Journal Of Research Technology & Engineering
www.jrte.org

Review Paper on Cyber Security Threats and Mitigations with emphasis on Risk-Based Prioritization for IoMT Security in Healthcare.

* W.P.S. Shehan Miraj Perera

SLIIT Business School, Sri Lanka Institute of Information Technology, Colombo Sri Lanka
* shehanmiraj.official@gmail.com

Received:07 Aug 2024; Revised:25 Aug 2024; Accepted: 15 Sep 2024; Available online: 10 Oct 2024

Abstract— The advent of the Internet of Medical Things (IoMT) has revolutionized healthcare delivery but has also introduced unprecedented cybersecurity challenges. This paper presents a comprehensive review of the literature surrounding cybersecurity implications for IoMT deployments, drawing insights from classic and current studies.

In this review we will delve into the diverse landscape of cybersecurity threats facing IoMT ecosystems, types of cyber-attacks targeting IoMT devices, exploring the multifaceted impact of cybersecurity incidents on stakeholders within the healthcare ecosystem, explain the consequences for patients, healthcare providers, regulatory bodies, and healthcare organizations.

The paper also evaluates existing risk assessment methodologies and mitigation strategies tailored for IoMT environments, emphasizing the importance of Risk-based Prioritizing Framework (RBPF). This review has also identified several avenues for future research, including the integration of artificial intelligence for threat detection, the development of secure communication protocols, and the exploration of decentralized data management approaches. By synthesizing insights from the literature, this paper contributes to the advancement of cybersecurity practices in healthcare and underscores the importance of interdisciplinary collaboration in addressing IoMT security challenges effectively.

Index Terms— Cybersecurity, Risk-based prioritization Healthcare, Internet of Medical Things (IoMT), Medical Device Security, Risk Assessment, Threat Mitigation

INTRODUCTION

The Internet of Things (IoT) is revolutionizing various industries and healthcare is no exception. The underlying foundation for IoMT came from the explosion of the IoT in general. IoMT specifically refers to the application of IoT technology in the healthcare industry (Mehtab Alam 2022). By connecting medical devices, sensors and wearables to a network, the IoMT creates powerful ecosystem for remote patient monitoring (Ala Al-Fuqaha 2015), medication adherence monitoring to track patients' medication usage patterns (Valérie Santschi, et al. 2014), staff and assets tracking, wearable health devices (Shyamal Patel 2012), Telemedicine and telehealth (Rashid Bashshur 2020), Smart healthcare facilities (Islam, et al. 2015) and more proactive approach to healthcare. Both IoT and IoMT involve the use of interconnected devices that collect, transmit and exchange data over the internet or other networks. They rely on data analytics to derive insights

from the vast amount of data generated by connected devices and allow real-time tracking of assets, better decision-making (Angela-Tafadzwa Shumba 2022), diagnostics and intervention when necessary

Cybersecurity threats facing IoMT systems.

While the IoMT offers a promising future for healthcare, its increased interconnected nature and reliance on network connectivity, they become potential targets for cyber-attacks (Clemens Scott Kruse 2017). As all digital technology promising betterment, intentionally or unintentionally carries a risk. Security is important for medical devices, health information communications for healthcare and e-healthcare services. Any weakness or information leakage due to cyberattacks for the IoMT devices due to poor methods of authentication and access control, the system, and the setting entirely and seriously harm by incoming and outgoing data (Jean-Paul A. Yaacoub 2020). Literature provides insights into the diverse range of cyberthreats faced by IoMT systems in healthcare (Mudassar Mushtaq 2022) (Argaw 2020).

This review paper aims to delve into the landscape of cybersecurity threats and mitigations in IoMT environments, with a specific focus on risk-based prioritization strategies. By synthesizing existing research and methodologies, this paper seeks to provide insights into effective approaches for securing IoMT deployments and mitigating associated risks, thereby contributing to the advancement of cybersecurity practices in healthcare.

Research objectives.

Synthesize the current state of knowledge regarding cybersecurity threats and vulnerabilities inherent in IoMT ecosystems, including but not limited to device tampering, data breaches, and unauthorized access.

Explore the multifaceted impact of cybersecurity incidents on various stakeholders within the healthcare ecosystem, encompassing patients, healthcare providers, medical device manufacturers, regulatory bodies, and healthcare organizations.

Evaluate the effectiveness of existing risk assessment methodologies and security frameworks tailored for IoMT environments in identifying, assessing, and mitigating cybersecurity risks.

Examine the role of regulatory policies, standards, and compliance requirements in shaping cybersecurity practices and governance frameworks for IoMT deployments.

Discuss the implications of cybersecurity challenges and mitigation strategies on patient care, data privacy, and the overall integrity of healthcare delivery in the era of interconnected medical devices.

Identify gaps and areas for future research, including the development of novel security solutions, integration of cybersecurity into medical device lifecycle management, and the establishment of collaborative initiatives to address IoMT security challenges holistically.

Methodology

As this review aims to analyze the relationship between the cybersecurity threats, mitigation and Risk-based prioritization and propose strategies for managing cyber risks in the context of IoMT security in healthcare, the primary method of data collection involved electronic database searches, focusing on reputable digital libraries such as IEEE, PubMed, Science direct, Sage publishers, and scholarly search engines such as google scholar allowing for the inclusion of relevant and recent research literatures.

Literature review

Cybersecurity threats on the IoMT have emerged as a critical concern within the healthcare sector, prompting extensive research into security requirements and solutions. And it is a significant concern in the healthcare sector due to several key factors. For example, IoMT devices often collect and transmit highly sensitive patient data including medical history, vital signs and treatment information (Groppe 2020) cyberattacks could expose this data, leading to identity theft, insurance fraud or even patient harm, disruption in critical care potential for life-threatening consequences of inadequate IoMT (Preç 2022), the surface is expanded for malicious actors. Each device can be an entry point for unauthorized access, data breaches or disruption of critical healthcare services, and many IoMT devices prioritize functionality and affordability over robust security features (Pintu Kumar Sadhu 2022). Some common cybersecurity threats supported by literature can review as follows: Malware attacks including viruses, worms and ransomware exploiting vulnerabilities in medical devices compromising patient safety and data security. Threats such as ransomware attacks targeting healthcare organizations and supply chain vulnerabilities in medical devices pose significant challenges to the security and resilience of IoMT deployments. Data breaches occur when unauthorized parties gain access to sensitive patient information stored on IoMT devices or transmitted across networks. Insider threats that involve malicious actions by individuals within healthcare organizations, for example its employees, contractors, or business associates intentionally misuse their privileges to access or manipulate sensitive data. Denial-of -Service (DoS) attacks disrupt the availability of IoMT services by overwhelming networks, services or devices with a flood of malicious traffic hindering the care delivery and compromise reliability of critical medical systems. IoMT devices often rely on complex supply chains involving multiple vendors and third-party suppliers. Supply chain attacks target vulnerabilities in the manufacturing, distribution, or maintenance processes of these devices. May caused injecting malicious codes or tamper with hardware components. Lastly, Zero-Day Exploits which target previously unknown vulnerabilities in IoMT software or firmware. Attackers exploit before they are patched or mitigated, making it more challenging for healthcare organizations to defend against emerging threats. (Hui Suo 2012) (Newaz 2021) (Lee 2022) (Shancang Li 2016) (Thavavel Vaiyapuri 2021) (Eric M. Hutchins s.d.) Moreover, the emergence of novel attack techniques, such as side-channel attacks exploiting physical properties of medical devices, further underscores the need for continuous adaptation of security measures.

Table. 1. Types of cybersecurity threats

Threat Category	Description
Malware Infections	Malicious software designed to compromise IoMT devices, steal sensitive data, or disrupt healthcare operations.
Unauthorized Access	Unauthorized access to IoMT devices or systems, potentially leading to data breaches, manipulation of medical data, or interference with patient care.
Supply Chain Attacks	Attacks targeting the supply chain of medical devices, including tampering with components, counterfeit products, or supply chain compromises.
Ransomware	Malware that encrypts data or systems and demands ransom payments for decryption, posing significant risks to healthcare organizations and patient care.
Insider Threats	Threats posed by authorized users with access to IoMT systems, including negligent or malicious actions leading to data breaches or system compromise.

The following table 1 provides several kinds of cybersecurity threats that occur to IoMT systems. Malware Infection IoMT devices are compromised with malicious software, which results in data leakage or loss of sensitive information, or degraded healthcare operations. These types of attacks can cripple hospital systems or expose private medical records. It could be unauthorized access to IoMT devices or systems by some external party, which can lead to data breaches, manipulation of medical data, or interference with patient care in such a manner as to endanger lives.Supply chain attacks include the vulnerabilities within the supply chain of a medical device where threats may tamper with constituent components, introduce counterfeit products, or otherwise compromise a supply chain. These might lead to malfunctioning medical devices or create vulnerabilities in care systems. Of a specific type of malware, ransomware encrypts critical data or systems and requires a ransom for decryption. This could lead to severe disruptions in healthcare organizations, as many times, they would require access to patient records and systems for the delivery of care, insider threats are posed by individuals who have authorized access to IoMT systems. Such individuals might be negligent or malicious, leading to a breach or system compromise that places patient safety and data integrity at risk.

Fig. 1 Threat categorizing

Perception layer	**Application layer**	**Network layer**
Threats related to sensors, actuators and data collection	Threats targeting software applications and services	Threats affecting communication channels and network infrastructure.

Furthermore, According to Threat categorizing Figure 1, perception layer, application layer, and network layer. Perception layer threats refer to those affecting sensors, actuators, and data acquisition devices in IoMT. In fact, such sensors and actuators collect data about patients and take

necessary control decisions on medical devices. An application layer consists of threats against the software applications and services used to handle and store medical information, and these are widely exploited through known vulnerabilities in healthcare software. Finally, it defines the threats that are covered at the network layer, composed of the communication channels and the infrastructure of the network for data transmission between IoMT devices, health providers, and data storage; an eventual failure in any of them could affect the overall health environment and the integrity and functionality of IoMT systems.

Impacts on stakeholders.

The impact of inadequate cybersecurity in the IoMT extends beyond individual devices to the broader healthcare ecosystem. **Stakeholders** can be organized into a stakeholder mapping diagram based on their involvement, influence, and interest in ensuring the security and integrity of healthcare systems and patient data.

Table 1. Healthcare stakeholders map in the context of cybersecurity and IoMT in healthcare ecosystem

Primary stakeholders	**Secondary stakeholders**		**Tertiary stakeholders**
Patients	Healthcare organizations		Health insurance providers
	IT departments	Clinical engineering	
Healthcare providers	Medical device manufactures		Research intuitions
	Regulatory agencies		Legal and compliance entities
			Government agencies
			Cybersecurity vendors

Cybersecurity incidents in IoMT environments have profound implications for stakeholders that have indicated in the (TABLE ABOVE) within the healthcare ecosystem.

On one hand, patients, as the ultimate beneficiaries of healthcare services, are particularly vulnerable to privacy breaches and compromised medical data. Malamas (2021) highlight the potential consequences of data breaches on patient trust and confidence in healthcare providers (V. Malamas 2021) (Marzyeh Ghassemi 2020). Moreover, unauthorized access to medical devices or tampering with treatment protocols can directly impact patient safety, underscoring the criticality of securing IoMT systems against cyber threats. In fact, compromised privacy impacts on individual's trust and confidence in healthcare organizations (Kelly Caine 2013). When breaches occur personal health information will be exposed or accessed by unauthorized parties leading to identity theft, medical fraud and emotional distress. **On the other hand, Healthcare providers** face operational disruptions and reputational damage (Adil Hussain Seh 2020) in the event of a cyber-attack, as demonstrated in the study by Mahmood (2023) (Mahmood, et al. 2023) The loss of access to critical medical data, disruption of clinical workflows, and downtime of essential healthcare services can have far-reaching consequences for patient care and organizational resilience. Additionally, **healthcare organizations** bear the responsibility of ensuring compliance with regulatory requirements such as HIPAA regulations mandate (Association 2024) safeguards for patients' Protected Health Information (PHI). Non-compliance can result in legal consequences and financial penalties. Regulatory bodies may impose sanctions for negligence or inadequate security measures.

Hence the providers are obliged to maintain the integrity of IoMT systems. Cybersecurity breaches impose financial burdens on costs for incident responses, data recovery, legal expenses, cybersecurity measure and breach mitigation (Aziz Jamal 2009). Literature provides the implications of cyberattacks targeting intellectual properties, for example, theft or compromise of proprietary information, trade secrets and research data. These causes undermine innovation and competitiveness for healthcare businesses and the industry (Usman Tariq 2023)

Regulatory bodies or government agencies such as Food and Drug Administration (FDA) regulate and update medical devices' safety and security standards, impose requirements on manufactures and healthcare providers. (Adil Hussain Seh 2020). The stakeholder face challenges due to its rapidly evolving nature of IoMT technologies to enforce cybersecurity regulations and standards (Se-Ra Oh 2021), increased scrutiny, regulating IoMT devices fragmented across different agencies depending on the specific function of the device lead to inconsistencies and loopholes in cybersecurity requirements (ENISA is working towards a cyber secure and resilient Health Sector in the EU s.d.), IoMT devices' global scope in term of their difference in development and utilizing country accountable for breaches that occur outside their home judication (Zakes 2923).

Regulatory Policies and Compliance

Regulatory frameworks play a crucial role in shaping cybersecurity practices and governance structures for IoMT deployments. Classic studies by Sadhu et al. (2022) and Alsubaei et al. (2019) highlight the need for comprehensive regulatory policies to ensure the security and privacy of medical data in IoMT environments. Regulatory bodies such as the Food and Drug Administration (FDA) and the European Medicines Agency (EMA) have issued guidelines and standards for medical device manufacturers, healthcare providers, and software developers to enhance the security of IoMT systems. Recent research by IEEE Journals & Magazine (2023) examines the implications of regulatory compliance on healthcare organizations and the challenges of aligning security practices with evolving standards. Compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR) requires healthcare organizations to implement robust security controls, conduct regular risk assessments, and maintain documentation of security measures. Moreover, the literature emphasizes the importance of interoperability and information sharing among regulatory agencies, industry stakeholders, and cybersecurity researchers to address the dynamic nature of cyber threats in healthcare settings (Pintu Kumar Sadhu 2022) (Faisal Alsubaei 2019). The following table summarizes the challenges and implications of regulatory compliance for healthcare organizations and IoMT manufacturers.

Table 2. Challenges in IoMT technology in healthcare

Challenge	Implication
Evolving Standards	Compliance costs, resource allocation
Interoperability	Compatibility issues, data sharing concerns
Enforcement	Penalties for non-compliance, legal risks

Risk Assessment Methodologies

In the context of IoMT and cybersecurity threats risk assessment is crucial for various reasons. Even IoMT holds immense promise for healthcare, its rapid integration exposes a critical security vulnerability. Most IoMT devices are limited in the capability of detecting and preventing cyberattacks themselves. Mostly because these devices often prioritize functionality and cost-effectiveness over robust security features. Literature emphasizes the importance of effective risk assessment and mitigation strategies as essential components of cybersecurity governance frameworks for IoMT deployments. Malam as et al (V. Malamas 2021) discuss the importance of robust risk assessment methodologies tailored for IoMT environments. The goal of a robust risk assessment is to provide a structured framework for stakeholders to Identify, Prioritize and Mitigate cybersecurity risks effectively and respond to risks proactively to minimize negative outcomes. Firstly, this breakdown can be explored in various risk assessment approaches. (TABLE) provides the strengths and weaknesses of each approach, along with considerations for risk mitigation strategies and decision context.

Table 3. Risk assessment methodologies

Methodologies	Description	Strengths	Weaknesses	Applicability
QL methods	Subjective assessment of risk likelihood and impact. May rely on expert judgement and experience to assess risk. Describe the likelihood and impact of threats in QL terms (Amin 2018)	Easier to implement.	Subjective judgments may lack precision.	Moderate. Suitable for initial risk identification and high-level risk prioritization.
QT methods	Involving numerical values to various risk parameters like probability, impact, and exposure.	Provides numerical estimates of risk, aiding in prioritization and decision making.	Requires significant data and expertise.	High. Useful for assessing specific cyber risks in IoMT systems.
Mixed methods	Combines elements of both QL and QT methodologies to leverage their respective strengths and mitigate weaknesses.	Integrates both subjective and objective assessments for a more thorough	May increase the complexity as the integration of QT an QL components.	High. Suitable for assessing cybersecurity risks in complex IoMT ecosystems where multiple factors

		understanding of risks and allows for tailoring to suit the specific needs and characteristics of IoMT environments.		influence the risk levels.
Vulnerability-based methods	Focuses on identifying weaknesses that attackers can exploit.	Provides detailed understanding of specific weaknesses and enables targeted remediation effort.	Might not consider the complete risk picture alone.	Useful for identifying technical weaknesses in IoMT systems and guiding patching and mitigation efforts.
Threat based methods	Focuses on identifying potential threats to IoMT systems and analyzing their capabilities, motivation and attacks.	Provides information about attackers and allows organizations to prioritize security measures and focus on the most relevant threats.	Might overlook entirely new or unconventional attack techniques.	Uses to prioritize security controls, resource allocation and incident response protocols.

Frameworks and Mitigation Strategies

Earlier we reviewed the cybersecurity threats and challenges in the IoMT devices. To combat these challenges, a combination of frameworks and mitigation strategies are crucial. Frameworks provide a structured approach to managing IoMT security risks. Karie et al. conduct a comprehensive review of security standards and frameworks for IoT-based smart environments, providing valuable insights into the landscape of cybersecurity protocols applicable to IoMT systems (Nickson M. Karie 2021). Their analysis serves as a foundation for implementing robust security measures tailored to the unique requirements of healthcare IoT ecosystems.

2 foundation aspects for robust security measures in healthcare IoMT ecosystems:

I. Leveraging existing security standards and frameworks for IoT environments.
II. Adapting these frameworks to address the specific needs of healthcare IoMT. Almost all

frameworks offer a strong foundation, IoMT has unique security requirements. As we previously seen, for example, patient data is highly sensitive, and any compromise could have severe consequences.

Salih et al. present an IoT security risk management model tailored for the healthcare industry, emphasizing the importance of proactive risk assessment and mitigation strategies to combat emerging threats (Fathi I. Salih 2019). This approach underscores the necessity of aligning cybersecurity measures with the unique operational and regulatory requirements of healthcare organizations.

Radoglou-Grammatikis et al. propose a novel approach combining software-defined networking and reinforcement learning for modelling, detecting, and mitigating threats against industrial healthcare systems (Panagiotis Radoglou-Grammatikis 2022). By leveraging advanced technologies, this framework enhances the resilience of IoMT infrastructures against evolving cyber threats.

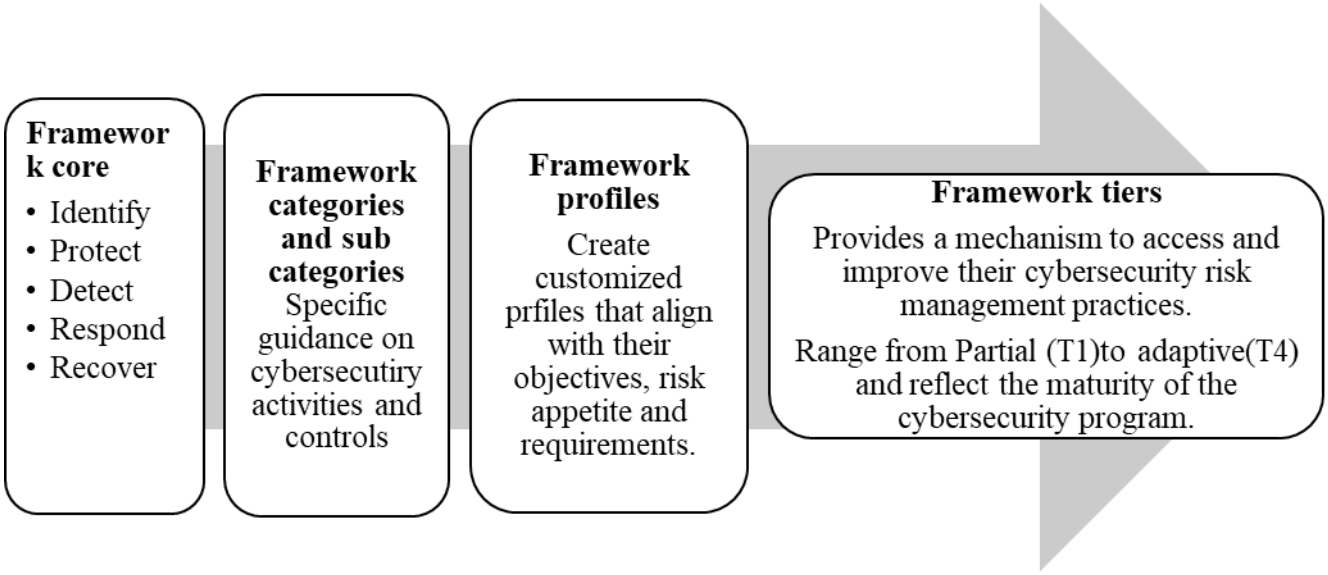

Fig. 1 NIST framework.

National Institute of Standards and Technology (NIST) is a flexible framework that offers a high-level structure for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents. In a regional context, Kandasamy et al. analyze cyberattacks in Asian organizations, offering perspectives from the NIST to enhance cybersecurity posture in healthcare settings (Kamalanathan Kandasamy 2022). Their study underscores the importance of adopting international best practices to mitigate cyber risks effectively. It is a voluntary and not mandatory for compliance. Healthcare organizations can choose to adopt it based on their cybersecurity requirements and objectives. The framework is built on a risk-based approach.

Risk Assessment Model for healthcare Associations (RAMA), a solution specifically designed for healthcare organizations. It provides a systematic approach to identify, prioritize and mitigate cybersecurity risks associated with IoMT and healthcare IT systems. And compared to NIST this model is tailored for healthcare instead for general purposes. Smylie et al. (Michail Smyrlis 2024) introduce RAMA, this framework enables healthcare institutions to proactively manage threats and safeguard patient data effectively.

Risk based prioritization framework (RBPF)

In addressing cybersecurity challenges within the realm of Internet of Medical Things (IoMT) security in healthcare, a crucial aspect lies in the development and application of a robust risk-based prioritization framework. This framework serves as a strategic tool for healthcare organizations to effectively allocate resources towards mitigating the most critical vulnerabilities and threats. As emphasized by (Mahmood, et al. 2023), such a framework involves assessing the likelihood and impact of potential threats, thereby enabling informed decision-making in resource allocation and risk mitigation efforts.

Table 5. RBPF components.

Stage	Activity
Risk Identification	Review security assessments and penetration testing reports.
	Consult threat intelligence feeds to understand current cyber threats in healthcare systems.
	Analyze the capabilities and motivations of potential attackers.
Risk Assessment	Evaluate each risk based on Likelihood and Impact on
	- Patient safety
	- Data privacy
	- Financial losses
	- Reputational damage
Risk Prioritization	Assign a priority level (High, Medium, Low) to each risk.
Risk Mitigation	Select and implement appropriate mitigation strategies.

Cybersecurity Mitigation strategies for IoMT based on Risk-based prioritization framework.

A risk-based prioritization framework helps guide the selection and implementation of Cybersecurity mitigation strategies for IoMT based on their potential impact and likelihood.

Risk assessment and prioritization: using RBPF to identify and assess potential threats and vulnerabilities associated with IoMT devices and systems. By conducting a comprehensive risk assessment to identify vulnerabilities and threats specific to IoMT devices. Prioritize risks based on their likelihood and impact in healthcare such as patient safety, data privacy, financial loses and reputational damages etc. Targeted mitigation strategies based on risk level: once risks are prioritized, appropriate mitigation strategies are selected. For instance,

Here are the explain about RBPF example analysis in IoMT healthcare system
High risk - Implement robust mitigation strategies with minimal tradeoffs for high priority risks. Patching critical vulnerabilities, Network segmentation, segmenting the network to isolate IoMT devices from the critical systems lead to limiting the impact of breach and prevents lateral movement by attackers. Encrypting sensitive data at storage and transmission. That ensures end-to end encryption to protect patient information.

Medium risk - Implement a balanced approach for medium priority risks, considering effectiveness, cost and impact on device functionality. Enforce least privilege access control for user accounts.

Low risk - Consider cost-effective mitigation strategies or monitor the risk for potential changes. By keeping IoMT device firmware and software up to date. Regularly Apply security patches to address known vulnerabilities

Continuous monitoring and improvement: regularly monitoring IoMT systems and network activity for new vulnerabilities and threats. And re-evaluate risks based on new information and adjust mitigation strategies as needed to maintain a robust security posture.

RBPF based mitigation strategy selection prioritizes security investments towards the most critical threats, optimizing resource utilization, implementing the most impact mitigation strategies based on the risk level and improve the IoMT security posture. Furthermore, it can be more effective and comprehensive if the RBPF combines with roader security frameworks like NIST we discussed before.
Integrating threat intelligence to stay updated on the evolving cyber threat landscape also be a practical aspect for better functioning.

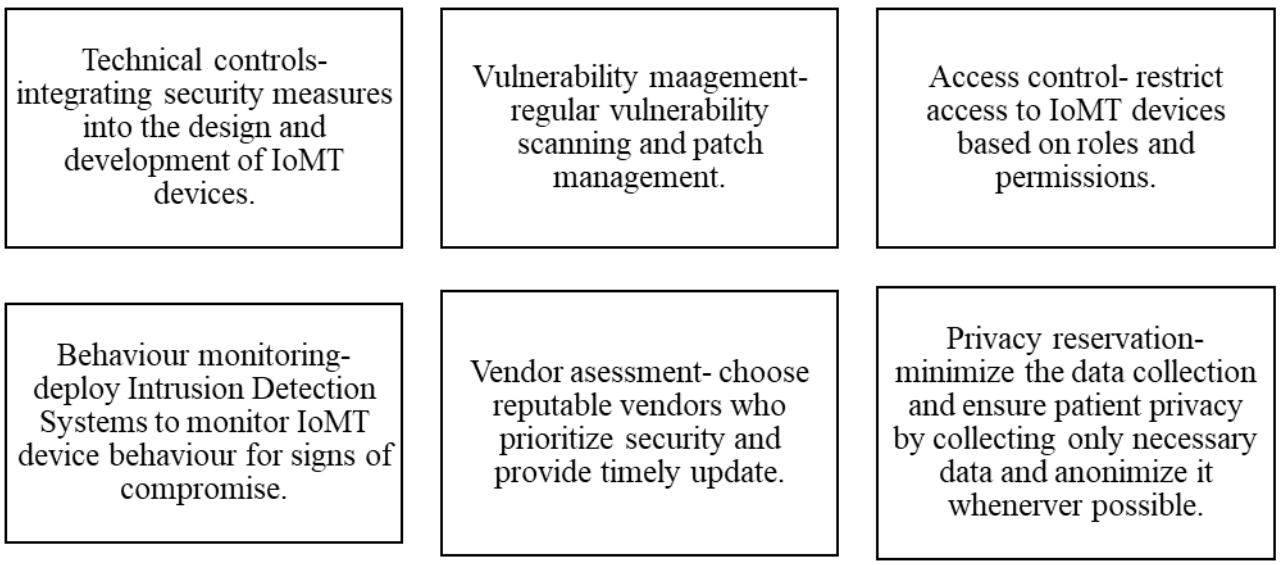

Fig. 3 Cybersecurity mitigation strategies

Security Model for Internet of Medical Things

The security model (Figer 4) for IoMT necessitates a comprehensive approach that integrates various security measures to safeguard the integrity and confidentiality of patient data amidst evolving cyber threats. Drawing from the insights provided by (Mahmood, et al. 2023), security model entails the implementation of advanced security architectures tailored specifically for the unique requirements of IoMT systems. These architectures encompass encryption protocols, access control mechanisms, intrusion detection systems, and secure communication protocols, among others, to fortify the defense against unauthorized access and data breaches. And the literature underscores the imperative for healthcare organizations to adopt proactive risk management strategies and robust security models to mitigate the multifaceted cybersecurity threats posed to IoMT systems in healthcare. By leveraging insights from advanced technologies, collaborative frameworks, and international best practices, healthcare organizations can bolster their cybersecurity posture and uphold the integrity and confidentiality of patient data in an increasingly interconnected healthcare landscape.

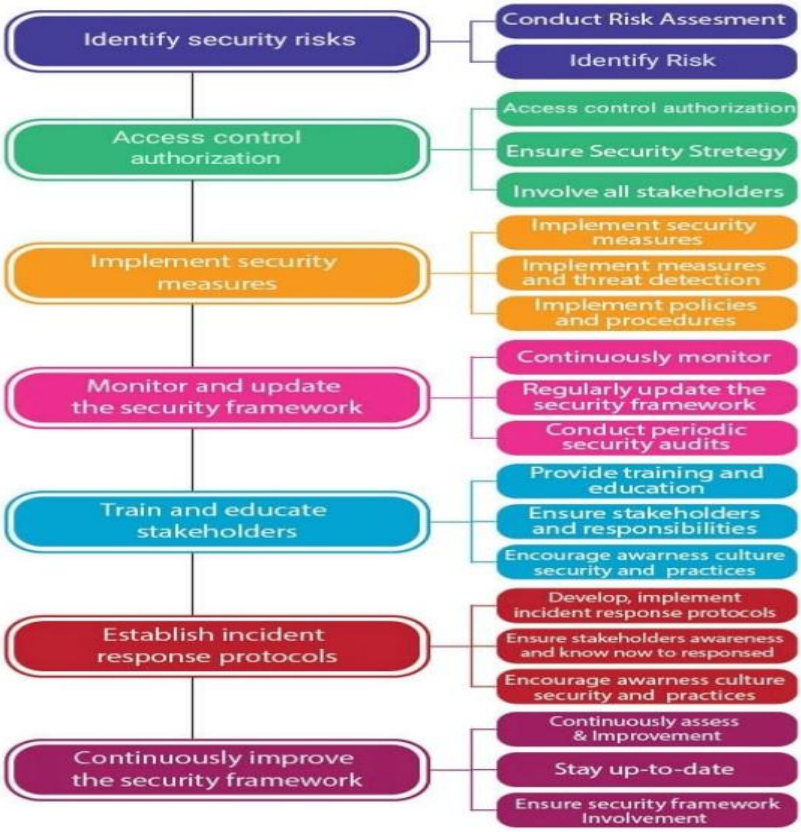

Fig. 4 The security model for internet of medical things

Future research

While the literature on cybersecurity implications for the Internet of Medical Things (IoMT) has expanded considerably in recent years, there are still significant gaps and areas for future research. Despite the growing recognition of IoMT security challenges, there remains a need for further exploration and innovation to address the evolving threat landscape and ensure the resilience of healthcare systems. Despite the interdisciplinary nature of IoMT cybersecurity, there is a notable lack of collaboration between cybersecurity experts, healthcare professionals, and policymakers. Future research should focus on fostering greater collaboration and knowledge exchange among these stakeholders to develop holistic approaches to IoMT security. The integration of emerging technologies such as artificial intelligence (AI) for threat detection in the context of cybersecurity for IoMT for example, AI driven anomaly detection, deep learning for intrusion detection, machine learning, AI for cybersecurity decision support, real-time adaptive cyber defines. and blockchain introduces new opportunities and challenges for IoMT security. Research is needed to explore the potential applications of AI in threat detection and anomaly identification within IoMT ecosystems, as well as the feasibility and effectiveness of blockchain-based solutions for securing medical data and transactions. Moreover, with the increasing volume and complexity of medical data generated by IoMT devices, preserving patient privacy becomes paramount. Future research should investigate advanced encryption techniques, differential privacy mechanisms, and secure multiparty computation protocols to protect sensitive medical information while enabling data sharing and analysis for research and clinical purposes. The supply chain for medical devices is susceptible to various cybersecurity risks, including counterfeit components, tampering, and supply chain attacks. Research is needed to develop robust supply chain security measures, such as blockchain-based traceability solutions, secure boot mechanisms, and supply chain risk management frameworks, to ensure the integrity and authenticity of IoMT devices throughout their lifecycle. Regulatory compliance with existing standards and regulations is essential for ensuring the security and privacy of IoMT deployments. However, the regulatory landscape for IoMT security is still evolving, with gaps and inconsistencies across different jurisdictions. Future research should focus on harmonizing regulatory frameworks, evaluating the effectiveness of existing regulations in addressing emerging threats, and developing guidelines for regulatory compliance in IoMT environments.

Conclusion

In conclusion, IoMT cybersecurity is a complex and constantly evolving domain, where the type of threats will span from traditional vulnerabilities to risks that will rise accordingly with the increase in the number of connected devices. The review underlined the decisive impact of cybersecurity incidents on the stakeholders involved in healthcare and assured that active countermeasures will be required for the security of IoMT systems. In addition, among the identified research gaps, there were those that needed an interdisciplinary approach in research explorations for the emerging technologies. This will help healthcare organizations focus their mitigation strategies by applying RBPF to high-risk areas with a view to better protection of patient data and healthcare operations. Further innovation and collaboration will be needed to make deployments of IoMT more secure and resilient.

REFERENCES

Adil Hussain Seh, 1 Mohammad Zarour,2 Mamdouh Alenezi,Amal Krishna Sarkar, Alka Agrawal, Rajeev Kumar, and Raees Ahmad Khan. 2020. "Healthcare Data Breaches: Insights and Implications." Healthcare 133 (8): 1-18. doi:https://doi.org/10.3390/healthcare8020133.

Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash. 2015. "Internet of Things: A Survey on Enabling Technologies, Protocols and Applications." IEEE Communications Surveys & Tutorials (IEEE xplore) 17 (4). doi:DOI:10.1109/COMST.2015.2444095.

Amin, S., Choo, K.K.R., & Hannington, C. 2018. "Security and Privacy in IoMT for Healthcare: A Survey." Electronics (MDPI) 7 (6).

Angela-Tafadzwa Shumba, Teodoro Montanaro, Ilaria Sergi, Luca Fachechi, Massimo De Vittorio, Luigi Patrono. 2022. "Leveraging IoT-Aware Technologies and AI Techniques for Real-Time Critical Healthcare Applications." Sensors (MDPI) 22. doi:https://doi.org/10.3390/s22197675.

Argaw, S.T., Troncoso-Pastoriza, J.R., Lacey, D. et al. 2020. "Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks." BMC Med Inform Decis Mak 20: 146. doi:https://doi.org/10.1186/s12911-020-01161-7.

Association, American Medical. 2024. AMA. American Medical Association. https://www.ama-assn.org/practice-management/hipaa/hipaa-security-rule-risk-analysis.

Aziz Jamal, Kirsten McKenzie and Michele Clark. 2009. "The Impact of Health Information Technology on the Quality of Medical and Health Care: A Systematic Review." Health Information Management Journal (Sage Journals) 38 (3): 26-27. doi:10.1177/183335830903800305.

Clemens Scott Kruse, Benjamin Frederick, Taylor Jacobson and D. Kyle Monticone. 2017. "Cybersecurity in healthcare: A systematic review of modern threats and trends." Technology and Health Care (IOS Press) 25 (1): 1-10. doi:10.3233/THC-161263.

Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin, Ph.D. n.d. "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusions kill chains." 14.

Faisal Alsubaei, Abdullah Abuhussein, Vivek Shandilya, Sajjan Shiva. 2019. "IoMT-SAF: Internet of Medical Things Security Assessment Framework." Intern of Things (Science Direct) 8. doi:https://doi.org/10.1016/j.iot.2019.100123.

Fathi I. Salih, Nur A. Abu Bakar, Noor H. Hassan, Farashazillah Yahya, Nazri Kama, Jalal Shah. 2019. "IoT Security risk management model for healthcare industry." Malaysian journal of computer science (3). doi:https://doi.org/10.22452/mjcs.sp2019no3.9.

Groppe, Karen D. 2020. "Healthcare Information and Management Systems Society (HIMSS) ." https://www.himss.org/sites/hde/files/media/file/2020/11/16/2020_himss_cybersecurity_survey_final.pdf.

Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu. 2012. “Security in the Internet of Things: A Review.” International Conference on Computer Science and Electronics Engineering. IEEE. doi: 10.1109/ICCSEE.2012.373.

Islam, S. M. Riazul, Daehan Kwak, MD. Humaun Kabir, Mahmud Hossain, and Kyung-Sup Kwak. 2015. “The Internet of Things for Health Care: A Comprehensive Survey.” (IEEE) 3: 678-708. doi:10.1109/ACCESS.2015.2437951.

Jean-Paul A. Yaacoub, Mohamad Noura, Hassan N. Noura, Ola Salman, Elias Yaacoub, Raphaël Couturier, Ali Chehab. 2020. “Securing internet of medical things systems: Limitations, issues and recommendations.” Future Generation Computer Systems (Elsevier) 105: 581-606. doi:https://doi.org/10.1016/j.future.2019.12.028.

Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achthan, Venkat P. Rangan. 2022. “Digital Healthcare - Cyberattacks in Asian Organizations: An Analysis of Vulnerabilities, Risks, NIST Perspectives, and Recommendations.” IEEE access 10: 12345-12364. doi:10.1109/ACCESS.2022.3145372.

Kelly Caine, Rima Hanania. 2013. “Patients want granular privacy control over health information in electronic medical records.” J Am Med Inform Assoc 20: 7-15. doi:10.1136/amiajnl-2012-001023.

Lee, In. 2022. “Analysis of Insider Threats in the Healthcare Industry: A Text Mining Approach.” Information (MDPI) 13 (9). doi:https://doi.org/10.3390/info13090404.

Mahmood, Mudasir, Muhammad Ijaz Khan, Ziauddin, Hameed Hussain, Inayat Khan, and Shahid Rahma. 2023. “Improving Security Architecture of Internet of Medical Things: A Systematic Literature Review.” IEEE access 11: 107725-107753. doi:10.1109/ACCESS.2023.3281655.

Marzyeh Ghassemi, Tristan Naumann, Peter Schulam, Andrew L. Beam, Irene Y. Chen, Rajesh Ranganath. 2020. “A Review of Challenges and Opportunities in Machine Learning for Health.” https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7233077/.

Mazliza Othmana, Alaba Ayotunde Fadele, Ibrahim Abaker Targio Hashem, Faiz Alotaibi. 2017. “Internet of things Security: A Survey.” Journal of Network and Computer Applications. doi:10.1016/j.jnca.2017.04.002.

Mehtab Alam, Ihtiram Raza Khan, M. Afshar Alam, Farheen Siddiqui, Safdar Tanweer. 2022. “IoT Framework for Healthcare: A Review.” IEEE World Conference on Applied Intelligence and Computing. Sonbhadra. doi:DOI:10.1109/AIC55036.2022.9848923.

Michail Smyrlis, Evangelos Floros, Ioannis Basdekis, Dumitru-Bogdan Prelipcean, Aristeidis Sotiropoulos, Herve Debar, Apostolis Zarras, and George Spanoudakis. 2024. “RAMA: a risk assessment solution for healthcare organizations.” International Journal of Information Security (Springer). doi:https://doi.org/10.1007/s10207-024-00820-4.

Mudassar Mushtaq, Munam Ali Shah, Azhar Ghafoor. 2022. “The internet of medicl things (IoMT): security threats and issues affecting digital economy.” (IEEE Xplore). https://www.researchgate.net/publication/357005661_The_internet_of_medical_things_iomt_security_threats_and_issues_affecting_digital_economy.

Newaz, Akm Iqtidar and Sikder, Amit Kumar and Rahman, Mohammad Ashiqur and Uluagac, A. Selcuk. 2021. “A Survey on Security and Privacy Issues in Modern Healthcare Systems: Attacks and Defenses.” (Association for Computing Machinery) 2 (3). doi:10.1145/3453176.

Nickson M. Karie, Nor Masri Sahri, Wencheng Yang, Craig Valli, Victor R. Kebande. 2021. “A Review of Security Standards and Frameworks for IoT-Based smart environemnts,.” IEEE Access 9: 121975-121995. doi:10.1109/ACCESS.2021.3109886.

Panagiotis Radoglou-Grammatikis, Konstantinos Rompolos,, Panagiotis Sarigiannidis, Vasileios Argyriou et al. 2022. “Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach.” IEEE Xplore (IEEE) 18 (3): 2041-2052. doi:10.1109/TII.2021.3093905.

Pintu Kumar Sadhu, Venkata P. Yanambaka, Ahmed Abdelgawad, and Kumar Yelamarthi. 2022. “Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions.” Sensors (MDPI) 22 (15): 5517. doi:https://doi.org/10.3390/s22155517.

Preç, Ejona. 2022. “ISACA.” https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2022/addressing-security-risks-to-medical-iot-devices.

Rashid Bashshur, Charles R. Doarn, Julio M. Frenk, Joseph C. Kvedar, and James O. Woolliscroft. 2020. “Telemedicine and the COVID-19 Pandemic, Lessons for the Future.” Telemedicine and e-health (Mary Ann Liebert, Inc) 26 (5): 371-375. doi: https://doi.org/10.1089/tmj.2020.29040.rb.

Se-Ra Oh, Young-Duk Seo, Euijong Lee, Young-Gab Kim. 2021. “A Comprehensive Survey on Security and Privacy for Electronic Health data.” International journal of Environmenal Research and Public Health (PubMed Central) 18 (18): 9668. doi:10.3390/ijerph18189668.

Shancang Li, Theo Tryfonas, Honglei Li. 2016. “The Internet of Things: a security point of view.” Internet research (Emerald Insight) 26 (3): 337-359. doi: 10.1108/IntR-07-2014-0173.

Shyamal Patel, Hyung Park, Paolo Bonato, Leighton Chan and Mary Rodgers. 2012. “A review of wearable sensors and systems with application in rehabilitation.” Journal of NeuroEngineering and Rehabilitation (BioMed entral) 9 (21). doi: https://doi.org/10.1186/1743-0003-9-21.

Thavavel Vaiyapuri, Adel Binbusayyis, Vijayakumar Varadarajan. 2021. “Security, Privacy and Trust in IoMT Enabled Smart Healthcare System: a systematic review of current and future trends.” International Journal of Advanced Computer Science and Applications 12 (2): 731-737

Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, Kamran Shaukat. 2023. “A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review.” Sensors (MDPI) 3. doi:https://doi.org/10.3390/s23084117.

V. Malamas, F. Chantzis, T. K. Dasaklis, G. Stergiopoulos, P. Kotzanikolaou and C. Douligeris,. 2021. “Risk Assessment Methodologies for the Internet of Medical Things: A Survey and Comparative Appraisal.” IEEE access (IEE) 9: 40049-40075. doi:10.1109/ACCESS.2021.3064682.

Valérie Santschi, PharmD, PhD, MD, PhD Arnaud Chiolero, MSc, MLIS April L. Colosimo, PhD Robert W. Platt, PhD Patrick Taffé, MD Michel Burnier, MD, MPH Bernard Burnand, and MD, MSc Gilles

Paradis. 2014. “Improving Blood Pressure Control Through Pharmacist Interventions: A Meta-Analysis of Randomized Controlled Trials.” Journal of the American Heart Association 3 (2). doi:https://doi.org/10.1161/JAHA.113.000718

Zakes, Albe. 2923. “HIMSS.” HIMSS Healthcare Cybersecurity Survey Report. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey HIMSS Healthcare Cybersecurity Survey Report.