Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 2 August 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 188-206
DOI: https://doi.org/10.51903/jtie.v5i2.528

A Critical Evaluation of IoMT Security Frameworks in Resource-Constrained Healthcare Systems

Arinaitwe Winfred*[1], Kayeyo Margaret[2], Olusegun Ganiyu[3]
Email: winfred.arinaitwe@studmc.kiu.ac.ug, margaret.kareyo@kiu.ac.ug, ganiyu.shefiu@kiu.ac.ug
[1,2]*Department of Information Technology, Kampala International University, Uganda*
[3]*Department of Computer Science, Kampala International University, Uganda*
*Corresponding Author

Abstract
The increasing adoption of Internet of Medical Things (IoMT) technologies within healthcare systems has significantly improved real-time patient monitoring, clinical decision-making, and health information exchange. However, the integration of interconnected medical devices has simultaneously expanded the cybersecurity threat landscape, particularly within resource-constrained healthcare environments characterized by limited technical capacity, inadequate governance mechanisms, and insufficient cybersecurity expertise. This study critically evaluated existing cybersecurity frameworks for Information Sharing-Enabled IoMT systems, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework, COBIT, Critical Information Infrastructure Protection (CIIP), and the IoT Security Foundation (IoTSF) Security Compliance Framework. The study employed a mixed-method exploratory research design combining systematic literature review, comparative framework analysis, and descriptive quantitative assessment conducted at St. Francis Hospital Nsambya and Uganda Martyrs Hospital Lubaga. Quantitative findings were analyzed using descriptive statistics, while qualitative findings were synthesized thematically. The findings revealed that existing frameworks provide fragmented security solutions that inadequately integrate technical security controls, governance mechanisms, healthcare operational requirements, and socio-behavioral determinants necessary for secure IoMT implementation in low-resource healthcare contexts. Based on the identified gaps, the study proposes an integrated healthcare-oriented IoMT cybersecurity framework that combines governance, technical safeguards, compliance mechanisms, and socio-behavioral dimensions to strengthen secure information sharing and cybersecurity resilience within resource-constrained healthcare institutions. The study concludes that context-specific and integrated cybersecurity frameworks are essential for enhancing secure information sharing and sustainable IoMT adoption in developing healthcare systems.

Keywords: *Cybersecurity Frameworks, Healthcare Systems, Information Sharing, Internet of Medical Things, IoMT Security.*

I. INTRODUCTION

Healthcare systems are currently undergoing rapid digital transformation, which has resulted in increased adoption of Internet of Medical Things (IoMT) technology that connects medical devices and sensors with health information systems for use in patient care and clinical decision-making (Fikri & Muchlis, 2026; Udonna et al., 2025; Zahra et al., 2025). IoMT technologies enable healthcare organizations to conduct continuous patient monitoring and telemedicine services while they share medical data with other providers (Islam et al., 2022). Healthcare institutions face increased cybersecurity risks because information-sharing IoMT networks create wider entry points for cyber-attacks. Healthcare organizations have become more attractive targets for ransomware attacks, data breaches, and device manipulation because cybercriminals know that medical data holds high value, which supports their mission-critical operations (Coventry & Branley, 2023).

Received on April 2026; Revised on May 2026; Accepted on Juni 2026; Published on August 2026

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 2 August 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 188-206
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

Resource-constrained organizations experience increased risk because their financial restrictions, weak regulatory systems, and lack of cybersecurity experts prevent them from implementing proper security measures. Healthcare organizations struggle to apply existing cybersecurity frameworks, which protect information systems, to their specific needs in IoMT environments. Existing frameworks fail to meet healthcare requirements because they were developed to protect conventional enterprise systems, which cannot manage complex socio-technical systems that operate in real-time and safeguard patient safety.

Although existing cybersecurity frameworks such as the NIST Cybersecurity Framework, COBIT, CIIP, and IoTSF provide important governance, risk management, and technical security mechanisms, they remain insufficiently adapted to the operational realities of healthcare-based IoMT ecosystems in resource-constrained environments. Most existing frameworks emphasize isolated dimensions of cybersecurity, such as governance compliance, technical controls, or infrastructure resilience, while inadequately integrating healthcare-specific operational workflows, human behavioral dynamics, interoperability requirements, and contextual implementation challenges associated with low-resource healthcare systems. Furthermore, limited empirical evidence exists regarding how healthcare institutions in developing countries operationalize these frameworks within Information Sharing-Enabled IoMT environments. Consequently, there remains a significant theoretical and practical gap in the development of an integrated cybersecurity framework capable of simultaneously addressing technical, governance, socio-behavioral, and contextual healthcare security requirements. This study therefore evaluated current security frameworks to assess their ability to protect information-sharing IoMT systems used in healthcare facilities with limited resources.

II. LITERATURE REVIEW

The rapid advancement of the Internet of Medical Things (IoMT) has transformed healthcare systems globally by enabling interconnected medical devices, wearable sensors, cloud platforms, and hospital information systems to support real-time patient monitoring, diagnostics, and clinical decision-making. IoMT technologies improve healthcare accessibility, operational efficiency, and patient-centered care through continuous data collection and seamless information exchange among healthcare providers (Hireche et al., 2022; Sadhu et al., 2022). Healthcare organizations increasingly rely on IoMT ecosystems to support telemedicine, remote diagnostics, chronic disease management, and emergency response systems, especially following the accelerated digital transformation triggered by global health emergencies.

However, despite these operational benefits, IoMT systems have introduced complex cybersecurity vulnerabilities associated with device heterogeneity, insecure communication

protocols, interoperability challenges, and insufficient security governance mechanisms (Ghubaish et al., 2023; Khatiwada & Yang, 2022). The interconnected nature of IoMT infrastructures significantly enlarges attack surfaces and exposes healthcare systems to cyber threats capable of compromising patient safety, data confidentiality, and healthcare continuity.

Existing literature demonstrates that healthcare institutions are among the most targeted sectors for cyberattacks because of the high value of electronic medical records and the mission-critical nature of healthcare operations. According to the World Health Organization, healthcare cyber incidents have increased substantially due to the expansion of digital health technologies and interconnected healthcare infrastructures. Coventry and Branley (2023) argue that ransomware attacks, phishing schemes, insider threats, and distributed denial-of-service attacks increasingly target healthcare environments because service disruptions directly threaten patient outcomes. IoMT devices remain particularly vulnerable because many devices operate with limited computational resources, outdated firmware, weak authentication protocols, and inadequate encryption mechanisms (Dzamesi & Elsayed, 2025; Hireche et al., 2022). These vulnerabilities are further amplified within resource-constrained healthcare environments characterized by poor cybersecurity investment, inadequate technical expertise, weak regulatory enforcement, and insufficient digital governance structures.

Scholars have emphasized that IoMT cybersecurity differs significantly from conventional enterprise cybersecurity because healthcare systems involve safety-critical operations where cyber incidents may directly endanger human lives. (Ghubaish et al., 2023) Note that traditional cybersecurity models prioritize data confidentiality and system availability but often fail to adequately address patient safety, medical device interoperability, and real-time operational continuity within healthcare ecosystems. Similarly, (Deb et al., 2025) argue that IoMT security requires holistic risk management approaches capable of integrating device-level security, network security, cloud security, and healthcare operational governance into a unified framework. Existing cybersecurity architectures frequently adopt fragmented approaches that isolate technical controls from governance and human behavioral factors, thereby limiting their effectiveness in complex healthcare environments.

The National Institute of Standards and Technology Cybersecurity Framework remains one of the most widely adopted cybersecurity governance frameworks globally. The framework organizes cybersecurity activities into five core functions, namely Identify, Protect, Detect, Respond, and Recover, to strengthen organizational cyber resilience. The NIST framework has been widely praised for its flexibility, scalability, and risk-based approach applicable across multiple sectors

(Risk Assessment of Heterogeneous IoMT Devices, 2023). However, several studies indicate that the framework was originally designed for general information systems and therefore inadequately addresses healthcare-specific operational complexities associated with IoMT ecosystems. (Hireche et al., 2022) observed that NIST implementation within healthcare institutions often focuses heavily on technical controls while neglecting socio-behavioral dimensions such as user awareness, organizational culture, and healthcare workflow integration. In resource-constrained healthcare institutions, implementation challenges are further intensified by limited financial resources and inadequate cybersecurity personnel.

Similarly, ISACA's COBIT framework provides governance and management guidelines for enterprise information technology systems. COBIT emphasizes risk management, accountability, compliance, and alignment between organizational objectives and information systems governance. While COBIT contributes significantly to institutional cybersecurity governance, scholars argue that the framework remains insufficiently adaptable to dynamic IoMT healthcare environments that require continuous device interoperability, real-time clinical responsiveness, and patient-centered operational flexibility (Bhushan et al., 2023). Furthermore, COBIT implementation demands mature organizational governance structures that are often absent within healthcare institutions operating in low-resource settings. Consequently, healthcare organizations in developing countries struggle to operationalize COBIT principles effectively within decentralized and resource-limited healthcare infrastructures.

Critical Information Infrastructure Protection (CIIP) frameworks have also gained prominence in protecting healthcare infrastructures against cyber disruptions because healthcare institutions are increasingly classified as critical national infrastructure. CIIP frameworks primarily focus on safeguarding infrastructure resilience, ensuring service continuity, and minimizing disruptions arising from cyber threats, physical attacks, or system failures. However, current literature indicates that CIIP models focus predominantly on national infrastructure resilience while offering limited guidance on healthcare-specific device security, patient data governance, and clinical operational integration (Jaidi et al., 2025). Resource-constrained healthcare institutions particularly encounter implementation barriers because CIIP strategies often require advanced technological infrastructure, extensive policy coordination, and national-level cybersecurity capabilities that remain underdeveloped in many developing countries.

The IoT Security Foundation (IoTSF) Security Compliance Framework was developed to improve IoT device security through standardized security principles, compliance guidelines, and best practices for secure device manufacturing and deployment. The framework addresses device authentication, secure software updates, encryption, vulnerability management, and lifecycle

security management. Although IoTSF contributes significantly to IoT device security standardization, scholars have criticized its limited contextual adaptation to healthcare-specific environments characterized by complex interoperability requirements and socio-technical operational challenges (Sadhu et al., 2022). Additionally, the framework emphasizes technical compliance mechanisms while providing limited consideration for governance integration, healthcare workflow dynamics, and user behavioral vulnerabilities prevalent within healthcare systems.

Recent studies increasingly advocate for integrated and healthcare-oriented cybersecurity frameworks capable of addressing the multidimensional nature of IoMT ecosystems. (Bhushan et al., 2023) contend that future IoMT security frameworks must integrate governance mechanisms, artificial intelligence-driven threat detection, lightweight encryption protocols, and human-centered security practices to achieve sustainable cybersecurity resilience. Similarly, (Si-Ahmed et al., 2024) proposed explainable machine learning-based frameworks capable of enhancing anomaly detection and predictive cybersecurity management within IoMT systems. However, many emerging frameworks remain theoretical and lack empirical validation within real-world healthcare environments, especially in low-resource healthcare institutions across developing countries.

Another major concern highlighted within literature involves the socio-behavioral dimensions of healthcare cybersecurity. Studies indicate that human factors such as poor password management, inadequate cybersecurity awareness, insider negligence, and resistance to technology adoption significantly contribute to cybersecurity vulnerabilities within healthcare institutions (Coventry & Branley, 2023). Healthcare professionals frequently prioritize patient care efficiency over cybersecurity compliance, thereby unintentionally bypassing security protocols to maintain operational continuity. This challenge becomes more severe in resource-constrained healthcare environments where cybersecurity training programs, digital literacy initiatives, and institutional cybersecurity cultures remain underdeveloped. Consequently, cybersecurity frameworks that fail to integrate human behavioral considerations remain insufficient for healthcare IoMT ecosystems.

Interoperability challenges also emerge consistently within IoMT cybersecurity literature. IoMT ecosystems involve multiple interconnected devices, cloud systems, electronic health record platforms, and communication technologies operating across heterogeneous environments. According to (Kumar and Tripathi, 2021), interoperability limitations create fragmented security architectures that weaken system-wide cybersecurity resilience. Secure information sharing requires standardized communication protocols, coordinated governance structures, and

integrated security controls capable of protecting healthcare data throughout its lifecycle. Existing cybersecurity frameworks frequently address isolated components of interoperability without providing comprehensive healthcare-specific integration mechanisms necessary for resource-constrained environments.

Literature further reveals that developing countries face unique cybersecurity challenges associated with weak institutional capacity, limited cybersecurity regulations, inadequate infrastructure investment, and dependence on imported medical technologies. Many healthcare institutions within low-resource settings continue operating outdated systems lacking basic cybersecurity safeguards such as encryption, access control mechanisms, and continuous vulnerability monitoring (WHO, 2025). Additionally, the shortage of cybersecurity professionals and limited organizational awareness significantly constrain the effective implementation of existing cybersecurity frameworks within healthcare systems. Consequently, scholars increasingly advocate for context-specific cybersecurity frameworks tailored to the operational realities of healthcare institutions in developing countries.

III. RESEARCH METHOD

A. Research Design

This study employed a mixed-method exploratory research design integrating systematic literature review, comparative framework analysis, and descriptive quantitative assessment of cybersecurity functionalities within selected healthcare institutions. The mixed-method approach was considered appropriate because the study sought to both critically evaluate existing theoretical cybersecurity frameworks and empirically examine practical cybersecurity implementation within healthcare-based IoMT environments. The qualitative component enabled in-depth comparative synthesis of existing cybersecurity frameworks, while the quantitative component facilitated the assessment of institutional cybersecurity practices and perceptions regarding Information Sharing-Enabled IoMT systems.

B. Study Area

The empirical component of the study was conducted at St. Francis Hospital Nsambya and Uganda Martyrs Hospital Lubaga. The two hospitals were purposively selected because they represent major healthcare institutions implementing digital healthcare systems and interconnected medical technologies within resource-constrained operational environments. Their adoption of health information systems and IoMT-related technologies provided an appropriate context for evaluating cybersecurity implementation practices associated with secure health information sharing.

C. Target Population and Sampling

The study targeted healthcare administrators, information technology personnel, clinical staff, and health information management personnel involved in digital healthcare operations and cybersecurity management. Purposive sampling was employed to select respondents with adequate knowledge and experience regarding IoMT implementation and cybersecurity practices within the selected hospitals.

D. Data Collection Methods

Data were collected using two complementary approaches. First, a systematic review of peer-reviewed journal articles, cybersecurity standards, policy documents, and international framework publications published between 2020 and 2024 was conducted to evaluate existing IoMT cybersecurity frameworks. Second, primary quantitative data were collected from respondents within the selected hospitals using a structured questionnaire designed to assess institutional cybersecurity functionalities across device-level, network-level, and data-level security dimensions.

E. Research Instrument

The questionnaire was structured using a five-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5). The instrument measured respondent perceptions regarding IoMT security functionalities, including device protection mechanisms, authentication controls, network security practices, encryption mechanisms, vulnerability assessment procedures, monitoring systems, and data access controls.

F. Data Analysis

Quantitative data were analyzed using descriptive statistical techniques, including frequencies, percentages, means, and standard deviations, to evaluate respondent perceptions regarding cybersecurity implementation practices. Qualitative findings from the systematic literature review and framework evaluation were analyzed using thematic comparative synthesis to identify conceptual overlaps, operational gaps, governance limitations, and socio-technical security deficiencies within existing cybersecurity frameworks.

G. Ethical Considerations

Ethical considerations were observed throughout the study process. Institutional permissions were obtained from the participating healthcare facilities before data collection. Respondents participated voluntarily, and confidentiality and anonymity were maintained throughout the

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 2 August 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 188-206
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

research process. The study ensured that collected data were used strictly for academic and research purposes.:

IV. RESULT

A. Comparative Evaluation of Existing Framework

The findings presented in Table 1 demonstrate that the selected healthcare institutions exhibit a moderately developed cybersecurity posture across device-level, network-level, and data-level security dimensions, although important operational and strategic vulnerabilities remain evident. The overall mean score of 3.26 with a relatively low standard deviation (0.74) suggests that respondents generally perceived the implemented cybersecurity functionalities as significant, indicating the existence of foundational security mechanisms within the healthcare institutions. However, the moderate mean ranges observed across device-level and data-level security dimensions reveal that cybersecurity implementation remains only partially mature and may not sufficiently address the complex security demands associated with Information Sharing-Enabled Internet of Medical Things (IoMT) ecosystems. The comparatively wider mean range within network-level security (2.54–4.26) further suggests institutional inconsistencies in network monitoring, access control enforcement, and intrusion management practices.

Table 1. Cybersecurity Posture Assessment in Selected Healthcare Institutions

Security Level	Key Focus	Mean Range	Overall Std. Dev	Interpretation
Device Level Security	Device access and protection controls	3.00 – 3.30	≈0.75	Moderate to Significant
Network Level Security	Network access, monitoring, and controls	2.54 – 4.26	≈0.72	Moderate to Very Significant
Data Level Security	Data access, storage, and protection	2.81 – 3.24	≈0.76	Moderate
Cross-Institutional Perception	**Nsambya & Lubaga Hospitals**	**Consistent**	**Low variability**	**Stable perceptions**
Overall Security Functionalities	Aggregate of all levels	3.26	0.74	Significant

These findings imply that while healthcare institutions have initiated cybersecurity implementation efforts, the operationalization of comprehensive and integrated IoMT security architectures remains fragmented. The observed low variability in cross-institutional perceptions between St. Francis Hospital Nsambya and Uganda Martyrs Hospital Lubaga additionally indicates that the identified cybersecurity challenges are likely systemic within resource-constrained healthcare environments rather than institution-specific anomalies. This pattern reinforces concerns raised in previous studies that healthcare institutions in developing countries often implement isolated security controls without achieving comprehensive governance integration, interoperability protection, or continuous cybersecurity resilience within interconnected healthcare infrastructures.

The implications of these findings are both theoretically and practically significant for the advancement of healthcare cybersecurity governance within resource-constrained environments. From a theoretical perspective, the findings provide empirical evidence supporting the argument that existing cybersecurity frameworks inadequately integrate the multidimensional requirements of healthcare-based IoMT ecosystems, particularly the simultaneous coordination of technical safeguards, governance mechanisms, compliance structures, and socio-behavioral security practices. The moderate implementation levels observed across all security domains suggest that healthcare institutions may possess basic technological safeguards while lacking the institutional cybersecurity maturity necessary for sustaining secure information sharing and real-time interoperability within highly interconnected digital healthcare systems. Practically, the findings imply that healthcare institutions remain vulnerable to cybersecurity breaches, unauthorized data access, network intrusions, and operational disruptions that may compromise patient confidentiality, clinical continuity, and healthcare service reliability.

The results therefore underscore the urgent need for an integrated healthcare-oriented cybersecurity framework capable of harmonizing device security, network governance, data protection, workforce cybersecurity awareness, and regulatory compliance within low-resource healthcare settings. Furthermore, the consistency of perceptions across the two hospitals suggests that cybersecurity weaknesses within Ugandan healthcare institutions may reflect broader structural limitations associated with funding constraints, limited cybersecurity expertise, inadequate policy enforcement, and insufficient institutional preparedness for emerging IoMT-related cyber threats. Consequently, policymakers, healthcare administrators, and cybersecurity practitioners should prioritize the development of context-sensitive cybersecurity strategies that move beyond fragmented technical interventions toward holistic and institutionally embedded cybersecurity governance models capable of supporting resilient and secure healthcare information-sharing ecosystems.

B. Hospital Cybersecurity Assessment Findings

The cybersecurity assessment findings from St. Francis Hospital Nsambya and Uganda Martyrs Hospital Lubaga reveal that the healthcare institutions have made notable progress toward implementing foundational cybersecurity mechanisms necessary for supporting Information Sharing-Enabled Internet of Medical Things (IoMT) systems. The findings indicate the existence of moderate device-level, network-level, and data-level security functionalities, suggesting that both institutions have recognized the growing importance of cybersecurity within digitally enabled healthcare environments. Device-level controls such as authentication procedures,

restricted device access, and basic endpoint protection mechanisms were reported to be moderately implemented, while network-level functionalities demonstrated relatively stronger performance, particularly in areas related to network monitoring and access management.

However, the findings further indicate that implementation effectiveness remains inconsistent across different security domains, with some respondents expressing uncertainty regarding the adequacy and operational reliability of existing cybersecurity controls. The variability observed within network-level security measures suggests that although some departments may possess stronger cybersecurity infrastructure, institutional implementation lacks uniformity and standardized operational enforcement. Additionally, moderate scores within data-level security imply that healthcare institutions may still face challenges associated with secure storage, encryption, access management, and real-time protection of sensitive patient information within interconnected healthcare systems.

The implications of these findings suggest that the selected healthcare institutions are currently operating within transitional cybersecurity environments characterized by partial technological adoption but limited institutional cybersecurity maturity. Although the presence of moderate cybersecurity functionalities reflects positive institutional efforts toward digital security enhancement, the findings indicate that cybersecurity implementation remains predominantly reactive rather than strategically integrated into healthcare governance and operational planning. This partial implementation may expose healthcare systems to persistent risks associated with unauthorized system access, cyberattacks, data breaches, ransomware threats, and operational disruptions capable of compromising patient safety and healthcare continuity.

The findings further imply that existing cybersecurity practices may not sufficiently support the complexity of modern IoMT ecosystems, where interconnected medical devices continuously exchange sensitive clinical information across multiple digital platforms. From a broader institutional perspective, the assessment findings highlight the urgent need for healthcare organizations within resource-constrained environments to strengthen cybersecurity governance structures, establish standardized implementation procedures, improve workforce cybersecurity awareness, and invest in comprehensive security architectures capable of supporting secure interoperability and resilient healthcare information-sharing systems. Consequently, the findings reinforce the necessity for integrated and context-sensitive cybersecurity frameworks specifically tailored to the operational realities of low-resource healthcare institutions.

C. Identified Security Gaps

The study identified several critical cybersecurity gaps that continue to undermine the effective protection of Information Sharing-Enabled Internet of Medical Things (IoMT) systems within the

selected healthcare institutions. One of the most significant gaps relates to the fragmented implementation of cybersecurity functionalities across device-level, network-level, and data-level security domains. Although foundational security controls were reported to exist, the findings indicate the absence of a fully integrated cybersecurity architecture capable of simultaneously coordinating governance mechanisms, technical safeguards, regulatory compliance, and socio-behavioral security practices. The moderate implementation scores across several cybersecurity dimensions suggest that many institutional controls remain inadequately enforced, inconsistently monitored, or insufficiently aligned with the evolving cybersecurity demands of interconnected healthcare environments.

Furthermore, the findings reveal weaknesses in institutional cybersecurity preparedness, particularly regarding continuous monitoring, real-time threat detection, advanced encryption practices, incident response coordination, and user-centered cybersecurity awareness. The absence of comprehensive and harmonized cybersecurity governance frameworks may therefore limit the institutions' capacity to effectively manage emerging cyber threats associated with interconnected medical devices, cloud-based health systems, and digital information-sharing infrastructures. These findings demonstrate that existing cybersecurity practices remain largely fragmented and operationally isolated, thereby reducing institutional resilience against increasingly sophisticated cyber threats targeting healthcare systems globally.

The identified cybersecurity gaps carry substantial implications for healthcare service delivery, patient data protection, institutional resilience, and national digital health transformation efforts within resource-constrained environments. The absence of integrated cybersecurity governance structures increases the likelihood of unauthorized access to sensitive patient information, disruption of clinical operations, loss of data integrity, and reduced trust in digital healthcare systems. Additionally, the identified weaknesses in workforce cybersecurity awareness and institutional compliance mechanisms suggest that healthcare personnel may remain vulnerable to phishing attacks, credential compromise, insider threats, and operational errors capable of exposing critical healthcare systems to cyber exploitation.

From a policy and governance perspective, the findings imply that existing cybersecurity frameworks such as NIST, COBIT, CIIP, and IoTSF may inadequately address the contextual realities of healthcare institutions operating within low-resource settings where infrastructural limitations, financial constraints, and limited cybersecurity expertise significantly affect implementation capacity. Consequently, the study highlights the necessity for healthcare institutions and policymakers to transition from fragmented technical interventions toward

Journal of Technology Informatics and Engineering (JTIE)
Vol. 5 No. 2 August 2026
E-ISSN: 2961-9068; P-ISSN: 2961-8215, Pages 188-206
Journal Link: https://jtie.stekom.ac.id/index.php/jtie/index

holistic cybersecurity governance approaches that integrate technological safeguards, institutional policy enforcement, workforce capacity building, continuous risk assessment, and healthcare-specific operational requirements. Addressing these identified gaps is therefore essential for strengthening healthcare cybersecurity resilience, safeguarding patient confidentiality, and ensuring the sustainable and secure adoption of IoMT technologies within developing healthcare systems.

D. Proposed Integrated Framework

The results of the comparative evaluation of existing security frameworks and theory in the context of information-sharing systems within the Internet of Medical Things (IoMT) in healthcare reveal a landscape characterized by significant deficiencies and gaps. The analysis shows that different security frameworks provide essential security components for healthcare environments but deliver these components through incomplete and uncoordinated methods. To address these gaps, the conceptual architecture of the proposed integrated framework is illustrated in Figure 1.

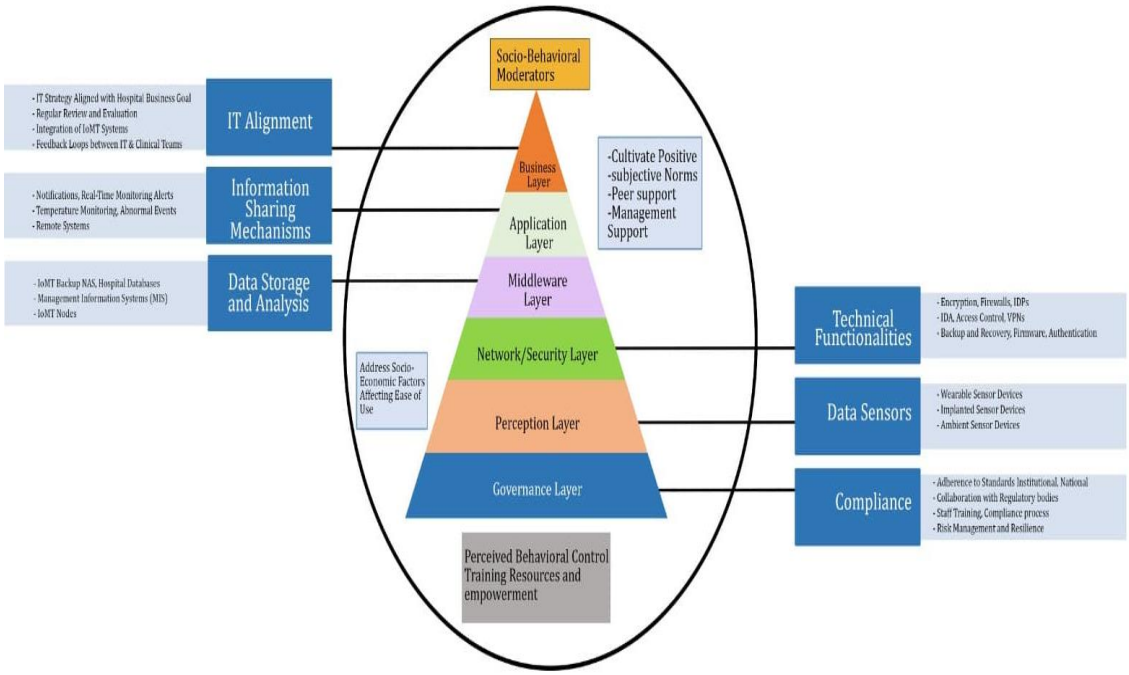

Figure 1. Synthesized/Proposed Conceptual Framework Architecture

The proposed framework was synthesized from the comparative evaluation of existing cybersecurity frameworks, empirical findings obtained from the selected healthcare institutions, and the identified socio-technical security gaps associated with Information Sharing-Enabled IoMT systems. The synthesis process revealed that existing frameworks inadequately integrate four critical dimensions simultaneously: technical cybersecurity safeguards, governance and

compliance mechanisms, healthcare operational requirements, and socio-behavioral determinants influencing security adoption and compliance. Consequently, the proposed framework integrates these dimensions into a unified architecture specifically designed for healthcare institutions operating within resource-constrained environments. The specific contributions of the proposed framework in comparison to existing models are outlined in Table 2.

Table 2. Comparative Contribution

Existing Framework	Major Strength	Major Limitation	Contribution of Proposed Framework
NIST CSF	Risk management and governance	Limited healthcare operational specificity	Integrates healthcare operational workflows
COBIT	IT governance alignment	Weak IoMT technical implementation guidance	Incorporates technical IoMT security controls
CIIP	Infrastructure resilience	Generic sector-level protection	Adapts security controls to healthcare settings
IoTSF	Device-level IoMT security	Limited governance and behavioral integration	Integrates governance, compliance, and socio-behavioral dimensions

V. DISCUSSION

The findings of this study demonstrate that existing cybersecurity frameworks remain conceptually fragmented and operationally insufficient in addressing the multidimensional security requirements associated with Information Sharing-Enabled Internet of Medical Things (IoMT) ecosystems within healthcare environments. Although frameworks such as the NIST Cybersecurity Framework, COBIT, Critical Information Infrastructure Protection (CIIP), and the IoT Security Foundation (IoTSF) provide important guidance on governance structures, risk management procedures, infrastructure protection, and technical security controls, the findings indicate that these frameworks inadequately integrate the complex socio-technical realities characterizing healthcare-based IoMT systems. In particular, the evaluated frameworks exhibit limited capacity to simultaneously address healthcare interoperability requirements, real-time clinical workflows, continuous medical device communication, patient data sensitivity, institutional governance enforcement, and workforce cybersecurity behavior within resource-constrained operational contexts.

The moderate implementation levels observed across device-level, network-level, and data-level security dimensions further suggest that healthcare institutions may adopt isolated cybersecurity functionalities without establishing comprehensive and institutionally embedded security architectures capable of sustaining resilient healthcare information-sharing systems. These findings corroborate (Ahmed et al., 2024), who argued that fragmented cybersecurity governance frameworks significantly weaken institutional resilience and increase systemic vulnerabilities within healthcare IoMT ecosystems. Similarly, (Alsubaei et al., 2022) observed that conventional

cybersecurity models often fail to accommodate the socio-technical complexity associated with interconnected medical devices, decentralized health information systems, and dynamic clinical communication processes. The present findings therefore extend existing scholarship by demonstrating that the limitations of existing cybersecurity frameworks become even more pronounced within resource-constrained healthcare environments characterized by infrastructural limitations, inadequate cybersecurity expertise, weak policy enforcement, and constrained institutional financing.

From a theoretical perspective, the findings reinforce socio-technical systems theory by demonstrating that healthcare cybersecurity effectiveness cannot be achieved through isolated technical safeguards alone but instead requires the simultaneous integration of governance structures, technological controls, institutional policies, and human behavioral compliance mechanisms. The findings reveal that cybersecurity vulnerabilities within healthcare-based IoMT systems emerge not only from technical infrastructure deficiencies but also from organizational, behavioral, and governance-related weaknesses that collectively influence institutional cybersecurity resilience. This multidimensional interpretation supports emerging theoretical arguments that healthcare cybersecurity should be conceptualized as an integrated socio-technical governance ecosystem rather than a purely technological challenge. Practically, the findings carry significant implications for healthcare institutions operating within low-resource environments such as Uganda, where rapid digital health transformation frequently occurs without proportional investment in cybersecurity infrastructure, workforce training, and institutional preparedness.

The identified implementation inconsistencies across security domains suggest that many healthcare institutions remain vulnerable to cyberattacks, unauthorized access, ransomware incidents, interoperability failures, and patient data breaches capable of disrupting healthcare continuity and compromising patient safety. Furthermore, the findings imply that globally developed cybersecurity frameworks may not be directly transferable to low-resource healthcare systems without contextual adaptation to local infrastructural realities, institutional governance capacities, and healthcare operational constraints. Consequently, the study highlights the urgent need for context-sensitive and healthcare-oriented cybersecurity frameworks capable of integrating technical safeguards, governance enforcement, compliance mechanisms, workforce cybersecurity awareness, and operational healthcare requirements into a unified institutional cybersecurity strategy. Such integration is essential for strengthening cybersecurity resilience, safeguarding sensitive patient information, enhancing secure healthcare interoperability, and supporting the sustainable adoption of IoMT technologies within developing healthcare systems.

Despite its contributions, the study presents several limitations. First, the empirical assessment was limited to two healthcare institutions, which may constrain the generalizability of the findings to other healthcare contexts. Second, the study primarily utilized descriptive statistical analysis and did not undertake advanced inferential modeling to establish causal relationships between cybersecurity dimensions. Third, the proposed framework was conceptually synthesized and was not empirically validated through real-world implementation. Future studies should therefore conduct multi-institutional validation and longitudinal implementation assessments to evaluate the operational effectiveness of the proposed framework.

VI. CONCLUSION AND RECOMMENDATION

This research critically evaluated the existing cybersecurity frameworks that protect information-sharing Internet of Medical Things systems that operate in healthcare settings. The NIST CSF, COBIT, CIIP, and IoTSF frameworks establish fundamental security standards, yet these frameworks fail to provide solutions for all technical, organizational, behavioral, and environmental issues that occur in healthcare facilities with limited resources. The study recommends the development of a healthcare-oriented IoMT security framework that integrates technical safeguards, governance structures, and socio-behavioral factors to enhance secure information sharing and system sustainability. The study contributes to the growing body of knowledge on healthcare cybersecurity by proposing an integrated IoMT security framework tailored to the operational realities of resource-constrained healthcare environments. Unlike existing frameworks that address isolated dimensions of cybersecurity, the proposed framework simultaneously integrates governance mechanisms, technical safeguards, compliance structures, and socio-behavioral determinants necessary for secure information sharing within healthcare IoMT ecosystems. Future research should focus on empirical validation of the framework across diverse healthcare institutions and evaluate its effectiveness in enhancing cybersecurity resilience and secure clinical interoperability.

REFERENCES

Adeleye, A., Adewuyi, A. A. O., Enyiorji, P. U., Ajayi, O. O., Tsambatare, T. E., Oloke, K., & Abijo, I. (2024). The Convergence of Cybersecurity, Internet of Things (IoT), and Data Analytics: Safeguarding Smart Ecosystems. *World Journal of Advanced Research and Reviews*, *23*(1), 379–394. https://doi.org/10.30574/wjarr.2024.23.1.1993

Aferudin, F., & Ramli, K. (2022). The Development of Cybersecurity Information Sharing Framework for National Critical Information Infrastructure in Indonesia. *Budapest International Research and Critics Institute (BIRCI-Journal)*, *5*(3), 21379–21389. https://doi.org/10.33258/birci.v5i3.6297

Africa Cyber Security Report. (2020). *Local Perspective on Data Protection and Privacy Laws: Insights from African SMEs*. Cyber ERM. https://www.cybererm.com/insights/africa-cyber-security-report-2020

Ahimbisibwe, B., & Nabende, P. (2022). A Conceptual Framework for Assessing Information Security Management Practices in Selected Universities in Uganda. *Journal of Digital Science*, *4*(1), 21–29. https://doi.org/10.33847/2686-8296.4.1_2

Ahimbisibwe, B. K., & Nabende, P. (2023). The Institutionalisation of Information Security Management Practices in Selected Organisations in Uganda. *International Journal of Advanced Research*, *6*(1), 48–63. https://doi.org/10.37284/ijar.6.1.1155

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H., & Baskerville, R. L. (2020). How Integration of Cyber Security Management and Incident Response Enables Organizational Learning. *Journal of the Association for Information Science and Technology*, *71*(8), 939–953. https://doi.org/10.1002/asi.24311

Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How Can Organizations Develop Situation Awareness for Incident Response: A Case Study of Management Practice. *Computers & Security*, *101*, 102122. https://doi.org/10.1016/j.cose.2020.102122

Ahmad, I., Shahid, F., Ahmad, I., Islam, J., Haque, K. N., & Harjula, E. (2022). Adaptive Lightweight Security for Performance Efficiency in Critical Healthcare Monitoring. *IEEE Access*, *10*, 121111–121124. https://doi.org/10.1109/access.2022.3222343

Ahmed, S. F., Alam, M. S. B., Afrin, S., Rafa, S. J., Rafa, N., & Gandomi, A. H. (2024). Insights into Internet of Medical Things (IoMT): Data Fusion, Security Issues and Potential Solutions. *Information Fusion*, *102*, 102060. https://doi.org/10.1016/j.inffus.2023.102060

Ahmed, S. K. (2024). The Pillars of Trustworthiness in Qualitative Research. *Journal of Medicine, Surgery, and Public Health*, *2*, 100051. https://doi.org/10.1016/j.glmedi.2024.100051

Ahmid, M., & Kazar, O. (2023). A Comprehensive Review of the Internet of Things Security. *Journal of Applied Security Research*, *18*(3), 289–305. https://doi.org/10.1080/19361610.2021.1962677

Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. *Computers & Security*, *132*, 103352. https://doi.org/10.1016/j.cose.2023.103352

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-t

Ajzen, I. (2020). The Theory of Planned Behavior: Frequently Asked Questions. *Human Behavior and Emerging Technologies*, *2*(4), 314–324. https://doi.org/10.1002/hbe2.211

Akbar, S., Coiera, E., & Magrabi, F. (2020). Safety Concerns with Consumer-Facing Mobile Health Applications and Their Consequences: A Scoping Review. *Journal of the American Medical Informatics Association*, *27*(2), 330–340. https://doi.org/10.1093/jamia/ocz175

Akello, M., Coutinho, S., N-Mboowa, M. G., Bukirwa, V. D., Natukunda, A., Lubyayi, L., Nabakooza, G., Cose, S., & Elliott, A. M. (2020). Continuous Research Monitoring Improves the Quality of Research Conduct and Compliance Among Research Trainees: Internal Evaluation of a Monitoring Programme. *AAS Open Research*, *3*, 57. https://doi.org/10.12688/aasopenres.13117.1

Al-Dosari, K., & Fetais, N. (2023). Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach. *Electronics*, *12*(17), 3629. https://doi.org/10.3390/electronics12173629

Al-Hawamleh, A. (2024). Cyber Resilience Framework: Strengthening Defenses and Enhancing Continuity in Business Security. *International Journal of Computing and Digital Systems*, *15*(1), 1315–1331. https://doi.org/10.12785/ijcds/150193

Al Harbi, S., Aljohani, B., Elmasry, L., Baldovino, F. L., Raviz, K. B., Altowairqi, L., & Alshlowi, S. (2024). Streamlining Patient Flow and Enhancing Operational Efficiency Through Case Management Implementation. *BMJ Open Quality*, *13*(1), e002484. https://doi.org/10.1136/bmjoq-2023-002484

Alsubaei, F., Abuhussein, A., & Shiva, S. (2022). Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment. *IEEE Internet of Things Journal*, *9*(3), 1762–1779. https://doi.org/10.1109/jiot.2021.3094052

Annamalai, P., Sikamani, K. T., Manjula, V. S., Kannan, R. J., Murugan, S., & Ankamma, K. (2024). Detecting Leaks and Faults in Underground Water Networks. *Journal of Electrical Systems*, *20*(4), 692–702. https://doi.org/10.52783/jes.2090

Baker, T., Asim, M., & Tawfik, H. (2024). A Systematic Review of IoMT Security Challenges and Mitigation Strategies. *Journal of Medical Systems*, *48*(2), 13. https://doi.org/10.1007/s10916-024-02035-2

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), 6177. https://doi.org/10.3390/su15076177

Coventry, L., & Branley, D. (2023). Cybersecurity in Healthcare: A Narrative Review of Trends, Threats, and Responses. *Health Informatics Journal*, *29*(1), 1–15. https://doi.org/10.1177/14604582231151833

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://arxiv.org/abs/2507.19609

Dzamesi, L., & Elsayed, N. (2025). A Review on the Security Vulnerabilities of the IoMT Against Malware Attacks and DDoS. *arXiv*. https://arxiv.org/abs/2501.07703

Fikri, H., & Muchlis, M. (2026). Decision-Support AI Health Dashboard Using Synthetic Data for Daily Health Monitoring. *Jurnal Ilmiah Sistem Informasi*, *5*(2), 429–441. https://doi.org/10.51903/mp66jy72

Geoffrey Getare Nyauma, & Manjula, V. S. (2023). Revolutionizing Legal and Business Processes of the Digital Age Using Blockchain Technology. *Journal of Applied Science, Information and Computing (JASIC)*, *4*(1), 1–11. https://doi.org/10.59568/jasic-2023-4-1-01

Ghubaish, A., Salman, T., Zolanvari, M., Unal, D., Al-Ali, A., & Jain, R. (2023). Recent Advances in the Internet of Medical Things (IoMT) Systems Security. *IEEE Internet of Things Journal*, *10*(3), 2318–2336. https://doi.org/10.1109/jiot.2022.3211516

Hireche, R., Mansouri, H., & Pathan, A.-S. K. (2022). Security and Privacy Management in Internet of Medical Things (IoMT): A Synthesis. *Journal of Cybersecurity and Privacy*, *2*(3), 640–661. https://doi.org/10.3390/jcp2030033

Islam, S. M. R., Kwak, D., Kabir, M. H., Hossain, M., & Kwak, K. S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*, *3*, 678–708. https://doi.org/10.1109/access.2015.2437951

Jaidi, F., Ben Ali, A., & Hamdi, M. (2025). An Internet of Medical Things Cyber Security Assessment Model (IoMT-CySAM). *Healthcare Analytics*, *8*, 100245. https://doi.org/10.1016/j.health.2025.100245

Khatiwada, P., & Yang, B. (2022). An Overview on Security and Privacy of Data in IoMT Devices: Performance Metrics, Merits, Demerits, and Challenges. *Studies in Health Technology and Informatics*, *299*, 126–136. https://doi.org/10.3233/shti220970

Kumar, R., & Tripathi, R. (2021). Towards Design and Implementation of Security and Privacy Framework for Internet of Medical Things (IoMT) by Leveraging Blockchain and IPFS Technology. *The Journal of Supercomputing*, *77*(8), 7916–7955. https://doi.org/10.1007/s11227-020-03570-x

Sadhu, P. K., Yanambaka, V. P., Abdelgawad, A., & Yelamarthi, K. (2022). Prospect of Internet of Medical Things: A Review on Security Requirements and Solutions. *Sensors*, *22*(15), 5517. https://doi.org/10.3390/s22155517

Sharmila, E. M. N., Al-Garadi, M. A., & Boustia, N. (2024). IoMT Applications, Benefits, and Future Challenges in Healthcare. *Advances in Fuzzy-Based Internet of Medical Things (IoMT)*, 1–23. https://doi.org/10.1002/9781394285228.ch1

Si-Ahmed, A., Al-Garadi, M. A., & Boustia, N. (2024). Explainable Machine Learning-Based Security and Privacy Protection Framework for Internet of Medical Things Systems. *arXiv*. https://doi.org/10.48550/arxiv.2403.09752

Udonna, U., Umoren, I., & Ansa, G. (2025). Contextual Framework for Remote Intelligent Monitoring and Detection System for Prediction of Pregnancy Complications. *JTIE : Journal of Technology Informatics and Engineering*, *4*(2), 225–251. https://doi.org/10.51903/jtie.v4i2.244

Vadivel, M., Sridevi, V., Manjula, V. S., Vimal, S. P., Arockiajesuraj, Y., & Murugan, S. (2025). Gait Instability Detection with Temporal Convolutional Networks for Orthopedic Patients. *Proceedings of the 4th International Conference on Innovative Mechanisms for Industry Applications (ICIMIA-2025)*, 112–118. https://doi.org/10.1109/icimia2025.093

World Health Organization. (2025). *Cybersecurity and Privacy Maturity Assessment and Strengthening for Digital Health Information Systems*. WHO Regional Office for Europe. https://www.who.int/europe/news/item/26-03-2025-who-europe-launches-guide-to-strengthen-cybersecurity-in-digital-health

Yener, R., Hassan, M., & Bashir, M. (2025). Threats and Security Strategies for IoMT Infusion Pumps. *arXiv*. https://arxiv.org/abs/2509.14604

Zahra, Z., Melyani, M., Yusuf, F., Herawati, M. T., Royanti, S., & Rosihana, A. D. (2025). Implementation of Expert System Applications Using Forward Chaining to Detect Dental Health. *JMI: Journal of Management and Informatics*, *4*(3), 1105–1126. https://doi.org/10.51903/jmi.v4i3.212