Information Technology Studies Journal (ITECH)
Vol 1 (2) 2024 : 89-101

Advancement in IoT-enabled Healthcare System: a Systematic Review of Technologies and Securities Issues

Kemajuan dalam Sistem Layanan Kesehatan yang mendukung IoT: Tinjauan Sistematis terhadap Masalah Teknologi dan Isu Keamanan

Amelia Putri[1], Rian Ardianto[2]
Universitas Islam Indonesia, Universitas Harapan Bangsa
*rianardianto@uhb.ac.id

**Corresponding Author*

ABSTRACT
IoT (Internet of Things)-based health systems offer the potential for digital transformation in healthcare, but face significant security challenges that require serious attention. This research aims to identify and analyze security challenges in IoT-based health systems and evaluate existing solutions to overcome these challenges. The research method used is a systematic review using the PRISMA approach, collecting articles from reputable databases such as Scopus, IEEE Xplore, and PubMed. The research results show that although IoT technology can improve real-time patient monitoring and operational efficiency, vulnerability to cyberattacks and data privacy concerns remain major obstacles. The implications of these findings indicate the need for the development of stronger security solutions and comprehensive protection strategies to ensure successful implementation of IoT in health systems.
Keywords: IoT in Health, Health System Security, IoT Security Challenges, IoT Security Solutions, Systematic Review.

ABSTRAK
Sistem kesehatan berbasis IoT (Internet of Things) menawarkan potensi transformasi digital dalam perawatan kesehatan, tetapi menghadapi tantangan keamanan signifikan yang memerlukan perhatian serius. Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis tantangan keamanan dalam sistem kesehatan berbasis IoT serta mengevaluasi solusi yang ada untuk mengatasi tantangan tersebut. Metode penelitian yang digunakan adalah tinjauan sistematis dengan pendekatan PRISMA, mengumpulkan artikel dari database bereputasi seperti Scopus, IEEE Xplore, dan PubMed. Hasil penelitian menunjukkan bahwa meskipun teknologi IoT dapat meningkatkan pemantauan pasien secara real-time dan efisiensi operasional, kerentanan terhadap serangan siber dan masalah privasi data tetap menjadi kendala utama. Implikasi dari temuan ini menunjukkan perlunya pengembangan solusi keamanan yang lebih kuat dan strategi perlindungan yang komprehensif untuk memastikan keberhasilan penerapan IoT dalam sistem kesehatan.
Kata Kunci: IoT dalam Kesehatan, Keamanan Sistem Kesehatan, Tantangan Keamanan IoT, Solusi Keamanan IoT, Tinjauan Sistematis.

1. Introduction

IoT (Internet of Things)-based health systems refer to the application of IoT technology in the health sector to improve the quality of care, operational efficiency and patient health outcomes. This system involves devices connected over a network to monitor patient conditions in real-time, collect health data, and provide timely medical intervention. In the modern context, IoT adoption in healthcare offers great potential for digital transformation, including improved chronic disease management, remote monitoring, and personalization of care. However, along with these significant benefits, the importance of security in IoT-based healthcare systems cannot be ignored. Security is a top priority because sensitive health data and patient personal information can be a prime target for data breaches and cyberattacks.

In its implementation, IoT-based health systems face various complex security challenges. Hardware and software vulnerabilities, risks to patient data privacy, and threats to the integrity of data communications are major issues that require serious attention. For example, ransomware attacks targeting medical devices or health information systems have resulted in significant operational disruption, financial loss, and potential harm to patients. Such attacks can result in damage to medical devices, loss of access to vital data, and even potentially fatal medical errors. The impact of this security problem not only threatens patient safety but can also damage public trust in IoT-based health systems.

To deeply understand the security challenges faced by IoT-based health systems as well as the available solutions, this research focuses on the main question: "What are the most significant security challenges faced by IoT-based health systems today, and how do existing solutions address them?" these challenges?" This research aims to identify and analyze the various security challenges faced by these systems and evaluate the effectiveness of the solutions implemented to overcome these problems. Thus, it is hoped that this research will provide deeper insight into pressing security needs and inform the development of better security strategies for IoT-based health systems.

Although there has been a lot of research discussing security in IoT-based health systems, there are several shortcomings that still need to be addressed. Much of the existing literature tends to focus on specific technical aspects such as data encryption and device authentication, while analysis of holistic integration of security solutions is often inadequate. Significant gaps also exist in assessing the effectiveness of existing solutions in various real application contexts, as well as in understanding how new threats, such as AI-based attacks, affect IoT-based health systems. Additionally, studies investigating the long-term impact of security breaches on health outcomes and patient trust are limited.

Research on security challenges in IoT-based health systems is critical as these systems are increasingly adopted in modern health management. With increasing reliance on IoT technology, risks to patients' personal data and health are also increasing. Data security and patient privacy are critical aspects that must be protected to ensure the reliability and success of IoT-based health systems. This research is urgent because it helps identify vulnerabilities that may not have been detected and provides a basis for the development of more effective security strategies, thereby protecting health systems from evolving threats.

This research offers novelty by integrating an in-depth analysis of the security challenges faced in IoT-based health systems with currently implemented solutions. The new focus of this research includes mapping security challenges that have not yet been fully explored, such as the impact of AI-based attacks and issues related to device interoperability. Additionally, this research will present a comprehensive overview of the effectiveness of existing security solutions, as well as identify gaps in the approaches that have been used. These new aspects will provide a more comprehensive and current understanding of the security of IoT-based health systems.

The results of this literature review are expected to provide a significant contribution to the field of IoT-based health system security. By identifying key challenges and evaluating existing solutions, this research will provide useful insights for researchers, technology developers, and policy makers. These contributions include the development of practical recommendations to improve system security, as well as contributions to the establishment of policies that better protect health data and patient privacy. The impact of this research will strengthen the foundation of security in IoT-based health systems and encourage innovation in more effective protection strategies.

2. Methods

2.1. Collection of Articles

The article collection strategy for this literature review was carried out by accessing reputable international databases including Scopus, IEEE Xplore, and PubMed. This database was selected due to the coverage and quality of the journals listed, which ensures the relevance and credibility of the articles retrieved. The article collection process follows PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines to ensure transparency and consistency in literature selection. The PRISMA method involves identifying articles from specific databases, initial screening based on abstract and title, and then full evaluation of appropriate articles to ensure that only studies that meet the inclusion criteria are included in the literature review.

2.2. Search Keywords

A literature search was conducted using a combination of keywords and search phrases designed to capture relevant articles related to security in IoT-based health systems. Keywords used include: “IoT-enabled healthcare security”, “challenges in IoT healthcare systems”, “IoT healthcare security solutions”, and similar phrases related to security issues and solutions in this context. The use of these keywords aims to filter relevant and recent articles regarding security challenges and protection strategies implemented in IoT-based health systems.

2.3. Number of Articles Obtained

During the collection process, an initial total of 102 articles from various databases was found. After an initial screening stage, which included checking the title and abstract, the number of articles that met the topic and relevance criteria was reduced to 70 articles. This process ensures that the selected articles directly address security challenges and solutions in IoT-based health systems and are relevant to the focus of this research.

2.4. Inclusion and Exclusion Techniques

2.4.1. Inclusion Criteria

Articles included in this literature review must meet several inclusion criteria, namely:

1. Topic Relevance: Articles should directly address security challenges and solutions in IoT-based health systems.
2. Publication in Reputable Journals: Only articles published in reputable and peer-reviewed international journals are considered for inclusion.
3. Research Quality: Articles must be the result of research whose methodology can be justified and make a significant contribution to the understanding of security challenges in the context in question.

2.4.2. Exclusion Criteria

Articles were excluded from this review based on the following exclusion criteria:

1. Irrelevance: Articles that do not specifically address security challenges or solutions in IoT-based health systems, or that only touch the topic in passing without in-depth analysis.
2. Non-Peer-Reviewed Publication: Publications that have not gone through a peer review process, including technical reports and articles from unverified sources.
3. Methodological Quality: Articles that do not meet the methodological standards required for a comprehensive analysis or have deficiencies in research methodology.

3. Results and Discussions

3.1. Basic Concepts and Technology in IoT-Based Health Systems

3.1.1. Description of IoT-Based Health System

IoT-based health systems involve complex architectures, which integrate technologies such as radio-frequency identification (RFID), real-time localization systems (RTLS), and blockchain to monitor patient health, ensure secure data transmission, and enable remote health monitoring (Alqahtani, 2021; Oikonomou et al., 2021). The integration of IoT in the healthcare sector not only enables real-time tracking of patient health but also increases the accessibility of preventive healthcare services, transforming the healthcare system into a proactive, sustainable and coordinated network (Kelly et al., 2020). IoT devices such as physiological sensors facilitate remote monitoring of vital signs, supporting early detection of health problems and timely intervention by healthcare providers (Deursen et al., 2019).

In this context, IoT-based health systems ensure secure and scalable transmission of health data through optimized routing protocols and cryptographic algorithms, which maintain the confidentiality and integrity of sensitive medical information (Refaee et al., 2022). Innovative solutions such as the IoT-based Tetra Health Surveillance System (THSS) support monitoring of individuals with underlying health conditions or those living alone, thereby improving healthcare delivery and patient outcomes (Roy et al., 2021). Additionally, IoT devices integrated with Electronic Medical Records (EHR) enable the prediction of diseases such as heart conditions, which contributes to improved patient care and treatment outcomes (Bebortta, 2023).

The potential of IoT in healthcare is not only limited to health monitoring and data security but also includes efficient health data management. By combining IoT with cloud computing, health systems can achieve intelligent goals and applications that create safer, patient-centered care environments (Butpheng et al., 2020). Additionally, leveraging IoT embedded systems along with identity access management improves health data security, enabling healthcare organizations to protect sensitive information and deliver more efficient care services (Mwangi, 2024). IoT technologies combined with Semantic Web Technologies (SWT) have the potential to revolutionize the global health system, highlighting the transformative impact of next-generation technologies in the health sector (Edeh et al., 2022).

In conclusion, IoT-based health systems represent a significant advancement in healthcare delivery, offering a wide range of applications and benefits that improve patient care, enable remote monitoring, ensure data security, and drive innovation in disease prediction and management. By leveraging IoT technology, healthcare providers can enter a new era of proactive, personalized, and efficient care, ultimately improving patient outcomes and quality of life.

3.1.2. Key Technologies in Healthcare IoT

Foundational technologies in healthcare IoT include sensors and wearable devices, communications and networking systems, and analytics and cloud computing platforms. These technologies play a crucial role in transforming the health sector by enabling real-time health monitoring, remote patient care delivery, smart health sensors, preventive systems, and remote monitoring (Taryudi et al., 2022). IoT-based health monitoring systems generally involve IoT medical equipment, information and communication technology, Internet services, and medical data management and processing (Javid & Mirzaei, 2021). Additionally, the integration of IoT devices such as wearable health trackers equipped with various sensors facilitates remote patient monitoring and data transmission via telemedicine platforms, emphasizing a proactive and data-driven approach to patient care (Auwal, 2023).

Furthermore, the incorporation of Internet of Things (IoT) and blockchain technologies in the healthcare sector offers enhanced security features for traditional practices, data management, data sharing, remote patient monitoring, and drug analysis (Kamangar et al., 2023). IoT-driven intelligent health systems have the potential to significantly improve medical diagnostics and treatment, leading to improved patient outcomes and reduced healthcare costs (Manwal, 2019). Furthermore, IoT-based health applications are developing towards personalized health management systems by utilizing smart wearable sensors, IoT technology, and AI-based technology (Junaid et al., 2022).

In the realm of IoT-based health systems, the utilization of IoT devices with built-in sensors connected via the Internet, known as the Intelligent Internet of Health Things, opens up new opportunities for health service delivery (Kashyap et al., 2022). IoT applications in health extend to the development of fault-tolerant mHealth frameworks utilizing real-time wearable health data sensors, which significantly contribute to human health and well-being (Albahri et al., 2019). Overall, IoT technology in healthcare continues to evolve toward more efficient, data-driven, and patient-centric care delivery models, revolutionizing the traditional healthcare landscape.

3.2. Security Challenges in IoT-Based Health Systems

3.2.1. Identify Key Security Challenges

Security challenges in IoT-based healthcare systems include various aspects that need to be addressed to ensure the integrity and confidentiality of sensitive data. Device vulnerabilities, including hardware and software weaknesses, pose significant risks (Aruna, 2019). Threats to data privacy and integrity, such as data theft and cyberattacks, are critical concerns that must be addressed (Renjith et al., 2022). Risks to networks and communications, such as man-in-the-middle and denial-of-service attacks, highlight the importance of protecting data transmission (Oikonomou et al., 2021). Misconfiguration and security management can result in unauthorized access, highlighting the need for strong security settings and access controls (Hussain et al., 2021).

To overcome these challenges, researchers have explored innovative solutions. Blockchain technology has been proposed as a disruptive tool to improve security in IoT-based health monitoring systems by securing devices and ensuring tamper-proof data transmission (Oikonomou et al., 2021). Trust-based security frameworks have been developed to protect the large amount of personal information collected by IoT health systems (Renjith et al., 2022). Additionally, blockchain-based architectures have been proposed as a more resource-efficient alternative to conventional security mechanisms for IoT health monitoring systems (Oikonomou et al., 2021).

Research has also focused on specific security measures. For example, identifying and fixing vulnerabilities in IoT-based health monitors is critical to preventing loss or disclosure of sensitive patient data (Aruna, 2019). Secure and scalable health data transmission in IoT relies on optimized routing protocols and cryptographic algorithms to ensure data security across heterogeneous devices (Refaee et al., 2022). Additionally, security frameworks designed for real-time IoT health applications have been proposed to meet the unique security needs of these systems (Hussain et al., 2021).

3.2.2. Case Studies and Famous Security Incidents

Security incidents and breaches in IoT-based healthcare systems are a serious concern due to the vulnerabilities present in these systems. Unauthorized access, data breaches, system downtime, and various security threats pose risks to the confidentiality, integrity, and availability of sensitive health data (Obaid & Salman, 2022; Mwangi, 2024). The unique specifications of IoT technology in healthcare, such as large data volumes, a large number of cloud computing servers, and a large number of users, create substantial security challenges (Said, 2022). Issues such as time synchronization, storage, communication, authentication, and sensing layer issues further exacerbate security risks in IoT-based health systems (Javed et al., 2022).

IoT integration in health introduces a complex set of security and privacy challenges, which require a thorough review of IoT communications in smart health ecosystems (Jaime, 2023). Additionally, the resource-limited nature of IoT devices and non-standardized IoT architecture contribute to security vulnerabilities in IoT-based applications (Li et al., 2020; Bovenizer & Chetthamrongchai, 2023). Challenges such as breaches of confidential patient information and the need to maintain privacy and security in e-health systems emphasize the importance of addressing security issues in IoT-enabled health environments (Dahiya, 2023; Seh et al., 2021).

The adoption of IoT devices in healthcare enables real-time data collection and analysis, but centralized processing and storage can lead to data manipulation and privacy issues (Rattanawiboomsom, 2023). Additionally, the limitations of lightweight cryptographic designs for IoT in healthcare, along with the challenges of securing wireless communications in IoT systems, highlight the complexity of implementing strong security measures in IoT-based health systems (Tsantikidou & Sklavos, 2022; Patil, 2023). Ensuring secure data collection, transmission, and storage in IoT-based health systems is critical to preventing security incidents and breaches that could compromise patient data and system integrity (Yadav et al., 2022).

3.3. Solutions and Strategies to Overcome Security Challenges

3.3.1. Security and Protection Technology

To effectively address security challenges, organizations can implement a combination of security and protection technologies. Encryption and data protection are essential to safeguard sensitive information during data transmission and storage (Moridu, 2023). Authentication and access control mechanisms, such as strong authentication methods and role-based access control, help ensure that only authorized individuals can access certain resources, thereby reducing the risk of unauthorized access (Moridu, 2023). Additionally, threat detection and response systems, such as intrusion detection and automated response systems, are important for identifying and addressing security breaches in real-time (Zhu, 2019).

In the field of cyber security, technological advances offer innovative solutions to enhance security measures. For example, the use of blockchain technology can provide a secure framework for protecting industrial IoT data in sectors such as smart power grids (Umran et al., 2023). Additionally, the integration of deep learning architectures can strengthen the security of industrial wireless communications by leveraging channel frequency response analysis (Alhoraibi, 2024). This technology offers strong security measures to deal with ever-evolving cyber threats.

Furthermore, research on authentication methods continues to grow, with studies focusing on areas such as keystroke dynamics, typing pattern recognition, and biometric-based authentication (Alzahab et al., 2022; Dias, 2023). This approach aims to improve the accuracy and efficiency of the user authentication process, contributing to overall cybersecurity resilience.

3.3.2. Managerial and Policy Approach

To effectively address security challenges, organizations can adopt a managerial and policy approach that focuses on security and compliance policies, as well as proactive risk and security management strategies. When formulating security and compliance policies, it is important to consider relevant safety regulations and standards (Stojkov et al., 2021). Understanding employee behavioral factors and compliance with information security standards is essential in fighting cyber-related crimes and strengthening security mechanisms (Al., 2019). Additionally, strengthening security measures is necessary to protect against cyber threats and vulnerabilities, reducing the likelihood of criminal activity powered by artificial intelligence (Mou, 2023).

In terms of proactive risk and security management, organizations can benefit from adopting a comprehensive framework that includes prevention measures, detection and response strategies, and recovery and resilience planning to effectively mitigate risks (Ibiyemi, 2024). Improving monitoring mechanisms and implementing proactive controls can help organizations detect and respond quickly to emerging risks (Dadulla, 2024). Furthermore, proactive management strategies involve early diagnosis and management to quickly address security challenges (Hobbs et al., 2021).

Additionally, compliance with security standards is essential for organizations to ensure safety and security. Security standards facilitate security knowledge and best control practices in a systematic manner (Stojkov et al., 2021). It is important to establish appropriate standards and practices to ensure compliance of wearable device privacy policies with IoT regulations, especially regarding the security and privacy of captured data (Echenim, 2023). Organizations can also leverage integrated knowledge graphs to automate cloud data compliance, capturing various data compliance regulations, threats, and security controls needed to effectively mitigate risks (Joshi et al., 2020).

3.3.3. New Innovations and Trends in Healthcare IoT Security

In overcoming security challenges in Healthcare IoT, utilizing cutting-edge technologies such as blockchain, AI, and machine learning is very important. Blockchain technology offers decentralized processing and storage for IoT data, ensuring data integrity, transparency and secure storage (Rattanawiboomsom, 2023). Additionally, blockchain enables a decentralized approach in health systems, eliminating the drawbacks of centralized systems such as single points of failure (Alsemmeari et al., 2023). By integrating blockchain with IoT, many cybersecurity problems can be addressed effectively (Arachchige, 2023).

Additionally, AI and machine learning play a significant role in improving Healthcare IoT security. This technology can be used to develop risk mitigation strategies, improve data privacy, and overcome security and privacy challenges in Healthcare IoT systems (Khatun, 2023). AI can improve IoT security by providing intelligent monitoring and threat detection capabilities, thereby strengthening the overall security posture of Healthcare IoT systems (Wu et al., 2020).

Furthermore, the combination of blockchain technology and AI can offer a comprehensive solution to security challenges in Healthcare IoT. Blockchain can ensure the integrity and confidentiality of medical data, while AI can improve detection and response mechanisms to threats, creating a strong security framework for Healthcare IoT systems (Alandjani, 2023). This integration can result in the development of a resilient patient healthcare system that is in line with the UN's sustainable development goals (Alandjani, 2023).

3.4. Analysis and Discussion

3.4.1. Evaluate the Effectiveness of Existing Solutions

To assess the effectiveness of existing security solutions in addressing the identified challenges, various aspects of cybersecurity need to be considered. Boodai et al. (2023) emphasize the need for further research to develop more effective security solutions and risk assessment frameworks, highlighting the continuous evolution required in this field to adapt to different conditions and scenarios. Augusto-Gonzalez et al. (2019) discuss how improving existing cybersecurity services can create a more transparent environment and improve system self-defense through disruptive network security solutions, emphasizing the importance of continuously improving security measures to stay ahead in the face of cyber threats.

Nesara et al. (2020) focus on software security patch management, emphasizing the need to address socio-technical challenges and implement effective solutions. Uriawan (2024) explores patient data security in distributed systems, discussing solutions such as blockchain technology, data encryption, and access control mechanisms. These studies underscore the importance of leveraging advanced technology to effectively enhance security measures.

In addition, Kim (2024) discusses the development of lightweight cryptographic systems to balance security and resource efficiency in IoT applications. Alajlan et al. (2023) highlight cybersecurity challenges in blockchain-based IoT systems, emphasizing the need to address these challenges for widespread adoption and effectiveness. Handayani (2023) demonstrated the potential of blockchain technology in improving the security and privacy of patient data in healthcare, demonstrating the role of innovative solutions in addressing critical security concerns.

4. Conclusions

IoT-based health systems represent a significant breakthrough in healthcare delivery, offering a variety of applications and benefits that improve patient care. This technology enables remote health monitoring, ensures data security, and drives innovation in disease prediction and management. By leveraging IoT technology, healthcare providers can enter a new era of proactive, personalized, and efficient care, ultimately improving patient outcomes and quality of life.

4.1. Implications

The implications of implementing IoT in health systems are vast. First, this technology improves real-time patient monitoring capabilities, enabling early detection of health problems and timely intervention, which in turn can reduce healthcare costs. Second, the integration of IoT with other technologies such as blockchain and cloud computing can increase security and efficiency in managing health data. Third, an IoT-based health system can expand access to health services, especially for those who live in remote areas or have limited mobility.

4.2. Limitations

Although they offer many benefits, IoT-based health systems also have some limitations. Key challenges include data security and privacy issues, device vulnerabilities, and the risk of cyberattacks that can threaten the integrity and confidentiality of medical information. Additionally, implementing IoT technology in the healthcare sector requires significant initial investment and adaptation of existing infrastructure. These factors may be a barrier to widespread adoption of this technology, especially in countries with limited resources.

4.3. Future Research

Future research should focus on developing stronger security solutions to protect health data in IoT systems. Further studies are needed to explore new encryption technologies, security protocols, and more advanced authentication methods. Additionally, research should evaluate the effectiveness and efficiency of IoT-based health systems in various contexts and populations, including their impact on patient outcomes, healthcare costs, and quality of care. Research should also examine the long-term impacts of IoT use in health, including potential risks and benefits for society as a whole.

5. References

al., A. (2019). Employee behavioural factors and information security standard compliance in nigeria banks. International Journal of Computing and Digital Systems, 8(4), 387-396. https://doi.org/10.12785/ijcds/080407

Alajlan, R., Alhumam, N., & Frikha, M. (2023). Cybersecurity for blockchain-based iot systems: a review. Applied Sciences, 13(13), 7432. https://doi.org/10.3390/app13137432

Alandjani, G. (2023). Integrating ai with green internet of things in healthcare for achieving un's sdgs. tjjpt, 44(3), 513-521. https://doi.org/10.52783/tjjpt.v44.i3.330

Albahri, O., Albahri, A., Zaidan, A., Zaidan, B., Alsalem, M., Mohsin, A., … & Shareef, A. (2019). Fault-tolerant mhealth framework in the context of iot-based real-time wearable health data sensors. Ieee Access, 7, 50052-50080. https://doi.org/10.1109/access.2019.2910411

Alhoraibi, L. (2024). Enhancing industrial wireless communication security using deep learning architecture-based channel frequency response. Iet Signal Processing, 2024, 1-13. https://doi.org/10.1049/2024/8884688

Alqahtani, M. (2021). Iot within the saudi healthcare industry during covid-19., 469-483. https://doi.org/10.1007/978-3-030-82616-1_40

Alsemmeari, R., Dahab, M., Alsulami, A., Alturki, B., & Algarni, S. (2023). Resilient security framework using tnn and blockchain for iomt.. https://doi.org/10.20944/preprints202304.0500.v1

Alzahab, N., Iorio, A., Baldi, M., & Scalise, L. (2022). Effect of auditory stimuli on electroencephalography-based authentication.. https://doi.org/10.48550/arxiv.2206.14519

Arachchige, K. (2023). Evaluation of blockchain networks' scalability limitations in low-powered internet of things (iot) sensor networks. Future Internet, 15(9), 317. https://doi.org/10.3390/fi15090317

Aruna*, E. (2019). Identification and remediation of vulnerabilities in iot based health monitor. International Journal of Innovative Technology and Exploring Engineering, 2(9), 4361-4365. https://doi.org/10.35940/ijitee.b7805.129219

Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Αναγνωστόπουλος, M., Σπαθούλας, Γ., Giannoutakis, K., … & Nijdam, N. (2019). From internet of threats to internet of things: a cyber security architecture for smart homes.. https://doi.org/10.1109/camad.2019.8858493

Auwal, A. (2023). Iot integration in telemedicine: investigating the role of internet of things devices in facilitating remote patient monitoring and data transmission.. https://doi.org/10.21203/rs.3.rs-3419693/v1

Bebortta, S. (2023). Fedehr: a federated learning approach towards the prediction of heart diseases in iot-based electronic health records. Diagnostics, 13(20), 3166. https://doi.org/10.3390/diagnostics13203166

Bhardwaj, V., Pevzner, P., Rashtchian, C., & Safonova, Y. (2020). Trace reconstruction problems in computational biology.. https://doi.org/10.48550/arxiv.2010.06083

Boodai, J., Alqahtani, A., & Frikha, M. (2023). Review of physical layer security in 5g wireless networks. Applied Sciences, 13(12), 7277. https://doi.org/10.3390/app13127277

Bovenizer, W. and Chetthamrongchai, P. (2023). A comprehensive systematic and bibliometric review of the iot-based healthcare systems. Cluster Computing, 26(5), 3291-3317. https://doi.org/10.1007/s10586-023-04047-1

Butpheng, C., Yeh, K., & Xiong, H. (2020). Security and privacy in iot-cloud-based e-health systems—a comprehensive review. Symmetry, 12(7), 1191. https://doi.org/10.3390/sym12071191

Cappart, Q., Moisan, T., Rousseau, L., Prémont‑Schwarz, I., & Ciré, A. (2020). Combining reinforcement learning and constraint programming for combinatorial optimization.. https://doi.org/10.48550/arxiv.2006.01610

Dadulla, D. (2024). Risk management among department of tourism-accredited hotels in region viii. International Journal of Multidisciplinary Applied Business and Education Research, 5(5), 1744-1757. https://doi.org/10.11594/ijmaber.05.05.22

Dahiya, R. (2023). Facilitating healthcare sector through iot: issues, challenges, and its solutions. Eai Endorsed Transactions on Internet of Things, 9(4), e5. https://doi.org/10.4108/eetiot.v9i4.4317

Deursen, A., Zeeuw, A., Boer, P., Jansen, G., & Rompay, T. (2019). Digital inequalities in the internet of things: differences in attitudes, material access, skills, and usage. Information Communication & Society, 24(2), 258-276. https://doi.org/10.1080/1369118x.2019.1646777

Dias, T. (2023). Keyrecs: a keystroke dynamics and typing pattern recognition dataset. Data in Brief, 50, 109509. https://doi.org/10.1016/j.dib.2023.109509

Ding, D., Chang, Y., Wu, K., & Harnod, T. (2022). The organoid: a research model for ovarian cancer. Tzu Chi Medical Journal, 34(3), 255. https://doi.org/10.4103/tcmj.tcmj_63_21

Echenim, K. (2023). Ensuring privacy policy compliance of wearables with iot regulations.. https://doi.org/10.1109/tps-isa58951.2023.00039

Edeh, M., Otto, E., Richard-Nnabu, N., Ugboaja, S., Umoke, C., & Omachi, D. (2022). Potential of internet of things and semantic web technologies in the health sector. Nigerian Journal of Biotechnology, 38(2), 73-83. https://doi.org/10.4314/njb.v38i2.8

Handayani, I. (2023). Enhancing security and privacy of patient data in healthcare: a smartpls analysis of blockchain technology implementation. Iaic Transactions on Sustainable Digital Innovation (Itsdi), 5(1), 8-17. https://doi.org/10.34306/itsdi.v5i1.603

Hobbs, K., Krischak, M., Tejwani, R., Purves, J., Wiener, J., & Routh, J. (2021). The importance of early diagnosis and management of pediatric neurogenic bladder dysfunction. Research and Reports in Urology, Volume 13, 647-657. https://doi.org/10.2147/rru.s259307

Hussain, A., Ali, T., Althobiani, F., Draz, U., Irfan, M., Yasin, S., … & Alqhtani, S. (2021). Security framework for iot based real-time health applications. Electronics, 10(6), 719. https://doi.org/10.3390/electronics10060719

Ibiyemi, M. (2024). Safeguarding supply chains from cyber-physical system attacks frameworks and strategies. International Journal of Management & Entrepreneurship Research, 6(6), 2015-2023. https://doi.org/10.51594/ijmer.v6i6.1240

İSLAM, M., Hassan, M., ABDULLAHI, K., & GIDER, Z. (2022). Participation (islamic) banking in turkey: a bibliometric analysis and future research agenda. International Journal of Economics and Management, 16(2), 193-212. https://doi.org/10.47836/ijeam.16.2.04

Jaime, F. (2023). Strengthening privacy and data security in biomedical microelectromechanical systems by iot communication security and protection in smart healthcare. Sensors, 23(21), 8944. https://doi.org/10.3390/s23218944

Javed, L., Yakubu, B., Waleed, M., Khaliq, Z., Suleiman, A., & Mato, N. (2022). Bhc-iot: a survey on healthcare iot security issues and blockchain-based solution. International Journal of Electrical and Computer Engineering Research, 2(4), 1-9. https://doi.org/10.53375/ijecer.2022.302

Javid, S. and Mirzaei, A. (2021). Presenting a reliable routing approach in iot healthcare using the multiobjective-based multiagent approach. Wireless Communications and Mobile Computing, 2021, 1-20. https://doi.org/10.1155/2021/5572084

Joshi, K., Elluri, L., & Nagar, A. (2020). An integrated knowledge graph to automate cloud data compliance. Ieee Access, 8, 148541-148555. https://doi.org/10.1109/access.2020.3008964

Junaid, S., Imam, A., Balogun, A., Silva, L., Surakat, Y., Kumar, G., … & Mahamad, S. (2022). Recent advancements in emerging technologies for healthcare management systems: a survey. Healthcare, 10(10), 1940. https://doi.org/10.3390/healthcare10101940

Kamangar, Z., Memon, R., Memon, G., & Kamangar, U. (2023). Integration of internet of things and blockchain technology in healthcare domain: a systematic literature review. International Journal of Communication Systems, 36(16). https://doi.org/10.1002/dac.5582

Kashyap, V., Kumar, A., Kumar, A., & Hu, Y. (2022). A systematic survey on fog and iot driven healthcare: open challenges and research issues. Electronics, 11(17), 2668. https://doi.org/10.3390/electronics11172668

Kayal, M., Ballard, J., & Kayal, E. (2022). Transformative choices towards a sustainable academic publishing system. Ideas in Ecology and Evolution, 14. https://doi.org/10.24908/iee.2021.14.3.f

Kelly, J., Campbell, K., Gong, E., & Scuffham, P. (2020). The internet of things: impact and implications for health care delivery. Journal of Medical Internet Research, 22(11), e20135. https://doi.org/10.2196/20135

Khatun, M. (2023). Machine learning for healthcare-iot security: a review and risk mitigation. Ieee Access, 11, 145869-145896. https://doi.org/10.1109/access.2023.3346320

Kim, T. (2024). A study on impact of lightweight cryptographic systems on internet of things-based applications. Asia-Pacific Journal of Convergent Research Interchange, 10(1), 49-59. https://doi.org/10.47116/apjcri.2024.01.05

Kruesi, M. and Bazelmans, L. (2022). Resources, capabilities and competencies: a review of empirical hospitality and tourism research founded on the resource-based view of the firm. Journal of Hospitality and Tourism Insights, 6(2), 549-574. https://doi.org/10.1108/jhti-10-2021-0270

Li, J., Jinjin, C., Khan, F., Rehman, A., Balasubramaniam, V., Sun, J., … & Venu, P. (2020). A secured framework for sdn-based edge computing in iot-enabled healthcare system. Ieee Access, 8, 135479-135490. https://doi.org/10.1109/access.2020.3011503

Manwal, M. (2019). Smart healthcare systems: the impact of iot on medical diagnostics and treatment. Information Technology in Industry, 7(3), 68-77. https://doi.org/10.17762/itii.v7i3.814

Moridu, I. (2023). Analysis of the impact of changes in directors, it directors, and risk management of bsi (bris) on information technology performance and security and risk control at one of the bsi bank branches in bandung city. West Science Business and Management, 1(04), 288-295. https://doi.org/10.58812/wsbm.v1i04.227

Mou, B. (2023). Analysis of the role of compliance plan in ai criminal risk prevention-take ai criminal risk in network communication as example. International Journal of Communication Networks and Information Security (Ijcnis), 15(3), 154-167. https://doi.org/10.17762/ijcnis.v15i3.6242

Mwangi, E. (2024). Exploring iot embedded systems along the line of identity access management for enhanced health data security.. https://doi.org/10.22541/au.171215399.97252701/v1

Mwangi, E. (2024). Exploring iot embedded systems along the line of identity access management for enhanced health data security.. https://doi.org/10.22541/au.171215399.97252701/v1

Nesara, D., Jayatilaka, A., Zahedi, M., & Babar, M. (2020). Software security patch management -- a systematic literature review of challenges, approaches, tools and practices.. https://doi.org/10.48550/arxiv.2012.00544

Obaid, O. and Salman, S. (2022). Security and privacy in iot-based healthcare systems: a review., 29-40. https://doi.org/10.58496/mjcsc/2022/007

Oikonomou, F., Ribeiro, J., Μαντάς, Γ., Bastos, J., & Rodríguez, J. (2021). A hyperledger fabric-based blockchain architecture to secure iot-based health monitoring systems.. https://doi.org/10.1109/meditcom49071.2021.9647521

Oikonomou, F., Μαντάς, Γ., Cox, P., Saghezchi, F., Gil‐Castiñeira, F., & González, J. (2021). A blockchain-based architecture for secure iot-based health monitoring systems.. https://doi.org/10.1109/camad52502.2021.9617803

Patil, V. (2023). Securing wireless communication in cyber-physical systems and the internet of things: addressing security challenges. RJCSE, 4(1), 110-118. https://doi.org/10.52710/rjcse.69

Prindle, J. (2023). An open-source probabilistic record linkage process for records with family-level information: simulation study and applied analysis. Plos One, 18(10), e0291581. https://doi.org/10.1371/journal.pone.0291581

Rattanawiboomsom, V. (2023). Blockchain-enabled internet of things (iot) applications in healthcare: a systematic review of current trends and future opportunities. International Journal of Online and Biomedical Engineering (Ijoe), 19(10), 99-117. https://doi.org/10.3991/ijoe.v19i10.41399

Refaee, E., Parveen, S., Begum, K., Parveen, F., Raja, M., Gupta, S., … & Santhosh, K. (2022). Secure and scalable healthcare data transmission in iot based on optimized routing protocols for mobile computing applications. Wireless Communications and Mobile Computing, 2022, 1-12. https://doi.org/10.1155/2022/5665408

Renjith, P., Ramesh, K., & Balasubramani, S. (2022). An improved trust-based security framework for iot health care monitoring system.. https://doi.org/10.21203/rs.3.rs-1970278/v1

Roy, S., Ghosh, D., Sau, D., Nandy, S., Pal, M., Bhattacherjee, R., … & Bose, R. (2021). Iot-based tetra health surveillance system (thss). International Journal of Scientific Research and Management, 9(12), 639-649. https://doi.org/10.18535/ijsrm/v9i12.ec01

Said, O. (2022). Lbss: a lightweight blockchain-based security scheme for iot-enabled healthcare environment. Sensors, 22(20), 7948. https://doi.org/10.3390/s22207948

Seh, A., Al-Amri, J., Subahi, A., Agrawal, A., Kumar, R., & Khan, R. (2021). Machine learning based framework for maintaining privacy of healthcare data. Intelligent Automation & Soft Computing, 29(3), 697-712. https://doi.org/10.32604/iasc.2021.018048

Stojkov, M., Dalcekovic, N., Markoski, B., Milosavljević, B., & Sladić, G. (2021). Towards cross-standard compliance readiness: security requirements model for smart grid. Energies, 14(21), 6862. https://doi.org/10.3390/en14216862

Sun, Y., Li, M., Cao, S., Xu, Y., Wu, P., Xu, S., … & Liang, W. (2022). Optogenetics for understanding and treating brain injury: advances in the field and future prospects. International Journal of Molecular Sciences, 23(3), 1800. https://doi.org/10.3390/ijms23031800

Talló-Parra, O., Salas, M., & Manteca, X. (2023). Zoo animal welfare assessment: where do we stand?. Animals, 13(12), 1966. https://doi.org/10.3390/ani13121966

Taryudi, T., Lindayani, L., Mutiar, A., & Purnama, H. (2022). Perceptions of indonesian nurses toward the application of the internet of things in the future. Kne Life Sciences. https://doi.org/10.18502/kls.v7i2.10398

Tsantikidou, K. and Sklavos, N. (2022). Hardware limitations of lightweight cryptographic designs for iot in healthcare. Cryptography, 6(3), 45. https://doi.org/10.3390/cryptography6030045

Umran, S., Lu, S., Abduljabbar, Z., & Tang, X. (2023). A blockchain-based architecture for securing industrial iots data in electric smart grid. Computers Materials & Continua, 74(3), 5389-5416. https://doi.org/10.32604/cmc.2023.034331

Uriawan, W. (2024). Challenges and opportunities: improve patient data security and privacy in distributed systems.. https://doi.org/10.20944/preprints202407.0163.v1

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on artificial intelligence enhancing internet of things security: a survey. Ieee Access, 8, 153826-153848. https://doi.org/10.1109/access.2020.3018170

Yadav, K., Alharbi, A., Jain, A., & Ramadan, R. (2022). An iot based secure patient health monitoring system. Computers Materials & Continua, 70(2), 3637-3652. https://doi.org/10.32604/cmc.2022.020614

Zhu, L. (2019). A new intrusion detection and alarm correlation technology based on neural network. Eurasip Journal on Wireless Communications and Networking, 2019(1). https://doi.org/10.1186/s13638-019-1419-z

Žužek, T., Gosar, Ž., Kušar, J., & Berlec, T. (2021). A new product development model for smes: introducing agility to the plan-driven concurrent product development approach. Sustainability, 13(21), 12159. https://doi.org/10.3390/su132112159