DOI: 10.37943/22DOKU3034

Tamara Zhukabayeva
PhD, Professor, Department of Information Systems
zhukabayeva_tk@enu.kz, orcid.org/0000-0001-6345-5211
L.N. Gumilyov Eurasian National University, Kazakhstan

Aigul Adamova
PhD, Researcher, Department of Computer Science
Aigul.adamova@astanait.edu.kz, orcid.org/0000-0001-7773-9522
L.N. Gumilyov Eurasian National University, Kazakhstan

Assel Abdildayeva
PhD, Researcher
abass_81@mail.ru, orcid.org/0000-0002-6381-9350
L.N. Gumilyov Eurasian National University, Kazakhstan

Nurdaulet Karabayev
PhD student, Department of Information Systems
020419501012@enu.kz, orcid.org/0009-0008-6532-6382
L.N. Gumilyov Eurasian National University, Kazakhstan

EVALUATING AN ANALYTICAL MODEL OF CYBERATTACK EFFECTS ON AN IIoT SYSTEM WITH EDGE COMPUTING CAPABILITIES

Abstract: The Industrial Internet of Things (IIoT) is an important component of future industrial systems. Implementing edge computing in the IIoT can significantly reduce decision latency, save bandwidth resources, and protect privacy to some extent. But it is important to realize that edge computing is often resource-constrained, and devices are often spread across vast geographic areas, including intermittent network connectivity. Such conditions increase security vulnerabilities due to increased attack surfaces and physical availability. This paper addresses the problem of securing IIoT systems utilizing the concept of edge computing. An analytical model of attack influences is proposed, including typical scenarios and individual steps of attacks, both physical and software-informational in nature. The presented analytical model is designed to assess and analyze attack impacts on IIoT, implements the concept of boundary calculations, allows to analyze vulnerabilities of IIoT systems more effectively and develop measures to protect them. The model is designed to provide a comprehensive tool for securing critical infrastructures. The model includes typical attack scenarios, detailed attack steps, and impact classification. The developed model can be used for risk analysis, development of protection strategies, and security testing of IIoT systems. The conducted experimental study confirmed the relevance and practical significance of the developed model. The results of the study showed that IIoT-systems using edge computing are subject to a wide range of threats. The most critical are DoS attacks and Data Integrity Attacks. The obtained results emphasize the need to apply comprehensive security measures for IIoT systems with edge computing and confirm the effectiveness of the proposed analytical model.

Keywords: Industrial Internet of Things; edge computing; cybersecurity; threat model; attacks; physical attacks; software and information attacks; analytical model.

Received: 18.03.2025 Accepted: 24.06.2025 Published: 30.06.2025

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

Introduction

The Industrial Internet of Things (IIoT) plays a key role in the digital transformation of industry, enabling automation, optimization and control of production processes. The concept of edge computing, which involves processing data directly at the edge of the network, close to the data sources, reduces latency, reduces the load on centralized servers, and increases system autonomy. Figure 1 provides a graphical representation of the concept of edge computing. However, the distributed nature of edge computing and tight integration with physical devices create new challenges in cybersecurity.

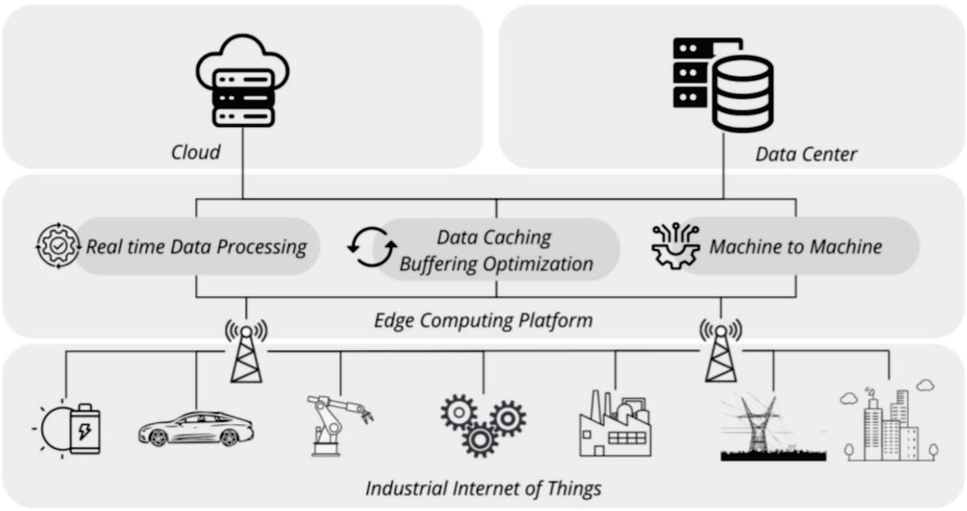

Figure 1. The concept of edge computing in the IIoT ecosystem

IIoT devices located at the edge of the network often have limited computing resources and may be physically vulnerable. This makes them an attractive target for attackers. Attacks on IIoT systems can have serious consequences such as disrupting production, damaging equipment, leaking sensitive information, and even jeopardizing the safety of personnel. Figure 2 summarizes the security issues and measures relative to each layer of the IIoT architecture. In this regard, the development of effective threat models and protection methods for IIoT systems using edge computing is an urgent task.

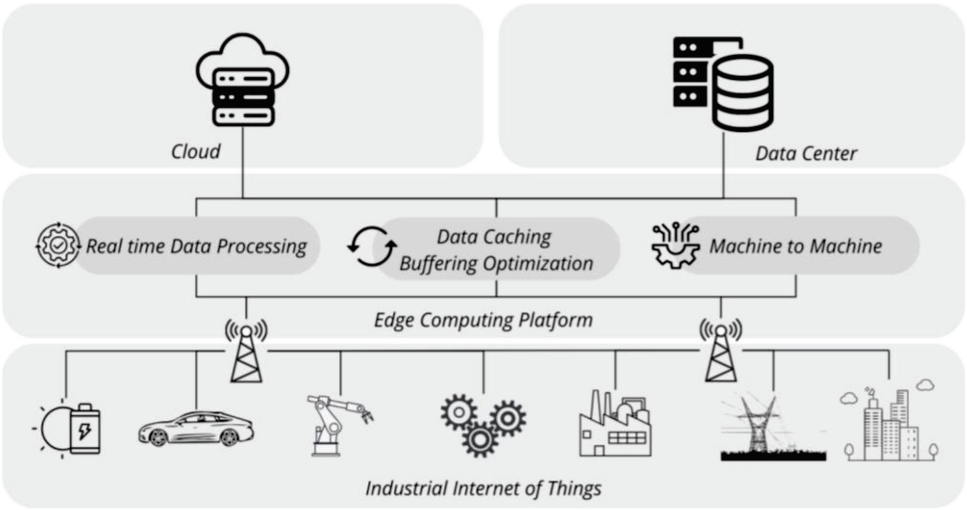

Figure 2. IIoT layered architecture, Security Issues and Security Measures

DOI: 10.37943/22DOKU3034

Edge computing contributes to the IIoT by decentralizing data processing, reducing latency, optimizing throughput, and improving reliability. They support real-time decision making in industrial applications by addressing issues such as hardware limitations and network security, providing scalability and enhanced data privacy [1]. The purpose of the proposed research is to build an analytical model of attack impacts on an IIoT system that realizes the concept of edge computing. The main contribution of the authors can be listed as follows:

- the proposed analytical model and experimental research methodology for IIoT systems;
- accounting for the impact of attacks on response time, data integrity, throughput, and loss metrics;
- design and implementation of an experimental environment with containerized services, attack simulation tools and telemetry to empirically test the adequacy of the proposed model.

The presented research is organized as follows, chapter two presents an analysis of existing approaches and an overview of current research, chapter three presents descriptions of the attacks under study, chapter four describes the proposed analytical model, description of the experimental study and results are presented in section five and conclusions with future vision are described in the conclusion.

Methods and Materials

Analysis of existing approaches

Existing approaches to threat modeling for IIoT are often based on generic cybersecurity models such as STRIDE [2], DREAD [3], and MITRE ATT&CK [4] (Figure 3). However, the specifics of IIoT related to the use of edge computing and interaction with the physical world require the development of specialized models.

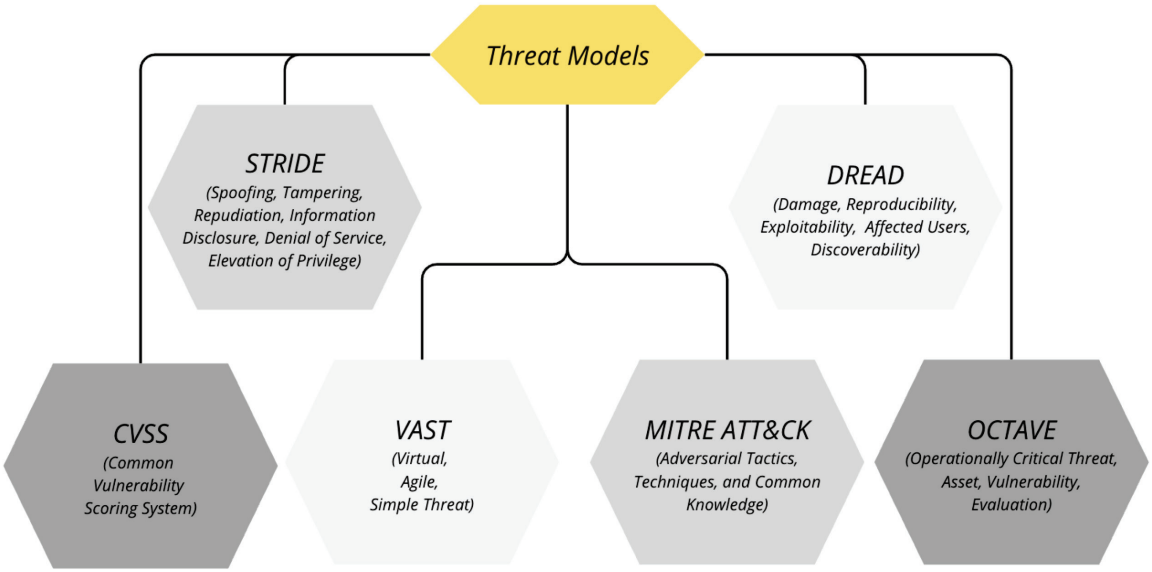

Figure 3. Common IIoT cybersecurity models

Some studies focus on specific types of attacks, such as denial of service (DoS) attacks, data integrity attacks, and privacy attacks [5], [6]. However, a comprehensive analysis that considers the interaction of different types of attacks and their impact on the system as a whole remains understudied. A systematic literature review of the last five years presents the security challenges associated with IIoT and edge computing, the types of attacks targeting these systems, and new solutions to mitigate the threats considered.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

The convergence of IIoT and edge computing presents a unique set of security challenges. IIoT systems, characterized by their interconnectivity and dependence on distributed devices, are inherently vulnerable to cyberattacks. Peripheral computing, while offering benefits such as reduced latency and increased efficiency, also expands the attack surface, making it a prime target for attackers [5], [6]. As already mentioned, the IIoT architecture consists of several layers, each with its own set of vulnerabilities. The perception layer, which is responsible for data collection, is often the target of attacks such as eavesdropping and data tampering. The network layer, which enables communication between devices, is susceptible to man-in-the-middle (MITM) and denial-of-service (DoS) attacks. The application layer that processes and analyzes data is vulnerable to malware and ransomware attacks [7], [8]. Edge computing, although complementary to IIoT, introduces additional security challenges. The distributed nature of edge computing makes it difficult to implement centralized security measures. Peripherals are often resource-constrained, making them an easy target for attackers. Common attacks on edge computing include third-party channel attacks, malware injection, and authentication and authorization attacks [9], [10]. Table 1 presents the works of researchers that propose methods to detect and prevent different types of attacks.

Table 1. Comparison of different types of attacks and methods

Work	Source, year	Type of attack	Method	Dataset	Limitations
[11]	IEEE Transactions on Industrial Informatics, 2022	Sybil	Federated Learning	-	Detection Vulnerability
[12]	IEEE Internet of Things Journal, 2023	DDoS	XGBoost CNN-LSTM	CICDDoS2019	Dataset Limitations
[13]	IEEE Access, 2021	DoS, Replay, False-Data-Injection	a digital signature-based security mechanism that offers authentication, integrity, and protection against cyber-attacks.	-	Protocol Vulnerabilities, Integration Challenges
[14]	IEEE Access, 2024	Replay, Jamming, Impersonation, MITM	a lightweight and efficient authentication framework		Scalability Issues
[15]	arXiv.Org, 2025	DDoS, MITM, Injection, Malware	an advanced IDS using a hybrid LSTM-CNN-Attention architecture	the Edge-IIoTset	lightweight architectures, model compression, federated learning
[16]	Arabian Journal for Science and Engineering, 2024	DoS, Advanced Persistent Threats, different types of cyber-attacks	Genetic Algorithms and Deep Learning	UNSW-NB 15	Dataset Limitations, Computational Complexity
[17]	arXiv.Org, 2024	Advanced Persistent Threats	featuring 20 attack techniques and invariant APT phases	CICAPT-IIoT	Dataset Imbalance, Dataset Imbalance

DOI: 10.37943/22DOKU3034

Work	Source, year	Type of attack	Method	Dataset	Limitations
[18]	Advances in Science and Engineering Technology International Conferences (ASET), 2024	MITM, Ransomware	Machine learning algorithms, logistic regression, decision tree, deep learning techniques, specifically recurrent, convolutional neural networks	Edge-IIoTset	Data Quality and Availability, Algorithmic Limitations, Computational Constraints
[19]	arXiv.Org, 2024	Backdoor, DDOS, MITM, Ransomware	Intrusion detection system	Edge-IIoTset	Limited attack types

IIoT and edge computing security is characterized by multiple attacks, each exploiting different vulnerabilities in the system architecture. The integration of IIoT and edge computing has led to significant security challenges that require robust solutions. The presented literature review explored the types of attacks targeting these systems, the vulnerabilities they exploit, and new solutions to mitigate these threats.

Description of attacks

DoS attacks are among the most common types of attacks targeting IIoT and edge computing systems. These attacks overwhelm the system with excessive traffic, leading to service disruption and potential system failures. In IIoT, DoS attacks can have serious consequences such as shutting down production lines or disrupting critical infrastructure [20], [21].

A DDoS attack on a victim server exhausts the resources of the target server, causing the victim server to refuse to connect to new legitimate clients. The server resource exhaustion can be either the throughput $P(\beta)$ or the buffer size of the victim server $P(M)$. Equation (1) gives the overall probability of resource exhaustion on the victim side [22].

$$T_D = 1 - \big(1 - P(\beta)\big)\big(1 - P(M)\big) \tag{1}$$

MITM attacks involve intercepting communication between two parties to steal sensitive information or inject malicious data. In the IIoT, MITM attacks can compromise the integrity of data transmitted between devices, leading to poor decisions or unauthorized access to sensitive information [23], [24]. The time complexity of the attack is represented by equation (2), where k_s, k_f, k_b are the three parts of the key: general, for forward and backward computation respectively and f is a factor that depends on the particular algorithm, together it takes into account the optimizations and reductions that can be applied in the attack process.

$$T_M = 2^{|k_s|+|k_b|} + 2^{|k_s|+|k_f|} + 2^{|k_s|+|k_b|+|k_f|-|f|} \tag{2}$$

Malware and ransomware attacks are increasingly targeting IIoT and edge computing systems. These attacks can compromise the functionality of industrial devices, leading to production stoppages or data breaches. Ransomware attacks, in particular, can have serious financial implications for industries, as attackers demand payment in exchange for restoring access to systems or data [25], [26]. Malware models describe the rate of change of states in a network, specifically device states relative to pre- and post-infection behavior. All devices representing the same state are grouped into a population with the same name, the size of which is tracked by the model. The malware dynamics $F(M[X])$ can be represented by formula (3), where $M[X]$ is a vector of states representing the size of different populations, is the current moment of discrete time.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

$$F(M[X]) = M[X+1] - M[X] \quad (3)$$

Side-Channel Attacks exploit information leaked from the system implementation rather than directly attacking the system itself. In edge computing, Side-Channel Attacks can target resource-constrained devices, compromising their security without directly compromising the system's defenses [27], [28]. Formula (4) represents a function that mathematically relates the measured data of a third-party channel to the inferred key, where: $C(t)$ is the measured data of the third-party channel, $L(k, x, t)$ is a function that models the behavior of the third-party channel depending on the assumed key k and input data x, S is a function that compares the measured and modeled data.

$$F(t, k) = S\big(C(t), L(k, x, t)\big) \quad (4)$$

Proposed analytical model

The proposed analytical model of attacking influences on IIoT-system, realizing the concept of edge computing, includes the following components: attack scenarios, individual attack steps, and types of influences (Figure 4). If attack scenarios represent the sequence of actions of an attacker to achieve a certain goal, then individual attack steps are the actions that are performed at each step of the scenario. Types of attacks are categorized into physical and software-information types.

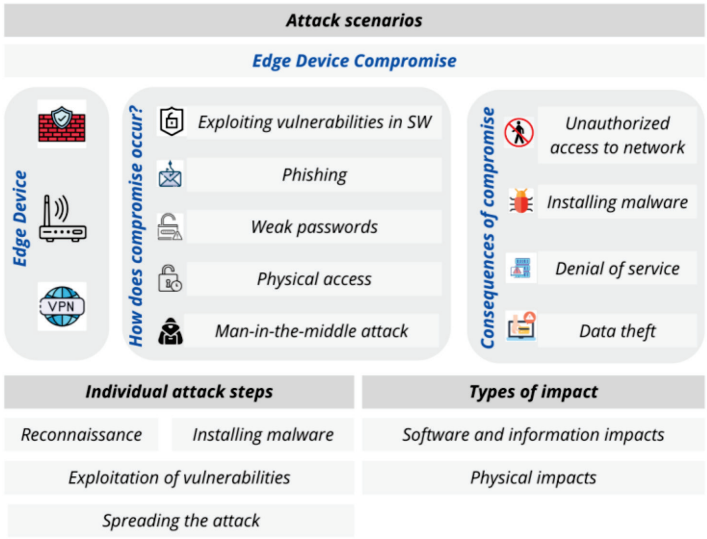

Figure 4. Common IIoT cybersecurity models

As an experiment, the presented work investigates the evaluation of the impact of the considered attacks on the IIoT system using the concept of boundary computing according to the proposed analytical model. The analytical model is aimed at identifying vulnerabilities in the system, analyzing its performance and resilience to attackers in real conditions. To conduct the experiment, IIoT system was used, which included elements such as sensors - for data collection, edge computing nodes - for data preprocessing, central server - for data processing and storage, and communication channels - for data transfer between sensors, edge nodes and server. The investigated system simulates the IIoT network and presents an opportunity to analyze the performance, fault tolerance and security in general. DoS attack, privacy attack, data integrity attack and edge node attack were simulated as attackers.

DOI: 10.37943/22DOKU3034

Results

An experimental environment was developed to evaluate the impact of cyberattacks on an IIoT system with edge computing capabilities. The testbed simulated a typical industrial architecture with the integration of IIoT devices, edge nodes, and cloud infrastructure. The experimental environment configuration includes the use of the Ubuntu 22.04 LTS (64-bit) operating system on all nodes deployed in a virtual environment using VMware Workstation Pro 17. The software architecture was created with containerization based on Docker Engine and Docker Compose for managing multi-container applications. The network topology was constructed as a star with Ethernet connections at 100 Mbps, and data is sent using secure TLS and HTTPS. The design consists of IIoT nodes—6 pieces, edge computing nodes—2, a cloud server operating as the server—1, and an attack node running Kali Linux 2023.2—1.

In order to simulate attacks and analyze the impact on the system, the initial step is to configure the system, in particular, the system was configured using standard network protocols to perform communication between network components. Initial configuration and calibration of sensors and edge computing nodes was performed. Baseline performance metrics without third-party interventions were collected as benchmark data. The metrics were: response time, data link load, throughput, and processing delay at the edge nodes. Table 2 demonstrates the Statistical Summary of IIoT System Performance Under Different Attack Types.

Table 2. Statistical Summary of IIoT System Performance Under Different Attack Types

Metric	Attack Type	Mean	Std. Dev
Response Time	No Attack	100	2,3
	DoS	500	12,7
	Integrity Attack	150	4,5
	Confidentiality Attack	130	3,8
	Edge Computing Attack	300	7,9
Bandwidth	No Attack	10	0,4
	DoS	2	0,5
	Integrity Attack	8	0,6
	Confidentiality Attack	9	0,3
	Edge Computing Attack	4	0,8
Data Integrity	No Attack	100	0,0
	DoS	80	4,5
	Integrity Attack	88	2,1
	Confidentiality Attack	92	3,1
	Edge Computing Attack	85	2,8
Data Loss	No Attack	0	0,0
	DoS	10	1,8
	Integrity Attack	5	1,1
	Confidentiality Attack	3	0,8
	Edge Computing Attack	8	1,4

After collecting the benchmark baselines, attack modeling was performed. For DoS attacks, a high traffic generation tool, the open-source program LOIC, was used to test the system's resilience to high load. For data integrity attacks, data tampering techniques, such as changing

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

the values transmitted from sensors, were used to test the impact on the system's processing and decision making. For privacy attacks, Wireshark analyzer software was used to intercept and analyze the traffic in order to demonstrate the possibility of intercepting the transmitted information. For edge computing attacks, attempts were made to manipulate data processing on nodes using the "Buffer Overflow" exploit.

Figure 5 shows the result of system response time under different attacks, and the DoS attack has adopted a significantly high response time index compared to the normal state of the system, which clearly indicates the system overload. Figure 6 shows the throughput result where the DoS attack and edge computing attack score is lower with respect to others, which shows the decreasing efficiency of the system. Figure 7 shows the result of the impact of different attacks on data integrity. Figure 8 shows the percentage of data loss based on different types of attacks. It is important to note that in DoS attacks the percentage of data loss is very high.

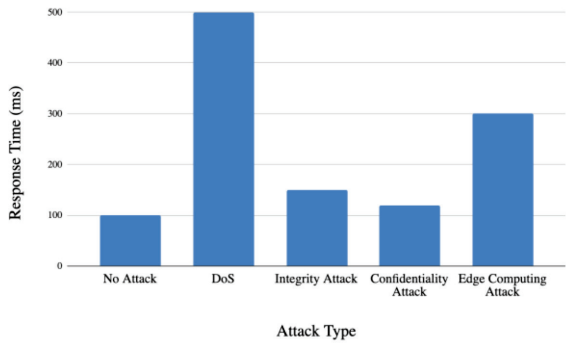

Figure 5. Response Time Based on Attack Type

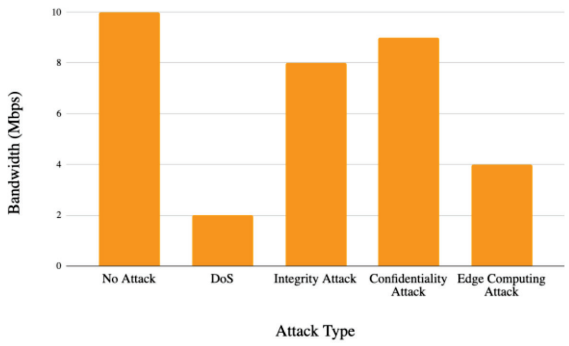

Figure 6. Bandwidth Based on Attack Type

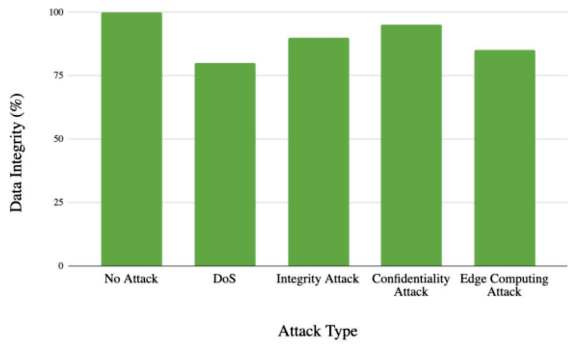

Figure 7. Data Integrity Based on Attack Type

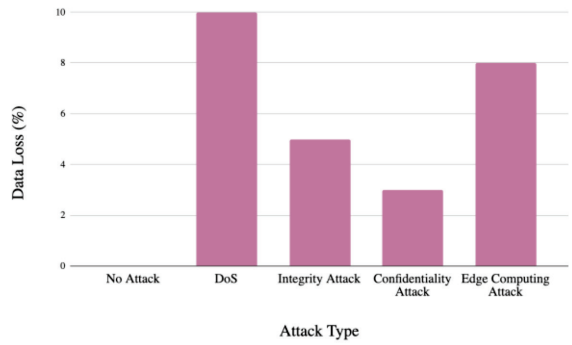

Figure 8. Data Loss Based on Attack Type

To assess the validity and application value of the proposed analytical model, a critical comparison of the results obtained with other relevant studies that examine similar metrics under attacks on IIoT systems with edge computing was performed [29], [30]. Table 3 summarizes the main contribution of publications regarding the investigated metrics under different types of attacks[31], [32], [33]. Note that the results obtained correspond to the bounds established by empirical studies, which emphasizes the correctness of the chosen approach. We also note that the proposed approach allows us to assess the impact of various threat vectors within a single analytical scenario, which increases its applied value for ensuring cyber resilience of IIoT systems.

DOI: 10.37943/22DOKU3034

Table 3. Comparison of Papers

Work	Metric	Attack Type	Contribution
[29]	Response Time	DoS	DoS attacks significantly increase the response time of edge devices
[30]		DoS	The proposed strategy allows to reduce the delay by 15-20%
[31]	Bandwidth	DoS	DoS causes a decrease in throughput of up to 20-30%
[32]	Data Integrity	Integrity Attack	Integrity attacks often go undetected without verification at the edge
[33]	Data Loss	DoS	Data losses reach 10-15% without fault tolerance mechanisms

Discussion and Conclusion

The paper proposes an analytical model of attacking influences on IIoT systems realizing the concept of edge computing. The model includes typical attack scenarios, individual steps and impact classification. The developed model can be used for risk analysis, development of protection strategies and security testing of IIoT systems. The experimental study demonstrated that an IIoT system using the concept of edge computing can be vulnerable to different types of attacks. The biggest impact on the system is from DoS attacks, which result in reduced throughput and increased response time, and data integrity attacks, which disrupt the correctness of the entire system.

Despite the conclusions achieved, the research possesses several limitations. Firstly, the limited scale of the experimental environment, this in turn makes it difficult to assess the scalability of the model in real conditions. Secondly, the experiments were conducted in a controlled laboratory environment using VMware and Docker, in this aspect the full range of factors inherent in real industrial systems is not taken into account. At the same time, only basic types of attacks were considered. In addition, the traffic and load were generated synthetically and do not reflect the full complexity of industrial device behavior. Edge nodes were modeled with simplified processing logic and basic protection, without the use of intelligent or adaptive mechanisms. Finally, the analytical model does not take into account strict timing requirements and does not include hardware limitations that may affect system performance and stability.

By utilizing technologies such as blockchain, AI, and zero-trust architecture, industries can improve the security and resilience of their IIoT and edge computing systems. Future research should focus on autonomous threat response, integration of new technologies, and privacy-preserving mechanisms to address the changing security landscape.

Acknowledgment

This research has been funded by the Committee of Science of the Ministry of Science and Higher Education of the Republic of Kazakhstan (Grant No. AP23489127 «Models and algorithms for increasing the security of cyber-physical systems of the industrial Internet of things using edge computing»).

References

[1] Kolapo, R., Kawu, F.M., Abdulmalik, A.D., Edem, U.A., Young, M.A., & Mordi, E.C. (2024). Edge computing: Revolutionizing data processing for IoT applications. *International Journal of Science and Research Archive*.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 22, JUNE 2025

[2] Turner, D., Ricciuto, A., Lewis, A., D'amico, F., Dhaliwal, J., Griffiths, A.M., ... & Dignass, A. (2021). STRIDE-II: an update on the Selecting Therapeutic Targets in Inflammatory Bowel Disease (STRIDE) Initiative of the International Organization for the Study of IBD (IOIBD): determining therapeutic goals for treat-to-target strategies in IBD. *Gastroenterology*, *160*(5), 1570-1583.
[3] Kim, K.H., Kim, K., & Kim, H.K. (2022). STRIDE-based threat modeling and DREAD evaluation for the distributed control system in the oil refinery. *ETRI Journal*, *44*(6), 991-1003.
[4] Xiong, W., Legrand, E., Åberg, O., & Lagerström, R. (2022). Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix. *Software and Systems Modeling*, *21*(1), 157-177.
[5] Zhukabayeva, T., Zholshiyeva, L., & Karabayev, N. (2024, October). Future Directions of Cybersecurity in Industrial Internet of Things Through Edge Computing. In *2024 9th International Conference on Computer Science and Engineering (UBMK)* (pp. 1-6). IEEE.
[6] Alotaibi, B. (2023). A survey on industrial Internet of Things security: Requirements, attacks, AI-based solutions, and edge computing opportunities. *Sensors*, *23*(17), 7470.
[7] Hosen, A.S., Sharma, P.K., Puthal, D., Ra, I.H., & Cho, G.H. (2023, July). SECBlock-IIoT: A Secure Blockchain-enabled Edge Computing Framework for Industrial Internet of Things. In *Proceedings of the Third International Symposium on Advanced Security on Software and Systems* (pp. 1-14).
[8] Kim, H.M., & Lee, K.H. (2022). IIoT malware detection using edge computing and deep learning for cybersecurity in smart factories. *Applied Sciences*, *12*(15), 7679
[9] Abosata, N., Al-Rubaye, S., Inalhan, G., & Emmanouilidis, C. (2021). Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. *Sensors*, *21*(11), 3654
[10] Shukla, D., & Sawarkar, S. D. (2025). Enhancing energy efficiency and QoS in 5G networks with dynamic resource optimisation green communication protocol. *International Journal of Wireless and Mobile Computing*, *28*(1), 68-85
[11] Xiao, X., Tang, Z., Li, C., Xiao, B., & Li, K. (2022). SCA: Sybil-based collusion attacks of IIoT data poisoning in federated learning. *IEEE Transactions on Industrial Informatics*, *19*(3), 2608-2618.
[12] Zainudin, A., Ahakonye, L. A. C., Akter, R., Kim, D. S., & Lee, J. M. (2022). An efficient hybrid-dnn for ddos detection and classification in software-defined iiot networks. *IEEE Internet of Things Journal*, *10*(10), 8491-8504.
[13] Laghari, S.U.A., Manickam, S., Al-Ani, A.K., Rehman, S.U., & Karuppayah, S. (2021). SECS/GEMsec: A mechanism for detection and prevention of cyber-attacks on SECS/GEM communications in industry 4.0 landscape. *IEEE Access*, *9*, 154380-154394
[14] Tanveer, M., Abd El-Latif, A. A., Ahmad, M., & Ateya, A. A. (2024). LEAF-IIoT: Lightweight and efficient authentication framework for the industrial internet of things. *IEEE Access*, *12*, 31771-31787.
[15] Gueriani, A., Kheddar, H., & Mazari, A. C. (2024, December). Adaptive Cyber-Attack Detection in IIoT Using Attention-Based LSTM-CNN Models. In *2024 International Conference on Telecommunications and Intelligent Systems (ICTIS)* (pp. 1-6). IEEE.
[16] Alkhafaji, N., Viana, T., & Al-Sherbaz, A. (2024). Integrated Genetic Algorithm and Deep Learning Approach for Effective Cyber-Attack Detection and Classification in Industrial Internet of Things (IIoT) Environments. *Arabian Journal for Science and Engineering*, 1-25.
[17] Ghiasvand, E., Ray, S., Iqbal, S., Dadkhah, S., & Ghorbani, A. A. (2024). CICAPT-IIOT: A provenance-based APT attack dataset for IIoT environment. *arXiv preprint arXiv:2407.11278*.
[18] Aslam, S., Alshoweky, M. M., & Saad, M. (2024, June). Binary and multiclass classification of attacks in edge iiot networks. In *2024 Advances in Science and Engineering Technology International Conferences (ASET)* (pp. 01-05). IEEE.
[19] Arsalan, M., Mubeen, M., Bilal, M., & Abbasi, S. F. (2024, August). 1D-CNN-IDS: 1D CNN-based intrusion detection system for IIoT. In *2024 29th International Conference on Automation and Computing (ICAC)* (pp. 1-4). IEEE.
[20] Hoang, T.M., Nguyen, T.T., Pham, T.A., & Nguyen, V.N. (2023, October). An IDS-Based DNN Model Deployed on the Edge Network to Detect Industrial IoT Attacks. In *International Conference on Intelligence of Things* (pp. 307-319). Cham: Springer Nature Switzerland.
[21] Sezgin, A., & Boyacı, A. (2023, May). A survey of privacy and security challenges in industrial settings. In *2023 11th international symposium on digital forensics and security (ISDFS)* (pp. 1-7). IEEE.

[22] Singhal, S., Medeira, P.A., Singhal, P., & Khorajiya, M. (2020). Detection of application layer DDoS attacks using big data technologies. *Journal of Discrete Mathematical Sciences and Cryptography, 23*, 563 - 571.
[23] Corallo, A., Lazoi, M., Lezzi, M., & Luperto, A. (2022). Cybersecurity awareness in the context of the Industrial Internet of Things: A systematic literature review. *Computers in Industry*, *137*, 103614.
[24] Mirani, A. A., Velasco-Hernandez, G., Awasthi, A., & Walsh, J. (2022). Key challenges and emerging technologies in industrial IoT architectures: A review. *Sensors*, *22*(15), 5836.
[25] Tariq, U., Ahanger, T. A., Ibrahim, A., & Bouteraa, Y. S. (2022). The industrial internet of things (iiot): an anomaly identification and countermeasure method. *Journal of Circuits, Systems and Computers*, *31*(12), 2250219.
[26] Xiao, W., Miao, Y., Fortino, G., Wu, D., Chen, M., & Hwang, K. (2021). Collaborative cloud-edge service cognition framework for DNN configuration toward smart IIoT. *IEEE Transactions on Industrial Informatics*, *18*(10), 7038-7047.
[27] Ahmed, A. A., Hasan, M. K., Alqahtani, A., Islam, S., Pandey, B., Rzayeva, L.,... & Alqahtani, N. (2024). Deep Learning Based Side-Channel Attack Detection for Mobile Devices Security in 5G Networks. *Tsinghua Science and Technology*, *30*(3), 1012-1026.
[28] Alli, A. A., Kassim, K., Mutwalibi, N., Hamid, H., & Ibrahim, L. (2021). Secure fog-cloud of things: architectures, opportunities and challenges. *Secure edge computing*, 3-20.
[29] R. Uddin, S. A. P. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," Ad Hoc Networks, vol. 152, p. 103322, Jan. 2024, doi: 10.1016/j.adhoc.2023.103322.
[30] Swati, S. Roy, J. Singh, and J. Mathew, "Securing IIoT systems against DDoS attacks with adaptive moving target defense strategies," Scientific Reports, vol. 15, no. 1, Mar. 2025, doi: 10.1038/s41598-025-93138-7.
[31] Chaudhary S., Mishra P. K. DDoS attacks in Industrial IoT: A survey //Computer Networks. – 2023. – Т. 236. – С. 110015.
[32] Mahadevappa P., Murugesan R.K. Review of data integrity attacks and mitigation methods in edge computing //International Conference on Advances in Cyber Security. – Singapore : Springer Singapore, 2021. – С. 505-514.
[33] Jayalaxmi P., Saha R., Kumar G., Kumar N., Kim T. -H. "A Taxonomy of Security Issues in Industrial Internet-of-Things: Scoping Review for Existing Solutions, Future Implications, and Research Challenges," in IEEE Access, vol. 9, pp. 25344-25359, 2021, doi: 10.1109/ACCESS.2021.3057766.