JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN 3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.95

Network Security Analysis in Internet of Things (IoT) Systems

Nova Oktapiana[1*], Dirja Nur Ilham[2], Fardiansyah[3], Depi Ginting[4], Fera Anugreni[5]
[1,2,3,4,5]Politeknik Aceh selatan, Indonesia
[1*]novaokt@gmail.com, [2]dirja.poltas@gmail.com, [3]fardian.poltas@gmail.com,[4]depiginting@poltas.ac.id,
[5]anugrenifera28@gmail.com

open access

***Corresponding Author**

Article History:
Submitted: 10-12-2025
Accepted: 22-12-2025
Published: 26-12-2025

Keywords:
Internet of Things, network security, IoT security, systematic literature review.

ABSTRACT

The rapid development of the Internet of Things (IoT) has significantly transformed various sectors, including industry, healthcare, smart cities, and agriculture. However, this growth has also increased the complexity and scale of network security vulnerabilities. IoT devices are typically resource-constrained and operate in heterogeneous network environments, making them attractive targets for cyberattacks. This study aims to analyze key network security challenges in IoT systems, evaluate solution technologies proposed in recent literature, and formulate evidence-based recommendations for improving IoT security. The research adopts a Systematic Literature Review (SLR) method by examining ten peer-reviewed articles published between 2020 and 2023 and indexed in IEEE Xplore, SpringerLink, and ACM Digital Library. The results indicate that major IoT security challenges include vulnerabilities in communication protocols, limited computational and energy resources, and the increasing prevalence of attacks such as Distributed Denial of Service (DDoS), spoofing, and ransomware. The most frequently proposed solutions involve machine learning-based anomaly detection, lightweight cryptographic mechanisms, layered security architectures using edge–fog–cloud computing, and blockchain integration to enhance authentication and data integrity. This study concludes that IoT security requires a holistic and multidisciplinary approach that integrates multiple complementary technologies within a unified security framework.

INTRODUCTION

The Internet of Things (IoT) represents a computing paradigm that enables physical objects embedded with sensors, actuators, and communication technologies to connect and exchange data through the internet (Qiu et al., 2021; Zhao & Ge, 2021). IoT adoption has expanded rapidly across multiple domains, such as Industry 4.0, smart cities, healthcare systems, transportation, and smart agriculture, supporting operational efficiency, automation, and real-time data-driven decision making (Qiu et al., 2021).

Despite its benefits, IoT development introduces significant network security challenges. The large number of interconnected devices, technological heterogeneity, limited computational power, and reliance on wireless communication substantially increase the attack surface (Sicari et al., 2021; Smith, 2022). Many IoT devices are designed with an emphasis on cost efficiency and functionality, often resulting in inadequate security mechanisms (Zhou et al., 2022).

Recent years have seen numerous security incidents involving IoT systems, including Distributed Denial of Service (DDoS) attacks, data breaches, device hijacking, and ransomware (Ahmed & Li, 2022; Chen et al., 2023). These incidents highlight the need for comprehensive and integrated security strategies. Therefore, this study aims to identify the primary network security challenges in IoT environments and analyze solution approaches proposed in recent academic literature using a Systematic Literature Review methodology (Kitchenham & Charters, 2007).

LITERATURE REVIEW

Existing studies on IoT network security commonly classify security risks into four core dimensions: confidentiality, integrity, availability, and authentication (Smith, 2022; Zhou et al., 2022). These risks are often intensified by the use of lightweight communication protocols, such as MQTT and CoAP, which provide limited built-in security features (Lee & Patel, 2021).

JATAED
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
E-ISSN 3031-0903
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.95

Artificial intelligence (AI) techniques, particularly machine learning and deep learning, have gained attention for enhancing intrusion detection and anomaly identification in IoT networks. These approaches have demonstrated promising results in detecting DDoS attacks, abnormal traffic patterns, and unauthorized access attempts (Ferrag et al., 2021; Zhang et al., 2023).

Blockchain technology has also been proposed as a solution to improve trust, authentication, and data integrity in IoT environments through decentralized and tamper-resistant mechanisms (Kumar & Kim, 2022; Khan et al., 2022). However, blockchain-based solutions still face challenges related to scalability, latency, and computational overhead (Khan et al., 2022).

From an architectural perspective, edge and fog computing paradigms enable data processing closer to IoT devices, improving response time and reducing security risks associated with centralized cloud architectures (Wang et al., 2021; Nguyen et al., 2023). Additionally, the limited resources of IoT devices have encouraged the adoption of lightweight cryptographic algorithms as alternatives to conventional encryption techniques (Al-Ghaili et al., 2021; Yassein et al., 2022).

RESEARCH METHOD

This study employs a Systematic Literature Review (SLR) to provide a structured and reproducible analysis of IoT network security challenges and solutions. The SLR method is widely used to synthesize existing research systematically and transparently, ensuring the reliability and validity of the review process (Kitchenham & Charters, 2007). The SLR process consists of planning, literature identification, selection, and analysis stages.

Relevant articles were retrieved from IEEE Xplore, SpringerLink, and ACM Digital Library using keywords related to IoT security and network security. Inclusion criteria required that articles be published between 2020 and 2023 and explicitly address IoT security threats, challenges, or mitigation techniques, in line with common practices in recent IoT security reviews (Smith, 2022; Nguyen et al., 2023). The selected studies were analyzed using thematic analysis to identify dominant security issues and commonly proposed solutions (Zhang et al., 2023).

Research Method Flowchart

The research methodology is illustrated through the following flowchart, which outlines the sequential stages of the Systematic Literature Review process:

JATAED
E-ISSN 3031-0903
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.95

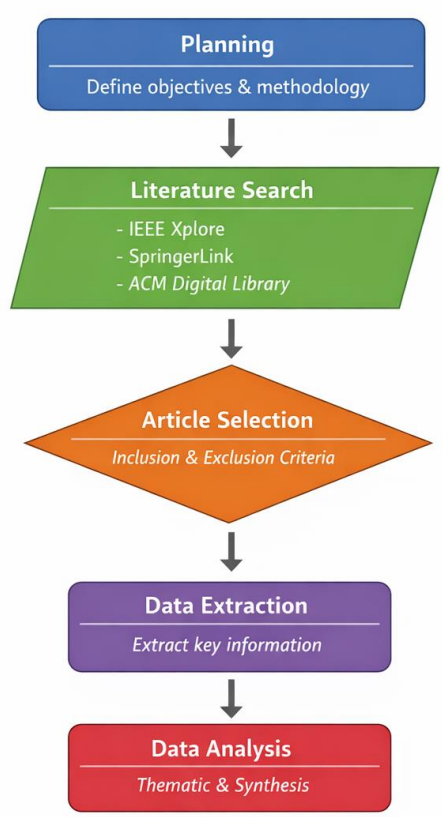

Figure 1. Research Method Flowchart

The research methodology follows a Systematic Literature Review (SLR) approach to ensure a structured, transparent, and reproducible analysis of IoT network security challenges and solutions (Kitchenham & Charters, 2007). The process begins with research planning, where the objectives, scope, and review protocol are defined, followed by a systematic literature search conducted using relevant keywords across IEEE Xplore, SpringerLink, and the ACM Digital Library. The retrieved studies are then screened and selected based on predefined inclusion and exclusion criteria, ensuring relevance to IoT security threats and mitigation techniques. Subsequently, data extraction is performed to collect key information related to security challenges, attack types, and proposed solutions. Finally, thematic analysis and synthesis are applied to classify and interpret the findings, forming the basis for discussion, conclusions, and recommendations. This methodological flow ensures transparency and supports the reproducibility of the review process.

RESULTS

The results of the Systematic Literature Review indicate that IoT network security challenges can be categorized into three main groups: technical limitations, attack threats, and governance-related issues such as privacy and policy. Technical challenges are primarily associated with vulnerabilities in communication protocols and the limited computational, memory, and energy resources of IoT devices (Lee & Patel, 2021; Al-Ghaili et al., 2021).

From the threat perspective, Distributed Denial of Service (DDoS) attacks, unauthorized access, and malware, including ransomware, are identified as the most dominant attack types targeting IoT environments (Ahmed & Li, 2022; Chen et al., 2023). These attacks exploit weak authentication mechanisms and insufficient traffic monitoring capabilities in IoT networks.

The reviewed literature also highlights several widely adopted mitigation approaches. Machine learning-based anomaly detection techniques are frequently proposed to identify abnormal traffic patterns in IoT networks (Ferrag et al., 2021; Zhang et al., 2023). In addition, lightweight cryptographic schemes are commonly recommended to secure data transmission while accommodating the constrained resources of IoT devices (Yassein et al., 2022).

DISCUSSION

JATAED
E-ISSN 3031-0903
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.95

The findings demonstrate that no single security mechanism is sufficient to address the diverse and complex challenges present in IoT networks. As a result, an integrated and multi-layered security approach is necessary. Combining edge or fog computing architectures with artificial intelligence-based intrusion detection systems enables faster and more localized threat detection, thereby reducing response time and dependency on centralized cloud infrastructures (Wang et al., 2021; Nguyen et al., 2023).

Blockchain-based security solutions offer advantages in terms of decentralized authentication and data integrity; however, they may introduce additional latency and scalability issues, particularly in large-scale IoT deployments (Khan et al., 2022). Similarly, while lightweight cryptographic algorithms are suitable for constrained devices, their long-term robustness against evolving attack techniques requires further investigation (Al-Ghaili et al., 2021).

Therefore, a defense-in-depth strategy that integrates multiple complementary technologies and adheres to established security standards, such as NIST IR 8259, is considered the most effective approach for enhancing IoT network security (NIST, 2020; Smith, 2022).

CONCLUSION

This study concludes that IoT network security is a multidimensional problem that requires a holistic and integrated approach. Machine learning, lightweight cryptography, edge computing architectures, and blockchain technologies should be combined within a unified security framework to effectively mitigate threats (Smith, 2022; Nguyen et al., 2023). In addition, the adoption of recognized security standards and increased security awareness among developers and users are essential to ensure the long-term security of IoT systems (NIST, 2020; Sicari et al., 2021).

REFERENCE

Ahmed, T., & Li, C. (2022). Detection and mitigation of DDoS attacks in IoT networks using hybrid techniques. *International Journal of Computer Networks & Communications, 14*(2), 1–16.

Al-Ghaili, A. M., Kasim, S., & Shaari, R. (2021). Lightweight cryptography for Internet of Things: A survey. *Journal of Network and Computer Applications, 182*, 103036. https://doi.org/10.1016/j.jnca.2021.103036

Chen, X., Zhang, H., Li, Y., & Zhou, M. (2023). Ransomware attacks on IoT-based healthcare systems: Analysis and mitigation strategies. *Journal of Medical Systems, 47*(4), 1–12. https://doi.org/10.1007/s10916-023-01923-7

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2021). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419. https://doi.org/10.1016/j.jisa.2019.102419

Khan, M. A., Salah, K., & Jayaraman, R. (2022). Blockchain-based secure data sharing for Internet of Things: A survey. *IEEE Internet of Things Journal, 9*(5), 3548–3572. https://doi.org/10.1109/JIOT.2021.3097814

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. Keele University and Durham University.

Kumar, S., & Kim, H. (2022). A blockchain-based secure communication framework for IoT networks. *IEEE Access, 10*, 12345–12358. https://doi.org/10.1109/ACCESS.2022.3145678

Lee, K., & Patel, R. (2021). Vulnerability analysis of lightweight IoT communication protocols. In *Proceedings of the International Conference on Computer Security* (pp. 123–135). Springer.

National Institute of Standards and Technology. (2020). *IoT device cybersecurity capability core baseline (NIST IR 8259)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.IR.8259

Nguyen, T. T., Reddi, V. J., & Choi, D. (2023). Edge computing security for IoT: Threats, solutions, and future directions. *IEEE Communications Surveys & Tutorials, 25*(1), 372–402. https://doi.org/10.1109/COMST.2022.3208894

Qiu, T., Chen, N., Li, K., Atiquzzaman, M., & Zhao, W. (2021). How can heterogeneous Internet of Things build our future: A survey. *IEEE Communications Surveys & Tutorials, 20*(3), 2011–2027. https://doi.org/10.1109/COMST.2017.2718610

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2021). Security, privacy, and trust in Internet of Things: The road ahead. *Computer Networks, 76*, 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Smith, J. (2022). A survey of IoT security: Risks, challenges, and solutions. *IEEE Internet of Things Journal, 9*(1), 1–15. https://doi.org/10.1109/JIOT.2021.3071549

Wang, L., Ranjan, R., Chen, J., & Benatallah, B. (2021). Cloud, edge, and fog computing in IoT security: A review. *Future Generation Computer Systems, 114*, 1–12. https://doi.org/10.1016/j.future.2020.07.045

JATAED
E-ISSN 3031-0903
Journal of Appropriate Technology for Agriculture, Environment, and Development
email: jataed@lkppl.org
Volume 3, **Number** 1, October 2025
https://doi.org/10.62671/jataed.v3i1.95

Yassein, M. B., Shatnawi, M. Q., Aljwarneh, S., & Al-Hatmi, R. (2022). Lightweight security algorithms for constrained IoT devices. *International Journal of Information Security Science*, *11*(2), 85–96.

Zhang, Y., Li, P., & Wang, X. (2023). Machine learning for anomaly detection in IoT networks: A comparative study. *ACM Computing Surveys*, *55*(8), 1–35. https://doi.org/10.1145/3560815

Zhao, K., & Ge, L. (2021). A survey on the Internet of Things security. *Proceedings of the IEEE, 109*(8), 1–20. https://doi.org/10.1109/JPROC.2021.3070698

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2022). The effect of IoT new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal*, *8*(3), 1601–1615.