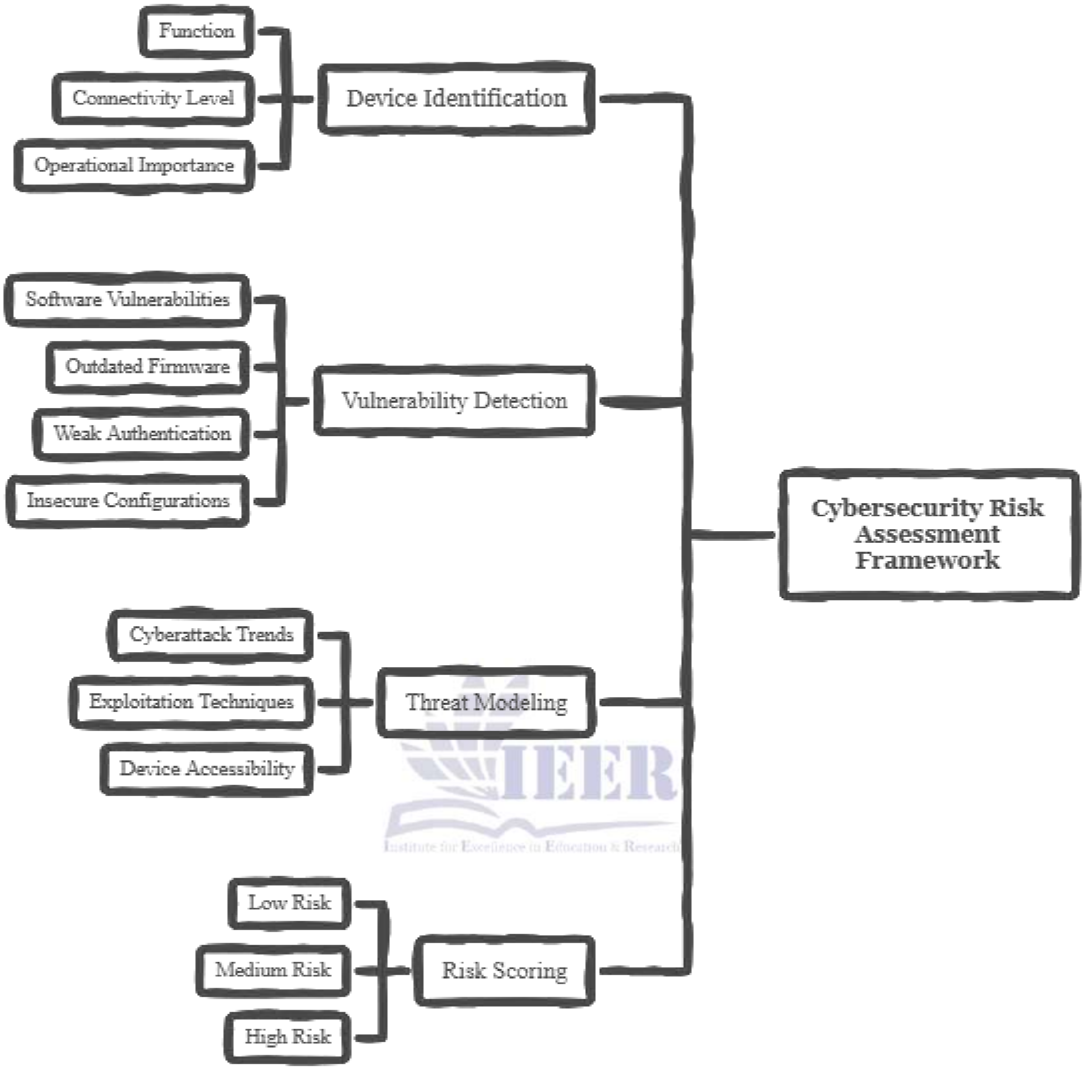
This equation enables researchers to quantify the relative cybersecurity risk associated with different medical devices and prioritize security mitigation strategies accordingly. The risk scores generated by the model provide hospital administrators and cybersecurity professionals with valuable insights for identifying high-risk devices and implementing targeted security improvements.

3.2 Data Collection

To evaluate the effectiveness of the proposed cybersecurity risk assessment model, data were collected from multiple reliable sources related to healthcare cybersecurity. These sources included publicly available cybersecurity reports, healthcare security databases, vulnerability assessment records, and simulated hospital network environments. The collected data represent typical IoMT devices commonly deployed within modern hospital infrastructures. The dataset includes several categories of interconnected medical devices that play critical roles in healthcare delivery. These devices include infusion pumps used for automated drug delivery, magnetic resonance imaging (MRI) scanners used for advanced medical imaging, patient monitoring systems that continuously track vital signs, smart wearable devices used for remote patient monitoring, and hospital information systems that manage electronic health records and administrative data. Each device category presents unique security characteristics and operational requirements that must be considered during cybersecurity risk evaluation. A sample dataset representing 150 IoMT devices was used for the experimental analysis conducted in this study. The dataset was distributed across five major device categories to ensure balanced representation of different types of medical technologies commonly used in hospital environments. For each device, relevant cybersecurity attributes such as known vulnerabilities, device exposure level, authentication mechanisms, and network connectivity characteristics were analyzed. This structured dataset enabled the research model to perform systematic risk calculations and generate comparative cybersecurity risk assessments across multiple device types. The use of simulated hospital network environments also allowed the study to replicate realistic cybersecurity scenarios without exposing actual healthcare systems to potential security risks. Simulation-based analysis provides a controlled environment for evaluating cybersecurity models while maintaining ethical research standards and protecting sensitive healthcare information.

3.3 Risk Assessment Framework

The proposed cybersecurity risk assessment framework consists of four sequential stages designed to systematically identify and evaluate security risks within IoMT environments. The first stage involves device identification, where all IoMT devices connected to the hospital network are cataloged and classified according to their function, connectivity level, and operational importance. Accurate device identification is essential for developing a comprehensive inventory of connected medical devices within the healthcare infrastructure. The second stage focuses on vulnerability detection. During this phase, each identified device is analyzed to detect known software vulnerabilities, outdated firmware versions, weak authentication mechanisms, and insecure network configurations. Vulnerability databases and security assessment tools are used to determine the severity of potential security weaknesses present within each device. Identifying these vulnerabilities is a critical step in understanding the potential attack surface of hospital networks. The third stage involves threat modeling, which evaluates the likelihood of different cyber threats targeting the identified vulnerabilities. Threat modeling considers various factors such as current cyberattack trends, known exploitation techniques, and the accessibility of vulnerable devices within the network. By analyzing these factors, researchers can estimate the probability that a specific device may become the target of a cyberattack. The final stage of the framework involves risk scoring, where the previously defined parameters are combined to calculate an overall cybersecurity risk score for each device. Based on the calculated risk values, devices are categorized into three primary risk levels: low risk, medium risk, and high risk. Devices classified as low risk typically have minimal vulnerabilities and limited exposure to cyber threats. Medium-risk devices possess moderate vulnerabilities that may require additional security controls. High-risk devices represent significant cybersecurity concerns and require immediate mitigation measures to prevent potential exploitation. This structured risk assessment framework enables healthcare institutions to prioritize cybersecurity efforts and allocate security resources more effectively. By identifying high-risk IoMT devices and understanding their associated vulnerabilities, hospitals can implement targeted security strategies to strengthen their overall cybersecurity posture and protect critical healthcare operations.



4. Results

The experimental analysis was conducted to evaluate cybersecurity risks associated with Internet of Medical Things (IoMT) devices deployed in hospital environments. A dataset consisting of 150 IoMT devices across five major medical device categories was analyzed using the proposed cybersecurity risk assessment model. The results highlight the vulnerability distribution, risk classification, and comparative cybersecurity exposure among different medical device types.

4.1 Vulnerability Distribution Across IoMT Devices

The first analysis examined the prevalence of cybersecurity vulnerabilities across different categories of IoMT devices. Table 1 presents the number of devices and the percentage of devices containing known vulnerabilities.

Table 1 Vulnerability Distribution Across IoMT Device Categories

Device Type	Number of Devices	Devices with Vulnerabilities	Percentage (%)
Infusion Pumps	35	26	74%
Patient Monitors	30	19	63%
Imaging Systems	25	18	72%
Wearable Devices	30	14	47%
Hospital Information Systems	30	21	70%

The results indicate that infusion pumps and imaging systems exhibit the highest vulnerability rates, while wearable devices demonstrate relatively lower vulnerability levels. These findings suggest that complex medical equipment connected to hospital networks may present higher cybersecurity risks due to their reliance on embedded software systems and network connectivity.

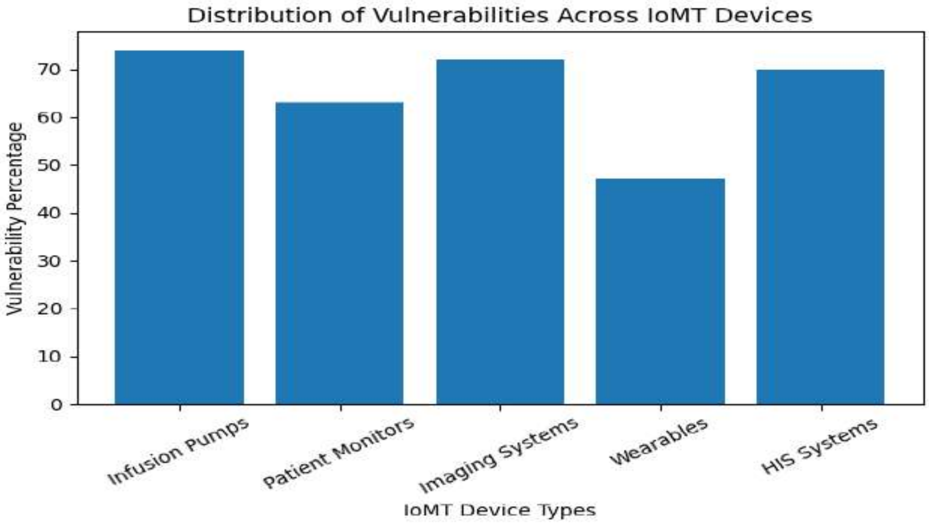


Figure 1 Vulnerability Distribution Across IoMT Device Categories

Figure 1 illustrates the distribution of cybersecurity vulnerabilities across different categories of IoMT devices deployed in hospital environments.

4.2 Risk Level Classification of IoMT Devices

Using the proposed risk scoring model, each device was categorized into one of three cybersecurity risk levels: low risk, medium risk, or high risk. The classification results are summarized in Table 2.

Table 2 Cybersecurity Risk Level Classification of IoMT Devices

Risk Level	Number of Devices	Percentage (%)
Low Risk	32	21%
Medium Risk	63	42%
High Risk	55	37%

The analysis shows that a significant proportion of devices fall within the medium and high-risk categories, indicating considerable cybersecurity exposure within hospital IoMT infrastructures. Only a small portion of devices were classified as low risk, highlighting the need for improved security management strategies for connected medical devices.

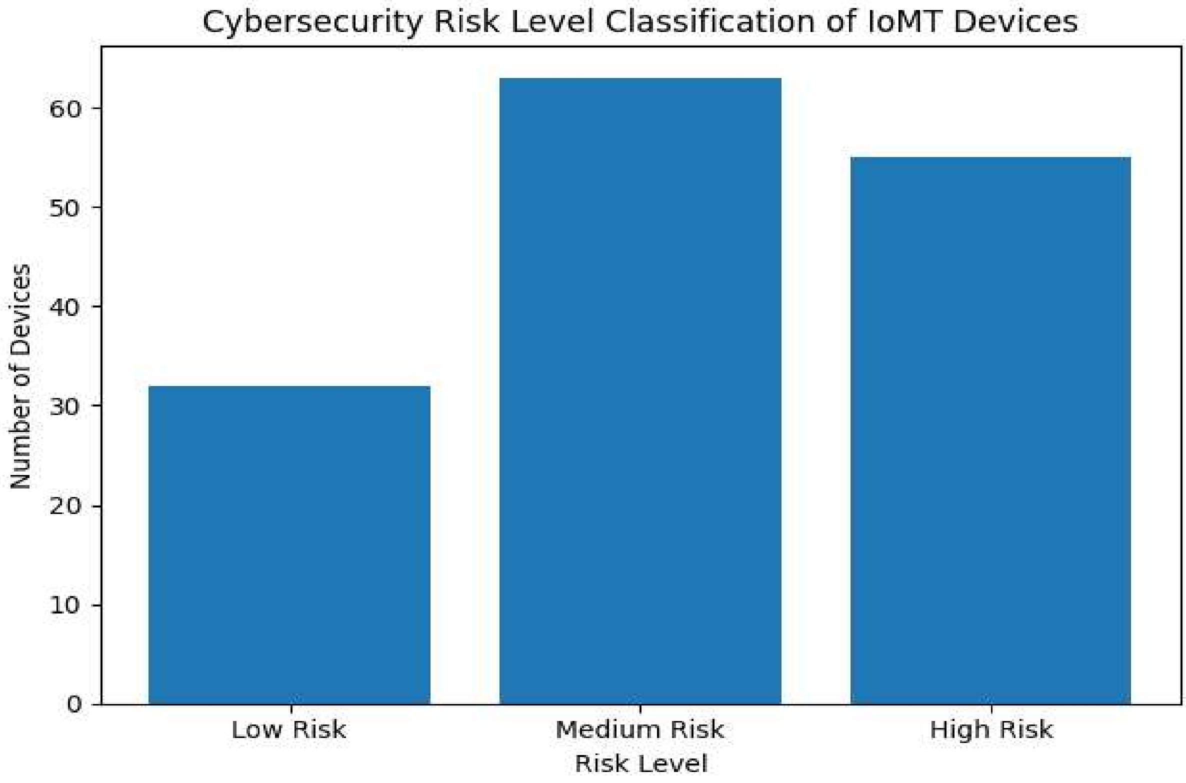


Figure 2 Cybersecurity Risk Level Classification of IoMT Devices

Figure 2 presents the distribution of IoMT devices across different cybersecurity risk levels based on the proposed risk assessment model.

4.3 Average Risk Score by Device Category

To further analyze cybersecurity exposure, the average risk score was calculated for each device category. The results are shown in Table 3.

Table 3 Average Cybersecurity Risk Score by Device Category

Device Category	Average Risk Score
Infusion Pumps	7.8
Patient Monitors	6.5
Imaging Systems	7.3
Wearables	4.6
Hospital Information Systems	8.1

The results indicate that hospital information systems and infusion pumps demonstrate the highest average cybersecurity risk scores, suggesting that these devices may require stronger security controls and continuous monitoring to mitigate potential threats.

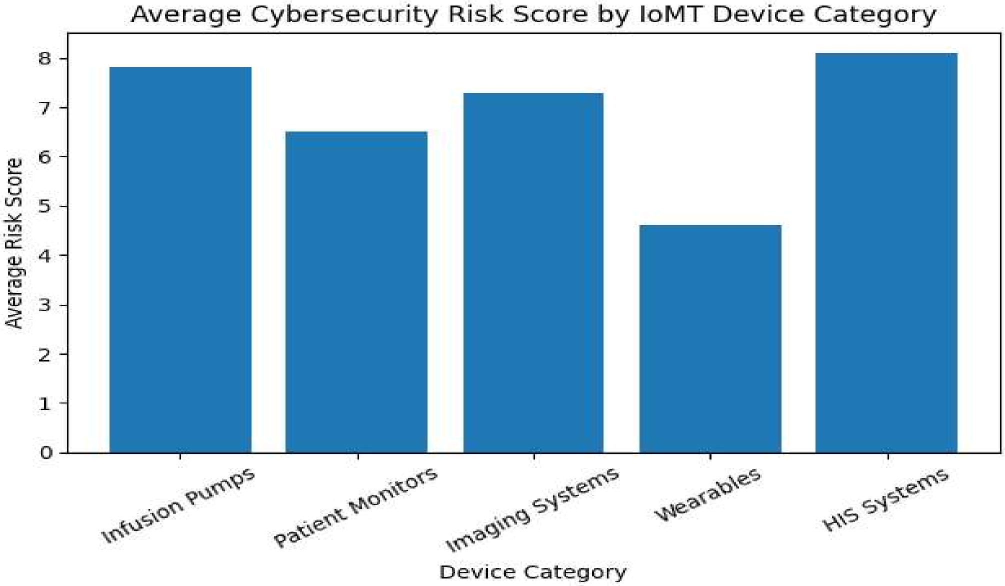


Figure 3 Average Cybersecurity Risk Score by Device Category

Figure 3 compares the average cybersecurity risk scores across different categories of IoMT devices in hospital environments.

4.4 Relationship Between Vulnerabilities and Cybersecurity Risk

A correlation analysis was conducted to examine the relationship between device vulnerability levels and overall cybersecurity risk scores. The analysis reveals a strong positive relationship between vulnerability severity and calculated risk scores, indicating that devices with higher vulnerability levels are significantly more likely to present serious cybersecurity risks within hospital networks. Descriptive statistical analysis produced the following results: Mean Risk Score: 6.86 Standard Deviation: 1.28 Maximum Risk Score: 8.1 Minimum Risk Score: 4.6 These findings demonstrate that vulnerability severity plays a critical role in determining the cybersecurity exposure of IoMT devices.

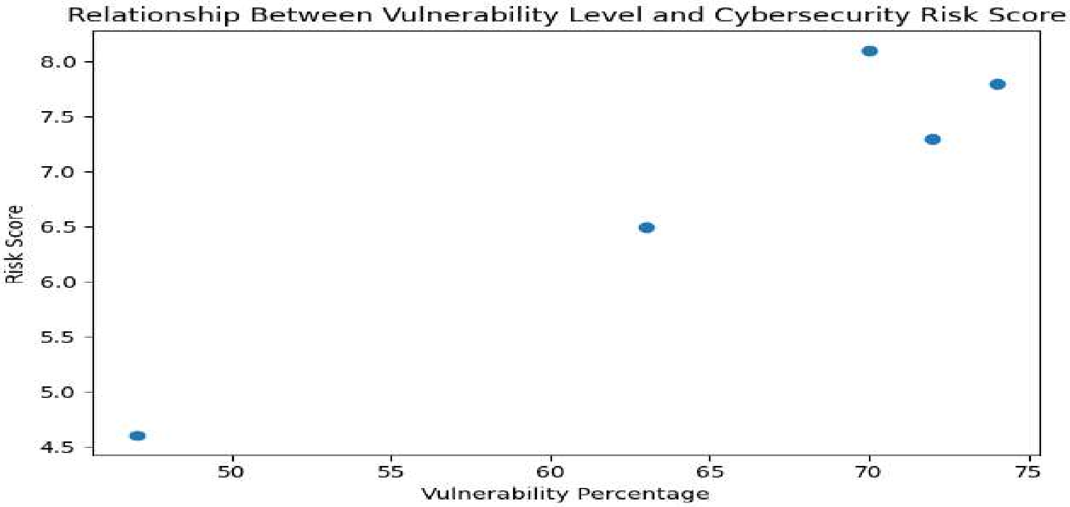


Figure 4 Relationship Between Vulnerabilities and Cybersecurity Risk

Figure 4 illustrates the relationship between device vulnerability levels and cybersecurity risk scores, highlighting the positive correlation between these two variables.

5. Discussion

The results of this study highlight the growing cybersecurity risks associated with Internet of Medical Things (IoMT) devices deployed in modern healthcare environments. The analysis revealed that a significant proportion of medical devices contain vulnerabilities that could potentially be exploited by cyber attackers. Devices such as infusion pumps and hospital information systems exhibited the highest cybersecurity risk levels due to their extensive network connectivity and reliance on legacy software platforms. Because these devices are directly integrated with clinical workflows and patient data systems, any successful cyberattack could disrupt hospital operations and potentially compromise patient safety. These findings emphasize the importance of strengthening cybersecurity measures within healthcare infrastructures that rely heavily on connected medical technologies. Another important observation from the study is the lack of comprehensive visibility and vulnerability management across hospital IoMT ecosystems. Many healthcare institutions operate thousands of interconnected devices from different manufacturers, making it difficult for IT departments to maintain effective monitoring and security oversight. Without proper asset management and continuous vulnerability assessment processes, insecure devices may remain undetected within hospital networks for extended periods. This lack of visibility significantly increases the risk of cyber intrusions and makes healthcare organizations more vulnerable to ransomware attacks, unauthorized device access, and data breaches. The proposed cybersecurity risk assessment model provides a systematic framework for evaluating and prioritizing security risks associated with IoMT devices. By integrating vulnerability severity, threat probability, and operational impact, the model enables healthcare organizations to identify high-risk devices and allocate cybersecurity resources more effectively. Furthermore, combining the proposed risk assessment approach with advanced technologies such as machine learning-based threat detection systems could further enhance hospital cybersecurity capabilities. Such integrated security solutions would allow healthcare institutions to proactively identify vulnerabilities, detect emerging threats in real time, and strengthen the overall resilience of healthcare systems against cyberattacks.

REFERENCES

[1] El-Saleh, Ayman A., et al. "The internet of medical things (IoMT): opportunities and challenges." *Wireless networks* 31.1 (2025): 327-344.

[2] Mathkor, Darin Mansor, et al. "Multirole of the internet of medical things (IoMT) in biomedical systems for managing smart healthcare systems: An overview of current and future innovative trends." *Journal of infection and public health* 17.4 (2024): 559-572.

[3] Saeed, Mahlaqa, et al. "Enhancing computer security through formal verification of cryptographic protocols using model checking and partial order techniques." *The Asian Bulletin of Big Data Management* 4.02 (2024): Science-4.

[4] Hamid, Khalid, et al. "Empowerments of Anti-Cancer Medicinal Structures by Modern Topological Invariants." *Journal of Medicinal and Chemical Sciences* 7.668-683 (2024).

[5] Bai, Yiting, Baiqian Gu, and Chao Tang. "Enhancing real-time patient monitoring in intensive care units with deep learning and the internet of things." *Big Data* (2025).

[6] El-Saleh, Ayman A., et al. "The internet of medical things (IoMT): opportunities and challenges." *Wireless networks* 31.1 (2025): 327-344.

[7] Nazir, Muhammad Ashraf, et al. "The Silent Guard: ML-Based Zero-Knowledge Proofs in Blockchain Security." *Spectrum of Engineering Sciences* (2025): 1659-1678.

[8] Ullah, Kaleem, et al. "Line Congestion Management in Modern Power Systems: A Case Study of Pakistan." *International Transactions on Electrical Energy Systems* 2024.1 (2024): 6893428.

[9] El-Saleh, Ayman A., et al. "The internet of medical things (IoMT): opportunities and challenges." *Wireless networks* 31.1 (2025): 327-344.

[10] Shanmugam, Bharanidharan, and Sami Azam. "Risk assessment of heterogeneous IoMT devices: a review." *Technologies* 11.1 (2023): 31.

[11] Qayyum, Muhammad Umer, et al. "Integrating AI in healthcare: Advancing petroleum fraud detection and enhancing vaccine development." *Global Journal of Universal Studies* 1.1 (2024): 172-189.

[12] Qadeer, Iqra, et al. "Psycho-therapeutic Intervention for Meta-cognitions and Emotional Regulation in Binge Eating Disorder: A Systematic Review." *Human Nature Journal of Social Sciences* 4.4 (2023): 39-50.

[13] Alsbatin, Loiy, et al. "Advancing IoMT security: Machine learning-based detection and classification of multi-protocol cyberattacks." *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications* 16.2 (2025): 228-247.

[14] Bhatt, Saurabhkumar I. "Cybersecurity risks in connected medical devices: mitigating threats to patient safety." *International journal of trend in scientific research and development* 9.2 (2025): 433-444.

[15] Islam, Mohyminul, et al. "Enhancing Intrusion Detection Systems with Synthetic Attack Data and Advanced Classification Models." *2025 IEEE 6th International Conference on Computer, Big Data, Artificial Intelligence (ICCBD+ AI)*. IEEE, 2025.

[16] Iqbal, Muhammad Waleed, et al. "MITIGATING DDOS ATTACKS ON IOT DEVICES: A HYBRID APPROACH USING AI AND BLOCKCHAIN." *Spectrum of Engineering Sciences* (2025): 1679-1697.

[17] Khan, Mudassar Ali, Ikram Ud Din, and Ahmad Almogren. "Securing access to internet of medical things using a graphical-password-based user authentication scheme." *Sustainability* 15.6 (2023): 5207.

[18] El-Taj, Homam, and Ala Hamarsheh. "Security Challenges and Mitigation Strategies for Internet of Medical Things (IoMT): A Cross-Layer Analysis of Embedded Systems and Networked Environments." *2025 International Conference on Electrical and Computer Engineering Researches (ICECER)*. IEEE, 2025.

[19] Abid, Misbah, et al. "USABILITY EVALUATION EMPOWERED GAMING PLATFORM: AN ANOVA-BASED STATISTICAL ANALYSIS." *Spectrum of Engineering Sciences* (2025): 1130-1153.

[20] Ibrar, Muhammad. *Threat detection during data migration from on premises servers to clouds*. Diss. New Mexico Highlands University, 2024.

[21] Romolo, Francesco Saverio, et al. "Health and cybercrime." *Eur Rev Digit Adm Law* 4.1 (2023): 287-297.

[22] Owolabi, Babatunde O. "Cyber-physical security in smart healthcare: protecting IoT-enabled medical devices from spyware, ransomware, and network-based exploits." *Int J Res Publ Rev* 6.3 (2025): 1812-26.

[23] MUHAMMAD, IBRAR, et al. "ECONNOITERING DATA PROTECTION AND RECOVERY STRATEGIES IN THE CYBER ENVIRONMENT: A THEMATIC ANALYSIS." *INTERNATIONAL JOURNAL* 8.4 (2024).

[24] Shah, Syed Muqadir Hussain, et al. "ML-BASED ANALYTICAL STUDY ON THE LEVEL OF SECURITY OF USER DATA ON SOCIAL MEDIA WEBSITE."

[25] George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors." *Partners Universal International Innovation Journal* 2.1 (2024): 51-75.

[26] Dadkhah, Sajjad, et al. "Ciciomt2024: Attack vectors in healthcare devices-a multi-protocol dataset for assessing iomt device security." (2024).

[27] Shaker, Bilawal, et al. "Enhancing grid resilience: Leveraging power from flexible load in modern power systems." *2023 18th International Conference on Emerging Technologies (ICET)*. IEEE, 2023.

[28]] Hamid, Khalid, et al. "ML-based Meta-Model Usability Evaluation of Mobile Medical Apps." *International Journal of Advanced Computer Science & Applications* 15.1 (2024).

[29] Stergiopoulos, George, et al. "Process-aware attacks on medication control of type-i diabetics using infusion pumps." *IEEE Systems Journal* 17.2 (2023): 1831-1842.

[30] Stergiopoulos, George, et al. "Process-aware attacks on medication control of type-i diabetics using infusion pumps." *IEEE Systems Journal* 17.2 (2023): 1831-1842.

[31] Riaz, Samavia, et al. "Software Development Empowered and Secured by Integrating A DevSecOps Design." *Journal of Computing & Biomedical Informatics* 8.02 (2025).

[32] Iqbal, Muhammad Waseem, et al. "Meta-analysis and investigation of usability attributes for evaluating operating systems." *Migration Letters* 21.5 (2024): 1363-1380.

[33] Inuwa, Muhammad Muhammad, and Resul Das. "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on IoT networks." *Internet of Things* 26 (2024): 101162.

[34] Chukwunweike, Joseph Nnaemeka, A. A. Adewale, and O. Osamuyi. "Advanced modelling and recurrent analysis in network security: Scrutiny of data and fault resolution." (2024).

[35] Delshadi, Amir Mohammad, et al. "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review." *Spectrum of Engineering Sciences* (2025): 36-48.

[36] Ibrar, Muhammad, et al. "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis." *International Journal for Electronic Crime Investigation* 8 (2024).

[37] Tyagi, Amit Kumar, and R. Seranmadevi. "Blockchain for enhancing security and privacy in the smart healthcare." *Digital Twin and Blockchain for Smart Cities* (2024): 343-370.

[38] Baligodugula, Vishnu Vardhan, Ashutosh Ghimire, and Fathi Amsaad. "An overview of secure network segmentation in connected IIoT environments." *Computing&AI Connect* 1.1 (2024): 1-10.

[39] Nazir, Talha, et al. "Transforming blood donation processes with blockchain and IOT integration: a augmented approach to secure and efficient healthcare practices." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[40] Hanif, Mehran, et al. "Evaluating Prompt Variability in Transformer-Based LLMs Through Discrete and Semantic PSI." *ASSAJ* 4.02 (2025): 1798-1809.

[41] Ahmed, Rana Hassam, Majid Hussain, and Ashraf Khalil. "Blockchain-based supply chain management in healthcare." *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems*. IGI Global Scientific Publishing, 2025. 107-132.

[42] Tariq, Muhammad Hannan, et al. "DECENTRALIZED APPLICATION FOR AUTO-INSURANCE INDUSTRY: AN INTERPLANETARY FILE SYSTEM AND BLOCKCHAIN-BASED PARADIGM FOR OPTIMAL DATA AND CLAIM MANAGEMENT."

[43] Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[44] Danish, Muhammad, et al. "Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN." *vol* 3 (2025): 18-36.

[45] Ksibi, Sondes, Faouzi Jaidi, and Adel Bouhoula. "MLRA-Sec: an adaptive and intelligent cyber-security-assessment model for internet of medical things (IoMT)." *International Journal of Information Security* 24.1 (2025): 21.

[46] Baligodugula, Vishnu Vardhan, Ashutosh Ghimire, and Fathi Amsaad. "An overview of secure network segmentation in connected IIoT environments." *Computing&AI Connect* 1.1 (2024): 1-10.