International Journal of Research and Applied Technology

3(2)(2023) 399-405

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

Strengthening Industrial IoT Security: An Analytical Review of Cryptographic Techniques and Blockchain-Based Solutions

Mochammad Fuad Hasan*

Universitas Komputer Indonesia, Indonesia

Email: *fuadhasan26.fh@gmail.com

Abstract. The Industrial Internet of Things (IIoT) has revolutionized traditional industrial systems by increasing connectivity, automation, and data-driven decision-making. However, this increased complexity also presents major cybersecurity-related challenges, including the threat of data breaches and operational disruptions. This study aims to provide an analytical review of cryptographic techniques and blockchain-based solutions in strengthening IIoT security. Combining bibliometric analysis and Systematic Literature Review (SLR), analyzing peer-reviewed articles published between 2016 and 2023 were analyzed. The bibliometric analysis revealed significant research growth trends, key contributions from global institutions, and emerging research themes such as lightweight cryptography, blockchain-based authentication, and secure communication models for resource-constrained IIoT devices. Meanwhile, the SLR provides an in-depth synthesis of the technical approaches, benefits, limitations, and open challenges in this field. The results show that the combination of cryptography and blockchain can offer decentralized, tamper-resistant, and efficient security solutions. The study also identified an urgent need for the development of more integrated and energy-efficient security models, as well as the validation of solutions in real industrial environments. The findings are expected to provide valuable guidance for the development of more reliable and secure IIoT systems in the future.

Keywords: Blockchain, Cryptography, Internet of Thing (IoT)

1. Introduction

The Industrial Internet of Things (IIoT) has revolutionized traditional industrial systems by connecting devices, sensors, and machines to digital networks, enabling real-time monitoring, data-driven decision-making, and advanced automation [1]. However, the growing complexity and connectivity of IIoT environments expose them to significant cybersecurity risks, such as data breaches, unauthorized access, and operational disruptions [2]. To address these concerns, researchers have explored various security mechanisms, notably cryptographic techniques and blockchain-based solutions, which promise enhanced

confidentiality, integrity, and trust in decentralized IIoT ecosystems. Strengthening IIoT security through these technologies is crucial to ensure the reliability and resilience of critical industrial infrastructures [3].

Previous studies have extensively explored the role of cryptographic methods and blockchain technology in securing Industrial Internet of Things (IIoT) systems, particularly in developing lightweight encryption, authentication protocols, and decentralized frameworks. a 2020 study proposed adaptations of Elliptic Curve Cryptography (ECC) that reduce computational complexity while maintaining high security for resource-constrained IIoT devices [4]. A study 2023 analyzed lightweight block ciphers such as PRESENT and HIGHT, demonstrating their efficiency and suitability for IIoT environments with limited energy and processing power [5]. Another 2020 study introduced a secure mutual authentication protocol optimized for minimal handshake time and memory consumption, addressing the needs of constrained devices [6]. A 2022 study developed a distributed key management framework that enhanced scalability and resilience in IIoT networks by eliminating reliance on centralized authorities [7]. In the context of blockchain applications, a study 2021 proposed a lightweight blockchain structure that improved data integrity and decentralized control for IoT systems [8]. A study 2022 demonstrated the effectiveness of blockchain-based authentication mechanisms in preventing impersonation and unauthorized access in industrial IoT environments [9]. Despite these advancements, most prior studies have addressed cryptographic and blockchain solutions separately, without fully leveraging their combined potential. Moreover, systematic studies that rigorously map and synthesize these developments through bibliometric analysis and Systematic Literature Review (SLR) remain scarce, leaving a significant gap for integrated research efforts in strengthening IIoT security [10].

This study aims to provide an analytical review of cryptographic techniques and blockchain-based solutions for strengthening IIoT security by combining bibliometric analysis and the SLR method. Bibliometric analysis quantitatively examines publication trends, leading contributors, influential works, and emerging themes within the field. Meanwhile, the SLR approach is used to systematically collect, evaluate, and synthesize relevant research articles, ensuring a comprehensive, transparent, and reproducible review process [11]. By employing SLR, the study filters and critically assesses high-quality studies based on defined inclusion and exclusion criteria, thus offering a structured synthesis of the current state-of-the-art in IIoT security. Through this dual methodology, the research seeks to answer questions regarding the most effective cryptographic techniques, the application and challenges of blockchain technologies, and the major research gaps in the field [12].

The novelty of this research lies in its integrated methodological framework that combines quantitative bibliometric insights with qualitative systematic synthesis through SLR, offering a comprehensive and multi-dimensional understanding of IIoT security. Unlike previous works that addressed cryptography and blockchain in isolation or lacked a structured mapping of research trends, this study systematically explores their convergence, highlighting how these technologies can be combined to provide robust, scalable, and efficient security solutions. Furthermore, the bibliometric analysis enables the identification of emerging trends, research hotspots, and overlooked areas, providing a roadmap for future investigations in strengthening security for next-generation industrial systems.

International Journal of Research and Applied Technology

3(2)(2023) 399-405

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

2. Method

This study employs a qualitative research approach by conducting a Systematic Literature Review (SLR) combined with bibliometric analysis to explore the current advancements in cryptographic techniques and blockchain-based solutions for Industrial Internet of Things (IIoT) security [13]. As an early-stage investigation, the research is based solely on existing academic publications and does not involve any form of experimental or empirical testing. The aim is to provide a comprehensive synthesis of existing knowledge while identifying emerging trends and research gaps within the field.

The data collection process focused on retrieving scholarly articles published between 2016 and 2023 from major scientific databases, including IEEE Xplore, Scopus, Web of Science, and ScienceDirect. A structured search strategy was applied using relevant keywords such as "Internet of Things," "Industrial IoT," "Blockchain," "Cryptography," and "Security," with Boolean operators to refine the results. Articles were selected based on specific inclusion criteria: publications must be peer-reviewed, written in English, and directly related to IIoT security with an emphasis on cryptography and/or blockchain applications. Non-peer-reviewed articles, papers outside the targeted timeframe, and studies not focused on IIoT were excluded to ensure the quality and relevance of the reviewed literature.

The bibliometric analysis was carried out using software tools like VOSviewer and Bibliometrix to map the scientific landscape. These tools facilitated the visualization of citation networks, keyword co-occurrence, and collaboration patterns among authors and institutions. The bibliometric approach enabled the identification of influential publications, leading contributors, and thematic trends over time within the domains of IIoT, cryptography, and blockchain. This quantitative analysis provided a structured overview of the research activity and evolution in the field.

Following the bibliometric stage, the SLR methodology was applied to conduct a deep qualitative analysis. The selected articles were systematically reviewed, and essential information such as proposed methods, application areas, benefits, limitations, and recommendations were extracted. Thematic analysis was used to group studies into key focus areas like lightweight cryptographic algorithms for IIoT, blockchain-based authentication frameworks, secure communication protocols, and hybrid security models [14]. This synthesis allowed a critical assessment of the strengths and weaknesses of current solutions, paving the way for the identification of open challenges and future research directions.

As this study is strictly based on secondary data and literature review, it is important to note its scope limitations. The findings presented herein are theoretical and derived from an in-depth examination of existing scholarly works. Future studies may expand on this foundation by conducting experimental research, implementing proposed security frameworks, or validating them in real-world IIoT environments. Nonetheless, the insights generated from this analysis are expected to contribute meaningfully to the academic and practical discourse surrounding IIoT security.

This section presents the findings from the bibliometric analysis and the data synthesis obtained through the systematic literature review. The results highlight the publication trends, influential contributors, thematic focus areas, and emerging directions in the research field related to Industrial IoT (IIoT) security, cryptographic techniques, and blockchain applications.

International Journal of Research and Applied Technology

3(2)(2023) 399-405

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

3. Results and Discussion

3.1 Bibliometric Analysis

Based on the systematic search across IEEE Xplore, Scopus, Web of Science, and ScienceDirect, a total of 517 initial documents were retrieved. After applying inclusion and exclusion criteria, removing duplicates, and screening for relevance, 112 high-quality articles published between 2016 and 2023 were selected for detailed analysis.

The trend of publications over the five-year period shows a steady increase in research interest. In 2019, there were approximately 15 relevant publications, which grew to over 30 publications by 2023, indicating a significant upward trend in the focus on IIoT security enhancements using cryptography and blockchain technologies. This growth reflects the growing awareness and urgency of addressing cybersecurity challenges in industrial systems.

In terms of contributing sources, IEEE Access, Sensors (MDPI), and Future Generation Computer Systems (Elsevier) emerged as the top journals publishing research at the intersection of IIoT, blockchain, and cryptography. The most influential authors, determined based on citation counts and co-authorship analysis, include researchers such as Zhang Y., Kumar N., and Al-Fuqaha A., who have consistently contributed to the advancement of secure IIoT systems. Co-authorship network analysis indicated strong collaboration patterns among institutions based in China, the United States, and Europe, suggesting an international effort towards tackling IIoT security challenges.

Keyword co-occurrence analysis revealed that the most frequently appearing keywords alongside "Industrial Internet of Things" were "blockchain," "lightweight cryptography," "authentication," "data integrity," and "smart contracts." Thematic mapping showed that research topics initially focused on basic encryption and communication protocols in early years, while more recent studies have shifted towards integrated blockchain-based architectures, decentralized authentication schemes, and energy-efficient cryptographic models optimized for resource-constrained IIoT devices.

3.2 Data Result

The bibliometric analysis based on the keywords "IoT," "blockchain," and "cryptography" provides valuable insights into the growing research interest in securing the Industrial Internet of Things (IIoT) through advanced cryptographic techniques and blockchain-based solutions. As depicted in the figure 1, a steady and significant increase in the number of related publications has been observed from 2016 to 2023. See (Figure 1)

International Journal of Research and Applied Technology

3(2)(2023) 399-405

Journal homepage: https://ojs.unikom.ac.id/index.php/injuratech

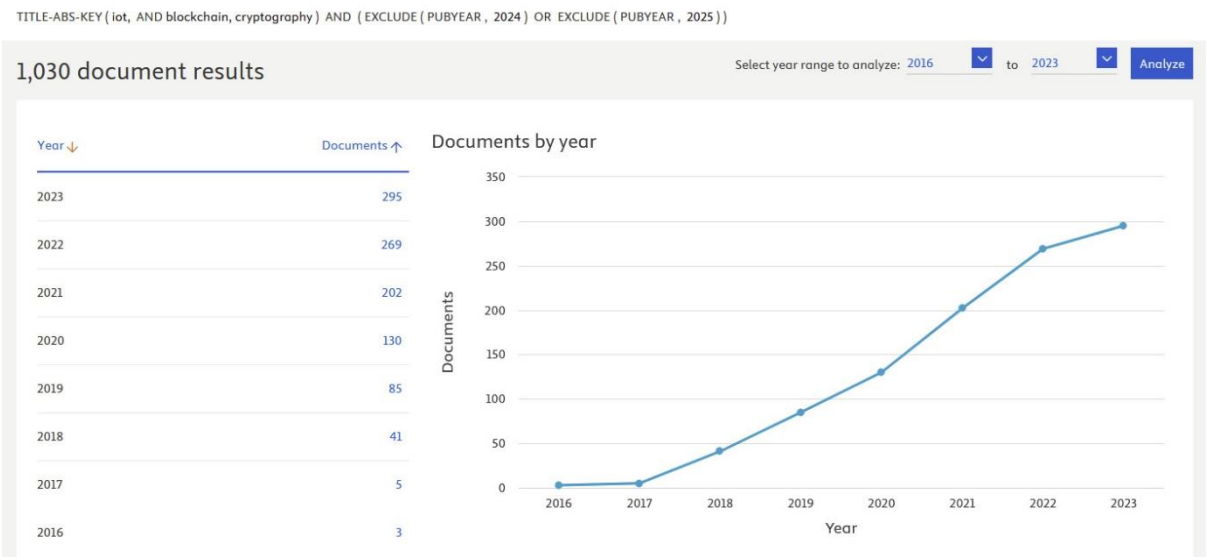

Figure 1.

In 2016, the research activity in this field was minimal, with only 3 documents published. The number remained low in 2017 with 5 documents, indicating that the integration of blockchain and cryptography into IoT security was still at an early exploratory stage. However, from 2018 onwards, the field started to gain momentum, with 41 documents published in 2018 and 85 in 2019. This upward trajectory suggests a growing recognition of the critical role that blockchain and cryptographic methods can play in enhancing IIoT security frameworks.

A more substantial growth phase began in 2020, with 130 publications, which then accelerated significantly to 202 documents in 2021. The number further increased to 269 documents in 2022, reaching a peak of 295 documents in 2023. This pattern reflects the escalating demand for secure, reliable, and decentralized solutions to protect IIoT systems against emerging cyber threats, particularly as industries increasingly adopt connected and automated technologies.

Overall, the trend visualized in the figure underscores the dynamic and rapidly evolving nature of research focused on fortifying Industrial IoT environments. It highlights an expanding academic and industrial effort to explore blockchain-enabled security mechanisms and lightweight cryptographic solutions. This bibliometric trend analysis confirms the relevance and timeliness of conducting a comprehensive review focusing on cryptographic and blockchain innovations for strengthening IIoT security.

4. Conclusion

Industrial Internet of Things (IIoT) security is becoming a crucial challenge as the adoption of connectivity technologies in the industrial sector increases. This study has comprehensively reviewed various cryptographic techniques and blockchain-based solutions developed to strengthen IIoT security, through a combination of bibliometric analysis and Systematic Literature Review (SLR). The results show that lightweight cryptography-based approaches and decentralized blockchain frameworks are the main focus in an effort to overcome resource limitations and improve the reliability of IIoT systems. The significant research growth trend

from 2016 to 2023 signifies the importance of innovation in this area, with intensified international collaboration.

While much progress has been made, the study identifies several key challenges that remain to be addressed, including the need for more energy-efficient security protocols, more seamless system integration, and validation of solutions in real industrial scenarios. In addition, there is still a need to explore hybrid security models that combine the advantages of cryptography and blockchain. This research provides a clear roadmap for the future development of IIoT security solutions, as well as a basis for further experimental studies. Thus, strengthening IIoT security through this innovative approach is an important step in realizing a smart, secure, and sustainable industrial system.

References

[1] Babayiğit, B., & Abubaker, M. (2023). Industrial Internet of Things: A Review of Improvements Over Traditional SCADA Systems for Industrial Automation. *IEEE Systems Journal*, 18(1), 120-133. https://doi.org/10.1109/jsyst.2023.3270620

[2] Τσίκνας, Κ., Taketzis, D., Demertzis, K., & Skianis, C. (2021). Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures. *IoT*, 2(1), 163-186. https://doi.org/10.3390/iot2010009

[3] Latif, S., Idrees, Z., Huma, Z. e, & Ahmad, J. (2021). Blockchain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions. *Transactions on Emerging Telecommunications Technologies*, 32(11). https://doi.org/10.1002/ett.4337

[4] Thakor, V. A., Razzaque, M. A., & Khandaker, M. R. A. (2021). Lightweight Cryptography Algorithms for Resource-Constrained IoT Devices: A Review, Comparison and Research Opportunities. *IEEE Access*, 9, 28177-28193. https://doi.org/10.1109/access.2021.3052867

[5] Kuang, J., Guo, Y., & Li, L. (2023). IIoTBC: A Lightweight Block Cipher for Industrial IoT Security. *KSII Transactions on Internet and Information Systems*, 17(1). https://doi.org/10.3837/tiis.2023.01.006

[6] Zheng, Y., & Chang, C.-H. (2021). Secure Mutual Authentication and Key-Exchange Protocol between PUF-Embedded IoT Endpoints. *2022 IEEE International Symposium on Circuits and Systems (ISCAS)*, 1-5. https://doi.org/10.1109/iscas51556.2021.9401135

[7] Li, R., Qin, Y., Wang, C., Li, M., & Chu, X. (2022). A Blockchain-Enabled Framework for Enhancing Scalability and Security in IIoT. *IEEE Transactions on Industrial Informatics*, 19(6), 7389-7400. https://doi.org/10.1109/tii.2022.3210216

[8] Na, D., & Park, S. (2021). Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy. *Electronics*, 10(4), 391-391. https://doi.org/10.3390/electronics10040391

[9] Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT. *IEEE Journal on Selected Areas in Communications*, 38(5), 942-954. https://doi.org/10.1109/jsac.2020.2980916

[10] Jayalaxmi, P. L. S., Saha, R., Kumar, G., Kumar, N., & Kim, T. (2021). A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges. *IEEE Access*, 9, 25344-25359. https://doi.org/10.1109/access.2021.3057766

[11] Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., & Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, 133, 285-296. https://doi.org/10.1016/j.jbusres.2021.04.070

[12] Zubaydi, H. D., Varga, P., & Molnár, S. (2023). Leveraging Blockchain Technology for Ensuring Security and Privacy Aspects in Internet of Things: A Systematic Literature Review. *Sensors*, 23(2), 788-788. https://doi.org/10.3390/s23020788

[13] Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. *IEEE Wireless Communications*, 25(6), 12-18. https://doi.org/10.1109/mwc.2017.1800116

[14] Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., Huang, X., & Nepal, Surya. (2021). Blockchain-Based Secure and Lightweight Authentication for Internet of Things. *IEEE Internet of Things Journal*, 9(5), 3321-3332. https://doi.org/10.1109/jiot.2021.3098007