JURNAL ILMU KOMPUTER
Volume 3 Nomor 1, Juli, 2025
ISSN: 3031-125X (ONLINE)
Penerbit: Program Studi Teknik Informatika S-2 Universitas Pamulang

A Review: Cyberattack Detection on IoT Devices in the Context of Large Data Volumes and Network Complexity

Mohammad Fachrudin Zikrullah [1], Tukiyat [2], Murni Handayani[3]
[1,2,3] Program Studi Teknik Informatika S-2, Universitas Pamulang
Email: [1]mochamadfachrudin@gmail.com, [2]dosen02711@unpam.ac.id , [3]murnie_h@yahoo.com

ABSTRACT

The Internet of Things (IoT) has become an essential part of everyday life, enabling devices to communicate and work together seamlessly, boosting productivity, efficiency, and convenience across various domains such as healthcare, transportation, manufacturing, and smart homes. However, as IoT adoption grows rapidly, so do the challenges related to cybersecurity. The vast amounts of data generated by these devices and the increasing complexity of IoT networks create vulnerabilities that cybercriminals are quick to exploit. Factors like the diversity of IoT devices, differing communication protocols, and inconsistent security standards only add to the problem. Cyberattacks such as Distributed Denial of Service (DDoS), malware, and data sniffing are becoming increasingly sophisticated, threatening the security and functionality of IoT ecosystems. To combat these issues, it is crucial to develop robust and adaptive methods that can detect and mitigate these threats in real-time. This paper reviews current methods for detecting cyberattacks on IoT devices, with a focus on integrating machine learning, data analytics, and blockchain technologies. Traditional rule-based systems, while effective against known threats, struggle to keep up with the complexity and ever-evolving nature of modern cyberattacks. Machine learning techniques, especially deep learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, have shown exceptional capabilities in analyzing large datasets to identify patterns and anomalies. Additionally, blockchain technology offers enhanced security through its decentralized and tamper-resistant nature, ensuring data integrity across IoT networks. The study explores IoT-related threats, discusses methodologies to counter them, and presents case studies to highlight the practical application of these advanced techniques. It emphasizes the need for scalable, efficient, and adaptable solutions to secure IoT ecosystems against the growing sophistication of cyber threats.

Keywords: IoT Security, Cyberattack Detection, Machine Learning, Deep Learning, Blockchain, Network Complexity, Large Data Volumes.

ABSTRAK

Internet of Things (IoT) telah menjadi bagian yang tak terpisahkan dari kehidupan sehari-hari, memungkinkan perangkat untuk saling terhubung dan bekerja sama secara efisien. Teknologi ini telah membawa banyak manfaat, seperti meningkatkan produktivitas, kenyamanan, dan efisiensi di berbagai bidang, mulai dari kesehatan, transportasi, hingga rumah pintar. Namun, seiring dengan meningkatnya penggunaan IoT, tantangan keamanan siber juga semakin kompleks. Data yang dihasilkan oleh perangkat IoT dalam jumlah besar, ditambah dengan keragaman perangkat dan protokol komunikasi, menciptakan celah yang rawan dieksploitasi oleh pelaku kejahatan siber. Serangan seperti Distributed Denial of Service (DDoS), malware, hingga penyadapan data menjadi semakin canggih dan mengancam keamanan serta fungsi ekosistem IoT. Untuk menghadapi ancaman ini, diperlukan pendekatan yang mampu mendeteksi dan menangani serangan secara cepat dan efektif. Jurnal ini membahas berbagai metode untuk mendeteksi serangan siber pada perangkat IoT, dengan fokus pada penggunaan pembelajaran mesin, analitik data, dan teknologi blockchain. Pendekatan tradisional berbasis aturan sering kali tidak cukup fleksibel untuk menghadapi ancaman siber modern yang terus berkembang. Di sisi lain, pembelajaran mesin, terutama model deep learning seperti Convolutional Neural Networks (CNNs) dan Long Short-Term Memory (LSTM), telah terbukti mampu menganalisis data besar dengan sangat baik untuk mendeteksi pola dan anomali. Selain itu, blockchain memberikan keamanan tambahan melalui sistem yang terdesentralisasi dan sulit dimanipulasi, sehingga memastikan data tetap aman dalam jaringan IoT. Makalah ini juga

menyertakan studi kasus untuk menunjukkan bagaimana metode-metode ini dapat diterapkan secara praktis. Dengan pendekatan yang skalabel, efisien, dan adaptif, ekosistem IoT dapat dilindungi dari ancaman siber yang terus berkembang..

Kata kunci : Keamanan IoT, Deteksi Serangan Siber, Pembelajaran Mesin, Deep Learning, Blockchain, Kompleksitas Jaringan, Volume Data Besar..

1. INTRODUCTION

The Internet of Things (IoT) has revolutionized the way we live and work, bringing smart devices into various industries such as healthcare, transportation, agriculture, and manufacturing. These devices enable real-time data sharing and automation, boosting efficiency and innovation on an unprecedented scale [1], [2]. From wearable health monitors to smart home systems and intelligent industrial tools, IoT has become a vital component of modern infrastructure. However, as IoT adoption continues to grow, it also introduces significant cybersecurity challenges. These challenges stem from the diverse range of IoT devices, inconsistent security protocols, and the decentralized nature of IoT networks, making them prime targets for cyberattacks .

One of the biggest concerns in IoT environments is the sheer volume of data generated by these interconnected systems. While this data is essential for driving analytics and decision-making, it also opens the door for exploitation by cybercriminals. Attacks such as Distributed Denial of Service (DDoS), ransomware, and data sniffing have become more sophisticated, targeting IoT networks to steal sensitive information or disrupt operations [3], [4]. Many IoT devices, ranging from simple sensors to advanced systems, are also limited by their computational resources, making it challenging to implement robust security measures [2], [5]. These factors highlight the urgent need for security solutions that are not only scalable but also adaptive to evolving threats.

Traditional security measures, such as rule-based intrusion detection systems, have struggled to keep up with the ever-changing nature of cyber threats. While these methods are effective for known attacks, they often fail to detect zero-day vulnerabilities or handle large-scale attacks in complex environments [5], [6]. This has led researchers to explore advanced solutions, particularly those powered by machine learning. Deep

learning models like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks have shown great potential in detecting patterns and anomalies in large datasets, making them ideal for securing IoT systems [1], [7]. Hybrid approaches that combine optimization algorithms, such as Harris Hawks Optimization, with machine learning techniques have further enhanced the accuracy and adaptability of intrusion detection systems [5].

Blockchain technology has also emerged as a promising solution to strengthen IoT security. With its decentralized and tamper-resistant structure, blockchain ensures data integrity and enables secure data exchanges, reducing the risks associated with centralized vulnerabilities [8], [9]. When integrated with machine learning, blockchain can form a robust security framework, improving the resilience of IoT networks against sophisticated cyber threats [2], [10]. Furthermore, emerging technologies like generative AI and large language models are beginning to play a complementary role in analyzing and detecting threats more effectively [1].

This study aims to explore advanced methods for detecting and mitigating cyberattacks on IoT systems. By leveraging machine learning, blockchain, and advanced analytics, this research seeks to address the limitations of traditional approaches and propose innovative, scalable solutions. The findings aim to provide actionable insights for strengthening IoT security, ensuring these systems remain efficient and resilient against ever-evolving cyber threats.

2. LITERATUR REVIEW

The rapid growth of IoT networks has brought immense benefits by enabling seamless connectivity and automation. However, this expansion has also introduced significant security risks. Among the most prominent threats are Distributed Denial of Service (DDoS) attacks, which use compromised IoT devices to flood networks with malicious traffic, disrupting operations and overwhelming systems [11]. Malware poses another major concern, targeting vulnerabilities in IoT firmware to gain control over devices, steal data, or even deploy ransomware. Additionally, sniffing and spoofing attacks compromise the integrity of IoT communications by intercepting or altering sensitive data, a particularly critical issue in sectors like healthcare and smart grids [12].

These evolving threats highlight the need for comprehensive strategies to secure IoT ecosystems effectively.

A secure communication framework is essential for IoT networks to function effectively. However, many IoT devices still rely on outdated or inadequate encryption protocols, leaving data exchanges vulnerable to interception. Weak authentication mechanisms, such as default or hardcoded passwords, further exacerbate these vulnerabilities, making unauthorized access alarmingly easy [13], [14], [15]. The decentralized and heterogeneous nature of IoT systems complicates matters, as the lack of uniform security standards creates gaps that attackers can exploit [16]. Without robust solutions to address these communication vulnerabilities, IoT networks will remain highly susceptible to attacks, compromising both privacy and system integrity across connected ecosystems.

Traditional rule-based intrusion detection systems (IDS) have been widely used to secure IoT networks. These systems rely on predefined rules and signatures to detect malicious activity. While effective against known threats, they are often ill-equipped to handle modern challenges such as zero-day exploits and the sheer volume of data generated by IoT devices [17]. Moreover, the complexity of IoT networks and the resource limitations of many devices exacerbate the shortcomings of these systems, leading to inefficiencies and high false-positive rates [8], [14], [18], [19], [20]. As IoT ecosystems continue to expand, the need for more adaptive and scalable detection methods becomes increasingly apparent.

To address the limitations of traditional systems, modern approaches leverage advanced technologies like machine learning and deep learning. These technologies enable real-time detection of threats by analyzing patterns and anomalies in large datasets. Deep learning models, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, are particularly effective at identifying complex attack signatures, offering a proactive approach to threat detection [21]. Additionally, unsupervised learning methods, such as clustering algorithms, allow for the detection of previously unknown threats by analyzing unlabeled data [22]. These innovations significantly improve detection accuracy while reducing false-positive rates, making them invaluable tools for securing IoT environments.

Blockchain technology has emerged as a promising solution to enhance IoT security. Its decentralized and tamper-resistant nature ensures that data exchanged between devices remains secure and trustworthy. Smart contracts, a feature of blockchain, enable automated and secure interactions between devices, reducing the risks of human error and unauthorized access [23]. Blockchain has proven particularly useful in applications like logistics and supply chains, where the integrity of data is paramount [24]. By addressing single points of failure in centralized systems, blockchain strengthens IoT security frameworks and ensures the integrity and authenticity of device communications [25].

Emerging technologies like generative AI and edge computing are further transforming the IoT security landscape. Generative AI can simulate complex attack scenarios, enhancing the training of detection systems and improving preparedness against evolving threats [26]. Edge computing, which processes data closer to its source, reduces latency and bandwidth requirements, making it particularly effective for resource-constrained IoT environments [27]. Together, these advancements hold great promise for building more resilient and adaptive IoT security frameworks. Future research should focus on integrating these technologies into cohesive solutions that balance scalability, efficiency, and real-time performance.

3. Methodology

This study employs a methodology designed to tackle the unique challenges of securing IoT networks, focusing on scalability, adaptability, and real-time responsiveness. The system architecture is built around three main components: IoT sensors, data gateways, and analytic servers. IoT sensors are responsible for collecting data from their environment, capturing parameters such as temperature, movement, or system activity. This data is transmitted to gateways, which serve as intermediaries to preprocess and forward the information to analytic servers. These servers, equipped with advanced computational capabilities, analyze the data in real time, enabling the swift detection of anomalies and potential cyber threats. The data flow across these components is carefully structured to support real-time processing, ensuring rapid identification and response to any security issues.

Data collection and processing play a crucial role in this methodology. The study utilizes a combination of simulated datasets, which allow controlled testing, and real-world IoT datasets that reflect practical conditions and challenges. To optimize the analysis, preprocessing techniques such as normalization and dimensionality reduction are applied. Normalization ensures that data from different sources is consistent and comparable by standardizing it to a common scale. Dimensionality reduction simplifies complex datasets by removing redundant or less significant features, improving the efficiency of the analysis while preserving critical information. These steps are essential for handling the large and diverse datasets typical of IoT environments.

For threat detection, the study incorporates advanced machine learning models, particularly deep learning techniques. Convolutional Neural Networks (CNNs) are used for spatial data processing, making them well-suited for identifying visual patterns and spatial relationships within IoT-generated data. Recurrent Neural Networks (RNNs) are employed to analyze sequential data, capturing temporal patterns in IoT communications. Long Short-Term Memory (LSTM) networks, a type of RNN designed to manage long-term dependencies, are particularly effective in detecting anomalies that develop over extended time periods. These models work together to ensure a comprehensive analysis of both immediate and historical data, enhancing the system's ability to identify complex threats.

Unsupervised learning techniques also play a key role in the detection process. Clustering algorithms such as K-Means are used to group similar data points and identify outliers or anomalies that deviate from expected patterns. This approach is especially valuable in IoT security, where many threats are previously unknown or lack labeled data for training it also enables the detection of new attack vectors, providing an additional layer of protection for IoT networks. This creates a scalable and adaptive framework for securing IoT ecosystems. The integration of both simulated and real-world datasets ensures that the system is not only theoretically sound but also practical and effective in addressing real-world security challenges. This approach provides a strong foundation for protecting IoT networks against an increasingly complex and evolving threat landscape.

4. DISCUSSION

Research indicates that machine learning-based approaches outperform traditional methods in detecting cyberattacks on IoT networks. Unlike rule-based systems, which rely on predefined signatures and patterns, machine learning algorithms adapt to evolving threats by analyzing large volumes of data and identifying anomalies in real-time. This adaptability makes them particularly effective in the dynamic and complex environments characteristic of IoT ecosystems. Machine learning techniques, such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, have demonstrated high accuracy in detecting sophisticated attack patterns, further solidifying their superiority over traditional detection methods.

Technologies like deep learning and blockchain hold immense potential for enhancing IoT security. Deep learning models can process vast amounts of high-dimensional data to detect complex and previously unknown threats. At the same time, blockchain offers a decentralized and tamper-resistant framework for securing data exchanges within IoT networks. Blockchain's ability to ensure data integrity and authenticity makes it a valuable tool for preventing unauthorized access and mitigating single points of failure. However, implementing these technologies comes with significant challenges. Both deep learning and blockchain require substantial computational power, energy resources, and infrastructure, which can be difficult to achieve in IoT environments characterized by resource-constrained devices with limited processing and power capabilities.

Given these challenges, further research is needed to develop resource-efficient solutions tailored for IoT devices with limited computational and energy capacities. Innovations in lightweight machine learning models, such as pruning or quantization techniques, could reduce the computational requirements of deep learning algorithms while maintaining their effectiveness. Similarly, advancements in blockchain technologies, such as lightweight consensus algorithms, could make them more suitable for IoT applications without compromising security. Exploring hybrid approaches that integrate machine learning and blockchain in an optimized manner also holds promise for creating scalable and energy-efficient IoT security frameworks.

Additionally, future studies should focus on practical deployment strategies that balance security with performance and cost. Real-world implementations often face constraints related to hardware, network latency, and energy consumption. Addressing these challenges requires interdisciplinary collaboration between researchers, engineers, and industry stakeholders to ensure that proposed solutions are not only robust but also feasible for widespread adoption. By focusing on resource efficiency and adaptability, these advancements can bridge the gap between cutting-edge security technologies and the practical needs of IoT networks.

5. Conclusion and Recommendations

The rapid integration of IoT into industries like healthcare, transportation, and manufacturing has revolutionized how we work and live. IoT has enabled real-time data sharing, advanced automation, and improved efficiency, offering immense benefits across various sectors. However, this widespread adoption has also introduced significant cybersecurity challenges, including Distributed Denial of Service (DDoS) attacks, malware threats, and communication vulnerabilities. Traditional rule-based security systems, while useful for addressing known threats, struggle to cope with modern, sophisticated cyberattacks. As IoT networks grow more complex, the need for advanced, adaptive, and scalable security solutions has become urgent. Machine learning, particularly deep learning techniques like Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) networks, has shown great promise in identifying complex attack patterns and anomalies. At the same time, blockchain technology offers a decentralized and tamper-resistant framework that secures data exchanges and ensures integrity. Despite these advancements, implementing such technologies is challenging due to the significant computational and energy demands, making them less practical for resource-constrained IoT devices. Finding ways to overcome these limitations is essential to creating more robust security solutions.

To address these challenges, several steps should be taken to guide future developments in IoT security. First, it is crucial to develop resource-efficient solutions by focusing on lightweight machine learning models that reduce computational demands without sacrificing performance. Techniques like pruning and quantization can be instrumental in this regard. Similarly, advancements in blockchain technology, such as

lightweight consensus mechanisms, should be explored to make them more feasible for IoT applications with limited resources. Second, real-world implementation strategies must be prioritized to address practical challenges such as hardware constraints, latency, and energy consumption. These considerations will help ensure that advanced solutions can be effectively deployed across diverse IoT environments.

Third, collaboration across disciplines is essential. Researchers, engineers, policymakers, and industry stakeholders must work together to align security solutions with practical needs and industry standards. This collaborative approach will ensure that new technologies are not only innovative but also realistic for widespread adoption. Fourth, hybrid solutions that combine the strengths of machine learning and blockchain technology should be explored. By integrating the predictive power of machine learning with the data integrity and decentralized nature of blockchain, these hybrid models can provide comprehensive security frameworks that are both adaptive and reliable. Finally, emerging technologies like generative AI and edge computing hold significant potential to further enhance IoT security. Generative AI can simulate diverse attack scenarios, improving preparedness, while edge computing allows for faster and more efficient data processing closer to the source, reducing strain on centralized systems.

By addressing these recommendations, IoT systems can become more secure, efficient, and resilient against evolving cyber threats. Bridging the gap between cutting-edge innovations and practical, real-world deployment will pave the way for robust, scalable, and adaptive IoT security frameworks, ensuring that the transformative potential of IoT is fully realized in a safe and secure manner.

6. DAFTAR PUSTAKA

[1] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, “Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models,” *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167–185, Jan. 2024, doi: 10.1016/J.IOTCPS.2023.12.003.

[2] A. Bhardwaj, S. Bharany, A. W. Abulfaraj, A. Osman Ibrahim, and W. Nagmeldin, “Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection

strategies for smart cities," *Egyptian Informatics Journal*, vol. 25, no. December 2023, p. 100443, 2024, doi: 10.1016/j.eij.2024.100443.

[3] S. K. Dash *et al.*, "Enhancing DDoS attack detection in IoT using PCA," *Egyptian Informatics Journal*, vol. 25, no. August 2023, p. 100450, 2024, doi: 10.1016/j.eij.2024.100450.

[4] A. Alzahrani and M. Z. Asghar, "Cyber vulnerabilities detection system in logistics-based IoT data exchange," *Egyptian Informatics Journal*, vol. 25, no. September 2023, p. 100448, 2024, doi: 10.1016/j.eij.2024.100448.

[5] M. Alazab, R. Abu Khurma, P. A. Castillo, B. Abu-Salih, A. Martín, and D. Camacho, "An effective networks intrusion detection approach based on hybrid Harris Hawks and multi-layer perceptron," *Egyptian Informatics Journal*, vol. 25, no. December 2023, p. 100423, 2024, doi: 10.1016/j.eij.2023.100423.

[6] H. Harb *et al.*, "An intelligent optimization strategy for nurse-patient scheduling in the Internet of Medical Things applications," *Egyptian Informatics Journal*, vol. 25, no. August 2023, p. 100451, 2024, doi: 10.1016/j.eij.2024.100451.

[7] B. Amma N.G., "En-RfRsK: An ensemble machine learning technique for prognostication of diabetes mellitus," *Egyptian Informatics Journal*, vol. 25, no. March 2023, p. 100441, 2024, doi: 10.1016/j.eij.2024.100441.

[8] S. Asaithambi, L. Ravi, M. Devarajan, A. S. Almazyad, G. Xiong, and A. W. Mohamed, "Enhancing enterprises trust mechanism through integrating blockchain technology into e-commerce platform for SMEs," *Egyptian Informatics Journal*, vol. 25, no. December 2023, p. 100444, 2024, doi: 10.1016/j.eij.2024.100444.

[9] J. K. Adeniyi *et al.*, "A biometrics-generated private/public key cryptography for a blockchain-based e-voting system," *Egyptian Informatics Journal*, vol. 25, no. December 2023, p. 100447, 2024, doi: 10.1016/j.eij.2024.100447.

[10] S. Sadhwani, U. K. Modi, R. Muthalagu, and P. M. Pawar, "SmartSentry: Cyber Threat Intelligence in Industrial IoT," *IEEE Access*, vol. 12, no.

December 2023, pp. 34720–34740, 2024, doi: 10.1109/ACCESS.2024.3371996.

[11] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial iot, cyber threats, and standards landscape: Evaluation and roadmap," *Sensors*, vol. 21, no. 11, pp. 1–30, 2021, doi: 10.3390/s21113901.

[12] E. Dolan and R. Widayanti, "Implementation of Authentication Systems on Hotspot Network Users to Improve Computer Network Security," *International Journal of Cyber and IT Service Management*, vol. 2, no. 1, pp. 88–94, 2022, doi: 10.34306/ijcitsm.v2i1.93.

[13] A. B. Li, H. Chen, and X. L. Xie, "Visible watermarking for 3D models based on 3D Boolean operation," *Egyptian Informatics Journal*, vol. 25, no. December 2023, 2024, doi: 10.1016/j.eij.2023.100436.

[14] Z. Guo, H. Li, and K. Li, "Dual subpopulation artificial bee colony algorithm based on individual gradation," *Egyptian Informatics Journal*, vol. 25, no. September 2023, p. 100452, 2024, doi: 10.1016/j.eij.2024.100452.

[15] W. Li, H. Li, Y. Wang, and Y. Han, "Optimizing flexible job shop scheduling with automated guided vehicles using a multi-strategy-driven genetic algorithm," *Egyptian Informatics Journal*, vol. 25, no. December 2023, p. 100437, 2024, doi: 10.1016/j.eij.2023.100437.

[16] R. D. Hapsari and K. G. Pambayun, "ANCAMAN CYBERCRIME DI INDONESIA: Sebuah Tinjauan Pustaka Sistematis," *Jurnal Konstituen*, vol. 5, no. 1, pp. 1–17, Oct. 2023, doi: 10.33701/jk.v5i1.3208.

[17] S. Mishra, A. Albarakati, and S. K. Sharma, "Cyber Threat Intelligence for IoT Using Machine Learning," *Processes*, vol. 10, no. 12, 2022, doi: 10.3390/pr10122673.

[18] F. Guo and H. Li, "A niche-based evolutionary algorithm with dual cooperative archive for solving constrained multi-objective optimization problems," *Egyptian Informatics Journal*, vol. 25, no. September 2023, p. 100422, 2024, doi: 10.1016/j.eij.2023.100422.

[19] M. Zhu, J. Jiang, and W. Gao, "A fast ADMM algorithm for sparse precision matrix estimation using lasso penalized D-trace loss," *Egyptian Informatics*

Journal, vol. 25, no. December 2023, p. 100425, 2024, doi: 10.1016/j.eij.2023.100425.

[20] W. Xiong, D. Zhu, R. Li, Y. Yao, C. Zhou, and S. Cheng, "An effective method for global optimization – Improved slime mould algorithm combine multiple strategies," *Egyptian Informatics Journal*, vol. 25, no. September 2023, p. 100442, 2024, doi: 10.1016/j.eij.2024.100442.

[21] F. H. Almukhtar, S. Wahhab Kareem, and F. Sami Khoshaba, "Design and development of an effective classifier for medical images based on machine learning and image segmentation," *Egyptian Informatics Journal*, vol. 25, no. March 2023, p. 100454, 2024, doi: 10.1016/j.eij.2024.100454.

[22] A. Neelkanth Chaudhari, "Cyber Physical Recommender Systems for IoT Based Applications," *American Journal of Science, Engineering and Technology*, vol. 5, no. 2, p. 82, 2020, doi: 10.11648/j.ajset.20200502.14.

[23] H. M. Reeve, A. M. Mescher, and A. F. Emery, "Experimental and numerical investigation of polymer preform heating," *American Society of Mechanical Engineers, Heat Transfer Division, (Publication) HTD*, vol. 369, no. 6, pp. 321–332, 2001, doi: 10.1115/imece2001/htd-24365.

[24] Z. Li *et al.*, "A Cyber-Physical Traffic Signaling System for Controlled Waterway in Inland River Based on Edge-centric IoT A Cyber-Physical Tra ffi c Signaling System for Controlled Waterway in Inland River Based on Edge-centric IoT," 2023.

[25] M. Es-sabry *et al.*, "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," *Egyptian Informatics Journal*, vol. 25, no. September 2023, p. 100449, 2024, doi: 10.1016/j.eij.2024.100449.

[26] S. Kumari, V. Tulshyan, and H. Tewari, "Cyber Security on the Edge: Efficient Enabling of Machine Learning on IoT Devices," *Information (Switzerland)*, vol. 15, no. 3, pp. 1–28, 2024, doi: 10.3390/info15030126.

[27] N. Wirtz *et al.*, *Securing CEI "By-Design."* 2021. doi: 10.1561/9781680836875.ch14.