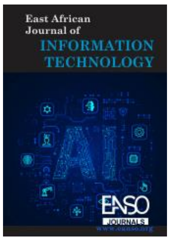

East African Journal of Information Technology
eajit.eanso.org
Volume 8, Issue 1, 2025
Print ISSN: 2707-5346 | Online ISSN: 2707-5354
Title DOI: https://doi.org/10.37284/2707-5354

EANSO
EAST AFRICAN NATURE & SCIENCE ORGANIZATION

Original Article

Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System

Sylvester Mugala[1], Kasongo Alfred[1], Linda Sibanda[1], Chisha Mulenga[1], Mulako Hachamba[1] & Henitha Mwiinga[1]*

[1] Eden University, P. O. Box 37727, Barlastone Park, Lusaka, Zambia.
* Author's ORCID ID; https://orcid.org/0009-0005-7301-2584; Email: smugala@edenuniversity.education

Article DOI: https://doi.org/10.37284/eajit.8.1.2896

Date Published:

18 April 2025

Keywords:

Medical IoT Devices, Privacy Protection, Digital Health, Healthcare Cybersecurity.

ABSTRACT

The integration of Internet of Things (IoT) devices in Zambia's healthcare system presents transformative opportunities for improving patient care, operational efficiency, and data management. However, the rapid adoption of IoT also introduces significant security and privacy risks, including vulnerabilities in device authentication, data breaches, and regulatory compliance challenges. This study systematically reviews existing literature on IoT security and privacy in healthcare, with a particular focus on Zambia's digital health landscape. It identifies key threats, including weak encryption mechanisms, unauthorized data access, and insufficient regulatory enforcement. The study further highlights best practices and emerging technologies, such as blockchain and artificial intelligence (AI) that can enhance IoT security. By examining Zambia's current regulatory framework in comparison to international standards, the study provides practical recommendations for strengthening cybersecurity policies, improving digital literacy, and fostering collaboration between stakeholders. Addressing these challenges is crucial for ensuring the secure and sustainable implementation of IoT in Zambia's healthcare system.

APA CITATION

Mugala, S., Kasongo, A., Sibanda, L., Mulenga, C., Hachamba, M. & Mwiinga, H. (2025). Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System. *East African Journal of Information Technology, 8*(1), 70-79. https://doi.org/10.37284/eajit.8.1.2896

CHICAGO CITATION

Mugala, Sylvester, Alfred Kasongo, Linda Sibanda, Chisha Mulenga, Mulako Hachamba and Henitha Mwiinga. 2025. "Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System". *East African Journal of Information Technology* 8 (1), 70-79. https://doi.org/10.37284/eajit.8.1.2896.

HARVARD CITATION

Mugala, S., Kasongo, A., Sibanda, L., Mulenga, C., Hachamba, M. & Mwiinga, H. (2025) "Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System", *East African Journal of Information Technology*, 8(1), pp. 70-79. doi: 10.37284/eajit.8.1.2896.

IEEE CITATION

S., Mugala, A., Kasongo, L., Sibanda, C., Mulenga, M., Hachamba & H., Mwiinga "Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System", *EAJIT*, vol. 8, no. 1, pp. 70-79, Apr. 2025.

MLA CITATION

Mugala, Sylvester, Alfred Kasongo, Linda Sibanda, Chisha Mulenga, Mulako Hachamba & Henitha Mwiinga "Exploring Security and Privacy Implications of IoT Devices in Zambia's Healthcare System". *East African Journal of Information Technology*, Vol. 8, no. 1, Apr. 2025, pp. 70-79, doi:10.37284/eajit.8.1.2896.

INTRODUCTION

Innovation in various industries has been significantly driven by advancements in digital technology, with IoT playing a pivotal role in enhancing service delivery and operational efficiency. Sectors such as healthcare, agriculture, transportation, education, and defence have leveraged IoT to optimize processes and improve outcomes (Van Hoang, 2024; Halubanza, 2024). In healthcare, for instance, IoT has enabled disease prevention, early diagnosis, remote patient monitoring, and personalized treatment. Additionally, it facilitates the collection, analysis, and secure storage of medical data, contributing to improved healthcare accessibility and quality (Hu et al., 2013). Recognizing these benefits, the Government of the Republic of Zambia (GRZ) developed the E-Health Policy 2017–2021 to address challenges in electronic health services, including the adoption of IoT-based solutions (GRZ, 2017). This initiative was further strengthened by the introduction of the Digital Health Strategy 2023, which underscores the government’s commitment to leveraging digital innovations for improved healthcare delivery (GRZ, 2023). These efforts highlight the growing importance of IoT in enhancing governance, patient care, and the overall efficiency of Zambia’s health sector.

IoT is defined as a network of intelligently connected devices and systems that utilize data collected from sensors, actuators, and other physical tools to enable automation and decision-making (Vujovic, 2015). The core stages of IoT include data collection, network aggregation, processing, storage, and optimization for future applications. These stages enable IoT to deliver tailored benefits across various domains. For enterprises, IoT enhances productivity, decision-making, and service delivery, particularly in manufacturing and logistics (Musonda et al., 2025). For consumers, IoT improves energy efficiency, security, healthcare, education, and overall quality of life. In healthcare, IoT fosters a technology-mediated relationship between stakeholders, enabling seamless communication and collaboration among healthcare providers, patients, and policymakers. This interconnected ecosystem has the potential to address critical challenges in healthcare, such as resource allocation, patient monitoring, and data management.

The integration of IoT in healthcare has also paved the way for innovative solutions such as wearable devices, smart medical equipment, and telemedicine platforms. Wearable devices, for instance, allow continuous monitoring of vital signs, enabling early detection of health issues and timely interventions. Smart medical equipment enhances diagnostic accuracy and treatment precision, reducing the risk of human error. Telemedicine platforms powered by IoT facilitate remote consultations, making healthcare accessible to underserved populations (Owen & Kellr, 2025). These advancements not only improve patient outcomes but also reduce the burden on healthcare systems by minimizing hospital visits and optimizing resource utilization. As IoT continues to evolve, its potential to transform healthcare delivery and improve public health outcomes remains unparalleled.

Moreover, the adoption of IoT in Zambia’s healthcare sector aligns with global trends and best practices, positioning the country to address its unique healthcare challenges effectively. By leveraging IoT technologies, Zambia can enhance its healthcare infrastructure, improve data-driven decision-making, and ensure equitable access to quality healthcare services. The government’s commitment to digital health, as evidenced by the E-Health Policy and Digital Health Strategy, demonstrates a forward-thinking approach to harnessing technology for national development (Nzazi, 2025). With continued investment and collaboration among stakeholders, IoT has the potential to revolutionize Zambia’s healthcare landscape, ultimately contributing to the achievement of universal health coverage and improved public health outcomes.

Despite its potential, the successful integration of IoT in Zambia’s healthcare system depends on addressing several challenges, including inadequate infrastructure, limited digital literacy, and concerns about data security and privacy (Mphande, 2020). Strengthening ICT infrastructure, investing in capacity-building initiatives, and formulating robust cybersecurity policies will be crucial in ensuring the effective and sustainable deployment of IoT solutions (Teh, & Rana, 2023). Furthermore, fostering partnerships between the public and private sectors can accelerate innovation and resource mobilization, enabling more efficient healthcare delivery. As Zambia continues its digital transformation journey, a strategic and inclusive approach to IoT adoption will be essential in maximizing its benefits and overcoming existing barriers. Thus, the study aims to scholarly analyze IoT security and privacy challenges in healthcare, evaluate Zambia's regulatory framework against international standards, and propose actionable strategies for secure IoT adoption. By highlighting best practices and emerging technologies—such as blockchain and AI—the research identifies solutions to enhance IoT security. Furthermore, through a comparative analysis of Zambia's policies with global benchmarks, the study provides practical recommendations to strengthen cybersecurity policies, improve digital literacy, and foster stakeholder collaboration. Addressing these challenges is critical to ensuring the secure and sustainable integration of IoT in Zambia's healthcare system.

SECURITY IMPLICATIONS OF IoT DEVICES IN HEALTHCARE

Vulnerabilities in IoT Devices

The security implications of IoT devices in healthcare have been a subject of significant concern for both researchers and industry experts. Various studies, including those by Ketu and Mishra (2021), Mamdouh et al. (2021), Samasundaram (2021), and Sivan (2021), have extensively examined vulnerabilities associated with these technologies. A key issue highlighted is the presence of weak authentication mechanisms, which allow unauthorized individuals to exploit system weaknesses, gaining access to critical patient data and device controls. Additionally, a lack of encryption protocols leaves IoT devices susceptible to data interception, increasing the risk of cyberattacks (Mamdouh et al., 2021). Another critical vulnerability is the inadequate implementation of secure firmware updates, exposing devices to malware attacks that could compromise healthcare systems (Vujovic, 2015). These vulnerabilities underscore the urgent need for implementing multi-factor authentication, advanced encryption methods, and secure update management to safeguard IoT devices in healthcare environments.

Data Privacy and Confidentiality

Ensuring data privacy and confidentiality remains a fundamental challenge in IoT-driven healthcare systems. Unauthorized access to patient data can result in identity theft, fraud, and disruptions to healthcare services, significantly affecting patient trust and institutional credibility (Sharma & Chen, 2022). Researchers such as Ketu and Mishra (2021) and Sivan et al. (2021) emphasize that data breaches in healthcare IoT environments can have severe consequences, including financial and reputational damages. Moreover, inadequate supply chain security poses an additional risk, as malicious actors may introduce vulnerabilities into IoT devices during the manufacturing process, further exacerbating cybersecurity concerns. Recent cyberattacks targeting healthcare infrastructure have demonstrated how ransomware and other malicious software exploit these weaknesses, causing critical service disruptions (Wu et al., 2020). Strengthening access control mechanisms, adopting advanced encryption techniques, and establishing comprehensive cybersecurity training programs for healthcare professionals are essential measures to mitigate these risks.

Regulatory Compliance

Compliance with regulatory frameworks is crucial for enhancing the security of IoT devices in healthcare. Zambia's legal framework for digital health security, as outlined in the E-Health Policy 2017–2021 and the Digital Health Strategy 2023, emphasizes the need for secure healthcare data management (GRZ, 2017; GRZ, 2023). However, when compared to international standards such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union, Zambia's regulations may require further strengthening to comprehensively address emerging threats (Mamdouh et al., 2021; Samasundaram, 2021). Additionally, researchers highlight the importance of patch management, ensuring that IoT devices receive timely security updates to mitigate vulnerabilities (Sivan et al., 2021). Another critical aspect of regulatory compliance is education and training, as many healthcare professionals and end-users lack sufficient knowledge of IoT security risks. By strengthening cybersecurity regulations, enforcing strict compliance measures, and fostering public-private partnerships, Zambia can create a more secure digital health ecosystem that aligns with global best practices.

PRIVACY IMPLICATIONS OF IOT DEVICES IN HEALTHCARE

Data Security and Encryption

The security of patient data is a fundamental concern in healthcare IoT systems, necessitating robust encryption mechanisms to protect sensitive information from cyber threats. Various researchers, including Shahid (2022), Sadek (2022), Kelly (2020), and Karunarathne (2021), have extensively explored the significance of securing patient data collected by IoT devices. End-to-end encryption plays a crucial role in safeguarding data as it moves between IoT devices, cloud storage, and healthcare providers, ensuring that unauthorized entities cannot access or manipulate the information (Sivan et al., 2021). Additionally, cloud storage security measures, including multi-factor authentication, firewalls, and intrusion detection systems, are essential in mitigating risks associated with data breaches (Mamdouh et al., 2021). Despite these security measures, a lack of standardized encryption protocols across different IoT systems remains a critical challenge, increasing the risk of cyber threats (Ketu & Mishra, 2021). Strengthening encryption protocols and enforcing stringent access controls can significantly enhance data security and prevent unauthorized disclosures in IoT-driven healthcare environments.

Data Ownership and Consent

The question of data ownership and patient consent remains a critical ethical and legal issue in the deployment of IoT devices in healthcare. Authors such as Shahid (2022) and Karunarathne (2021) have raised concerns regarding who should own and control the data generated by IoT devices, advocating for clear patient consent mechanisms. Patients have the right to control their health data, including how it is collected, stored, and shared (Samasundaram, 2021). However, many healthcare IoT systems operate without clear guidelines on patient consent, leading to potential misuse of personal health information. Ethical concerns also arise regarding data sharing with third parties, such as insurance companies and pharmaceutical firms, without explicit patient approval (Mamdouh et al., 2021). Additionally, interoperability challenges further complicate data access, as different IoT systems may have varying policies on data storage and sharing (Kelly, 2020). To address these challenges, regulatory frameworks should establish clear policies on data ownership and ensure that patients provide informed consent before their data is accessed or shared. Implementing transparent data governance structures will enhance patient trust and promote ethical handling of sensitive health information.

User Awareness and Education

A significant barrier to ensuring privacy in healthcare IoT is the lack of awareness and education among users, including healthcare professionals and patients. Many researchers, including Sadek (2022) and Kelly (2020), emphasize the need for user education on privacy risks associated with IoT devices. Healthcare professionals often lack sufficient training on cybersecurity best practices, making IoT systems more vulnerable to breaches and unauthorized access (Ketu & Mishra, 2021). Additionally, patients are often unaware of IoT security risks, such as phishing attacks and weak passwords, which can compromise their personal health information (Sivan et al., 2021). Some authors suggest that increasing awareness through cybersecurity training, privacy policies, and digital literacy initiatives can improve decision-making regarding data protection (Karunarathne, 2021). Providing regular cybersecurity training for healthcare professionals and launching public awareness campaigns on data protection can help mitigate these risks. By fostering a culture of cybersecurity awareness, healthcare institutions can enhance the privacy and security of IoT-driven healthcare services.

METHODOLOGY

This study adopts a systematic and structured methodology to examine the existing literature on IoT security and privacy in healthcare. The research process began with the collection of relevant articles, reports, and policy documents from reputable databases such as IEEE Xplore, PubMed, Springer, and Google Scholar. The inclusion criteria were carefully defined to ensure the relevance and quality of the selected studies, focusing exclusively on peer-reviewed articles published between 2015 and 2024 that addressed IoT applications in healthcare, particularly in developing countries. After applying these criteria, 85 articles were selected for in-depth review, with the sample size determined by thematic saturation—the point at which additional sources ceased to yield new insights into the research questions. Additionally, articles addressing security, privacy, and regulatory frameworks were prioritized. Studies unrelated to healthcare or lacking empirical evidence were excluded to maintain the rigour and focus of the review. The selected literature was then analyzed to identify common themes, research gaps, and actionable recommendations.

The study framework is structured into three key components: data collection, data analysis, and a comparative approach. During the data collection phase, relevant materials such as regulatory policies, security reports, and academic studies were gathered. The data analysis phase utilized thematic analysis to categorize and examine security threats, vulnerabilities, and mitigation strategies discussed in the literature. This approach allowed for the identification of recurring patterns and critical insights into the challenges and solutions related to IoT security in healthcare.

Finally, the study incorporates a comparative approach to contextualize the findings within the Zambian healthcare landscape. By analyzing Zambia’s regulatory framework in comparison to international standards, the study highlights areas of alignment and divergence. This comparative analysis not only provides a deeper understanding of the local context but also offers insights into how global best practices can be adapted to address the unique challenges faced by developing countries. Through this methodological approach, the review aims to contribute to the growing body of knowledge on IoT security and privacy in healthcare, while offering practical recommendations for policymakers, healthcare providers, and other stakeholders.

FINDINGS AND DISCUSSION

Identified Security Gaps

The findings reveal several security gaps in the implementation of IoT devices in healthcare, posing risks to data integrity, privacy, and patient safety (Obaid, & Salman, 2022). One critical issue is the inconsistent implementation of encryption standards across different IoT platforms, which exposes sensitive patient data to unauthorized access and cyber threats (Joshua et al., 2022). Many healthcare IoT systems lack clear guidelines on data encryption both in transit and at rest, making them vulnerable to breaches. Additionally, healthcare providers and IoT device manufacturers often struggle to fully comprehend and adhere to existing regulatory requirements, leading to non-compliance and inadequate security measures (Bazanye, 2022). These challenges underscore the need for robust security frameworks and continuous vulnerability assessments to identify and mitigate risks associated with IoT-based healthcare solutions.

Regulatory and Compliance Challenges

A significant gap noted in the study is the limited enforcement of regulatory policies governing IoT security in healthcare (Sicari et al., 2017). While various international frameworks, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), provide guidelines for data protection, many healthcare providers lack the awareness or resources to implement these standards effectively (Schmidt, 2020). In Zambia, the absence of comprehensive and updated regulations tailored to digital health security further complicates compliance efforts. The lack of standardized protocols for data exchange and storage leads to data fragmentation, making interoperability and security enforcement difficult (Muyunda, & Mpundu, 2023). To bridge this gap, policymakers must establish clear regulatory frameworks that align with global best practices while considering the unique challenges of Zambia’s healthcare landscape.

Training and Awareness Deficiencies

The findings also highlight a critical deficiency in cybersecurity training among healthcare personnel and end-users of IoT devices (Javaid et al., 2023). Many healthcare providers lack the necessary skills to recognize and respond to security threats, increasing the likelihood of breaches caused by human error or social engineering attacks. Furthermore, patients often have limited control over their health data, with minimal options for managing, deleting, or restricting access to their information (Magyar, 2017). The study suggests that comprehensive training programs tailored for healthcare professionals, IoT device manufacturers, and policymakers can enhance cybersecurity awareness and preparedness (Nifakos et al., 2021). Additionally, increasing patient education on data security best practices will empower users to take an active role in protecting their personal health information.

The Intersection of IoT and Emerging Technologies

The integration of artificial intelligence (AI) with IoT devices presents both opportunities and challenges for healthcare security. While AI-driven systems enhance real-time monitoring, diagnostics, and predictive analytics, they also introduce new security risks, such as algorithmic vulnerabilities and adversarial attacks (Olutimehin et al., 2025). The study notes that research has largely focused on technical aspects of IoT security, often overlooking the human factor, which remains a major point of vulnerability. Moreover, supply chain security is a growing concern, as IoT devices can be compromised during manufacturing, distribution, or software updates (Sobb et al., 2020). Strengthening security throughout the device lifecycle—through better patch management, strict supply chain verification, and AI-driven threat detection—will be essential in ensuring the safe and effective deployment of IoT in healthcare.

Current State of the Research

The current state of research on IoT security and privacy has been significantly shaped by the contributions of various authors and experts, including Aboubakar (2022), Beniwall (2022), and Korte (2021). Their works provide valuable insights into the evolving landscape of IoT security, highlighting key themes, research gaps, and recommendations. These authors emphasize that identity and access management, along with device authentication, are central themes in IoT security research. Ensuring that only authorized devices can access sensitive data is critical to mitigating risks such as unauthorized access and data breaches. Additionally, their research underscores the importance of robust authentication mechanisms to safeguard IoT ecosystems, particularly in healthcare, where data sensitivity is paramount.

Another prominent theme identified in the current research is the use of machine learning and anomaly detection to enhance IoT security. Authors such as Beniwall (2022) and Nizeti (2020) highlight how machine learning algorithms can analyze patterns of behaviour in IoT devices, enabling the detection of unusual or malicious activities. This proactive approach to security is particularly relevant in healthcare, where IoT devices often handle critical patient data. By leveraging machine learning, researchers aim to develop systems that can identify and respond to security threats in real-time, thereby reducing vulnerabilities and improving the overall resilience of IoT networks.

Blockchain technology has also emerged as a significant theme in IoT security research, as noted by Aboubakar (2022) and Korte (2021). Blockchain offers a decentralized and tamper-proof method for recording and verifying transactions, making it a promising solution for enhancing the integrity and trustworthiness of IoT data. In healthcare, blockchain can be used to secure patient records, ensure data provenance, and facilitate secure data sharing among stakeholders. The adoption of blockchain in IoT systems is seen as a way to address challenges related to data tampering, unauthorized access, and lack of transparency, which are critical concerns in the healthcare sector.

Privacy-preserving techniques, such as differential privacy, have gained traction in IoT research, as highlighted by the works of Nizeti (2020) and Korte (2021). These techniques aim to protect sensitive data by introducing noise or obfuscation, ensuring that individual data points cannot be easily identified. In the context of healthcare IoT, where patient data is highly sensitive, differential privacy offers a way to balance data utility with privacy protection. Researchers are exploring how these techniques can be integrated into IoT systems to safeguard patient information while still enabling valuable data analysis. Overall, the current state of research reflects a growing emphasis on innovative solutions to address the complex security and privacy challenges posed by IoT in healthcare.

RECOMMENDATIONS FOR IMPROVING SECURITY AND PRIVACY

Strengthening Regulatory Frameworks

To address security and privacy concerns in healthcare IoT, regulatory frameworks must be reinforced. The enforcement of Zambia’s Data Protection Act (2021) should be expanded to include healthcare-specific guidelines that address IoT-related vulnerabilities. Additionally, introducing national cybersecurity standards for medical IoT devices would ensure that all devices meet minimum security requirements before deployment. Policymakers should align these standards with international best practices, such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA), to enhance patient data protection and compliance.

Improving IoT Security Measures

Implementing robust security measures is crucial in mitigating cyber threats to IoT healthcare systems. End-to-end encryption and multi-factor authentication (MFA) should be mandatory for all IoT healthcare devices to prevent unauthorized access and data breaches. Furthermore, establishing mandatory software update protocols will ensure that devices receive timely security patches, addressing vulnerabilities before they can be exploited. Healthcare institutions should collaborate with IoT manufacturers to enforce these security measures, making them an industry standard rather than an optional feature.

Increasing Awareness and Training

Many security breaches result from human error, making cybersecurity education a vital component of IoT security. Developing comprehensive cybersecurity training programs for healthcare workers will equip them with the skills needed to identify and mitigate threats. Additionally, public awareness campaigns on patient data rights and privacy concerns should be launched to educate individuals about protecting their health information. These initiatives will empower both healthcare providers and patients to take proactive steps in securing IoT healthcare systems.

Encouraging Local Research and Innovation

Investing in research collaborations between Zambian universities, tech startups, and the Ministry of Health can drive the development of indigenous cybersecurity solutions tailored to local healthcare challenges. Encouraging the local manufacturing of IoT devices with built-in security features will also help reduce reliance on foreign supply chains, minimizing the risks associated with compromised hardware. These initiatives will not only strengthen security but also foster economic growth and technological advancement in Zambia's digital health sector.

Leveraging Blockchain and AI for Security

Advanced technologies like blockchain and artificial intelligence (AI) can significantly enhance healthcare IoT security. Blockchain can be used for secure health data management, ensuring that medical records remain tamper-proof and accessible only to authorized users. AI-driven anomaly detection systems can continuously monitor IoT networks for suspicious activities, providing real-time threat identification and mitigation. By integrating these technologies into Zambia's digital health infrastructure, the security and privacy of IoT-based healthcare services can be significantly strengthened.

CONCLUSION

The integration of IoT into Zambia's healthcare system presents a transformative opportunity to improve service delivery, enhance patient outcomes, and optimize resource utilization. However, this technological advancement also brings significant security and privacy challenges that must be addressed to ensure its sustainable adoption. This review has identified critical vulnerabilities, such as weak device authentication, data breaches, and insufficient regulatory frameworks, which pose risks to patient data and overall system integrity. To mitigate these challenges, practical recommendations include strengthening regulatory enforcement, investing in cybersecurity infrastructure, and fostering collaboration between government, private sector, and international partners. By addressing these issues, Zambia can harness the full potential of IoT to revolutionize its healthcare sector while safeguarding sensitive patient information.

Looking ahead, future research should focus on developing context-specific security frameworks tailored to Zambia's unique healthcare landscape. Additionally, improving digital literacy among healthcare professionals and stakeholders will be essential to effectively manage and mitigate cybersecurity risks. Emerging technologies such as blockchain and artificial intelligence (AI) offer promising solutions for enhancing data integrity, automating threat detection, and ensuring secure data sharing. By prioritizing these measures, Zambia can build a resilient and secure IoT-enabled healthcare system that not only addresses current challenges but also sets a foundation for long-term innovation and growth in the sector.

REFERENCES

Aboubakar, M. (2022). A review of IoT network management: Current status and perspectives. *Volume 34, Issue No. 7.*

Bazanye, K. P. (2022). Factors influencing user adherence towards privacy standards in the usage of Internet of Things devices in South Africa.

Beniwall, B. (2022). A systematic literature review on IoT gateways. *Journal of King Saud University - Computer and Information Sciences, 30*(10).

F. Hu, D. Xie, & S. Shen. (2013). On the application of the Internet of Things in the field of medical and healthcare. In *2013 IEEE International Conference on Communications (ICC)*. IEEE.

Halubanza, B. (2024). *A framework for an early warning system for the management of the spread of locust invasion based on artificial intelligence technologies* [Doctoral dissertation, The University of Zambia].

Javaid, M., Haleem, A., Singh, R. P., & Suman, R. (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications*, *1*, 100016.

Joshua, E. S. N., Bhattacharyya, D., & Rao, N. T. (2022). Managing information security risk and Internet of Things (IoT) impact on challenges of medicinal problems with complex settings: A complete systematic approach. In *Multi-chaos, fractal and multi-fractional artificial intelligence of different complex systems* (pp. 291–310). Academic Press.

Karuranathne, S. (2021). Security and privacy in IoT smart healthcare. *IEEE Access*, *25*(4).

Kelly, J. T. (2020). The Internet of Things: Impact and implications for health care delivery. *Journal of Medical Internet Research*, *22*(11).

Ketu, S., & Mishra, P. K. (2021). Internet of Healthcare Things: A contemporary survey. *Journal of Network and Computer Applications*, *192*, 103179.

Korte, A. (2021). Internet of Things (IoT) technology research in business and management literature. *Technology in Society*, *16*(6).

Magyar, G. (2017, November). Blockchain: Solving the privacy and research availability tradeoff for EHR data: A new disruptive technology in health data management. In *2017 IEEE 30th Neumann Colloquium (NC)* (pp. 000135–000140). IEEE.

Mamdouh, M., Awad, A. I., Hamed, H. F. A., & Khalaf, A. A. M. (2020). Outlook on security and privacy in IoHT: Key challenges and future vision. In *Joint European-US Workshop on Applications of Invariance in Computer Vision* (pp. 721–730). Springer.

Mphande, T. (2020). *A secure patient monitoring and tracking system using RFID and Internet of Things for the University Teaching Hospital* [Doctoral dissertation, University of Zambia].

Musonda, I., Onososen, A., & Moyo, T. (2025). *Digital transitioning in the built environment of developing countries*. Taylor & Francis.

Muyunda, L., & Mpundu, M. (2023). Mapping the regulatory framework for telemedicine in Zambia: A content analysis. *International Journal of Membrane Science and Technology*, *10*, 3445–3461.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors*, *21*(15), 5119.

Nzazi, E. (2025). Unraveling the urban landscape: Assessing the influence of informal settlements on spatial planning in Lusaka, Zambia. *Open Access Library Journal*, *12*(2), 1–20.

Obaid, O. I., & Salman, S. A. B. (2022). Security and privacy in IoT-based healthcare systems: A review. *Mesopotamian Journal of Computer Science*, *2022*, 29–39.

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial threats to AI-driven systems: Exploring the attack surface of machine learning models and countermeasures. *SSRN*. https://ssrn.com/abstract=5137026

Owen, A., & Kellr, S. (2025). Transforming telemedicine: Leveraging cloud-enabled IoT devices for enhanced patient engagement.

Sadek, I. (2022). Security and privacy in the Internet of Things healthcare systems: Toward a robust solution in real-life deployment.

Schmidt, A. (2020). Regulatory challenges in healthcare IT: Ensuring compliance with

HIPAA and GDPR. *Academic Journal of Science and Technology, 3*(1), 1–7.

Shahid, J. (2022). *Data protection and privacy of the Internet of Healthcare Things (IoHTs)*. National University of Sciences and Technology.

Sharma, S., & Verma, V. K. (2022). An integrated exploration on Internet of Things and wireless sensor networks. *Wireless Personal Communications, 124*(3), 2735–2770.

Sicari, S., Rizzardi, A., Grieco, L. A., Piro, G., & Coen-Porisini, A. (2017). A policy enforcement framework for Internet of Things applications in the smart health. *Smart Health, 3,* 39–74.

Sivan, R. (2021). *Security and privacy in cloud-based e-health system* [Doctoral dissertation, University of Putra Malaysia].

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics, 9*(11), 1864.

Somasundaram, R., & Thirugnanam, M. (2021). Review of security challenges in healthcare Internet of Things. *Wireless Networks, 27*(8), 5503–5509.

Teh, D., & Rana, T. (2023). The use of Internet of Things, Big Data analytics and artificial intelligence for attaining UN's SDGs. In *Handbook of big data and analytics in accounting and auditing* (pp. 235–253). Springer Nature Singapore.

Van Hoang, T. (2024). Impact of integrated artificial intelligence and Internet of Things technologies on smart city transformation. *Journal of Technical Education Science, 19*(Special Issue 01), 64–73.

Vujovic, V. (2015). A connection between Internet of Things and Resource-Oriented Architecture. In *2015 European Conference on Smart Objects, Systems and Technologies (Smart SysTech)*. IEEE.

Wu, W., Yang, P., Zhang, W., Zhou, C., & Shen, X. (2020). Accuracy-guaranteed collaborative DNN inference in industrial IoT via deep reinforcement learning. *IEEE Transactions on Industrial Informatics, 17*(7), 4988–4998.