How an Internet of Medical Things Architecture addresses cyberattack risk in Healthcare

Enbei Yu
University of Melbourne
enbeiyu@gmail.com

Ruisi Qian
University of Melbourne
daisyqian2002@gmail.com

Jiajia Wang
University of Melbourne
bulabula1111j@gmail.com

Pingting Wu
University of Melbourne
pingtingwu1231@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

The integration of the Internet of Things (IoT) into healthcare, known as the Internet of Medical Things (IoMT), offers transformative benefits for patient care and treatment management. However, this evolution generates significant security vulnerabilities that expose healthcare systems to cyberattack. This study aims to fill knowledge gaps about how cyberattack affects the IoMT architecture. We propose solutions to key challenges across IoMT layers—perception, network, middleware, application, and business—after analysing literature and case studies. Vulnerability notifications are complex, access controls are inadequate, and security responsibility is inconsistently understood. Solutions include implementing advanced technologies, optimising accountability, accessing policy, and promoting organisational security awareness.

1. Introduction

The integration of the Internet of Things (IoT) into healthcare, known as the Internet of Medical Things (IoMT) or Healthcare IoT, is transforming the medical landscape (Verma et al., 2022). According to Alsubaei et al. (2017), IoMT is poised to enhance treatment efficacy, streamline disease management, minimise errors, elevate patient experiences, optimise medication use, and decrease healthcare expenses. Over the next few decades, IoMT is projected to play a crucial role in preventing fatal outcomes and enhancing national productivity, especially in developing countries (Nayak et al., 2022).

However, the rise of IoMT devices brings major security vulnerabilities, including issues with authentication, data transmission encryption, and managing complex, scalable systems design (Nayak et al., 2022). Interconnectivity creates additional cybersecurity risks, and the healthcare industry frequently ranks among the most vulnerable to cyberattack (Coventry & Branley, 2018). Cyberattack has increased, with billions of medical records stolen globally, and medical identity theft on the rise (Ganai et al., 2022). The digitisation of medical information and its accessibility across multiple networks indicates that cyberattack could potentially impact the health of millions of patients (Ganai et al., 2022).

This study aims to summarise the existing literature and address gaps in conducting the research question: "How does cyberattack impact the internet of medical things architecture and how do we address it?" This paper will review literature on IoMT layers and cyberattack targeting these layers, present case studies illustrating the practical implications of these threats, discuss the findings, and offer conclusions and limitations of the research.

2. Literature review

2.1 IoMT 5-layer Architecture

The IoMT architecture, as Figure 1 shows, is usually composed of five flexible IoT layers integrated to interconnect many heterogeneous objects (Alsubaei et al., 2017).

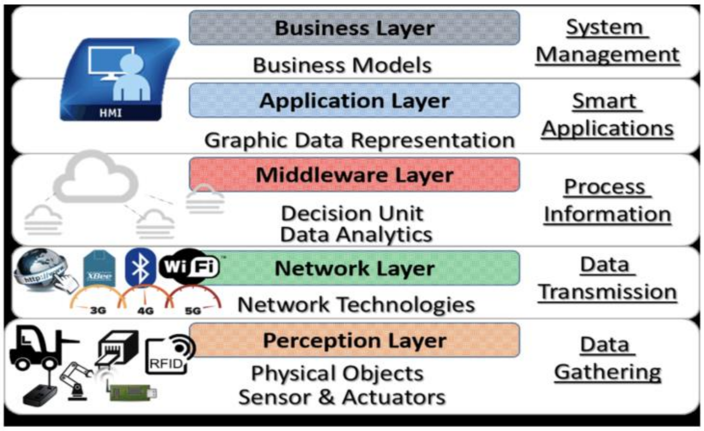


Figure 1 - IoMT 5-layer architecture (Antao et al., 2018)

The responsibilities of the five layers are described below.

Perception Layer

The perception layer consists of sensor devices to collect structured or unstructured information about the environment, such as radio frequency identification, infrared sensors and GPS (Kelly et al., 2020; Uslu et al., 2020). They identify other smart objects from the nodes and collect physical parameters and location information including patient medical information, medical device information and infrastructure location information, which are systematically converted into digital data and transmitted to the network layer (Islam et al., 2022; Djenna & Eddine 2018). This layer is important for patient health monitoring as these sensors ensure that patients are in an environment where their physical parameters are captured and monitored in real time, leading to timely and correct diagnosis (Alsubaei, 2017).

Network Layer

In this layer, data is communicated and interconnections between systems and platforms are managed (Uslu et al., 2020). The data collected by the perception layer is transmitted to the processing unit via wired or wireless network protocols. Objects communicate with each other mainly at high frequencies via technologies such as Zigbee, wi-fi and Bluetooth (Kelly et al., 2020). Data is then subsequently routed to the middleware layer (Nasiri et al., 2021).

Middleware Layer

Services and requesters are matched here according to names and addresses so that devices providing the same service are linked to the database for management and efficient data exchange (Al-Fuqaha et al., 2015; Verma et al., 2022). Furthermore, this layer filters out unnecessary data transmitted from the network layer and aggregates for data exploration (Islam et al., 2023). Technologies such as databases, cloud processing and big data processing are applied to process and make decisions to provide services to the lower layers and enable access control to the devices (Sethi & Sarangi, 2017).

Application Layer

Interfaces for users to connect with IoMT devices through the middleware are provided at this layer to allow users to access the services they request (Al-Fuqaha et al., 2015; Alsubaei et al. 2017). Here data is interpreted and applied to application-specific services for global management and to predict the future state of physical things (Nasiri et al., 2021). Currently, device applications are mostly driven by artificial intelligence and deep machine learning, which enables healthcare professionals to gain visibility into unseen situations and enhance diagnostic capabilities and optimise disease management with the help of big data analytics (Kelly et al. 2020).

Business Layer

This layer oversees and optimises the business logic and process cycle of the entire IoMT architecture (Alsubaei et al., 2017; Verma et al., 2022). Data from the application layer is transferred to this layer to create models and process diagrams for different businesses, and the IoMT system is designed, implemented, and developed here (Alsubaei et al., 2017). This layer also includes monitoring and management of other layers and user privacy (Al-Fuqaha et al. 2015).

2.2 What is Cyberattack?

A cyberattack is any unauthorised act that breaches the security policy of a cyber asset, targeting computer systems or networks to steal, alter, or destroy critical data (Biju et al., 2019; Li & Liu, 2021). Cyberattacks may be conducted by individuals or organised groups. The objective is to gain access to critical data so that it can be stolen, altered, or tampered with (Biju et al., 2019; Li & Liu, 2021). This kind of attack leads to compromised data and disruption, and subsequent cybercrimes including information and identity theft (Biju et al., 2019).

Types of Cyberattack in IoMT

Nissim and Kintzlinger (2019) stated that a cyberattack in healthcare can be defined as any effort to gain unauthorised access with the aim of stealing, modifying, destroying, or disabling personal or medical data. Thus, understanding the various types of cyberattack is crucial for preventing them and enhancing the protection of sensitive medical information and patient privacy.

Previous study has typically classified cyberattack into two categories: passive and active. Aijaz et al. (2021) further classified active attacks into more specific classes such as modification, interruption, and fabrication attacks under active attacks (see Figure 2). Frumento (2019) proposed similar broad categories of cyberattack: opportunistic attacks (OAs) and targeted attacks (TAs). OAs are more passive which is characterised by the attacker deploying a wide variety of available offensive tools against a lot of domains and users (Frumento, 2019). While the TAs are executed by skilled individuals using sophisticated techniques and 'human engineering' to target specific entities (Frumento, 2019).

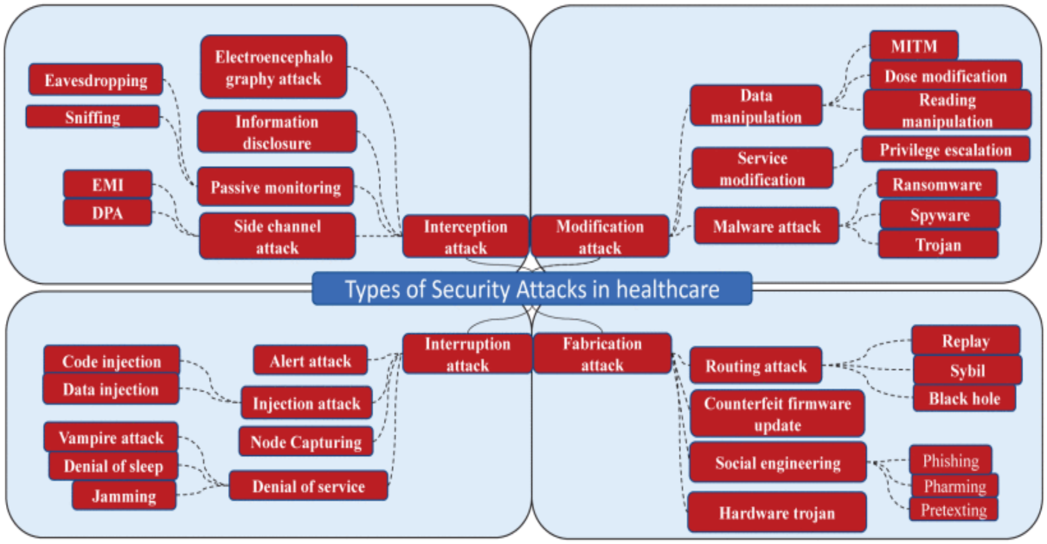


Figure 2: Cyberattacks in the healthcare system (Aijaz et al., 2021)

Alsubaei et al. (2017) categorise the methods of IoMT attack into four types: social engineering, configuration/implementation error, software/hardware bugs and malware based on the negative influence of attacks. Whereas Razaque et al. (2019) classify the cyberattack according to the flow of medical data and cybersecurity vulnerabilities in medical domain systems into four main types: information collection, database, website, and operation device (see Figure 3).

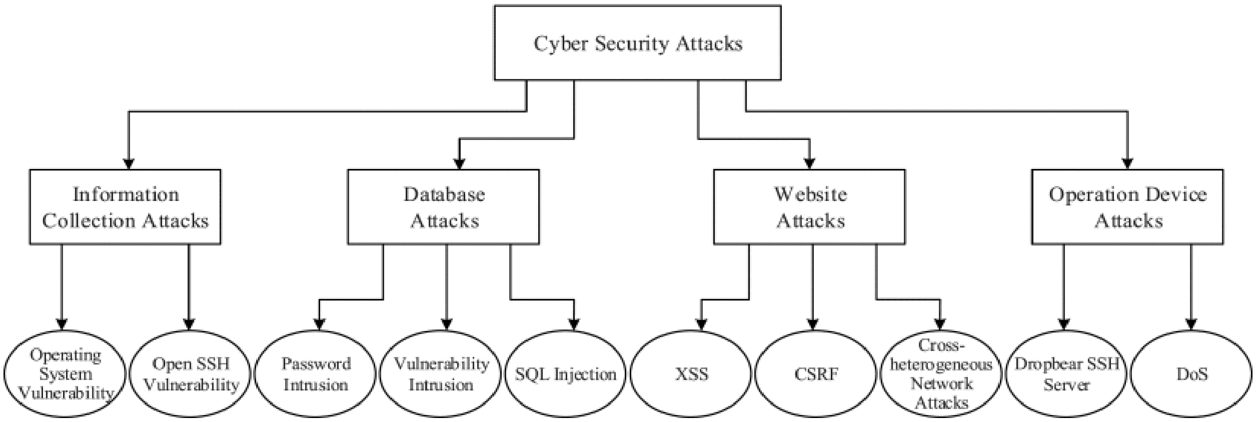


Figure 3: Classification of cyber security attacks (Razaque et al., 2019)

These studies collectively advance the understanding of cyberattack within healthcare IoT but do not sufficiently address how different types of attacks impact the various architectural layers of IoT systems. This omission highlights a significant gap: there is a pressing need for targeted research aimed at identifying specific vulnerabilities across the different layers of healthcare IoT architectures.

3. Case Analysis

3.1 Cases in Cyberattack and IoMT

Healthcare organisations under the structure of IoMT face a rising threat of cyberattack, which leads to a significant risk to the data security and the continuous operation of the organisations.

Cyberattack may target individual devices in the system, such as medical imaging equipment that is vulnerable to cybersecurity threats. Israeli experts demonstrated how to secretly hack a computed tomography scanner (Mirsky et al., 2019). By using artificial intelligence-related computer algorithms, they developed a manipulation framework called CT-GAN that could be automatically executed by malware (Solomon, 2018). The Picture Archiving and Communication System used to manage CT scanners and the standard formats used for data transfer and storage are exposed to the Internet without encryption (Kovacs, 2019). Attackers could thus install CT-GAN that controls the entire CT operation easily and modifies imaging records (Solomon, 2018). This not only led to misdiagnosis but also made patients' personal information available to the attackers for ransom (Kan, 2019).

However, cyberattack to a single layer can have an impact on the entire IoMT system and its operation. Denial of service (DoS), a form of physical attack, is the most destructive threat to IoMT (Djenna & Eddine, 2018). A children's hospital in Boston suffered such an attack in 2014, when its legitimate communications were blocked because its IP addresses were flooded with spam data to overload the system (Radware, 2015). The hospital suffered huge losses since the Internet services it provided were affected, including prescription delivery and loss of access to electronic health records and internal e-mail systems, resulting in administrative closure (Wall, 2022).

Malware is now the most serious threat to cybersecurity in healthcare (Thamer & Alubady, 2021). In 2017, a windows vulnerability was exploited to compromise computers in 150 countries through a ransomware called

WannaCry (Branch et al, 2017). WannaCry blocked communication between devices by encrypting valuable files or locked down computers (Zaman et al, 2022). Several UK health organisations were disrupted for four days because hospitals, ambulance services and doctors' offices were locked out of their digital systems and medical equipment (Bhosale et al., 2021). Clinical and surgical appointments were cancelled and ambulance routes were altered (Bhosale et al., 2021). The attack exposed patients' lives to great danger and thus the hospitals lost money and reputation.

Recognising the enormous impact of cyberattack, health organisations have begun to take measures to defend IoMT against such attack. According to Reagin and Gentry (2018), perimeter defenses such as antivirus software and firewalls are the preferred choice in healthcare to protect application endpoint devices. Blockchain is also increasingly being used to dynamically encrypt and secure data sharing and patient information storage across network systems (Kuo, 2019). Control of user access to systems through multi-factor authentication and monitoring of user account log activity is also being implemented. UK health organisations have adopted attack surface reduction rules to monitor their remote access infrastructure, which lets them respond to anomalies promptly (Zorz, 2020). In addition, the National Health Service (NHS) has started using the Data Security and Protection Toolkit to conduct security risk assessments for organisations that need access to NHS patient information and systems, which is important to ensure business continuity (He et al., 2021).

3.2 Impacts of Cyberattack on IoMT Architecture

Real-world evidence has demonstrated the serious challenges healthcare institutions face due to cyberattack. Various literature has studied the impact of cyberattack on IoT-based systems across the industry from the point of view of system architecture, assessing the different security challenges faced across layers (Lin et al., 2017; Xu et al, 2020; Msgna, 2022). With the continuous development of organisational IoMT and the increased support of IoT for intelligent healthcare (Minoli et al., 2017; Koutli et al., 2019), the possibility of advanced forms of cyberattack and vulnerabilities has also increased. As a result, IoMT must be designed to meet essential requirements in the areas of data security, patient privacy protection, and overall system reliability. (Islam et al., 2015). Analysing primary assets, different threat events, vulnerabilities, and potential impacts at each layer specifically could help better understand how to manage the influence of cyberattack on the IoMT architecture.

Assets

Assets are the valuable components that play crucial roles in the overall functioning of the organisational system. These can be categorised into physical objects, data, links or protocols, and software (Msgna, 2022). The primary assets in the healthcare industry include wearable devices, environmental devices, fixed devices, and the data collected by these devices (Alsubaei et al., 2017; Verma et al., 2022). The network layer transmits the collected data through wired and wireless methods, making communication protocols that define data exchange standards between devices and systems significant assets (Verma et al., 2022). The middleware layer controls data collection and filtering through IoT platforms, databases, and cloud storage (Verma et al., 2022). Mobile health apps and web portals in the application layer provide patients with access to their health data and facilitate communication. Lastly, the business layer encompasses vital business data and insights for strategy and decision-making.

Threats

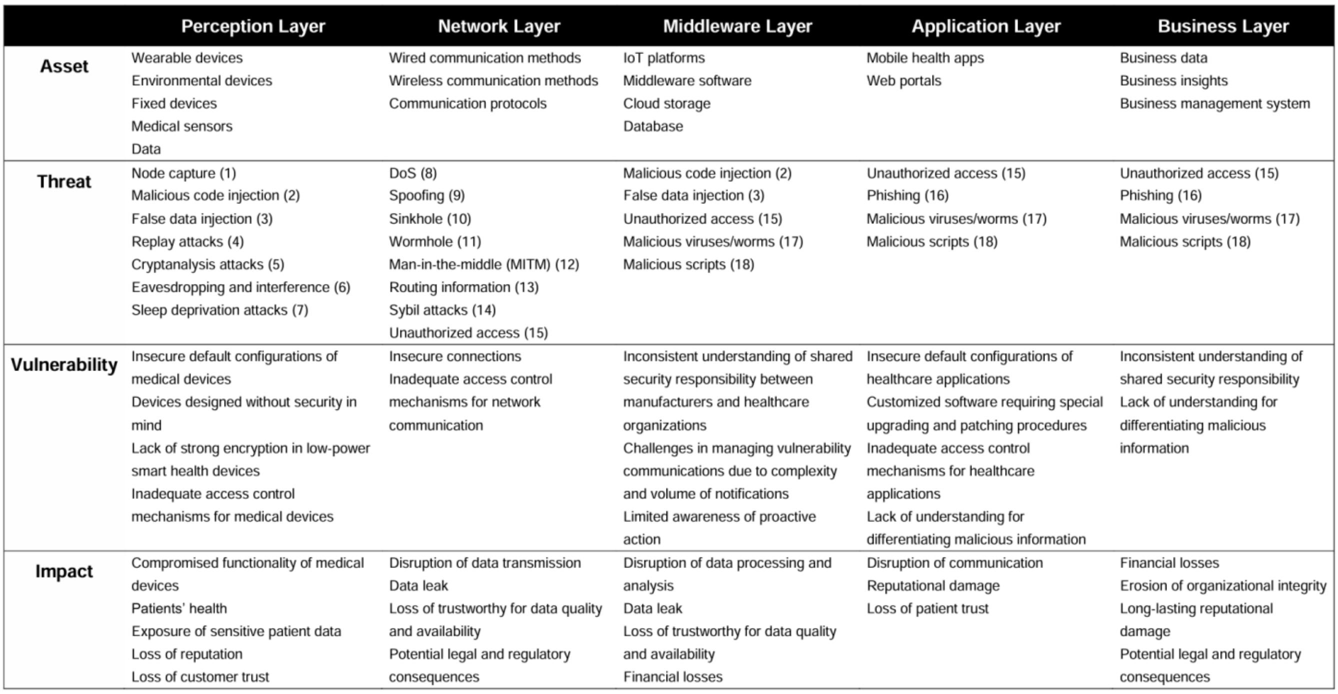
The threat delivered by cyberattack is a deliberate activity with the potential for causing harm to IoMT architecture. For example, networked medical devices can be reprogrammed, reconfigured, disabled, or even forged by malicious behavior (Djenna & Eddine, 2018). Previous findings have revealed that the perception layer faces possible threats such as unauthorised access or control (1), installation of malicious software (2), injection of inaccurate or misleading data(3), capturing and replaying previously transmitted data to deceive devices (4), cryptanalysis among sensors to extract private information (5), intercepting or interfering with device communication (6), and exhausting device battery or resources(7) (Lin et al., 2017; Xu et al., 2020). In the network layer, cyberattack is mostly related to wireless connectivity and include DoS (8), impersonating legitimate devices or users (9), attracting network traffic to a compromised node (10), creating unauthorised hidden communication channels between compromised nodes (11), intercepting and manipulating transmitted data (12), tampering with routing information (13), creating multiple fake identities (14), and unauthorised access (15) (Lin et al., 2017; Xu et al., 2020). The application layer is primarily susceptible to software attacks, such as phishing (16), spreading self-replicating malicious code (17), and injecting malicious scripts (18) (Lin et al., 2017; Xu et al., 2020). This proposed approach can be implemented in IoMT architecture with appropriate adjustments made to accommodate the unique characteristics of the specific assets.

Vulnerabilities

IoMT architecture is vulnerable to cyber threats due to the large amounts of valuable private data flowing through and within its layers. Many medical devices possess significant vulnerabilities in their cybersecurity, including default settings that lack adequate security measures, proprietary software that necessitates specialised processes for upgrades and patches, and a design process that fails to prioritise security considerations from the outset (GAO, 2023). Additionally, there is an inconsistent understanding of shared security responsibility between manufacturers and healthcare organisations (GAO, 2023). Smart health devices are typically low power and often lack strong encryption. This can lead to insecure connections and potential exposure of sensitive information over the Internet (Ahamed & Rajan, 2016). Furthermore, inadequate access control mechanisms enable attackers to view or modify personal data. Healthcare institutions also face challenges in managing vulnerable communications due to the complexity and volume of notifications, as well as limited awareness of proactive resource utilisation (GAO, 2023). This lack of awareness can be exploited by attackers through psychological manipulation techniques such as phishing emails, malicious calls and text messages, and tricking employees and users into leaking sensitive information (Lin et al., 2017; Msgna, 2022).

Impacts

Impacts are the negative consequences that arise when threats successfully exploit vulnerabilities in assets. Alsubaei et al. (2017) mentioned that one of the most critical impacts is the potential risk to patient health since compromised medical devices may impair functionality, putting patients in danger or delaying critical care. Furthermore, the exposure of sensitive patient data could violate privacy and potentially lead to identity theft (GAO, 2023). The monetary impact can be substantial because healthcare organisations need to allocate additional budgets to restore compromised data and hardware, as well as to resume business operations (Alsubaei et al., 2017; GAO, 2023). Moreover, any tangible or intangible loss resulting from a cyberattack can lead to a loss of brand value and patient trust (Alsubaei et al., 2017).



	Perception Layer	Network Layer	Middleware Layer	Application Layer	Business Layer
Asset	Wearable devices Environmental devices Fixed devices Medical sensors Data	Wired communication methods Wireless communication methods Communication protocols	IoT platforms Middleware software Cloud storage Database	Mobile health apps Web portals	Business data Business insights Business management system
Threat	Node capture (1) Malicious code injection (2) False data injection (3) Replay attacks (4) Cryptanalysis attacks (5) Eavesdropping and interference (6) Sleep deprivation attacks (7)	DoS (8) Spoofing (9) Sinkhole (10) Wormhole (11) Man-in-the-middle (MITM) (12) Routing information (13) Sybil attacks (14) Unauthorized access (15)	Malicious code injection (2) False data injection (3) Unauthorized access (15) Malicious viruses/worms (17) Malicious scripts (18)	Unauthorized access (15) Phishing (16) Malicious viruses/worms (17) Malicious scripts (18)	Unauthorized access (15) Phishing (16) Malicious viruses/worms (17) Malicious scripts (18)
Vulnerability	Insecure default configurations of medical devices Devices designed without security in mind Lack of strong encryption in low-power smart health devices Inadequate access control mechanisms for medical devices	Insecure connections Inadequate access control mechanisms for network communication	Inconsistent understanding of shared security responsibility between manufacturers and healthcare organizations Challenges in managing vulnerability communications due to complexity and volume of notifications Limited awareness of proactive action	Insecure default configurations of healthcare applications Customized software requiring special upgrading and patching procedures Inadequate access control mechanisms for healthcare applications Lack of understanding for differentiating malicious information	Inconsistent understanding of shared security responsibility Lack of understanding for differentiating malicious information
Impact	Compromised functionality of medical devices Patients' health Exposure of sensitive patient data Loss of reputation Loss of customer trust	Disruption of data transmission Data leak Loss of trustworthy for data quality and availability Potential legal and regulatory consequences	Disruption of data processing and analysis Data leak Loss of trustworthy for data quality and availability Financial losses	Disruption of communication Reputational damage Loss of patient trust	Financial losses Erosion of organizational integrity Long-lasting reputational damage Potential legal and regulatory consequences

Table1. Cyberattack impacts on IoMT Architecture

4. Discussion

While progress has been made in understanding and addressing the risks and vulnerabilities associated with IoMT systems, there are still numerous challenges that need concentrated attention and solutions. By examining every layer of the IoMT architecture, distinct challenges influenced by cyberattack that impact all five layers of the architecture are listed below:

Challenge 1: Complexity and Volume of Vulnerability Notifications

The Middleware Layer specifically mentions the difficulty in managing vulnerability communications due to the complexity and volume of these notifications. The IoMT ecosystem includes numerous IoT platforms, middleware software, cloud storage, and databases, making it difficult to keep track of vulnerabilities and security patches. Each component may have its own set of vulnerabilities and updates, resulting in a flood of notifications for healthcare organisations to handle. This challenge can result in delays or oversight in applying critical security patches, leaving systems vulnerable to cyberattack (Al-Turkistani et al., 2019). It also raises the possibility of security breaches and compromises, putting sensitive patient data and medical device integrity at risk (Zambare & Liu, 2024).

Challenge 2: Inadequate Access Control Mechanisms Across Layers

Vulnerabilities due to insufficient access control mechanisms are identified at multiple layers, including the Threat, Middleware, Application, and Business Layers. This identifies a widespread problem in which unauthorised access to sensitive data and critical systems is not adequately addressed. Weak access controls can be the result of insecure default configurations, a lack of encryption, or insufficient authentication mechanisms (Mawel & Sambasivam, 2023). Inadequate access controls allow for a variety of cyber threats, such as unauthorised access, data breaches, and manipulation of medical devices and patient data. This can result in decreased patient safety, a loss of trust in healthcare services, and regulatory noncompliance.

Challenge 3: Inconsistent Understanding of Shared Security Responsibility

The Middleware and Business Layers highlight issues caused by manufacturers and healthcare organisations' inconsistent understanding of shared security responsibility. This suggests a lack of clarity or agreement on who is responsible for ensuring the security of IoMT systems and data. Manufacturers may believe that healthcare organisations are solely responsible for implementing security measures, whereas healthcare organisations may expect manufacturers to provide inherently secure products. This challenge can lead to gaps in security measures because both parties may overlook critical aspects of security. It can also cause disagreements or delays in addressing security flaws and implementing necessary safeguards (GAO, 2023). Finally, it undermines the overall security posture of IoMT systems, increasing the likelihood of successful cyberattacks.

To address the specific challenges that have been identified in each layer of the IoMT framework, resolutions are listed below for each challenge:

Solutions to challenge 1:

Threat Layer:

- Apply automated threat detection systems to identify and prioritise vulnerabilities based on severity (Amthor et al., 2019).
- Develop platforms for sharing threat intelligence to enhance cooperation among healthcare organisations and security researchers, enabling them to identify and address new security threats effectively (Mavzer et al., 2021).

Middleware Layer:

- Use centralised vulnerability management platforms to consolidate and streamline vulnerability notifications from IoT platforms, middleware software, cloud storage, and databases (Mira & Alsmadi, 2019).
- Implement automated patch management systems to ensure that security updates are deployed in a timely manner across all middleware components (Mira & Alsmadi, 2019).

Application Layer:

- To improve security in mobile health apps and web portals, integrate vulnerability scanning tools during development and testing.
- Establish open lines of communication between application developers and security teams so that vulnerability notifications can be addressed quickly, and patches can be applied accordingly.

Solutions to challenge 2:

Threat Layer:

- To prevent medical devices and sensitive data from unauthorised access, implement robust authentication mechanisms (Kumar et al., 2021), such as multi-factor authentication, within the Threat Layer.
- Encrypt communication channels between nodes to prevent eavesdropping and data interception (Mawel & Sambasivam, 2023).

Middleware Layer:

- Establish role-based access control (RBAC) policies to restrict access to sensitive data and critical system functions, based on the roles and privileges of users (Ameer et al., 2023).
- Use encryption-at-rest and encryption-in-transit mechanisms to protect data stored in the cloud and transferred between middleware components.

Application Layer:

- Include strong user authentication and authorisation mechanisms in mobile health apps and web portals to ensure that only authorised users can access patient data and perform sensitive tasks.
- Use secure coding techniques and frameworks to create applications that are resistant to common vulnerabilities like SQL injection (Gupta et al., 2023) and cross-site scripting (XSS) (Sharma & Babbar, 2023) attacks.

Solutions to challenge 3:

Middleware Layer:

- To ensure security, IoT platform providers, middleware vendors, and healthcare organisations should have clear contractual agreements outlining their responsibilities (Marquardson & Asadi, 2023).
- Provide comprehensive security documentation and guidelines to healthcare organisations for the secure configuration and use of middleware components.

Business Layer:

- Encourage open communication and collaboration among manufacturers, healthcare organisations, and regulatory bodies to standardise security requirements for IoMT systems.
- Conduct regular security awareness training sessions for both manufacturers and healthcare professionals to ensure a shared understanding of security best practices and regulatory compliance requirements (Bhushan et al., 2023).

5. Conclusion

This report has investigated the impact of cyberattack on the Internet of Medical Things (IoMT) architecture across the five layers by evaluating assets, threats, vulnerabilities, and related consequences. Challenges include the complexity and volume of vulnerability notifications, inadequate access control mechanisms, and an inconsistent understanding of shared security responsibility.

This research focuses on the need for a more comprehensive understanding of the unique security challenges posed by the integration of IoT in the healthcare industry. This paper also emphasises the importance of implementing robust security measures across all layers of the IoMT architecture to mitigate the risk of cyberattacks. Therefore, the prioritisation of cybersecurity as an integral part of healthcare organizations' IoMT strategy has been recommended. This involves investing in advanced security technologies, developing accountable access policy, providing regular security training, and fostering a culture of security awareness.

6. Limitation

This study faces several limitations. Firstly, it relies on secondary research, including literature reviews and existing case studies, which might not capture the full spectrum of cyber threats or the most recent advancements in cyberattack methods. Future studies could employ qualitative research methods such interviewing cybersecurity experts and healthcare professionals to gather up-to-date information on the evolving landscape of IoMT architecture. Secondly, our study predominantly addresses the theoretical frameworks and potential impacts of cyber threats, lacking empirical data to quantify the real-world consequences of these attacks on healthcare systems. Therefore, conducting surveys, analysing incident reports, and examining post-attack recovery processes to obtain actual data could be leveraged in future exploration. This could provide more concrete and actionable insights for healthcare organisations to enhance their cybersecurity strategies.

7. References

Ahamed, J., & Rajan, A. V. (2016). Internet of Things (IoT): Application systems and security vulnerabilities. 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA), 1-5.

Aijaz, M. A., Nazir, M., & Anwar, M. N. (2021). Classification of Security Attacks in Healthcare and associated Cyber-harms. 2021 First International Conference on Advances in Computing and Future Communication Technologies (ICACFCT), 166-173.

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2444095

Al-Turkistani, H. F., Aldobaian, S., & Latif, R. (2021). Enterprise Architecture Frameworks Assessment: Capabilities, Cyber Security and Resiliency Review. 2021 1st International Conference on Artificial Intelligence and Data Analytics (CAIDA), Artificial Intelligence and Data Analytics (CAIDA), 2021 1st International Conference On, 79–84. https://doi.org/10.1109/CAIDA51941.2021.9425343

Alsubaei, F. S., Abuhussein, A., & Shiva, S. G. (2017). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. 2017 IEEE 42nd Conference on Local Computer Networks Workshops (LCN Workshops), 112-120.

Ameer, S., Benson, J., & Sandhu, R. (2023). Hybrid Approaches (ABAC and RBAC) Toward Secure Access Control in Smart Home IoT. IEEE Transactions on Dependable and Secure Computing, 20(5), 4032-4051. https://doi.org/10.1109/TDSC.2022.3216297

Amthor, P., Fischer, D., Kühnhauser, W.E., & Stelzer,D. (2019). Automated Cyber Threat Sensing and Responding: Integrating Threat Intelligence into Security-Policy-Controlled Systems. Proceedings of the 14th International Conference on Availability, Reliability and Security. https://doi.org/10.1145/3339252.3340509

Antao, L., Pinto, R., Reis, J., & Goncalves, G. (2018). Requirements for Testing and Validating the Industrial Internet of Things. 2018 IEEE International Conference on Software Testing, Verification and Validation Workshops (ICSTW), Software Testing, Verification and Validation Workshops (ICSTW), 2018 IEEE International Conference on, ICSTW, 110–115. https://doi.org/10.1109/ICSTW.2018.00036

Bhosale, K. S., Nenova, M., & Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. 2021 Sixth Junior Conference on Lighting (Lighting), Lighting (Lighting), 2021 Sixth Junior Conference On, 1–6. https://doi.org/10.1109/Lighting49406.2021.9598947

Bhushan, B., Kumar, A., Agarwal, A. K., Kumar, A., Bhattacharya, P., & Kumar, A. (2023). Towards a Secure and Sustainable Internet of Medical Things (IoMT): Requirements, Design Challenges, Security Techniques, and Future Trends. SUSTAINABILITY, 15(7). https://doi.org/10.3390/su15076177

Biju, J. M., Gopal, N., & Prakash, A. J. (2019). Cyber Attacks and Its Different Types. International Research Journal of Engineering and Technology, 6(3): 70-74. DOI:10.35940/ijitee.L1019.10812S319

Branch, L. E., Eller, W. S., Bias, T. K., McCawley, M. A., Myers, D. J., Gerber, B. J., & Bassler, J. R. (2019). Trends in Malware Attacks against United States Healthcare Organizations, 2016-2017. Global Biosecurity. https://doi.org/10.31646/gbio.7

Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas, 113, 48-52. https://doi.org/10.1016/j.maturitas.2018.04.008

Djenna, A., & Saïdouni, D.-E. (2018). Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure. 2018 2nd Cyber Security in Networking Conference (CSNet), 1-4.

Frumento, E. (2019). Cybersecurity and the Evolutions of Healthcare: Challenges and Threats Behind Its Evolution. In G. Andreoni, P. Perego, & E. Frumento (Eds.), m_Health Current and Future Applications (pp. 35-69). Springer International Publishing. https://doi.org/10.1007/978-3-030-02182-5_4

Ganai, P., Bag, A., Sable, A., Abdullah, K. H., Bhatia, S., & Pant, B. (2022). A Detailed Investigation of Implementation of Internet of Things (IOT) in Cyber Security in Healthcare Sector. https://doi.org/10.1109/ICACITE53722.2022.9823887

Gupta, A., Tyagi, L. K., & Mohamed, A. (2023). A Machine Learning Methodology for Detecting SQL Injection Attacks. 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS),

Islam, M. M., Nooruddin, S., Karray, F., & Muhammad, G. (2022). Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. IEEE Internet of Things Journal, 10(4), 3611-3641. https://doi.org/10.1109/JIOT.2022.3228795

Islam, M. M., Nooruddin, S., Karray, F., & Muhammad, G. (2023). Internet of Things: Device Capabilities, Architectures, Protocols, and Smart Applications in Healthcare Domain. IEEE Internet of Things Journal, Internet of Things Journal, IEEE, IEEE Internet Things J, 10(4), 3611–3641. https://doi.org/10.1109/JIOT.2022.3228795

Kan, M. (2019). Scary Hacking Threat: Editing X-Ray Images to Add or Remove Cancer. Retrieved from PCMag: https://www.pcmag.com/news/scary-hacking-threat-editing-x-ray-images-to-add-or-remove-cancer

Kelly, J. T., Campbell, K. L., Gong, E., & Scuffham, P. (2020). The Internet of Things: Impact and Implications for Health Care Delivery [Viewpoint]. J Med Internet Res, 22(11), e20135. https://doi.org/10.2196/20135

Kintzlinger, M., & Nissim, N. (2019). Keep an eye on your personal belongings! The security of personal medical devices and their ecosystems. Journal of Biomedical Informatics, 95, 103233. https://doi.org/https://doi.org/10.1016/j.jbi.2019.103233

Koutli, M., Theologou, N., Tryferidis, A., Tzovaras, D., Kagkini, A., Zandes, D., . . . Vanya, S. (2019). Secure IoT e-Health Applications using VICINITY Framework and GDPR Guidelines. 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), 263-270.

Kovacs, E. (2019, April 5). Hackers Can Add, Remove Cancer From CT Scans: Researchers. Retrieved from SecurityWeek: https://www.securityweek.com/hackers-can-add-remove-cancer-ct-scans-researchers/

Kumar, J. N. S., Ravimaran, S., & Sathish, A. (2021). Robust Security With Strong Authentication in Mobile Cloud Computing Based on Trefoil Congruity Framework. JOURNAL OF ORGANIZATIONAL AND END USER COMPUTING, 33(6). https://doi.org/10.4018/JOEUC.20211101.oa11

Kuo, T.-T., Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms: A systematic review and healthcare examples. Journal of the American Medical Informatics Association : JAMIA, 26. https://doi.org/10.1093/jamia/ocy185

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186. https://doi.org/https://doi.org/10.1016/j.egyr.2021.08.126

Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. IEEE Internet of Things Journal, 4, 1125-1142.

Marquardson , J., & Asadi , M. (2023). Cybersecurity Assessment for a Manufacturing Company Using Risk Registers: A Teaching Case. Information Systems Education Journal, 21(3), 62-69.

Mavzer, K. B., Konieczna, E., Alves, H., Yucel, C., Chalkias, I., Mallis, D., Cetinkaya, D., & Sanchez, L. A. G. (2021). Trust and Quality Computation for Cyber Threat Intelligence Sharing Platforms. 2021 IEEE International Conference on Cyber Security and Resilience (CSR), Cyber Security and Resilience (CSR), 2021 IEEE International Conference On, 360–365. https://doi.org/10.1109/CSR51186.2021.9527975

Mawel, M., & Sambasivam, S. (2023). Exploring the Strategic Cybersecurity Defense Information Technology Managers Can Implement to Reduce Healthcare Data Breaches. Information Systems Education Journal, 21(2), 4-11.

Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT Considerations, Requirements, and Architectures for Smart Buildings—Energy Optimization and Next-Generation Building Management Systems. IEEE Internet of Things Journal, 4, 269-283.

Mira, F., & Alsmadi, I. (2019). Review of Analysis on IoT Components, Devices and Layers Security. 2019 International Conference on Information Science and Communications Technologies (ICISCT), Information Science and Communications Technologies (ICISCT), 2019 International Conference On, 1–6. https://doi.org/10.1109/ICISCT47635.2019.9012037

Mirsky, Y., Mahler, T., Shelef, I., & Elovici, Y. (2019). CT-GAN: Malicious Tampering of 3D Medical Imagery using Deep Learning.

Msgna, M. (2022). Anatomy of attacks on IoT systems: review of attacks, impacts and countermeasures. Journal of Surveillance, Security and Safety.

Nasiri, S., Sadoughi, F., Dehnad, A., Tadayon, M., & Ahmadi, H. (2021). Layered Architecture for Internet of Things-based Healthcare System: A Systematic Literature Review. Informatica, 45. https://doi.org/10.31449/inf.v45i4.3601

Nayak, J., Meher, S. K., Souri, A., Naik, B., & Vimal, S. (2022). Extreme learning machine and bayesian optimization-driven intelligent framework for IoMT cyber-attack detection. The Journal of Supercomputing, 78(13), 14866-14891. https://doi.org/10.1007/s11227-022-04453-z

Radware. (2015, October 20). DDoS Case Study: Boston Children's Hospital DDoS Attack Mitigation. Retrieved from Radware: https://www.radware.com/security/ddos-experts-insider/ert-case-studies/boston-childrens-hospital-ddos-mitigation-case-study/

Razaque, A., Amsaad, F., Khan, M. J., Hariri, S., Chen, S., Siting, C., & Ji, X. (2019). Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain. IEEE Access, 7, 168774-168797. https://doi.org/10.1109/ACCESS.2019.2950849

Reagin, M. J., & Gentry, M. V. (2018). Enterprise Cybersecurity: Building a Successful Defense Program. Frontiers of Health Services Management, 35(1), 13-22. https://doi.org/10.1097/hap.0000000000000037

Riazul Islam, S. M., Kwak, D., Humaun Kabir, M., Hossain, M. S., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. IEEE Access, 3, 678-708.

Sharma, A., & Babbar, H. (2023). Safeguarding Web Environments Through Supervised Learning-Based Cross-Site Scripting Detection. 2023 3rd International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON)

Sethi, P., & Sarangi, S. R. (2017). Internet of Things: Architectures, Protocols, and Applications. Journal of Electrical and Computer Engineering, 2017. https://doi.org/10.1155/2017/9324035

Solomon, S. (2018). Medical imaging devices are vulnerable to cyber-attacks, Israeli team warns. Retrieved from The Times of Israel: https://www.timesofisrael.com/medical-imaging-devices-are-vulnerable-to-cyber-attacks-israeli-teams-warns/#openwebComments

Thamer, N., & Alubady, R. (2021). A Survey of Ransomware Attacks for Healthcare Systems: Risks, Challenges, Solutions and Opportunity of Research. 2021 1st Babylon International Conference on Information Technology and Science (BICITS),

Tripathi, V., Devesh, P., Singh, B., Pant, V., & Kumar, V. (2019). A Comprehensive Analysis and Solution of Cyber Attacks using Machine Learning Techniques. International Journal of Innovative Technology and Exploring Engineering, 8, 70-74. https://doi.org/10.35940/ijitee.L1019.10812S319

U.S. Government Accountability Office. (2023, December 21). Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination. Government Accountability Office. Retrieved May 8, 2024, from https://www.gao.gov/products/gao-24-106683

Uslu, B. Ç., Okay, E., & Dursun, E. (2020). Analysis of factors affecting IoT-based smart hospital design. Journal of Cloud Computing, 9(1), 67. https://doi.org/10.1186/s13677-020-00215-5

Verma, N., Singh, S., & Prasad, D. (2022). A Review on existing IoT Architecture and Communication Protocols used in Healthcare Monitoring System. Journal of The Institution of Engineers (India): Series B, 103(1), 245-257. https://doi.org/10.1007/s40031-021-00632-3

Wall, T. (2022). Throwback Attack: An "ethical" DDoS attack on a children's hospital. Retrieved from Industrial Cybersecurity Pulse: https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-ethical-ddos-attack-on-a-childrens-hospital/

Xu, H., Liang, F., & Yu, W. (2020). Internet of Things: Architecture, Key Applications, and Security Impacts. In X. Shen, X. Lin, & K. Zhang (Eds.), Encyclopedia of Wireless Networks (pp. 672-681). Springer International Publishing. https://doi.org/10.1007/978-3-319-78262-1_330

Zaman, S., Khandaker, M. R. A., Khan, R. T., Tariq, F., & Wong, K. K. (2022). Thinking Out of the Blocks: Holochain for Distributed Security in IoT Healthcare. IEEE Access, 10, 37064-37081. https://doi.org/10.1109/ACCESS.2022.3163580

Zambare, P., & Liu, Y. (2024). Understanding Security Challenges and Defending Access Control Models for Cloud-Based Internet of Things Network. In: Puthal, D., Mohanty, S., Choi, BY. (eds) Internet of Things. Advances in Information and Communication Technology. IFIPIoT 2023. IFIP Advances in Information and Communication Technology, vol 684. Springer, Cham. https://doi.org/10.1007/978-3-031-45882-8_13

Zorz, Z. (2020). Vulnerable VPN appliances at healthcare organizations open doors for ransomware gangs. Retrieved from Help Net Security: https://www.helpnetsecurity.com/2020/04/02/vpn-healthcare-ransomware