Pervasive Computing in Healthcare: Security Risks and Strategic Mitigation Frameworks

Hezbone Ocholi[1], Bertha Kakai Mating'i[2], Eric Okeno Anyonje[3], Aseneth Jepchirchir[4], Sandra Khagayi[5]
[1,2]*Bukura Agricultural College, Kakamega*
[3]*Office of the Director Public Prosecutions, Nairobi*
[4]*Meteitei High School, Kapsabet*
[5]*The Sigalagala National Polytechnic, Kakamega*

Abstract- Pervasive computing is transforming healthcare by enabling continuous patient monitoring, intelligent diagnostics, context-aware applications, and interconnected medical devices. Despite these benefits, such technologies introduce significant security, privacy, and patient safety risks because of their distributed structures, diverse devices, and constant real-time data exchange. This paper conducts a systematic literature review to examine security risks within pervasive healthcare environments and to synthesize strategic mitigation frameworks documented in peer-reviewed studies. The review identifies key risk domains, including breaches of data confidentiality, vulnerabilities at the device level, insecure communication protocols, interoperability weaknesses, adversarial artificial intelligence (AI) threats, and gaps in regulatory compliance. Mitigation strategies are grouped into architectural controls, cryptographic solutions, identity and access management mechanisms, AI-driven threat detection, blockchain-based integrity measures, and governance frameworks. The findings show that although technical protections are developing quickly, organizational and policy-level safeguards remain relatively less mature. Therefore, a multi-layered strategic mitigation framework is proposed to strengthen resilience in pervasive healthcare ecosystems.

Index Terms— Pervasive healthcare, IoT security, medical device security, cybersecurity, AI threats, blockchain, Mitigation frameworks.

I. INTRODUCTION

Patient care is now a continuous, data-driven, and proactive service thanks to perivasive computing in healthcare, where wearable technology, smart sensors, and Internet of Things devices are seamlessly linked into medical systems [1]. With real-time data, decisions can be made more quickly and patients can now be monitored around-the-clock. However, there are now significant security issues as a result of this rapid expansion. With over 60% of healthcare businesses reporting care disruptions, recent forecasts for 2026 demonstrate that cyberattacks are more than just technical issues [2]; they now directly impact patient safety. Healthcare providers must implement proactive, all-encompassing, and strategic security frameworks in order to safeguard this vital infrastructure, going beyond reactive security measures.

Weiser [3] introduced the idea of pervasive (ubiquitous) computing, which aims to integrate computer technology into daily life. Wearable sensors, implanted devices, wireless body area networks (WBANs), Internet of Things (IoT) medical systems, cloud-based electronic health records (EHRs), and artificial intelligence (AI)-powered clinical decision support systems are some examples of how this paradigm is being applied in the healthcare industry. Predictive analytics, remote care delivery, and real-time monitoring are made possible by these technologies. However, the cyber-attack surface is greatly increased by the distributed and resource-constrained nature of ubiquitous healthcare systems. IoT-based healthcare systems have been shown in earlier research to be especially vulnerable to denial-of-service attacks, data breaches, and unauthorized device manipulation [4].

Because clinical systems are life-critical and medical data has a high market value, the healthcare industry continues to be one of the most often targeted sectors for cyberattacks. Although regulatory frameworks like GDPR and HIPAA aim to reduce these risks, resilience

cannot be ensured by compliance alone [5]. An integrated and strategic framework for risk mitigation is therefore necessary. This study aims to: Systematically review security risks in pervasive healthcare systems; Categorize mitigation strategies proposed in the literature; Identify research and governance gaps; Propose a conceptual multi-layered mitigation framework.

II. LITERATURE REVIEW

A. Architecture of Pervasive Healthcare Systems

Pervasive healthcare systems are structured as layered cyber-physical architectures that integrate wireless networking, distributed computing, physiological sensing, and advanced analytics [6]. At the foundational layer, wearable and implantable medical devices—such as insulin delivery systems, implantable neuro-stimulators, and advanced ECG monitors—capture real-time biometric data within Wireless Body Area Networks (WBANs). These devices typically rely on low-power communication standards such as Bluetooth Low Energy (BLE) and IEEE 802.15.6 to transmit data to nearby gateways or edge nodes because of their limited computational capacity and battery constraints [7].

The intermediate edge or fog layer performs preliminary analytics, including signal conditioning, event detection, and data aggregation [8]. By processing time-sensitive data locally, edge components reduce latency and enhance responsiveness to critical clinical events. Only filtered or summarized datasets are forwarded to the enterprise layer, thereby improving bandwidth efficiency. At the enterprise level, cloud-hosted Electronic Health Record (EHR) platforms integrate with AI-driven diagnostic engines to enable predictive modeling, clinical decision support, and population-level analytics.

While this distributed architecture enables intelligent and continuous care delivery, it also expands the attack surface [9]. The heterogeneity of device manufacturers, communication standards, and software stacks introduces interoperability gaps and inconsistent security baselines [10]. Large-scale deployments complicate cryptographic key distribution, device authentication, and lifecycle management. In multi-stakeholder ecosystems involving patients, clinicians, vendors, and cloud providers, trust governance becomes inherently complex [11]. Without comprehensive identity management frameworks like strong encryption mechanisms, adaptive intrusion detection systems and zero-trust enforcement, pervasive healthcare infrastructures remain exposed to unauthorized access, device compromise, service disruption, and adversarial interference with AI-driven diagnostics.

B. Security Risk Domains

1) Data Confidentiality and Privacy

Data confidentiality remains a foundational requirement in pervasive healthcare due to the sensitivity of medical records, biometric streams, and behavioral metadata [12]. Breaches frequently result from insecure APIs, weak authentication controls, misconfigured cloud storage, and inadequate encryption practices. Continuous data transmission from distributed IoT sensors further enlarges the attack surface.

Regulatory frameworks such as the General Data Protection Regulation and the Health Insurance Portability and Accountability Act mandate strict safeguards for personal health information, yet implementation inconsistencies persist across jurisdictions [13]. End-to-end encryption, context-aware access control, anonymization techniques, and privacy-by-design principles are therefore essential. In their absence, healthcare institutions face risks including identity theft, insurance fraud, reputational damage, and regulatory penalties [14].

2) Device-Level Vulnerabilities

Medical IoT devices often operate under strict energy and processing limitations, leading to security trade-offs during design and deployment [15]. Many devices lack hardware-based root-of-trust modules, secure boot processes, cryptographically signed firmware updates, and robust mutual authentication protocols. These deficiencies enable firmware manipulation, malware injection, and unauthorized remote control. Regulatory advisories from the U.S. Food and Drug Administration have repeatedly highlighted exploitable vulnerabilities in pacemakers, infusion pumps, and imaging systems [16]. Device-level compromise directly affects patient safety, transforming cybersecurity from an IT concern into a clinical risk management issue.

3) Network and Communication Threats

Wireless communication channels across WBANs, edge nodes, and cloud platforms are inherently vulnerable to interception and disruption [17]. Common attack vectors include man-in-the-middle (MitM) attacks, replay attacks, and distributed denial-of-service (DDoS) attacks. The open nature of wireless media and the mobility of medical devices exacerbate exposure. Because many WBAN nodes rely on lightweight cryptographic schemes, they may be insufficient against advanced adversaries [18]. If communication pathways are compromised, data integrity, availability, and real-time responsiveness are jeopardized. This undermines both operational continuity and clinical reliability.

4) AI-Specific Threats

The integration of artificial intelligence into diagnostics introduces a distinct class of adversarial risks [19]. Data poisoning attacks manipulate training datasets to bias predictive outcomes, while model inversion and membership inference techniques may reconstruct sensitive patient data from trained models. Adversarial examples—subtly modified medical images or signals—can induce misclassification and incorrect clinical decisions. Given that AI systems increasingly function as decision-support tools in high-stakes therapeutic environments, ensuring robustness, explainability, and secure model lifecycle management is essential [20]. Without these safeguards, trust in AI-driven healthcare may erode.

5) Regulatory and Governance Risks

Regulatory compliance constitutes both a legal and operational risk domain in pervasive healthcare ecosystems. Frameworks such as the GDPR and HIPAA establish stringent obligations concerning consent management, breach notification, and cross-border data transfer [21]. More recently, the NIS2 Directive has expanded cybersecurity responsibilities for critical sectors, including healthcare providers. However, fragmented enforcement and divergent privacy norms complicate governance in cross-border telehealth deployments [22]. Harmonized compliance structures that integrate legal, technical, and clinical risk considerations are therefore necessary to ensure sustainable security alignment.

C. Mitigation Strategies

Mitigating pervasive healthcare risks requires a multi-layered, security-by-design approach that embeds cybersecurity controls throughout the system lifecycle [23]. Rather than treating security as an auxiliary function, strategic mitigation integrates architectural controls, cryptographic assurance, identity governance, AI resilience, and regulatory alignment into a unified framework.

1) Zero-Trust Architecture (ZTA)

Zero-Trust Architecture operationalizes the principle of continuous verification. Under this model, no user, device, or workload is inherently trusted based on network location [24]. Strong identity frameworks—including multi-factor authentication, device certificates, and hardware-backed credentials—validate clinicians, biomedical devices, and AI services. Micro-perimeter enforcement restricts access to least-privilege levels, thereby minimizing exposure of EHR systems and clinical databases. Zero-trust principles are particularly effective in mitigating insider threats and preventing privilege escalation within hospital networks [25].

2) Network Segmentation and Micro-Segmentation

Segmenting IoMT devices into dedicated VLANs or software-defined network partitions limits lateral movement in the event of compromise [26]. For example, a breached wearable sensor should not gain access to hospital finance systems or critical care units. Micro-segmentation extends isolation to workload-level enforcement within cloud and data center environments [27]. Combined with strict firewall policies and network access control mechanisms, segmentation significantly reduces attack propagation across interconnected infrastructures.

3) Advanced Encryption and Secure Data Handling

End-to-end encryption safeguards confidentiality and integrity across distributed healthcare ecosystems. Strong symmetric encryption, such as AES-256, protects data at rest, while TLS or DTLS secures data in transit [28]. For resource-constrained devices, elliptic curve cryptography (ECC) provides efficient yet robust protection. Effective key lifecycle management—including generation, distribution, rotation, and revocation—is essential. Encryption alone is insufficient without secure storage and rigorous access governance [29].

4) AI-Based Intrusion Detection and Anomaly Monitoring

Traditional signature-based intrusion detection systems struggle against zero-day exploits and polymorphic malware [30]. AI-driven anomaly detection enhances visibility by identifying deviations in network traffic, device telemetry, or user behavior. In healthcare settings, such systems can detect abnormal access to radiology archives or irregular command sequences to infusion pumps. However, these detection systems must themselves be hardened against adversarial manipulation and model drift [31]. Continuous retraining, validation, and explainability audits are required to preserve operational reliability.

5) Blockchain for Integrity Assurance

Blockchain-based architectures introduce tamper-evident record-keeping through distributed ledger mechanisms. By securing transactions using cryptographic hashing and consensus algorithms, blockchain enhances auditability and non-repudiation in multi-institutional care coordination [32]. This approach is particularly valuable in cross-border telemedicine and insurance claims processing. Nevertheless, scalability constraints, latency overhead, and energy consumption remain significant deployment challenges in high-throughput clinical contexts.

6) Governance and Risk Management Alignment

Technical controls must be embedded within broader cybersecurity governance structures. The U.S. Food and Drug Administration emphasizes integrating cybersecurity risk management into medical device safety lifecycles [33]. Risk-based governance includes continuous threat modeling, vulnerability disclosure programs, supply-chain assessment, and structured incident response planning. Aligning cybersecurity with patient safety objectives ensures that resilience extends beyond technical robustness to operational and regulatory continuity [34].

D. Governance and Procedural Frameworks

Comprehensive asset management forms the foundation of cybersecurity governance in pervasive healthcare systems. Accurate, real-time inventories across IT, OT, and IoMT environments reduce exposure to unmanaged endpoints and shadow devices [35]. The National Institute of Standards and Technology Cybersecurity Framework underscores asset identification as a core control under its "Identify" function [36]. Without clear asset visibility, vulnerability management and patching processes remain incomplete. Third-Party Risk Management (TPRM) is equally critical. Healthcare providers increasingly depend on external vendors for cloud services, AI analytics, and device manufacturing [37]. Regulatory guidance from the U.S. Food and Drug Administration highlights the importance of Software Bills of Materials (SBOMs) to enhance supply-chain transparency [38]. Robust TPRM requires contractual security clauses, compliance audits, and continuous monitoring. Active device lifecycle management further mitigates risk. Many medical devices operate beyond standard IT lifecycles and may run unsupported operating systems [39]. Risk-based patch prioritization, firmware validation, coordinated vulnerability disclosure, and secure decommissioning processes are therefore essential to maintain patient safety and system integrity [40].

E. Human and Organizational Factors

Technological safeguards alone cannot secure pervasive healthcare ecosystems. Human error remains a dominant cause of breaches, particularly through phishing and social engineering attacks. Healthcare professionals often operate under time pressure, making them susceptible to deceptive communications [41]. Security culture must therefore be institutionalized through continuous training, leadership accountability, and simulated attack exercises. Regulatory agencies such as the Cybersecurity and Infrastructure Security Agency recommend structured incident response models encompassing preparation, detection, containment, recovery, and post-incident evaluation [42]. Healthcare organizations must also prepare for "digital darkness" scenarios, including ransomware-induced system outages. Downtime procedures, manual documentation protocols, backup communication channels, and regular simulation drills are essential to ensure continuity of patient care during prolonged IT disruptions.

III. DISCUSSION

The literature demonstrates that security risks in pervasive healthcare are multi-layered and

interdependent. Although technical countermeasures—such as encryption, segmentation, and intrusion detection—are advancing rapidly, they often operate in isolation from broader governance and clinical safety frameworks.

A critical structural challenge lies in heterogeneous device manufacturing standards, which produce uneven security baselines across IoMT ecosystems. Interoperability gaps and inconsistent patching strategies sustain exploitable attack surfaces. Furthermore, cybersecurity governance frequently remains siloed within IT departments, while clinical governance focuses on patient safety and quality assurance. This separation weakens the recognition of cyber threats as direct clinical risk vectors. Privacy governance also tends to prioritize institutional compliance over patient-centric transparency and granular consent management. Meanwhile, mitigation strategies remain predominantly reactive, emphasizing incident response rather than predictive resilience engineering.

Sustainable cybersecurity in pervasive healthcare therefore requires an integrated, multi-layered strategic mitigation framework. Such a framework must unify device hardening, secure network architectures, AI-resilient analytics, cryptographic safeguards, and harmonized governance structures. Only coordinated controls across device, communication, analytics, and policy domains can achieve systemic resilience.

IV. FINDINGS

The systematic review confirms that security risks in pervasive healthcare environments are inherently complex and span devices, networks, data, analytics, and governance layers. IoT-enabled medical devices present the highest vulnerability concentration due to resource limitations, irregular patching, and heterogeneous manufacturing standards.AI-based anomaly detection systems demonstrate strong potential for identifying advanced threats, yet standardized validation benchmarks remain underdeveloped. Blockchain-based approaches enhance data integrity and traceability but face scalability and performance constraints in high-throughput settings.

Beyond technical vulnerabilities, fragmented governance structures, insufficient workforce training, and weak security cultures significantly amplify systemic exposure. No existing framework comprehensively addresses the entire pervasive healthcare stack in an integrated, end-to-end manner. These findings support the necessity of a multi-layered strategic mitigation framework that aligns architectural controls, cryptographic mechanisms, AI-driven detection, identity governance, and regulatory compliance. Strengthening resilience in pervasive healthcare ecosystems requires coordinated action across technological, organizational, and policy dimensions.

V. PROPOSED CONCEPTUAL FRAMEWORK

The framework comprises four interdependent layers:

1. Clinical & Network Layer – Patient data protection, IoT device security, network segmentation.
2. Technical Security Layer – Encryption, secure communication protocols, device hardening, blockchain integrity.
3. AI & Analytics Layer – AI-driven threat detection, behavioral monitoring, anomaly analysis.
4. Governance & Policy Layer – Regulatory compliance, risk management policies, continuous auditing.

This layered architecture aligns technical safeguards with governance mechanisms to create defense-in-depth resilience.

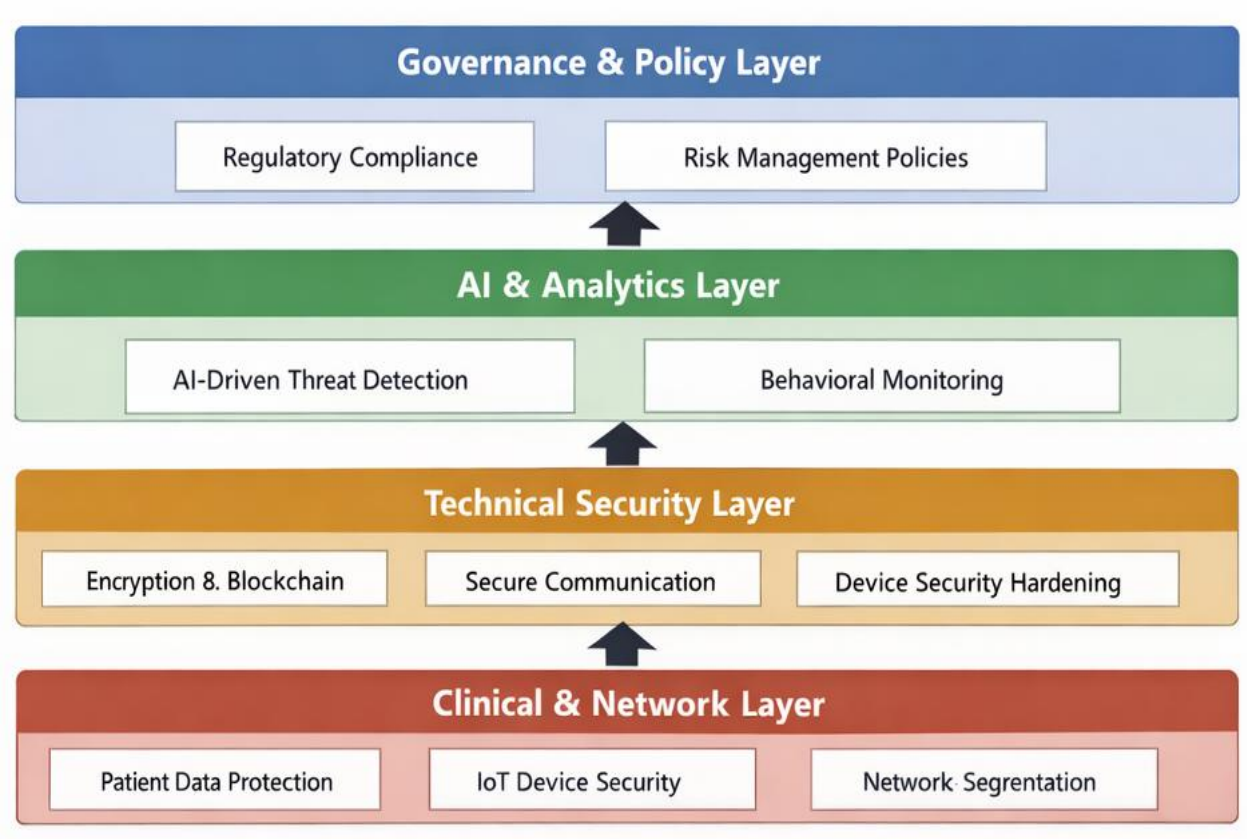

Fig. 1 *The proposed Integrated Risk Mitigation Framework for Pervasive Healthcare Systems*

VI. CONCLUSION

Pervasive computing offers transformative healthcare capabilities but introduces substantial cybersecurity and privacy risks. Current mitigation strategies are fragmented across technical domains. A comprehensive, multi-layered framework integrating cryptographic controls, AI-driven monitoring, secure architectures, and governance alignment is essential for safeguarding pervasive healthcare ecosystems.
Future systems must transition from reactive security models toward predictive, intelligence-driven resilience strategies.

VII. LIMITATIONS

This review is limited by:

1. Rapid technological evolution in IoT and AI domains.
2. Variability in methodological rigor across reviewed studies.
3. Limited empirical validation of proposed frameworks in real-world clinical environments.

VIII. RECOMMENDATIONS FOR FUTURE RESEARCH

As threats evolve, future security will rely on post-quantum cryptography (to protect long-term health data) blockchain for immutable data integrity, and edge computing to keep data closer to the source and reduce transmission risks.

ACKNOWLEDGMENT

The author acknowledges the contributions of researchers in pervasive computing, healthcare informatics, and cybersecurity whose work informed this systematic synthesis.

REFERENCES

[1] H. Taherdoost, "Wearable healthcare and continuous vital sign monitoring with IoT integration," Computers, Materials, & Continua 81, vol. 1, p. 79, 2024.

[2] T. Baisley and Y. Cherrat, Cyber Threats and Engagements in 2022., 2023.

[3] M. Weiser, " Some computer science issues in ubiquitous computing.," Communications of the ACM, Vols. 36(7), pp. 75-84., 1993.

[4] T. Zhukabayeva, L. Zholshiyeva, N. Karabayev, S. Khan and N. Alnazzawi, "Cybersecurity solutions for industrial internet of things–edge computing integration: Challenges, threats, and future directions.," Sensors, Vols. 25(1), p. 213., 2025.

[5] Y. Varma, "Secure Data Backup Strategies for Machine Learning," Compliance and Risk Mitigation RegulatoInternational Journal of Emerging Trends in Computer Science and Information Technology, vol. 1(1), pp. 29-38, 2020.

[6] S. A. Haque, S. M. Aziz and M. Rahman, "Review of cyber-physical system in healthcare.," international journal of distributed sensor networks, Vols. 10(4), , p. 217415, 2014.

[7] M. S. Akbar, Z. Hussain, M. Sheng and R. & Shankaran, "Wireless body area sensor networks: Survey of mac and routing protocols for patient monitoring under IEEE 802.15. 4 and IEEE 802.15. 6.," Sensors, vol. 22(21), p. 8279., 2022.

[8] M. R. Anawar, S. Wang, M. Azam Zia, A. K. Jadoon, U. Akram and S. Raza, " Fog computing: An overview of big IoT data analytics.," Wireless Communications and Mobile Computing, Vols. 2018(1), p. 7157192, 2018.

[9] P. K. Surabhi, " Distributed edge-cloud healthcare architecture: A technical overview.," Journal of Computer Science and Technology Studies, vol. 7(4), pp. 701-711., 2025.

[10] A. Hazra, M. Adhikari, T. Amgoth and S. N. Srirama, " A comprehensive survey on interoperability for IIoT: Taxonomy, standards, and future directions.," ACM Computing Surveys (CSUR), vol. 55(1), pp. 1-35., 2021.

[11] L. Rozenblit, A. Price, A. Solomonides, A. L. Joseph, E. Koski, G. Srivastava and Y. Quintana, "Toward responsible AI governance: balancing multi-stakeholder perspectives on AI in healthcare.," International Journal of Medical Informatics, vol. 203, p. 106015., 2025.

[12] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez and A. Jerez-Calero, "Strengthening privacy and data security in biomedical microelectromechanical systems by IoT communication security and protection in smart healthcare.," Sensors, vol. 23(21), p. 8944., 2023.

[13] Y. Flaumenhaft and O. Ben-Assuli, "Personal health records, global policy and regulation review.," Health policy, vol. 122(8), pp. 815-826., 2018.

[14] S. S. Goswami and S. Mondal, "Data Security and Privacy Concerns in Digitized Medical Services: Implications for Malpractice Risk Management.," Spectrum of Decision Making and Applications, vol. 3(1), pp. 212-242, 2026.

[15] R. AlTawy and A. M. Youssef, "Security tradeoffs in cyber physical systems: A case study survey on implantable medical devices.," Ieee Access, vol. 4, pp. 959-979, 2016.

[16] C. M. Wright, Using Telemetry to Ensure Safe and Reliable Medical Device Operation: Experience with Defibrillators and Infusion Pumps., University of Southern California., 2021.

[17] A. A. THULNOON, A. M. JUBAIR, F. S. MUBAREK and S. A. ABD, "Wireless body area networks: A review of challenges, architecture, applications, technologies and interference mitigation for next-generation healthcare.," Applied Computer Science, vol. 21(3), pp. 137-161, 2025.

[18] I. Ullah, S. Zeadally, N. U. Amin, M. A. Khan and H. Khattak, "Lightweight and provable secure cross-domain access control scheme for internet of things (IoT) based wireless body area networks (WBAN).," Microprocessors and Microsystems, vol. 81, p. 103477, 2021.

[19] H. Javed, S. El-Sappagh and T. Abuhmed, "Robustness in deep learning models for medical diagnostics: security and adversarial challenges towards robust AI applications.," Artificial Intelligence Review, vol. 58(1), p. 12, 2024.

[20] Y. V. P. Kollipara, "Assured, Explainable, And Auditable AI For High-Stakes Decisions: A Survey Of Trustworthy Machine Learning In Mission-Critical Systems.," Journal of International Crisis & Risk Communication Research (JICRCR), vol. 8, 2025.

[21] R. Vadisetty and A. Polamarasetti, "Regulatory Framework for Digital Health, Data Privacy, and Cybersecurity.," In Sustainable Healthcare Systems in Africa , pp. 132-153, 2025.

[22] C. Onwuatuegwu, "TELEMEDICINE: CROSS-BORDER REGULATORY CHALLENGES IN VIRTUAL HEALTH CARE.," Hollex Journal of Legal studies and Public Policy, vol. 13(4), pp. 1-8, 2025.

[23] O. H. Aliu, A. L. Imoize, K. Noor, H. Ahmad and M. O. Ebute, "An Overview of Security and Privacy in Cyber-physical Systems: Emerging Trends and Strategies.," Security and Privacy of Cyber-Physical Systems, pp. 1-36, 2025.

[24] J. Luo, X. Liu and M. Fan, "A trust model based on fuzzy recommendation for mobile ad-hoc networks.," Computer networks, vol. 53(14), pp. 2396-2407, 2009.

[25] A. Batan, " Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments.," International Journal of Advanced Cybersecurity Systems, Technologies, and Applications, , vol. 8(12), pp. 10-19., 2024.

[26] N. Li, M. Xu, Q. Li, J. Liu, S. Bao, Y. Li and H. Zheng, "A review of security issues and solutions for precision health in Internet-of-Medical-Things systems.," Security and Safety, vol. 2, p. 2022010., 2023.

[27] S. Chennamsetty and S. A. Averineni, "From Network Segmentation to AI-Driven Zero Trust: A Systematic Survey of Micro-segmentation Technologies," in 7th International Conference on Electronics and Communication, Network and Computer Technology (ECNCT), 2025.

[28] S. K. Jangam, "Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices.," International Journal of AI, BigData, Computational and Management Studies, vol. 4(3), pp. 82-91, 2023.

[29] L. Zhou, V. Varadharajan and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage.," IEEE transactions on information forensics and security, vol. 8(12), pp. 1947-1960, 2013.

[30] T. Mahammad Sharief and A. Sirajudeen, "Attack and Impact Comparison of Various Attack Against IDPS Relevant to Malware and Zero-Day Exploits.," in Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (pp. 375-390), Singapore: Springer Nature Singapore., 2025, January.

[31] A. Alotaibi and M. A. Rassam, "Adversarial machine learning attacks against intrusion detection systems: A survey on strategies and defense.," Future Internet, vol. 15(2), p. 62, 2023.

[32] R. M. Mulajkar, A. A. Khatri, S. D. Gunjal, D. S. Galhe, S. B. Bhosale and A. P. Bangar, "Blockchain and AI Synergy in Vascular Data Management: Enhancing Trust, Traceability, and Diagnostic Accuracy in Healthcare Systems.," Vascular and Endovascular Review, vol. 8(15s), pp. 315-330., 2025.

[33] S. Schwartz, A. Ross, S. Carmody, P. Chase, S. C. Coley, J. Connolly and M. Zuk, " The evolving state of medical device cybersecurity.," Biomedical instrumentation & technology, vol. 52(2), pp. 103-111, 2018.

[34] E. Petrova and H. Al-Mansoori, "EVALUATING AND ENHANCING CYBERSECURITY AND RESILIENCE IN HEALTHCARE: A UNIFIED RISK AND COMPLIANCE FRAMEWORK.," International Journal of Cyber Threat Intelligence and Secure Networking, vol. 2(05), pp. 1-7, 2025.

[35] B. Shanmugam and S. Azam, "Risk assessment of heterogeneous IoMT devices: a review.," Technologies, vol. 11(1), p. 31, 2023.

[36] K. Waedt, A. Ciriello, M. Parekh and E. Bajramovic, "Automatic assets identification for smart cities: Prerequisites for cybersecurity risk assessments," in In 2016 IEEE international smart cities conference (ISC2) (pp. 1-6). IEEE., 2016, September.

[37] I. A. Essien, E. Cadet, J. O. Ajayi, E. D. Erigh and E. Obuse, "Third-party vendor risk assessment and compliance monitoring framework for highly regulated industries.," International Journal of Multidisciplinary Research and Growth Evaluation, vol. 2(5), pp. 569-580, 2021.

[38] S. Carmody, A. Coravos, G. Fahs, A. Hatch, J. Medina, B. Woods and J. Corman, "Building resilient medical technology supply chains with a software bill of materials.," npj Digital Medicine, vol. 4(1), p. 34, 2021.

[39] N. Carroll and I. Richardson, "Software-as-a-medical device: demystifying connected health

regulations.," Journal of Systems and Information Technology, vol. 18(2), pp. 186-215., 2016.

[40] A. A. Alzahrani, A Strategic Vision for Risk Management and Cybersecurity Enhancement in Technological Health Informatics., Shineeks Publishers.

[41] A. Cuschieri, " Nature of human error: implications for surgical practice.," Annals of surgery, vol. 244(5), pp. 642-648, 2006.

[42] S. Bima and W. Intan, "Integrating cyber incident response with disaster recovery for enhanced organizational resilience.," Manuscripts on the Artificial Intelligence and Digital Research, vol. 1(2), pp. 68-77, 2024.