Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI:
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

The Role of HRM in Managing Employee Privacy and Data Security in IoT-Enabled Healthcare Organisations

Muzammil Ahamed Mohammed, *MBA, University of Findlay, Findlay, Ohio, USA*
https://orcid.org/0009-0008-2129-6433
Farnaz Sharmin, *MAE/HRD, University of Findlay, Findlay, Ohio, USA*
https://orcid.org/0009-0009-5696-1365
Taslima Akter, *MBA, University of Findlay, Findlay, Ohio, USA*
https://orcid.org/0000-0003-1511-8549
Rezwanul Islam Rezvi, *MBA, Devry University, Columbus, Ohio, USA*
https://orcid.org/0009-0008-4104-4006
Mir Protik, *MBA, Devry University, Columbus, Ohio, USA*
https://orcid.org/0009-0006-3173-3874
Nayeema Nusrat, *MBA (AIS), Jagannath University, Dhaka, Bangladesh*
https://orcid.org/0009-0000-8277-2140
Shoaib Ahmed, MBA *(Finance), University of Education, Lahore, Pakistan*
Corresponding Author: Muzammil Ahamed Mohammed, **E-mail**: Muzz99126@gmail.com

| ABSTRACT

The current study explores the role of human resource management in facilitating privacy protection and data security of employees of IoT-enabled healthcare organisations, whereby constant monitoring and data production has become part of routine work processes. A qualitative research design was chosen and thematic analysis of secondary literature based on peer-reviewed journals, policy documents, and sources of reliable information on the industry. The method will allow synthesizing evidence on the governance, ethics, and workforce implications of IoT adoption in healthcare in a systematic manner. The analysis shows that there are four fundamental themes, which include: HR governance and data ethics, consent and transparency, surveillance and performance control and regulatory compliance. Results indicate that IoT has led to increased efficiency and control, but it also causes ethical threats, lack of trust, and increased vulnerability to data breaches when not regulated effectively. Implications: The research indicates that HRM is a key governance player that has to convert technical protections into ethical policies, consent, training, and compliance procedures that continue to keep employees trusting and the organisation legitimate. Future studies are needed to examine the perceptions of the IoT monitoring among employees, their longitudinal effects on trust and wellbeing, as well as the efficacy of integrated HR-IT models of governance within a variety of healthcare settings.

| KEYWORDS

Human Resource Management, Employee Privacy, Data Security, Internet of Things (IoT), Healthcare Organisations, Workplace Surveillance, Ethical Governance

| ARTICLE INFORMATION

ACCEPTED: 12 January 2026 **PUBLISHED:** 24 February 2026 **DOI:** 10.32996/jcsts.2026.8.4.9

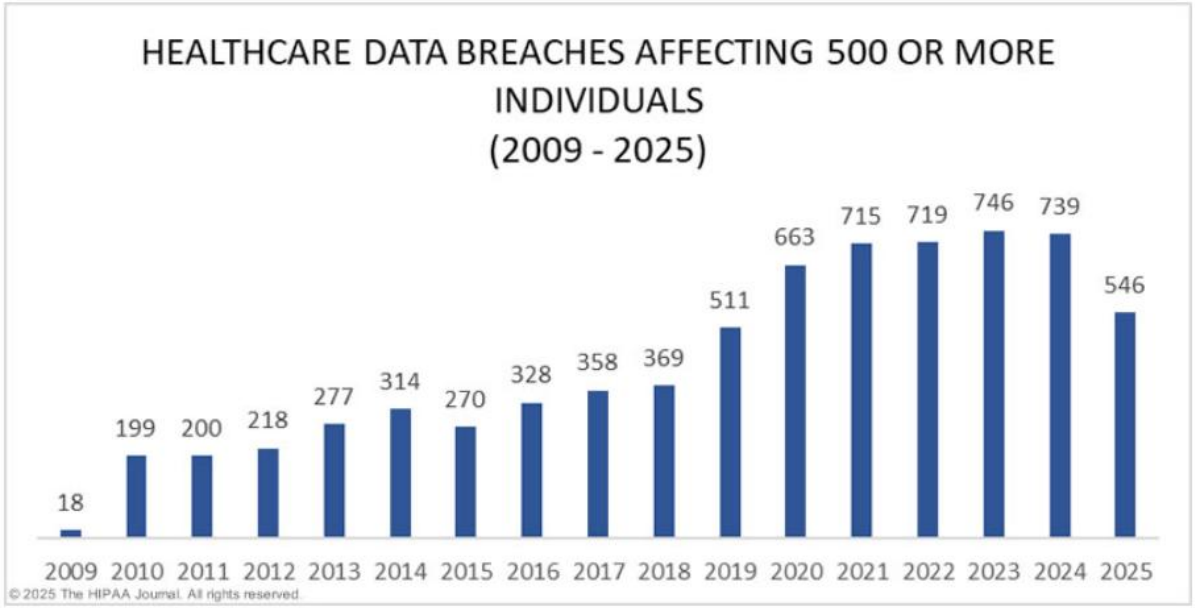
1. Introduction

Advanced digital innovation and growing cyber threat are combining to influence the role and work of healthcare organisations. In the last ten years, there has been an astronomical increase in high-scale healthcare data breaches, which have included over 700 data breach reports in 2023 alone and exposed between 133 million patient records, highlighting the extent and continuation of data protection lapses in the industry (Alder, 2025). Simultaneously, the active growth of Internet of Things technologies has changed the healthcare provision, and the global IoT healthcare market is estimated by approximately USD 140 billion in 2023 and is expected to grow at a rate of more than 20 percent in the coming years, which increases the organisational reliance on connected systems and data flows (Fortune Business Insights, 2025). Although digitalisation has increased efficiency and accessibility, it has also increased vulnerabilities, such as ransomware attacks, unauthorised access, and abuse of sensitive health information, which puts healthcare organisations and workforce through complex governance challenges (Jawad, 2024).

2. Problem Statement

The issue as to the IoT-enabled healthcare organisations is an ongoing and growing challenge. Figure 1 is a clear representation of a long-term trend of increasing large-scale healthcare data breaches of more than 500 individuals with a low of just under 20 breaches in 2009 to a high of around 750 breaches in 2023, then somewhat declines in 2024 and 2025 (Alder, 2025). This tendency is an indication of structural infirmities and not a transient disturbance. In 2023, hacking resulted in approximately 80 percent of breaches, which emphasizes the overall vulnerability to external cyber-attacks and not clarified internal mistakes (Alder, 2025). The effects are grave, and about 720 breaches occurred in 2024 and the average financial cost per breach was almost USD 10 million, which exerted a long-term burden on the healthcare operations and trust (Arundhati, 2025). The risks are compounded by the presence of non-standardised and disjointed IoT security protocols between interconnected healthcare systems which continue to expose sensitive data to threats (Zarkia & Usman, 2025).

Figure 1: Healthcare Data Breaches Affecting 500 or More Individuals (2009–2025)



(Alder, 2025)

3. Purpose and Objectives of the Study

This study is aimed at discussing the role that human resource management plays in ensuring the privacy of employees and enhancing data security in practices in the IoT-based healthcare organisations, where data collection and digital monitoring have become the new norm of daily activities. The study objectives are:

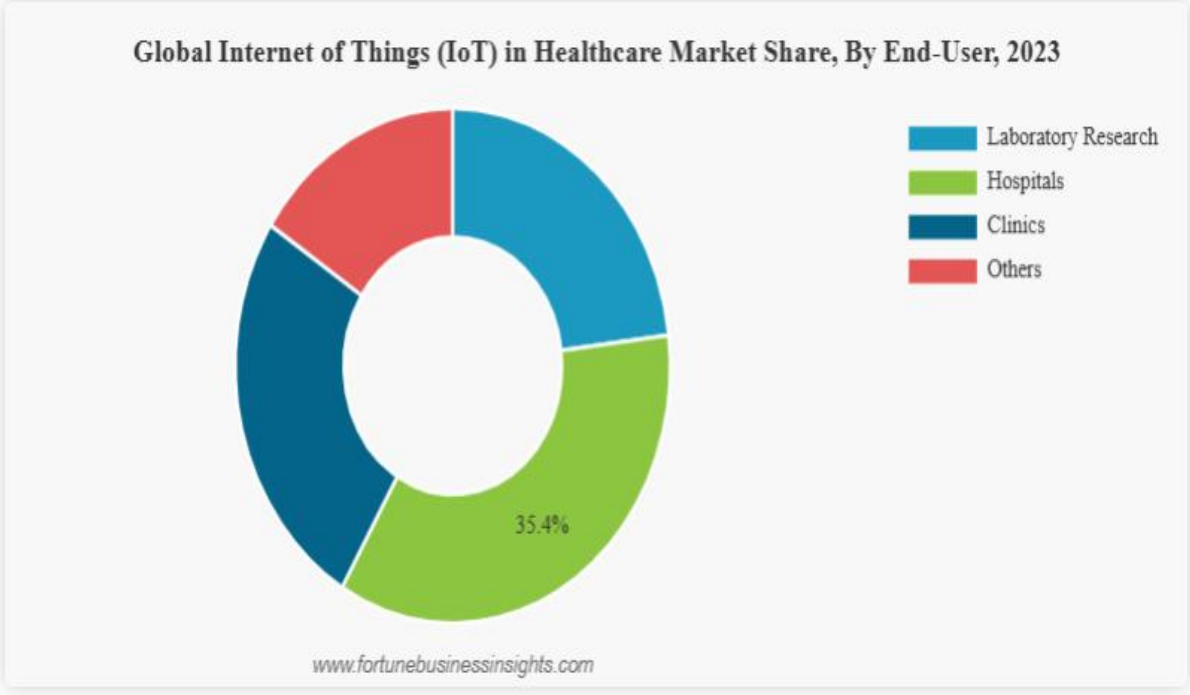
- To examine how HRM controls employee data and privacy in internet of things healthcare settings.
- To determine the major privacy and data security risks associated with employee monitoring technologies and related systems.
- To examine the effect of HR policies and practices on employee consent, transparency, and trust.
- To explore the role of HRM in the process of assisting regulatory compliance and organisational accountability in data protection.

4. Literature Review

The implementation of Internet of Things technologies in healthcare facilities has been growing at a very fast rate because organisations are seeking efficiency, automation, and constant data accessibility. The evidence presented on the market indicates that the core of this shift is connected medical devices and remote patient care, by integrating constant data creation into the daily healthcare practice (Fortune Business Insights, 2025). The shift is seen in Figure 2 with hospitals making more than a third of all healthcare IoT adoption in the world, noting how huge clinical settings were now dense networks of interconnected technologies. Nevertheless, these systems not only increase monitoring and decision support, but also increase the scale of governance and workforce oversight (Rehman et al., 2025).

Monitoring technologies among employees make this landscape even harder. Smartwatches and other wearables are increasingly applied to track, prompt and forecast behaviour in addition to clinical requirements into performance and wellbeing (Kohler et al., 2024). However, sensitive physiological and location information is revealed by these technologies, posing unique privacy and security threats in case of physical security deficiencies (Zhang et al., 2025). These are exacerbated by structural weaknesses in IoT ecosystems, where devices with limited resources and dynamic attack vectors endanger the entire healthcare infrastructures (Rasool et al., 2022).

Figure 2: Global Internet of Things (IoT) in Healthcare Market Share by End-User, 2023



(Fortune Business Insights, 2025)

In this context, HRM has a key role to play in governance. HR digital solutions provide real-time monitoring and analytics, but also introduce ethical and transparency issues that, when mismanaged, can lead to a lack of trust (Rezvi et al., 2025). Even though IoT-powered HR analytics can enhance efficacy, they need to be legitimate with transparent privacy guidelines and accountability approaches that comply with the regulatory framework (Podder et al., 2024).

5. Methodology

The research design chosen in this study is a qualitative one as it aims to investigate complicated phenomena of employee privacy and data security in the context of IoT-enabled healthcare facilities where there is no way to consider human experiences and organisational practices in terms of numerical values. The qualitative inquiry would be especially applicable to the study of attitudes, beliefs, and governance practices because it enables flexible and continuous interaction with current evidence and changing themes (Ali et al., 2024). The study utilizes a thematic analysis of the secondary literature based on peer-reviewed journals, academic books, and conference proceedings, published within the period of years 2016 to 2025, which allows identifying general patterns and understandings of studies. Inclusion and exclusion criteria were carefully chosen so as to be relevant, methodologically rigorous and in accordance to healthcare and digital governance settings. The interpretation is based on a set of accepted qualitative validation principles, such as transparency, reflexivity, and interpretive depth to enhance the credibility and coherence of the results synthesis (Im et al., 2023).

6. Results / Findings

Thematic Analysis

Theme	Source 1	Source 2	Source 3
Theme 1: HR governance and data ethics	Rezvi et al. (2025): "ethical problems, such as algorithmic bias and transparency."	Podder et al. (2024): "HR Analytics interconnect with applications of IoT that facilitates for better resource utilization and monitoring system."	Jawad (2024): "the importance of implementing robust security measures, ensuring patient privacy and fostering trust in digital healthcare systems."
Theme 2: Consent, transparency, and employee trust	Popoola et al. (2023): "a consent-based privacy model for decision-making in the information disclosure process."	Tazi et al. (2024): "patients and the general public express concerns about privacy and security with technologies like electronic health records (EHRs)."	Shammar et al. (2025): "the adoption of IoMT has raised significant privacy and security concerns."
Theme 3: Surveillance, performance management, and control	Köhler et al. (2024): "monitoring, nudging, and predicting… using aggregated user data to train machine learning algorithms."	Rasool et al. (2022): "the resource-constrained nature of these devices makes them vulnerable to immense security and privacy issues."	Rehman et al. (2025): "integrating technologies such as cloud computing, augmented reality and wearable devices."
Theme 4: Regulatory compliance and organisational responsibility	Marron (2024): "all HIPAA-covered entities and business associates must comply with the requirements of the Security Rule."	Arundhati (2025): "healthcare IT security compliance refers to the adherence to industry-specific regulations and frameworks designed to protect sensitive patient information."	Zarkia & Usman (2025): "IoT-enabled healthcare systems face persistent challenges, including a lack of standardized security protocols."

Theme 1: HR governance and data ethics

The results point out that HR governance has been an ethical anchor in the middle of the IoT-enabled healthcare organisations, especially as digital HR systems have an increasing influence on the monitoring and decision-making practices (Abood et al., 2025). The study by Rezvi et al. (2025) demonstrates that AI-based systems adopted in HR functions have a propensity to introduce bias and decrease transparency, throwing ethical responsibility off the shoulders of individual managers onto non-transparent technological procedures. This poses a governance issue to the HR, which has to make sure that the data-driven tools do not rely on efficiency object alone but instead on ethical considerations. The study by Podder et al. (2024) also shows that HR analytics made possible with the help of the IoT can enhance monitoring and resource utilisation, but the authors also emphasise that it requires the presence of clear privacy policies, and ethical governance cannot be spontaneous but should be developed. In the absence of such oversight, HR is prone to normalization of intrusive behaviours that hinder the autonomy of the employees. These conclusions make HR not only an administrative role but also a moral watchdog that must determine how far data should be used and make sure that technological competence does not eat ethical responsibility (Jawad, 2024; Alharbi et al., 2024).

Theme 2: Consent, transparency, and employee trust

Consent and transparency turns out to be the crucial determinants that define how employees trust digitally monitored healthcare settings. The article by Popoola et al. (2023) suggests consent-based blockchain models, allowing to control who has access to data and under what conditions, which allows embedding trust in a structure instead of keeping an informal promise. Nevertheless, lack of trust still exists where there is poor transparency. According to Tazi et al. (2024), patients and the general population are always worried about the sensitivity of accessing and reusing health-related data, which is indicative of widespread concerns that can be projected to the employee population. Shammar et al. (2025) support this with an issue of breaching privacy as a threat to trust directly, in terms of IoMT systems. Collectively, these studies indicate that trust does not merely exist in relation but is procedural: employees tend to be more accepting of monitoring when consent is made clear, access rules are visible, and the flows of data are comprehensible. HR thus becomes very important in transforming the technical consent mechanisms into trust practices which make sense and are human friendly.

Theme 3: Surveillance, performance management, and control

The IoT-enabled surveillance also transforms the performance management remarkably, and this is because surveillance will be offered at any time and not at a specific time. According to Kohler et al. (2024), wearable technologies can be divided into

monitoring, nudging, and predicting, which shows an expansion of performance data towards non-work activities in behavioural and physiological fields. The proportionality and control is a concern, given the fact that surveillance is integrated into the daily activities. Rasool et al. (2022) point out that the very devices that allow monitoring are frequently resource-limited and prone, which implies that surveillance resources can expose organisations and employees to increased security threats. Rehman et al. (2025) also demonstrate the profound implementation of wearables, cloud platforms, and analytics in healthcare infrastructures, so the surveillance can hardly be separated from the core operations. The findings imply that the HR should be proactive in setting limits to the extent of acceptable monitoring to ensure that performance management is facilitative, and it is not used as a mechanism of coercion.

Theme 4: Regulatory compliance and organisational responsibility

Data protection sets the minimum level of organisational responsibility on regulatory compliance. Marron (2024) well defines the fact that all the HIPAA-covered entities are obligated to adhere to the security requirements that are mandatory, leaving not much room to customize the protection of sensitive data. Nonetheless, compliance does not mean that protection is effective. Jawad (2024) insists that the necessary controls are encryption, multi-factor authentication and training of staff, which means that the burden of technical compliance should be shifted to the organisational culture and employee competence. The absence of standardised IoT security protocols is also listed as a chronic vulnerability by Zarkia and Usman (2025), which puts organisational vulnerability to breaches at greater risk. These results confirm the notion that compliance should be maintained by the HR not just in terms of policy implementation but also in terms of ongoing training, responsibility, and liaison with the IT departments, so that the regulatory requirements can be converted into daily practice.

7. How HRM Can Implement Effective Privacy and Data Security Practices

Human resource management can be instrumental in ensuring that effective privacy and data protection measures are entrenched in the IoT-enabled healthcare organisations by converting technical solutions into organisational everyday conduct. Design and enforcement of policies needed to be clear, especially where the HR analytics and integrated systems are incorporated in monitoring performance and optimising resources. Podder et al. (2024) note that cooperation and communication between HR functions is very important, as well as the development of clear privacy guidelines that establish acceptable limits of data use and access. In addition to policy, the employees consent arrangements should not be formal, but substantive, so that employees realize how their information is gathered and also the reason.

Arundhati (2025) favours the implementation of single compliance models to enhance accountability and minimize the risk management as a fragmented approach in healthcare organisations. These controls are further reinforced through training and awareness and organised risk models like STRIDE and DREAD that enable employees to identify threats and mitigation obligations, therefore, aligning the daily practice with organisational data protection objectives (Zhai et al., 2025).

8. Conclusion

As has been demonstrated in this research paper, the introduction of the IoT-based systems into the healthcare environment has essentially transformed the manner in which the data on the employees are created, tracked, and secured. Although networked technologies enable efficiency, real time monitoring and informed decision making, they equally heighten the privacy threats and ethical conflict among the workforce. The results indicate that human resource management plays a decisive role of balancing technological capability with employee trust, ethical governance and regulatory responsibility. Clear consent practices, efficient HR-led policies, and ongoing training are the key measures of protecting sensitive data. Finally, by integrating privacy and data protection into daily HR activities, healthcare organisations can optimize the benefits of the IoT and retain their legitimacy and trust as well as organisational stability.

9. Statements and Declarations

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

References

Abood, E. W., Yassin, A. A., Abduljabbar, Z. A., Nyangaresi, V. O., Abduljaleel, I. Q., Aldarwish, A. J. Y., & Neamah, H. A. (2025). Security challenges and analysis tools in Internet of Health Things: A comprehensive review. *Computers, Materials & Continua, 85*(2), 2305–2345. https://doi.org/10.32604/cmc.2025.066579

Alder, S. (2025). *Healthcare data breach statistics*. The HIPAA Journal. https://www.hipaajournal.com/healthcare-data-breach-statistics/

Alharbi, S. H., Alzahrani, A. M., Syed, T. A., & Alqahtany, S. S. (2024). Integrity and privacy assurance framework for remote healthcare monitoring based on IoT. *Computers, 13*(7), 164. https://doi.org/10.3390/computers13070164

Ali, M. D., Hatef, E. A. J. A., & Alamri, H. S. H. (2024). A concise review of qualitative research methods in healthcare research. *Journal of Young Pharmacists, 16*(3), 374–384. https://doi.org/10.5530/jyp.2024.16.49

Arundhati, G. (2025). *10 key healthcare IT security compliance standards and frameworks*. Scrut Automation. https://www.scrut.io/post/healthcare-cybersecurity-frameworks

Fortune Business Insights. (2025). *Internet of Things (IoT) in healthcare market size, share & industry analysis, by component, application, end-user, and regional forecast, 2024–2032*. https://www.fortunebusinessinsights.com/internet-of-things-iot-in-healthcare-market-102188

Im, D., Pyo, J., Lee, H., Jung, H., & Ock, M. (2023). Qualitative research in healthcare: Data analysis. *Journal of Preventive Medicine and Public Health, 56*(2), 100–110. https://doi.org/10.3961/jpmph.22.471

Jawad, L. A. (2024). Security and privacy in digital healthcare systems: Challenges and mitigation strategies. *Abhigyan*. https://doi.org/10.1177/09702385241233073

Köhler, C., Bartschke, A., Fürstenau, D., Schaaf, T., & Salgado-Baez, E. (2024). The value of smartwatches in the health care sector for monitoring, nudging, and predicting: Viewpoint on 25 years of research. *Journal of Medical Internet Research, 26*, e58936. https://doi.org/10.2196/58936

Marron, J. (2024). *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A cybersecurity resource guide* (NIST Special Publication 800-66r2). National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-66r2.pdf

Podder, S. K., Samanta, D., & Etemi, B. P. (2024). Impact of Internet of Things (IoT) applications on HR analytics and sustainable business practices in smart city. *Measurement Sensors, 35*, 101296. https://doi.org/10.1016/j.measen.2024.101296

Popoola, O., Rodrigues, M., Marchang, J., Shenfield, A., Ikpehai, A., & Popoola, J. (2023). A critical literature review of security and privacy in smart home healthcare schemes adopting IoT & blockchain: Problems, challenges and solutions. *Blockchain Research and Applications, 5*(2), 100178. https://doi.org/10.1016/j.bcra.2023.100178

Rasool, R. U., Ahmad, H. F., Rafique, W., Qayyum, A., & Qadir, J. (2022). Security and privacy of Internet of Medical Things: A contemporary review in the age of surveillance, botnets, and adversarial ML. *Journal of Network and Computer Applications, 201*, 103332. https://doi.org/10.1016/j.jnca.2022.103332

Rehman, A. U., Lu, S., Heyat, M. B. B., Iqbal, M. S., Parveen, S., Hayat, M. B., Akhtar, F., Ashraf, M. A., Khan, O., Pomary, D., & Sawan, M. (2025). Internet of Things in healthcare research: Trends, innovations, security considerations, challenges and future strategy. *International Journal of Intelligent Systems, 2025*(1). https://doi.org/10.1155/int/8546245

Rezvi, R. I., Rahman, K. O., Nasrullah, F., Islam, M. S., Hasan, M., Nusrat, N., Jishan, S. S., & Ahmed, S. (2025). The integration of artificial intelligence in human resource management in the U.S. retail sector. *Journal of Business and Management Studies, 7*(1), 273–278. https://doi.org/10.32996/jbms.2025.7.1.22

Shammar, E., Cui, X., Zahary, A., Alsamhi, S. H., & Al-Qaness, M. A. (2025). Threat to trust: A systematic review on Internet of Medical Things security. *Journal of Parallel and Distributed Computing, 206*, 105172. https://doi.org/10.1016/j.jpdc.2025.105172

Tazi, F., Nandakumar, A., Dykstra, J., Rajivan, P., & Das, S. (2024). SoK: Analyzing privacy and security of healthcare data from the user perspective. *ACM Transactions on Computing for Healthcare, 5*(2), 1–31. https://doi.org/10.1145/3650116

Zarkia, M. N. H., & Usman, S. (2025). IoT data breaches and privacy issues in healthcare system. *Open International Journal of Informatics, 13*(1), 41–55. https://doi.org/10.11113/oiji2025.13n1.327

Zhai, B., Akande, O. N., Agarwal, S., & Pak, W. (2025). Security risk assessment of Internet of Things health devices using DREAD and STRIDE models. *Ain Shams Engineering Journal, 16*(11), 103721. https://doi.org/10.1016/j.asej.2025.103721

Zhang, B., Chen, C., Lee, I., Lee, K., & Ong, K. (2025). A survey on security and privacy issues in wearable health monitoring devices. *Computers & Security, 155*, 104453. https://doi.org/10.1016/j.cose.2025.104453