INTERNATIONAL MULTI DISCIPLINARY JOURNAL FOR RESEARCH & DEVELOPMENT
eISSN 2394-6334 Impact factor: 7,854 Volume 13, issue 01 (2026)

Bridging Zero-Trust Security Architectures with Legacy Clinical Infrastructure: Governance, Trust, and Artificial Intelligence in Contemporary Hospital Cybersecurity

Dr. Omren Falcis
Faculty of Information Technology, University of Melbourne, Australia

Abstract:
The accelerating digital transformation of healthcare systems has intensified longstanding cybersecurity vulnerabilities, particularly those arising from the coexistence of advanced artificial intelligence–enabled applications and deeply entrenched legacy clinical infrastructures. Hospitals increasingly depend on networked clinical workstations, medical devices, and decision-support systems that were designed under perimeter-based security assumptions, yet now operate in threat environments characterized by lateral movement, ransomware, and sophisticated supply-chain attacks. Within this context, zero-trust security architectures have emerged as a dominant paradigm for rethinking trust, access control, and governance in healthcare cybersecurity. This article presents a comprehensive, theoretically grounded, and critically elaborated examination of zero-trust adoption in hospital clinical environments, with particular attention to the challenges posed by legacy operating systems and medical devices. Anchored in recent empirical and evaluative scholarship on Windows 11 adoption in hospital clinical workstations, this study integrates insights from cybersecurity governance, artificial intelligence accountability, blockchain-based trust mechanisms, and healthcare risk management to construct a holistic analytical framework (Nayeem, 2026).
The article advances three core arguments. First, it contends that zero-trust security in healthcare cannot be understood merely as a technical architecture but must be conceptualized as a socio-technical governance model that redefines institutional trust relationships among clinicians, patients, devices, vendors, and regulatory bodies. Second, it demonstrates that legacy systems are not simply technical obstacles to modernization but are embedded within clinical workflows, regulatory compliance regimes, and organizational learning processes, thereby complicating straightforward migration strategies. Third, it argues that artificial intelligence, while frequently positioned as an enabler of zero-trust enforcement and threat detection, simultaneously introduces new accountability, explainability, and ethical challenges that must be addressed through robust governance mechanisms.
Methodologically, the study adopts a qualitative, integrative research design grounded in interpretive analysis of peer-reviewed literature, policy documents, and industry reports. Drawing on established frameworks for systematic and mixed-methods appraisal, the analysis synthesizes diverse strands of scholarship to identify recurring patterns, tensions, and unresolved debates in the literature. The results highlight persistent gaps between zero-trust theoretical models and their practical implementation in healthcare settings, particularly in environments dominated by legacy operating systems and heterogeneous device ecosystems. The discussion extends these findings by situating them within broader debates on digital trust, cyber-resilience, and the future of healthcare information infrastructures.
By offering an extensive theoretical elaboration and critical discussion, this article contributes to scholarly understanding of healthcare cybersecurity governance and provides a foundation for future research on integrating zero-trust principles with legacy clinical systems. The findings underscore the necessity of aligning technical innovation with organizational learning, regulatory adaptation, and ethical accountability to achieve sustainable and trustworthy digital healthcare environments.

Keywords
Zero-trust architecture; healthcare cybersecurity; legacy medical systems; artificial intelligence governance; clinical workstations; digital trust

INTRODUCTION

The contemporary healthcare sector is undergoing a profound digital transformation characterized by the rapid integration of networked information systems, artificial intelligence–driven decision-support tools, and data-intensive clinical workflows. While these developments promise significant improvements in diagnostic accuracy, operational efficiency, and patient outcomes, they simultaneously expose healthcare organizations to unprecedented cybersecurity risks (Debnath, 2023). Unlike many other sectors, healthcare institutions must balance the imperatives of security, availability, and patient safety within environments that are often constrained by regulatory requirements, budgetary limitations, and deeply entrenched legacy technologies (Burrell, 2024). This confluence of factors has rendered traditional perimeter-based security models increasingly inadequate, prompting growing interest in zero-trust security architectures as a foundational paradigm for healthcare cybersecurity governance (Gellert et al., 2023).

Zero-trust architecture fundamentally challenges the assumption that entities within a network perimeter can be implicitly trusted. Instead, it advocates continuous verification, least-privilege access, and context-aware policy enforcement across users, devices, applications, and data flows (He et al., 2022). In healthcare settings, this paradigm shift has profound implications, as clinical environments are populated by a diverse array of actors, including clinicians, patients, administrative staff, biomedical devices, and third-party vendors. Each of these actors interacts with sensitive health information under varying conditions of risk and accountability, complicating the implementation of uniform security controls (Tyler & Viana, 2021). The challenge is further exacerbated by the prevalence of legacy operating systems and medical devices that were not designed to support modern authentication, encryption, or continuous monitoring mechanisms (Eastwood, 2024).

The persistence of legacy systems in healthcare is not merely a matter of technical inertia but reflects broader socio-organizational dynamics. Hospitals often rely on medical equipment with long operational lifespans, regulatory certifications, and vendor dependencies that make replacement costly and risky (Kaspersky, 2024). Moreover, clinical workflows are frequently optimized around familiar interfaces and stable systems, creating resistance to disruptive technological change. As a result, healthcare organizations find themselves in a paradoxical position: they are expected to adopt advanced cybersecurity paradigms such as zero trust while continuing to operate infrastructures that embody outdated security assumptions (Northcutt, 2005).

Recent scholarship has begun to address this tension by examining strategies for bridging zero-trust principles with legacy environments. Notably, evaluative research on the adoption of Windows 11 in hospital clinical workstations provides a concrete case through which to analyze the practical implications of modern operating system upgrades within zero-trust frameworks (Nayeem, 2026). This line of inquiry highlights both the potential benefits of enhanced security features, such as hardware-based isolation and improved identity management, and the challenges associated with compatibility, training, and workflow disruption. By situating operating system modernization within a broader governance and trust context, such studies underscore the need for integrative approaches that account for technical, organizational, and ethical dimensions of cybersecurity.

At the same time, artificial intelligence has emerged as a central component of contemporary cybersecurity strategies. AI-driven threat detection, anomaly analysis, and automated policy enforcement are frequently cited as key enablers of zero-trust implementation, particularly in complex and dynamic environments such as hospitals (Ajish, 2024). However, the deployment of AI in healthcare cybersecurity raises critical questions about accountability, transparency, and trustworthiness. Scholars have warned that opaque algorithms and automated decision-making processes may undermine clinical accountability and exacerbate existing power asymmetries within healthcare organizations (Habli et al., 2020). These concerns are amplified in zero-trust contexts, where access decisions may be continuously recalibrated by AI systems based on behavioral and contextual data.

In parallel, emerging technologies such as blockchain and federated identity management have been proposed as complementary mechanisms for enhancing trust and security in healthcare systems. Blockchain-based architectures promise immutable audit trails, decentralized trust, and enhanced data integrity, potentially addressing some of the governance challenges associated with AI-driven security controls (Kasralikar et al., 2025; Kaul, 2019). Federated identity frameworks, meanwhile, offer the possibility of reconciling zero-trust

principles with the distributed and collaborative nature of healthcare delivery (Huda et al., 2024). Yet, the integration of these technologies with legacy systems remains an open question, with limited empirical evidence on their feasibility and impact.

Despite the growing body of literature on zero trust, AI, and healthcare cybersecurity, several critical gaps remain. Much of the existing research focuses either on high-level conceptual models or on isolated technical solutions, with insufficient attention to the lived realities of hospital environments characterized by heterogeneous systems and constrained resources (Shojaei et al., 2024). Moreover, there is a tendency to treat legacy systems as temporary obstacles rather than as enduring features of healthcare infrastructures that must be governed and secured over extended periods (Vijayasekhar, 2022). This gap is particularly evident in discussions of operating system modernization, where the organizational and ethical implications of platform transitions are often underexplored.

Against this backdrop, the present article seeks to advance scholarly understanding of zero-trust security in healthcare by offering an extensive, integrative analysis that bridges technical architectures, organizational governance, and ethical accountability. Building on evaluative insights into Windows 11 adoption in hospital clinical workstations (Nayeem, 2026), the study examines how zero-trust principles can be operationalized in environments dominated by legacy systems and AI-driven applications. By synthesizing diverse strands of literature and engaging critically with competing perspectives, the article aims to move beyond prescriptive solutions toward a more nuanced understanding of cybersecurity as a socio-technical governance challenge in contemporary healthcare.

METHODOLOGY

The methodological approach adopted in this study is grounded in qualitative, interpretive research traditions that emphasize depth of analysis, theoretical integration, and critical engagement with existing scholarship. Given the complexity of zero-trust security implementation in healthcare and the absence of universally applicable empirical datasets, a text-based, integrative methodology was selected to enable comprehensive exploration of technical, organizational, and ethical dimensions (Hong et al., 2018). This approach aligns with established practices in healthcare informatics and cybersecurity research, where conceptual synthesis and critical review play a central role in theory development (Page et al., 2021).

The first stage of the methodology involved the systematic identification and examination of peer-reviewed journal articles, conference proceedings, policy reports, and industry analyses related to zero-trust architecture, healthcare cybersecurity, artificial intelligence governance, and legacy system management. Particular attention was given to studies that explicitly address healthcare contexts, as well as those that offer transferable insights from adjacent domains such as federal cloud security and critical infrastructure protection (Ofili et al., 2025). The evaluative study of Windows 11 adoption in hospital clinical workstations served as a focal point for grounding abstract concepts in concrete institutional practices (Nayeem, 2026).

Rather than employing a narrow inclusion-exclusion protocol typical of systematic reviews, this study adopted an integrative review strategy that prioritizes conceptual richness and cross-disciplinary dialogue. This decision reflects the recognition that zero-trust security in healthcare is not a discrete technical intervention but an evolving governance paradigm that intersects with organizational learning, regulatory compliance, and ethical accountability (Khan MJ, 2023). Sources were therefore selected based on their theoretical relevance, methodological rigor, and contribution to ongoing scholarly debates, rather than on strict methodological homogeneity.

The analytical process involved iterative reading, coding, and thematic synthesis of the selected literature. Key themes were identified through close textual analysis, including trust reconfiguration, legacy system persistence, AI-enabled security controls, and institutional governance. These themes were then examined in relation to one another to identify patterns of convergence and divergence across different strands of scholarship. For example, technical analyses of zero-trust enforcement mechanisms were juxtaposed with organizational studies of healthcare risk management to explore how abstract security principles translate into

operational realities (Burrell, 2024).

A critical component of the methodology was the reflexive examination of underlying assumptions within the literature. Many zero-trust models implicitly assume a level of infrastructural flexibility and resource availability that may not be realistic in healthcare settings characterized by aging equipment and constrained budgets (Eastwood, 2024). By interrogating these assumptions, the study sought to uncover implicit biases and normative expectations that shape contemporary cybersecurity discourse. This reflexive stance is consistent with calls for greater accountability and transparency in both AI deployment and cybersecurity governance (Habli et al., 2020).

Limitations of the methodological approach must also be acknowledged. As a qualitative, literature-based study, the findings are inherently interpretive and dependent on the scope and quality of available sources. While the integrative strategy enables broad theoretical synthesis, it cannot substitute for empirical validation through field studies or longitudinal data collection. Moreover, the rapidly evolving nature of cybersecurity threats and technologies means that some insights may be time-bound, requiring ongoing reassessment as new evidence emerges (Mandiant, 2022). Nonetheless, by grounding the analysis in recent and diverse scholarship, including evaluative research on operating system modernization (Nayeem, 2026), the study aims to provide a robust and enduring contribution to the field.

RESULTS

The results of the integrative analysis reveal a complex and often fragmented landscape of zero-trust adoption in healthcare, shaped by the interplay of technological innovation, organizational constraints, and evolving threat environments. Across the reviewed literature, there is broad consensus that zero-trust principles offer a compelling response to the limitations of perimeter-based security, particularly in environments characterized by high levels of internal threat and lateral movement (Ho et al., 2021). However, the translation of these principles into practice within hospital settings remains uneven and contested.

One of the most salient findings concerns the persistent centrality of legacy operating systems and medical devices in shaping cybersecurity outcomes. Studies consistently report that a significant proportion of healthcare organizations continue to rely on outdated platforms that lack native support for modern security features (Kaspersky, 2024). This reliance is not merely a technical liability but reflects deep-seated organizational dependencies, including vendor support agreements, regulatory certifications, and clinician familiarity. The evaluative analysis of Windows 11 adoption in hospital clinical workstations illustrates how operating system upgrades can serve as both a catalyst for enhanced security and a source of operational disruption (Nayeem, 2026). While Windows 11 introduces features aligned with zero-trust principles, such as improved identity integration and hardware-based isolation, its deployment requires substantial investment in hardware compatibility assessments, staff training, and workflow redesign.

Another key result relates to the role of artificial intelligence in enabling and complicating zero-trust implementation. AI-driven security tools are widely portrayed as essential for managing the scale and complexity of healthcare networks, enabling real-time anomaly detection and adaptive policy enforcement (Ajish, 2024). The literature indicates that such tools can significantly enhance visibility and responsiveness, particularly in detecting insider threats and compromised devices. However, concerns about algorithmic opacity and accountability are recurrent, with scholars warning that overreliance on automated decision-making may obscure responsibility for access denials or security incidents (Markus et al., 2021). These concerns are particularly acute in clinical contexts, where delayed or denied access to systems can have direct implications for patient care.

The analysis also highlights emerging interest in complementary technologies, such as blockchain and federated identity management, as mechanisms for enhancing trust and resilience in zero-trust healthcare environments. Blockchain-based solutions are credited with providing immutable audit trails and decentralized trust frameworks that align with the distributed nature of healthcare delivery (Kasralikar et al., 2025). Federated identity approaches, meanwhile, offer potential pathways for reconciling zero-trust access

controls with cross-organizational collaboration among healthcare providers (Huda et al., 2024). Despite their promise, the results indicate that empirical evidence of successful integration with legacy systems remains limited, underscoring the need for further research and pilot implementations.

Finally, the results reveal a notable gap between high-level policy advocacy for zero trust and the practical realities of healthcare cybersecurity governance. Regulatory and advisory bodies increasingly endorse zero-trust principles, yet provide limited guidance on managing transitional risks associated with legacy systems and AI deployment (Ghasemshirazi et al., 2023). This gap is reflected in the heterogeneous adoption patterns observed across healthcare organizations, with some institutions pursuing incremental modernization strategies while others remain constrained by technical debt and resource limitations. The findings suggest that without sustained organizational learning and governance reform, zero-trust adoption risks becoming a superficial compliance exercise rather than a transformative security paradigm (Nayeem, 2026).

DISCUSSION

The findings of this study invite a deeper theoretical and critical examination of zero-trust security as a socio-technical governance model in healthcare. At a conceptual level, zero trust represents a fundamental reconfiguration of how trust is constructed, operationalized, and enforced within digital systems. Rather than relying on static boundaries and implicit assumptions, zero-trust architectures posit trust as provisional, contextual, and continuously negotiated (He et al., 2022). In healthcare environments, this reconfiguration intersects with longstanding professional norms, ethical obligations, and regulatory frameworks that have traditionally relied on interpersonal trust and institutional reputation.

One of the most significant implications of the analysis concerns the reframing of legacy systems. Prevailing cybersecurity discourse often portrays legacy technologies as obstacles to be eliminated through modernization. However, the results suggest that such a framing overlooks the embeddedness of legacy systems within clinical practice and organizational memory (Burrell, 2024). From a socio-technical perspective, legacy systems embody accumulated knowledge, workflows, and trust relationships that cannot be easily disentangled from their technical substrates. The case of Windows 11 adoption in hospital clinical workstations illustrates how modernization initiatives must navigate these embedded dimensions, balancing security enhancements against the risk of disrupting clinical routines (Nayeem, 2026).

This perspective challenges deterministic narratives that equate technological advancement with improved security. Instead, it underscores the importance of organizational learning and adaptive governance in mediating the relationship between technology and risk. Drawing on theories of organizational learning, it can be argued that zero-trust adoption requires not only technical reconfiguration but also shifts in institutional culture, training, and accountability structures (Debnath, 2023). Without such shifts, zero-trust mechanisms may be resisted, circumvented, or misapplied, undermining their intended benefits.

The role of artificial intelligence further complicates this landscape. While AI-driven security tools align well with zero-trust principles of continuous verification and contextual awareness, they also introduce new forms of opacity and power asymmetry (Habli et al., 2020). In clinical settings, where accountability for patient outcomes is paramount, the delegation of access decisions to algorithms raises ethical questions about responsibility and explainability. Scholars of explainable AI argue that trust in automated systems depends on the ability of stakeholders to understand and contest their outputs (Markus et al., 2021). Applying this insight to zero-trust healthcare environments suggests that AI-enabled security controls must be designed with transparency and auditability in mind, particularly when interfacing with legacy systems that may lack robust logging or monitoring capabilities.

The discussion also highlights the potential and limitations of emerging trust-enhancing technologies such as blockchain. While blockchain-based architectures promise decentralized trust and immutable records, their integration into healthcare cybersecurity remains nascent and contested (Kasralikar et al., 2025). From a governance perspective, blockchain may shift trust from centralized authorities to distributed networks, raising questions about accountability, scalability, and regulatory oversight. These questions are particularly salient

in healthcare, where data stewardship and patient consent are subject to stringent legal and ethical constraints (Khan MM et al., 2025). The challenge, therefore, lies in aligning the technical affordances of blockchain with existing governance frameworks and legacy infrastructures.

Another critical dimension of the discussion concerns the broader threat environment facing healthcare organizations. High-profile cyber incidents, such as ransomware attacks on hospital systems, have underscored the inadequacy of traditional security models and galvanized interest in zero trust (Department of Health, 2018; Help Net Security, 2023). However, the reactive adoption of zero-trust frameworks in response to crises may lead to fragmented or superficial implementations that fail to address underlying structural vulnerabilities. The literature reviewed suggests that sustainable zero-trust adoption requires proactive investment in infrastructure modernization, workforce development, and cross-sector collaboration (Tyler & Viana, 2021).

From a policy perspective, the findings point to the need for more nuanced guidance on zero-trust implementation in healthcare. Existing policy statements often emphasize aspirational principles without providing concrete strategies for managing legacy systems and transitional risks (Khan MJ, 2023). By contrast, the evaluative insights into operating system modernization offer a more grounded understanding of the trade-offs involved in aligning technical platforms with zero-trust objectives (Nayeem, 2026). Policymakers and regulators could benefit from incorporating such empirical perspectives into standards and best-practice frameworks, thereby bridging the gap between theory and practice.

Limitations of the present study also warrant reflection. While the integrative methodology enables comprehensive theoretical synthesis, it cannot capture the full diversity of healthcare contexts or the dynamic evolution of cyber threats. Future research could complement this analysis with empirical case studies, longitudinal assessments of zero-trust adoption, and participatory research involving clinicians and IT professionals. Such approaches would enrich understanding of how zero-trust principles are negotiated and enacted in everyday practice, particularly in resource-constrained settings.

Looking ahead, the future of healthcare cybersecurity will likely be shaped by the convergence of zero-trust architectures, AI-driven analytics, and ongoing legacy system management. Rather than viewing these elements as discrete challenges, this discussion suggests the value of holistic governance frameworks that integrate technical, organizational, and ethical considerations. By reconceptualizing zero trust as a dynamic process of trust negotiation rather than a static architecture, healthcare organizations may be better positioned to navigate the complexities of digital transformation while safeguarding patient safety and institutional integrity (Nayeem, 2026).

CONCLUSION

This article has undertaken an extensive and critical examination of zero-trust security architectures within the context of contemporary healthcare, with particular emphasis on the enduring influence of legacy clinical systems and the growing role of artificial intelligence. Through an integrative analysis grounded in diverse strands of scholarship, the study has demonstrated that zero trust in healthcare cannot be reduced to a technical solution but must be understood as a socio-technical governance paradigm that reshapes institutional trust relationships, accountability mechanisms, and organizational learning processes.

The findings underscore that legacy systems are not merely residual artifacts of the past but active participants in the present cybersecurity landscape, shaping both vulnerabilities and constraints on innovation. Evaluative insights into the adoption of modern operating systems in hospital clinical workstations reveal the practical complexities of aligning technological modernization with zero-trust principles, highlighting the need for careful governance and stakeholder engagement (Nayeem, 2026). At the same time, the integration of AI and emerging trust technologies introduces new opportunities and challenges that demand rigorous ethical and regulatory oversight.

By situating zero-trust adoption within broader debates on trust, accountability, and digital governance, this study contributes to a more nuanced understanding of healthcare cybersecurity. It calls for future research and

policy development that move beyond prescriptive models toward adaptive, context-sensitive frameworks capable of accommodating the realities of legacy infrastructure and evolving technological ecosystems. Ultimately, the pursuit of secure and trustworthy healthcare systems will depend not only on technical innovation but on sustained commitment to governance, learning, and ethical responsibility.

REFERENCES

1. Kasralikar P, Polu OR, Chamarthi B, Veer Samara Sihman Bharattej Rupavath R, Patel S, Tumati R. Blockchain for securing AI-driven healthcare systems: a systematic review and future research perspectives. Cureus. 2025;17:e83136.

2. Northcutt S. Inside network perimeter security. 2nd ed. Sams; 2005.

3. Habli I, Lawton T, Porter Z. Artificial intelligence in health care: accountability and safety. Bulletin of the World Health Organization. 2020;98:251–256.

4. Nayeem M. Bridging zero-trust security and legacy medical devices: An evaluation of Windows 11 adoption in hospital clinical workstations. Frontiers in Emerging Artificial Intelligence and Machine Learning. 2026;3(1):1–8.

5. Debnath S. Integrating information technology in healthcare: recent developments, challenges, and future prospects for urban and regional health. World Journal of Advanced Research and Reviews. 2023;19(1):455–463.

6. Gellert GA, et al. Zero trust and the future of cybersecurity in healthcare delivery organizations. Journal of Hospital Administration. 2023;12(1):1–8.

7. Ajish D. The significance of artificial intelligence in zero trust technologies: a comprehensive review. Journal of Electrical Systems and Information Technology. 2024;11:30.

8. Eastwood B. Tips for health systems on managing legacy systems to strengthen security. HealthTech Magazine. 2024.

9. He Y, et al. A survey on zero trust architecture: challenges and future trends. Wireless Communications and Mobile Computing. 2022;2022:1–13.

10. Burrell DN. Understanding healthcare cybersecurity risk management complexity. Land Forces Academy Review. 2024;29:38–49.

11. Markus AF, Kors JA, Rijnbeek PR. The role of explainability in creating trustworthy artificial intelligence for health care: a comprehensive survey. Journal of Biomedical Informatics. 2021;113:103655.

12. Tyler D, Viana T. Trust no one? A framework for assisting healthcare organisations in transitioning to a zero-trust network architecture. Applied Sciences. 2021;11(16):1–18.

13. Kaspersky. Kaspersky finds 73% of healthcare providers use medical equipment with a legacy OS. 2024.

14. Ho G, et al. Hopper: modeling and detecting lateral movement (extended report). arXiv. 2021;1–20.

15. Ofili BT, Erhabor EO, Obasuyi OT. Enhancing federal cloud security with AI: zero trust, threat intelligence, and compliance. World Journal of Research and Review. 2025;25:2377–2400.

16. Hong QN, Pluye P, Fàbregues S, et al. Mixed methods appraisal tool (MMAT), version 2018. BMJ. 2018;1–7.

17. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for

reporting systematic reviews. BMJ. 2021;372:n71.

18. Help Net Security. Rising cyber incidents challenge healthcare organizations. 2023.

19. Department of Health. Investigation: WannaCry cyber-attack on the NHS. UK National Audit Office. 2018.

20. Ghasemshirazi S, Shirvani G, Alipour MA. Zero trust: applications, challenges, and opportunities. arXiv. 2023;1–23.

21. Khan MJ. Zero trust architecture: redefining network security paradigms in the digital age. World Journal of Advanced Research and Reviews. 2023;19(3):105–116.

22. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and privacy of technologies in health information systems: a systematic literature review. Computers. 2024;13(2):1–25.

23. Vijayasekhar D. Securing the future: strategies for modernizing legacy systems and enhancing cybersecurity. Journal of Artificial Intelligence and Cloud Computing. 2022;1(3):1–3.

24. Khan MM, Shah N, Shaikh N, Thabet A, Alrabayah T, Belkhair S. Towards secure and trusted AI in healthcare: a systematic review of emerging innovations and ethical challenges. International Journal of Medical Informatics. 2025;195:105780.

25. Kaul D. Blockchain-powered cyber-resilient microservices: AI-driven intrusion prevention with zero-trust policy enforcement. Journal of Mathematical and Computational Science. 2019;1–34.

26. Huda S, Islam MR, Abawajy J, Kottala VN, Ahmad S. A cyber risk assessment approach to federated identity management framework-based digital healthcare system. Sensors. 2024;24:5282.

27. Mandiant. M-Trends 2022 special report: executive summary. 2022.

28. International Conference on Communication Technologies (ComTech 2017). Institute of Electrical and Electronics Engineers; 2017.