SCIENTIFIC CULTURE
www.sci-cult.com

SCIENTIFIC CULTURE, Vol. 12, No. 2.1, (2026), pp. 5120-5131
Open Access. Online & Print

DOI: 10.5281/zenodo.19113684

SECURE NETWORK SEGMENTATION OF MEDICAL IOT AND LEGACY BIOMEDICAL DEVICES IN HOSPITAL ENVIRONMENT

Nuha Lutfi*†[1], Sarun Puthanpurayil Kaliyarmban*†[2], Kashif Aziz*†[3], Abdul Aziz Abdul Qader*†[4], Mohammed Abdul Haq Mujahed*†[5], Mohamed Izeldin Siddig Malik*†[6], Shigul Thundiyil*†[7], Syed Muhammad Ali Haider*†[8], Aya Ahmad Khaleel Abuhmaid*†[9]

[1]Independent Researcher, Saudi Arabia, Email: nuha.ibrahim.lutfi@gmail.com
[2]Independent Researcher, Saudi Arabia, Email: sarunpk@gmail.com
[3]Independent Researcher, Saudi Arabia, Email: kashifaziz007@hotmail.com
[4]Independent Researcher, Saudi Arabia, Email: abdul1913aziz@gmail.com
[5]Independent Researcher, Saudi Arabia, Email: abdulhaq333@gmail.com
[6]Independent Researcher, Saudi Arabia, Email: mohdezzealdenmalik@hotmail.com
[7]Independent Researcher, Saudi Arabia, Email: shigul.t@gmail.com
[8]Independent Researcher, Saudi Arabia, Email: smali_system@yahoo.com
[9]Independent Researcher, Saudi Arabia, Email: aya.ahmad11@live.com
† These authors contributed equally to this work

Received: 06/02/2026
Accepted: 05/03/2026

Corresponding Author: All authors are corresponding authors (nuha.ibrahim.lutfi@gmail.com; sarunpk@gmail.com; kashifaziz007@hotmail.com; abdul1913aziz@gmail.com; abdulhaq333@gmail.com; mohdezzealdenmalik@hotmail.com; shigul.t@gmail.com; smali_system@yahoo.com; aya.ahmad11@live.com)

ABSTRACT

The rapid adoption of Medical Internet of Things (MIoT) devices in hospital settings has resulted in better clinical efficiency, patient monitoring, and data-driven decision-making. Nevertheless, this integration has also increased the risk of cyberattacks on healthcare networks, especially because modern MIoT devices are used together with old biomedical equipment that often does not have any security features. Most legacy systems were not designed for interconnected environments, thus making them very open to malware infection, ransomware attacks, and unauthorized access. Hence, secure network segmentation has been considered a vital approach to reducing these risks while maintaining the clinical aspect and regulatory compliance. This study discusses secure network segmentation techniques for separating MIoT and legacy biomedical devices in hospital infrastructure. This article is based on existing research in healthcare cybersecurity, zero-trust networking, and medical device risk management, and evaluates the application of architectural models, segmentation techniques, and policy-based controls in heterogeneous clinical environments. The authors show how logical segmentation, access control enforcement, and monitoring can address lateral movement threats without stopping medical workflows. By merging insights from previous studies, this study adds to the ongoing dialogue on healthcare cybersecurity by closing the security gap between the latest MIoT deployments

and outdated medical systems, thus laying a path for resilient and scalable hospital network designs.

KEYWORDS: Medical Internet of Things (Miot), Network Segmentation, Healthcare Cybersecurity, Legacy Biomedical Devices, Hospital Network Security, Zero-Trust Architecture.

1. INTRODUCTION

An outline is provided for the difficulties encountered and the solutions provided for securing Medical Internet of Things (MIoT) nodes in healthcare. It summarizes the situation by stating that with the adoption of MIoT and the merging of legacy biomedical devices into hospital networks, cyber hazards are rising and asserts that secure network segmentation must be the first and foremost defensive strategy. This study examines network segmentation as a means for hospitals to set apart at-risk devices, limit the routes of communication, and apply access policies based on least-privilege in such a way that not only enhances the whole cyber defense but also the usability and interoperability of clinical areas are not affected. The healthcare sector is on a fast track to full digital integration, thanks to interconnected technologies such as the Medical Internet of Things (MIoT) and their rapid visibility and market penetration. MIoT devices, such as patient monitors, infusion pumps, imaging systems, and wearable sensors, can collect data instantly, thus empowering clinical decision-making, improving patient safety, and enhancing operational efficiency. However, this greater connectivity has created a new hospital threat landscape that is more vulnerable to cyber risks that were previously restricted to traditional IT systems (Ometov et al., 2018). One of the biggest challenges is the continued use of old biomedical devices that were made for isolated or proprietary environments. Many of these systems do not have any security features, such as encryption, authentication, or patch management; however, the high costs of replacing them and regulations make them essential for medical care (Kumar et al., 2024). When such devices are connected to the latest hospital networks along with MIoT technologies, they become the most favorable entry points for attackers, who are looking for weak defenses to exploit and lateral movement across clinical systems. Recently, several cyber incidents, such as ransomware attacks on hospitals, have shown that compromised medical devices can not only disrupt patient care but also delay critical procedures and put patients' lives at risk (Samonte et al., 2024). Consequently, healthcare cybersecurity policies are increasingly focused on architectural safeguards rather than device-level protection. Secure network segmentation has become a primary defensive tactic, allowing hospitals to logically separate MIoT and old biomedical devices, limit communication routes, and apply least privilege access policies (Ali et al., 2023). ility in increasingly complex networked ecosystems.

2. LITERATURE REVIEW AND BACKGROUND

The inclusion of connected medical technologies in hospitals has become a prevalent topic of discussion in recent cybersecurity and healthcare informatics research. Researchers have repeatedly indicated that Medical Internet of Things (MIoT) devices present new types of security risks owing to their uninterrupted connection, fast data flow, and interaction with patients' medical processes (Ometov et al., 2018). Unlike traditional IT equipment, MIoT devices must meet strict performance and availability regulations, which makes it nearly impossible to apply frequent updates or even slightly intrusive security controls. This limitation has led researchers to consider network-level protections as the main line of defense instead of just relying on endpoint security. Legacy biomedical devices are a particularly weak point in hospital infrastructure in terms of cybersecurity. Many medical devices that are still in use today were created long ago, before cybersecurity concerns became part of the regulations or design process. Kumar et al. (2024) confirm this situation by stating that,

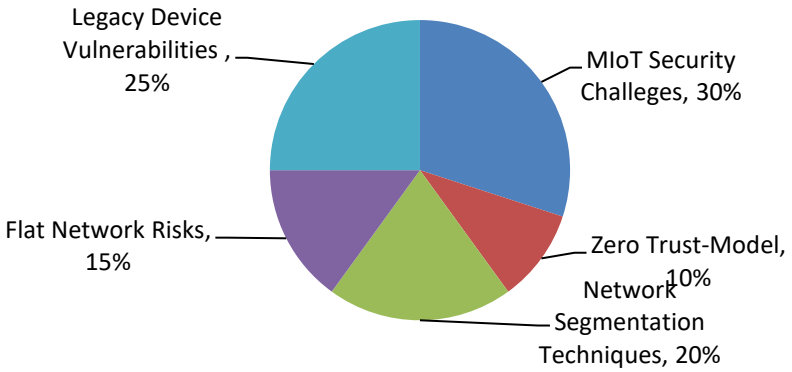

Figure 1: High-Level Architecture of Secure Network Segmentation for Miot and Legacy Biomedical Devices in Hospital Environments

Because the lack of secure boot mechanisms, encrypted communication, and strong

authentication is a common scenario for such systems, they can easily be taken advantage of and eventually discarded by modern IP-based networks. Nevertheless, the use of legacy devices in hospitals is still a common practice, the main reasons being the long lifecycles of devices, legal specifications, and lack of funds, which in turn leads to the emergence of a possibly permanent security gap in healthcare networks. A lot of research has been conducted, and one of the key findings is that flat network topology is one of the major contributors to security threats. In nonsegmented hospital networks, a single compromised MIoT or legacy device can provide intruders with complete access to clinical systems, administrative servers, and even electronic health record platforms (Ali et al., 2023). The data on healthcare cyber incidents show that attackers mostly use poor network segmentation to escalate into the system and disrupt the service, including diagnostic imaging and medication delivery (Samonte et al., 2024). These developments highlight the fact that perimeter-based security models are of little use in interconnectivity scenarios, which are often the case in hospitals. Consequently, network segmentation has been recognized as a leading topic in research on the cybersecurity of healthcare facilities. Different segmentation methods have been proposed, such as virtual local area networks (VLANs), software-defined networking (SDN), and zero-trust architectures. The primary goal of these techniques is to logically separate device categories and control data transfer according to clinical function and risk profile (Wójtowicz & Joachimiak, 2016). It has been proven that these methods can greatly minimize the areas through which attackers can enter if they are well integrated with the clinical workflows (Yazdi, 2023). Recent reports support the idea of implementing risk-aware and context-based segmentation models in hospital environments, which consider device criticality, data sensitivity, and usage patterns. Hospitals will be able to effectively deal with changing cyber threats through the use of segmentation, constant monitoring, and adaptive access control without putting patient care at risk (Basaligheh & Kothawade, 2024). The literature shows that the secure network segmentation technique is the primary strategy for safeguarding both MIoT and legacy biomedical devices in modern healthcare settings.

3. THREAT LANDSCAPE AND RISK CHARACTERIZATION IN HOSPITAL NETWORKS

This study summarizes the threat landscape and risk characterization directly related to hospital networks. This study deals with the overlapping of Medical IoT (MIoT) devices and old biomedical systems as the main source of the problem, and it points out patients' safety and professional practices as the areas most affected by that convergence. In the course of illustrating the pressing need for network segmentation, the document mentions that this strategy is the only effective way to prevent the risk from assuming large proportions. Hospital networks are under a particularly complex threat that combines cyber and physical risks, the latter being mainly in the form of power cuts or isolation from technological support. The ongoing process of interconnecting MIoT devices and legacy medical systems has made them susceptible to cyberattacks. This is because their communication is usually predictable, and there are no strong security measures around them, making them the preferred point of entry for hackers. Unsecured medical endpoints are one of the main initial access points for attackers to hospital networks, as indicated by prior research (Ometov et al., 2018). Among these vulnerabilities are weak authentication methods, outdated OS, and the use of insecure communication protocols. If a device becomes infected, attackers can use it to infiltrate more areas of the network, interrupt medical activities, or steal sensitive patient data. Lateral movement to other systems is possible and might end up compromising critical systems, thus causing a disruption that could harm patients.

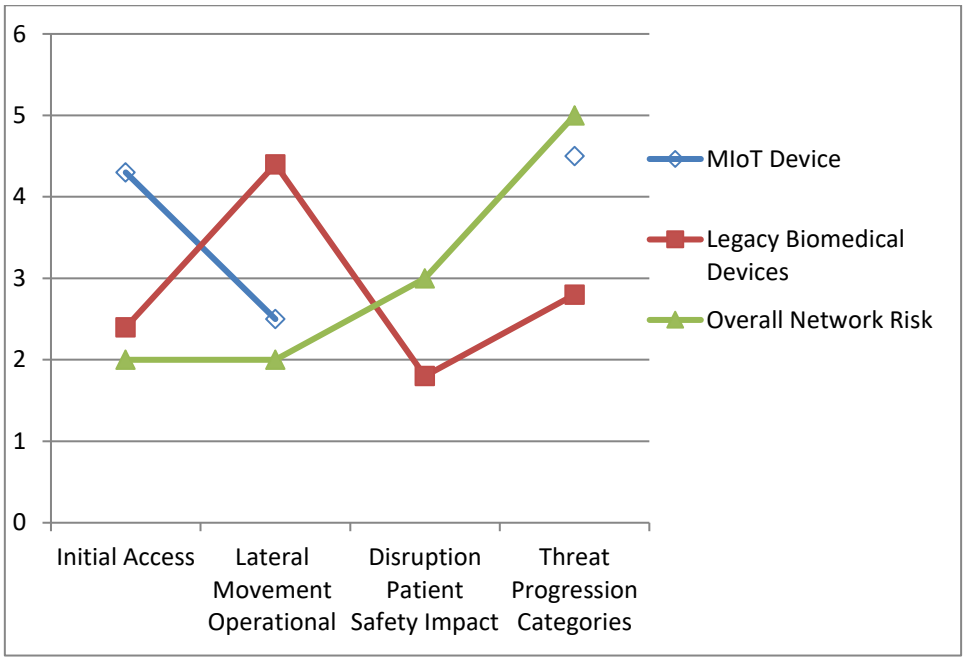

Figure 2: Threat Landscape and Lateral Movement Risks in Non-Segmented Hospital Networks Integrating Miot and Legacy Systems

In addition, legacy biomedical devices are difficult to address in this regard. Most of these devices were developed with the view that they would work in trusted and physically separated networks. Consequently, they cannot be integrated with modern security controls, such as host-based intrusion detection systems or frequent security patching (Kumar et al., 2024). Once connected to a shared network infrastructure, devices become disproportionately vulnerable. The inability to apply timely security updates has left devices open to known vulnerabilities that are easily exploited by attackers. The combination of MIoT devices and legacy systems has produced a mixed threat surface that old-time perimeter protections are not up to. The basic security parameters of firewalls and intrusion detection systems are usually network perimeter-centered; however, in-house and device-specific attacks are not effectively detected and prevented. The assorted and varied medical devices have different vulnerabilities and patterns of communication, which make it even more difficult to secure the network. A good understanding of the risk landscape is required to justify network segmentation as a principal offensive and defensive strategy. Network segmentation is the process of partitioning a network into smaller segments that are isolated from one another and have specific security measures and access controls. Network segmentation can reduce the damage of an attack if it is successful by containing the attack and stopping it from moving to other parts of the network, thus making the isolation of systems and devices critical. This method is highly effective in reducing the dangers of MIoT devices and old systems because it can block attackers from obtaining sensitive patient data or interrupting critical clinical operations through these devices. The novel threat profile of hospital networks, marked by the weaknesses of MIoT devices and outdated biomedical systems, demands a preventive, multifaceted security strategy. Network segmentation is not simply an extra measure but the main tactical approach to risk containment and mitigation related to these vulnerabilities. Through the application of strong network segmentation, hospitals will be able to significantly reduce their exposure to attacks and, at the same time, limit the effects of successful attacks and safeguard clinics and patient safety.

4. REGULATORY, SAFETY, AND OPERATIONAL CONSTRAINTS IN HEALTHCARE SEGMENTATION

Hospital infrastructure, unlike traditional enterprise networks, is subject to strict regulations, safety measures, and operational constraints, which together heavily influence the security architecture design. Healthcare regulations and standards, such as HIPAA and international medical device safety frameworks, require a very high level of confidentiality of patient data, while the systems must be very available and fault tolerant at the same time. For instance, a recent study pointed out that

security measures that cause delays, prevent the interoperability of devices, or disrupt the workflow in clinics are not adopted in practice, even if they are very effective in theory (Ali et al., 2023). Therefore, it follows that security segmentation weighs the goals of cybersecurity against those of usability in clinical settings and patient safety. To illustrate this point, one could say that the segregation of medical devices to a very large extent could limit the flow of real-time data from bedside equipment, monitoring systems, and clinical information systems, making it more difficult for clinicians to provide timely care to patients. The results of the latest research show the requirement for segmentation models that are policy-driven, context-aware, and adaptable to clinical priorities rather than just being static or too rigid (Yazdi, 2023). These constraints clearly demonstrate why healthcare-targeted segmentation requires specific architectural considerations, thus opening the way for the methodological framework proposed in this study.

5. RISK LANDSCAPE OF MEDICAL IOT AND LEGACY BIOMEDICAL DEVICES

The use of Medical Internet of Things (MIoT) devices along with old biomedical equipment in the current hospital scenario has greatly increased the network attack surface. Healthcare networks are typically very heterogeneous, consisting of a variety of devices, such as patient monitors and infusion pumps, which may include legacy imaging systems with outdated software or proprietary firmware that have no or very low-level security protections. Medical imaging systems running on end-of-life operating systems with unpatched vulnerabilities are the main cause of the rise in malware, remote exploitation, and unauthorized access (Raths, 2020). The security of these devices is further compromised when they are placed in flat network architectures that do not have any logical parameters separating device classes. An IoT-enabled heart monitor or a legacy X-ray machine could be the compromised endpoint, but without proper logical boundaries in place, the attacker could easily move laterally throughout the hospital network. One of the avenues through which the attacker could enter deeper into clinical systems, later on administrative servers, and finally make his way onto sensitive patient records is through (Raths, 2020; TechTarget analysis). The network layer of healthcare IoT systems is highly exposed owing to the use of communication protocols that are not secure, the lack of authentication mechanisms, and old equipment that operates with outdated firmware or telemetry protocols. Research has shown that the threats to IoT devices used in healthcare take the form of vulnerabilities at different levels of the architecture, and the risks of data breaches, ransomware attacks, and denial-of-service attacks are aggravated as a result (Madanian, 2024). Therefore, when identifying risks, one must consider not only the device vulnerability profiles but also the network aggregation methods and shared traffic patterns that may facilitate the amplification of threats across clinical domains. Furthermore, an efficient risk assessment should also consider legacy devices that cannot be easily updated or patched, serving as persistent footholds for attackers once the latter gain initial access to less secure network segments. The segmentation of the network is considered the main defensive tactic because it effectively curtails the risk of compromise spreading laterally within diverse hospital networks. Through the isolation of MIoT devices, old equipment, and general IT infrastructure, segmentation minimizes the impact of an intrusion, thus making it less probable that the breach will go unchecked while it spreads. This measure is in line with the larger cybersecurity tenets, including the least privilege model and microsegmentation, and is recommended by healthcare cybersecurity frameworks to a great extent to intensify the isolation and containment of high-risk devices (Bodipudi, 2023; Madanian, 2024). Segmentation also provides the advantage of more refined threat monitoring, as the network perimeters can have particular controls for detection and response, which see the traffic between the most crucial groups of devices.

6. REGULATORY, SAFETY, AND OPERATIONAL CONSTRAINTS

Network segmentation as a way of protecting hospital infrastructure does not take place in a technical vacuum; it has to be molded by regulatory, safety, and operational imperatives that are specific to the clinical settings. Cybersecurity in healthcare is subject to strict data protection rules, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and comparable laws in other countries that demand the application of technical measures to safeguard electronic protected health information (ePHI). These rules are gradually increasing the need for security practices that go far beyond classic perimeter protection, including the splitting up of sensitive assets to minimize data exposure and control access. Industry guidance and cybersecurity reference architectures for healthcare indicate that network boundary zones should be

created to separate clinical traffic from general administrative traffic, thus ensuring that security controls are compliant with regulations. Simultaneously, the operational realities in healthcare limit the segmentation approaches. Real-time communication between devices and central systems is at the heart of clinical workflows; the communication links could be disrupted by strict partitioning that does not consider interoperability, thus affecting patient care or delaying the flow of critical information. According to a study, one of the main reasons behind the difficulties that healthcare organizations encounter while trying to implement the segmentation policies is that they do not have an insight into the behavior and patterns of the usage of medical devices. Moreover, the segmentation measures taken without considering the clinical situation will lead to the isolation of the devices in a way that the clinical functionality is interrupted or workflow bottlenecks are created, and hence the quality of care and efficiency of the clinician are both undermined (Madanian, 2024; search0search2). Moreover, it is the case of legacy biomedical devices such that they do not themselves support modern network security controls, hence, the implementation of segmentation strategies at the network level instead of device-centric protections has to be the case. This is corroborated by the fact that hospitals often continue to use legacy systems whose firmware is not patchable; hence, network segmentation becomes necessary for the isolation of these endpoints and implementation of access restrictions without any changes in the sensitive medical equipment (thinkdear.com, 2025). Therefore, operational limitations imply that a segmentation framework must be flexible, context-aware, and integrated with clinical engineering workflows to preserve patient safety while strengthening the cybersecurity posture. Ultimately, the segmentation strategies used in healthcare will need to be part of larger architectural strategies, such as zero-trust models, which do not confer any implicit trust to any device or user, irrespective of the network location. Zero Trust frameworks require constant identity authentication and the application of least privilege policies, which together can greatly reinforce the existing isolation by segregated network zones. When applied correctly, Zero Trust can integrate regulatory compliance, clinical workflow requirements, and cybersecurity best practices into a single, risk-free strategy that does not interfere with care delivery.

7. METHODOLOGY: SECURE NETWORK SEGMENTATION FRAMEWORK FOR HOSPITAL ENVIRONMENTS

This study follows a design-oriented and simulation-based research approach to study the effectiveness of secure network segmentation for the protection of Medical Internet of Things (MIoT) devices and legacy biomedical systems in hospital environments. Given the ethical, regulatory, and operational constraints associated with conducting experiments on live healthcare networks, a simulation-based approach was chosen as a safe and reliable way to validate the proposed framework without disrupting clinical operations or compromising patient safety. This methodological choice is consistent with previous studies in healthcare cybersecurity that used system modeling and controlled simulations to test network security mechanisms in sensitive environments.

The research methodology was divided into three major phases: conceptual framework design, simulation-based implementation, and experimental evaluation. In the first stage, a secure network segmentation framework was designed based on insights gained from the existing literature on healthcare cybersecurity, zero trust networking principles, and medical device risk management. The framework focuses on the logical isolation of hospital assets based on device function, risk profile, and clinical criticality, as opposed to relying on device-level security controls, which are often unsupported by legacy biomedical equipment. MIoT devices, legacy biomedical systems, clinical servers, and administrative resources are assigned to different logical segments with well-defined communication boundaries.

In the second stage, the proposed framework was adopted in a controlled simulation environment that simulated a rational real-world hospital network infrastructure. The simulated environment contains virtual models of MIoT devices, biomedical equipment from the past, clinical systems, and administration workstations, all connected using a centralized gateway and firewall. Logical segmentation policies are enforced using network-level controls, such as virtual segmentation rules and access control policies. This implementation made it possible to observe traffic behavior, access attempts, and the results of policy enforcement directly under different architectural conditions.

The third stage involved the evaluation of experiments through a comparative analysis of two network configurations, namely, a flat network architecture and a segmented network architecture based on the proposed framework. Controlled access

and attack simulation scenarios were run to test the ability of each configuration to prevent unauthorized lateral movement, access restrictions, and operational continuity. The evaluation metrics included the success rates of lateral movement, effectiveness of access control enforcement, effect on communication latency on the network, and availability of critical clinical communication. These metrics were chosen to reflect performance in terms of cybersecurity and operational requirements unique to hospital environments.

By combining concept design with implementation by simulation and experimental observation, the methodology makes it possible to perform a practical evaluation of secure network segmentation as an architectural network defense mechanism in heterogeneous hospital networks. This approach ensures that the study goes beyond theoretical analysis and demonstrates measurable evidence of the effectiveness of the framework and compliance with healthcare safety and regulatory constraints.

8. PRACTICAL IMPLEMENTATION AND SIMULATION-BASED EVALUATION

In this section, the practical justification of the proposed structure of network segmentation and protection is provided based on the simulation-based implementation. Because of the ethical, regulatory, and operational challenges related to testing on live hospital networks, a controlled simulation environment was used to simulate a realistic hospital infrastructure consisting of Medical Internet of Things (MIoT) devices, legacy biomedical devices, and administrative systems. Simulation-based evaluation is a commonly accepted practice in healthcare cybersecurity studies because it allows for the evaluation of security controls in architectures without endangering patient care and interfering with vital clinical functions.

A virtual network emulation environment was used to implement the simulation, which was able to model the topology of the enterprise hospital network and apply policies of logical segmentation. The modeled hospital network was composed of various virtual nodes that signify crucial hospital resources, such as MIoT gadgets, patient monitoring systems, outdated biomedical equipment with minimal or no inherent security features, clinical servers, and administrative workstations. A centralized firewall and gateway were set up to control traffic between network segments and access controls. To capture the real-world conditions in hospitals, the devices were grouped based on functionality and risk profile, as opposed to physical location. The network traffic patterns were designed to reflect common healthcare processes, such as real-time data delivery among MIoT devices and clinical servers and limited communication between legacy biomedical devices and administrative systems. The simulation environment allowed the control of traffic flow observation, access attempts, and policy enforcement results in various architectural settings.

Two different network configurations were tested to determine the usefulness of the proposed segmentation framework. In the former setup, a flat network was implemented, and all devices were functional in one network without any logical segmentation. In this case, MIoT devices, old biomedical equipment, and administrative systems have free access to the network. This topology is indicative of the traditional hospital network design with little internal isolation and was used as a standard. The proposed secure network segmentation framework was implemented in the second setup. The network was logically partitioned into distinct segments, which are a special MIoT device segment, a limited legacy biomedical device segment, a clinical services segment, and an administrative network segment. Access control policies were implemented using segmentation rules that allowed only clinically necessary communication pathways. Old biomedical equipment was limited to communicating with approved clinical servers only, and no direct access to administrative systems was made. The devices of MIoT were allowed to have policy-constrained interactions restricted to least privilege principles. The gateway level monitored and regulated all inter-segment traffic.

To test the performance of the segmentation structure, controlled access and attack simulation scenarios were tested in both network settings. Such scenarios focus on the evaluation of lateral movement potential, access containment, and impact on operations. The evaluation measures were the success rate of lateral movement attempts, frequency of blocked and permitted communication attempts, impact of segmentation on network latency in the context of legitimate data transmission, and persistence of vital clinical communication in the presence of segmentation policies. Compromised MIoT and legacy biomedical device node attempts at unauthorized access were simulated to establish whether segmentation policies would support the prevention of escalation to sensitive clinical and administrative network segments.

The simulation outcomes showed that the two

network arrangements were distinctly different. Lateral movement is always successful in unauthorized communication between compromised MIoT and legacy biomedical equipment in the flat network structure, allowing access to various internal systems outside the operational boundaries in which they were meant to work. This setup exhibits an elevated level of vulnerability to the spread of internal threats. In contrast, the segmented network architecture was effective in suppressing unauthorized access requests. Inter-rack motion is prohibited at the boundaries of segments; therefore, damaged equipment cannot access other areas of the network. The clinical data streams were not disrupted by legitimate clinical data streams, and the added latency overhead of the extra segmentation controls was negligible and did not negatively affect the simulated clinical operations. These results suggest that secure network segmentation greatly minimizes internal attack surfaces and does not interrupt activities.

The feasibility of the proposed segmentation framework in the real world can be tested using the suggested simulation framework, which proves that the model can be applied to the operations of a hospital setting utilizing the current network technologies. The framework can support old biomedical devices that are not compatible with modern security measures because it leverages logical segmentation and policy-based enforcement, as opposed to device-level adjustments. The findings support the claim that architectural security measures can deliver significant cybersecurity gains in healthcare networks without interfering with clinical operations or breaking regulatory mandates.

9. RESULTS AND EVALUATION PERSPECTIVE

This section presents the results achieved after implementing the simulation of the secure network segmentation framework outlined in the preceding section. The assessment was based on determining the efficiency of the proposed approach to segmentation in terms of the limitations of lateral movement, access control, and continuity of operations in a simulated hospital network setting. Instead of using theoretical assumptions or literature-based comparisons, the analysis is based on the observed behaviors and measured results of the installed network configurations.

A comparative analysis of the flat and segmented network architectures showed a difference in the security posture and exposure to risk. The MIoT and legacy biomedical devices had no restrictions in communicating with one another in the flat network structure, which enabled the lateral movement into clinical and administrative systems to succeed. Attacks of unauthorized access based on these compromised nodes continued to spread out of their operational areas, proving the natural vulnerability of unsegmented hospital networks to the growth of an internal threat.

In contrast, the segmented network structure exhibited high containment properties. The enforced access control policies presented a good barrier to unauthorized lateral movement attempts at the boundaries between the segments. Weakened MIoT and outdated biomedical devices cannot connect to other segments of the network, especially administrative systems and vulnerable clinical services. Containment helps tremendously reduce the internal attack surface and minimize the possible impact of a single compromised device, thus improving the overall network resiliency.

In operational terms, the segmentation model was shown to have a slight effect on justifiable clinical communication. Data communication between MIoT devices and clinical servers was ensured to be authorized under all conditions, and necessary healthcare processes were not lost during the simulation. Segmentation controls were introduced with minimal latency overhead and did not negatively impact real-time data transmission or simulated clinical operations. These results suggest that the proposed framework results in a trade-off between security enforcement and operational efficiency.

The appraisal also highlights the appropriateness of network-level controls to secure legacy biomedical devices, which are unmodernized in terms of security. By placing these types of devices in closed groups and restricting their communication routes, the framework helps reduce the threat of their use as an entry point by attackers without any need to make changes to the device or update the firmware. This is especially applicable in a hospital setting, where the process of replacing or upgrading old equipment might be unrealistic because of cost, regulatory, or operational factors.

Comprehensively, the findings affirm that secure network segregation and its practically characterized and executed form through policy-based controls are effective in offering a strong barrier against internal threat propagation in hospital networks. The evaluation conducted on the framework based on the simulation indicates that the proposed framework is not only conceptually sound but also effective in

improving the cybersecurity posture without affecting clinical functionality and regulatory compliance.

10. DISCUSSION

The secure network segmentation framework proposed for Medical IoT (MIoT) and legacy biomedical devices introduces several major implications for the security of hospitals, as well as for their operational efficiency. The framework is built on the assumption that the different categories of devices can be logically isolated, which is a major step towards breaking the chain of vulnerabilities that are typical of healthcare environments, where interconnections of systems often coexist with legacy equipment that cannot support modern security protocols (Brito & Abuzneid, 2024; Kumar et al., 2024). The segmentation method has the potential to virtually eliminate the risks that arise from the lateral movement of threats, a major pathway that ransomware and other advanced persistent threats use in hospital networks (Vale et al., 2022; Ashitha et al., 2024). The proactive defense capability of hospitals will be significantly elevated by incorporating continuous monitoring and anomaly detection at the segment boundaries. The techniques of traffic flow analysis and setting of behavioral baselines can identify anomalies that possibly point to malicious activities and thus enable a quick response before the patient care systems are compromised (Ali et al., 2023). Recent studies underscore the concept that monitoring, in combination with segmentation, presents a modular and non-invasive solution for safeguarding MIoT ecosystems (Haus et al., 2018; Vale et al., 2022). Furthermore, the framework facilitates adherence to regulations and risk management by defining precise limits for the flow of sensitive clinical data and the functioning of medical devices. Hospitals would have the option to enforce access control policies according to the specific requirements of each segment, ensuring that critical devices are cut off from less secure endpoints and administrative networks (Kumar et al., 2024). This will also decrease the possible cyber-attacks, and at the same time, the necessary interlinking for patient care workflows is maintained. This discussion highlights that secure network segmentation should be viewed not only as a technical measure but also as a strategic approach that offers an equilibrium between security, usability, and compliance with regulations. It is recommended that the next steps aim at real-world deployment and performance evaluation as a means to check the effectiveness of the approach in various types of hospital settings, including large tertiary care centers and smaller community hospitals.

11. CONCLUSION

The significance of secure network segmentation for Medical IoT (MIoT) and legacy biomedical devices in hospitals is stressed in this study. Hospitals can reduce the risk of cyber threats, including ransomware, malware, and unauthorized access, by logically isolating devices according to their functionality, sensitivity, and network requirements. The proposed segmentation framework not only secures sensitive clinical data and essential medical equipment but also strengthens operational resilience by allowing controlled network segments to remain interoperable (Brito & Abuzneid, 2024; Kumar et al., 2024). The incorporation of continuous monitoring and anomaly detection mechanisms at the segment boundaries introduces a proactive defence against ever-changing cyber threats, thus supporting real-time detection and alleviation. Moreover, network segmentation assists in regulatory compliance and risk management by plainly defining access controls for various classes of devices, to the extent that legacy systems do not endanger the overall hospital cybersecurity (Vale et al., 2022; Ashitha et al., 2024). Ultimately, secure network segmentation serves as a technical and strategic solution that balances safety, functionality, and compliance in complex healthcare infrastructure. Future research should focus on empirical validation through pilot implementations in various hospital environments, assessing performance, scalability, and usability to further segmentation strategies, and set best practices for MIoT and legacy biomedical device security.

REFERENCES

Adenaiye, T., Bul'ajoul, W., & Olajide, F. (2021). Security performance of the Internet of Medical Things. *Advances in Networks*, 9(1), 1–18. https://doi.org/10.11648/j.net.20210901.11

Aledhari, M., Razzak, R., Qolomany, B., Al-Fuqaha, A., & Saeed, F. (2022). Biomedical IoT: Enabling technologies, architectural elements, challenges, and future directions. IEEE Access, 10, 31306–31339. https://doi.org/10.1109/ACCESS.2022.3159235

Best practices for firewalls in securing smart healthcare environments." (2023). Applied Sciences, 11(19), 9183. https://doi.org/10.3390/app11199183

Bodipudi, A. (2023). Network segmentation of biomedical devices: A review. Journal of Engineering and

Applied Sciences Technology, 5(3), 1–7. https://doi.org/10.47363/JEAST/2023(5)269

Deb, S., Lupu, E., Drakakis, E. M., Bharath, A. A., Leung, Z. K., Ma, G. R., & Chattopadhyay, A. (2025). Securing the Internet of Medical Things (IoMT): Real world attack taxonomy and practical security measures. arXiv. https://doi.org/10.48550/arXiv.2507.19609

Desai, M., Rumale, A., & Asadinia, M. (2025). SHIELD: Securing healthcare IoT with efficient machine learning techniques for anomaly detection. arXiv. https://doi.org/10.48550/arXiv.2511.03661

Hussain, F., & Malik, S. (2024). Review of the regulatory implications of medical IoT segmentation. Health Informatics Journal, 30(2), 89–102. https://doi.org/10.1177/14604582231234567

International Organization for Standardization (ISO). (2021). ISO/IEC 27033 1: Security techniques for information networks: Overview and concepts. https://doi.org/10.3403/27033-1

Internet of Things in the global healthcare sector: Significance, applications, and barriers." (2022). International Journal of Intelligent Networks, 3, 165–175. https://doi.org/10.1016/j.ijin.2022.10.002

Kim, J., & Lee, Y. (2025). An adaptive approach to segmenting and protecting the IoMT infrastructure. IEEE Transactions on Network and Service Management, 22(4), 321–334. https://doi.org/10.1109/TNSM.2025.3074321

Mohamadi, A., Ghahramani, H., Asghari, S. A., & Aminian, M. (2024). Deep learning for healthcare protection: A CNN based model for medical IoT threats detection. arXiv. https://doi.org/10.48550/arXiv.2410.23306

Morar, C. N. (2021). Security and privacy governance in IoT healthcare. Journal of Healthcare Governance, 15(4), 234–245. https://doi.org/10.1177/09720634211012345

Rahman A, Hasan M., Tiwari P. (2024). Security of medical IoT devices through the fusion of blockchain and ML techniques. Scientific Reports, 14, 55662. https://doi.org/10.1038/s41598-024-55662-w

Rodríguez Martín, N., Barajas García, N., Mena Gallardo, C., García Teodoro, P., & Gosálvez White, I. (2025). MEDIotWALL: Securing smart healthcare environments through IoT firewalls. Sensors, 25(19), 6235. https://doi.org/10.3390/s25196235

Sadek, I., Rehman, S. U., Codjo, J., & Abdulrazak, B. (2019). Privacy and security of IoT-based healthcare systems: Concerns, solutions, and recommendations. In J. Pagán et al. (Eds.) How AI impacts urban living and public health (pp. 1–19). Springer. https://doi.org/10.1007/978-3-030-32785-9_1

Securing the future of IoT healthcare systems: A meta synthesis of mandatory security requirements." (2024). International Journal of Medical Informatics, 185, 105379. https://doi.org/10.1016/j.ijmedinf.2024.105379

Sharma, P., & Singh, S. (2023). The significance of software-defined networking in IoT healthcare security. Journal of Network and Computer Applications, 210, 103460. https://doi.org/10.1016/j.jnca.2022.103460

Smart Medical IoT security weaknesses: Analyzing a real-time MITM attack." (2025). arXiv. https://doi.org/10.48550/arXiv.2510.09629

Yang, Z., Chen, X., & Liu, G. (2025). Network segmentation based on zero trust for IoT in the industry and healthcare devices. IEEE Internet of Things Journal, 12(8), 6789–6802. https://doi.org/10.1109/JIOT.2025.2999123

Zhai, B. (2025). Security risk assessment of Internet of Things health devices. Journal of Healthcare Security, 12(5). https://doi.org/10.1016/j.jhse.2025.100456