DOI: 10.34185/1991-7848.itmm.2026.01.093

CYBERSECURITY ON EDGE-DEVICES

Syzonenko R.[1] [ORCID], Klymenko S.[2] [ORCID]

[1]*Oles Honchar Dnipro National University, PhD Student, Ukraine*

[2] *Oles Honchar Dnipro National University, PhD in Engineering, Associate Professor, Ukraine*

Abstract. *In contemporary Industry 4.0 systems, the integration of edge and Internet of Things (IoT) devices facilitates the collection of real-time data, its local processing, and subsequent transmission, thereby significantly enhancing the efficiency of automated processes. Simultaneously, their extensive interconnection within networks engenders substantial cybersecurity concerns, including breaches of data confidentiality, integrity, and availability, as well as tangible physical consequences resulting from successful intrusions. This paper discusses the security requirements of the Industrial Internet of Things (IIoT), classifies threats according to architectural layers (perception, network, application), identifies primary sources of threats, and examines typical device vulnerabilities. Furthermore, it provides a comprehensive analysis of potential applications of artificial intelligence in anomaly detection and cyberattack identification. The benefits of edge computing for the enhancement of decentralized protection mechanisms are also explored. Additionally, the study investigates methods to improve resilience, including encryption techniques, intrusion detection systems, federated learning, and blockchain integration. The research emphasizes the necessity for a holistic approach to protecting resource-constrained devices, thereby ensuring the reliable operation of critical information and control systems.*

Keywords: *cybersecurity, edge computing, IoT devices, IIoT, industrial threats, AI solutions, vulnerabilities, Industry 4.0, intrusion detection, decentralized protection.*

Introduction. The emergence of Industry 4.0 technologies has led to the widespread implementation of Internet of Things and edge computing devices, which enable real-time data processing at the network's edge, thereby reducing latency and alleviating the load on cloud resources [1]. This significant paradigm shift presents new opportunities for automation, real-time monitoring, and data-driven decision-making. Nonetheless, the increasing proliferation of connected devices has concurrently expanded the attack surface considerably. Recent reports indicate that the number of incidents related to Industrial Internet of Things has more than doubled in recent years [2]. The purpose of this report is to analyze

current cybersecurity threats targeting edge and IoT devices, to classify associated vulnerabilities, and to review promising protective strategies, with particular emphasis on those leveraging artificial intelligence and edge-focused methodologies.

Main material. The security of IIoT systems relies on the extended CIA triad-confidentiality, integrity, and availability-augmented by additional elements such as authentication, authorization, fault tolerance, privacy, and secure data exchange [1]. Constraints such as limited computing resources, a diverse array of protocols, and extensive physical access to devices significantly contribute to numerous vulnerabilities.

Threats are classified according to IIoT architecture layers.

– The perception layer, comprising sensors and actuators, is vulnerable to an array of threats. These encompass jamming, node capture, cryptographic key leakage, energy resource attacks (such as sleep deprivation), and data tampering [1, 2].

– The network layer constitutes the third layer within the seven-layer OSI model. Of particular concern are the following types of cyberattacks: distributed denial of service (DDoS) attacks, man-in-the-middle attacks, Sybil attacks, fake traffic injection, and routing attacks such as black hole and gray hole attacks [3].

– The application layer is vulnerable to various cyber threats, including ransomware, malicious code injection, data corruption, API attacks, and side-channel attacks [4].

Threat sources are diverse, including state-sponsored campaigns, industrial espionage, automated malware, botnets, and insider configuration errors [2]. The most common vulnerabilities consist of unprotected protocols, default password usage, lack of software updates, buffer overflows, and weak encryption [5].

Contemporary solutions frequently employ artificial intelligence:

– The employment of deep learning models, such as LSTM, CNN, and autoencoder architectures, has been demonstrated to attain high accuracy in anomaly detection. Research indicates that these models can achieve accuracies ranging from 97% to 99% on various datasets such as Bot-IoT, TON IoT, and N-BaIoT [1, 6].

– The utilization of federated learning methodologies has emerged as a pivotal approach in ensuring the confidentiality and security of data.

– The adoption of hybrid methodologies that incorporate blockchain technology is crucial to guarantee the integrity and decentralized detection of DDoS attacks [3].

Edge computing provides considerable benefits, such as lower latency and diminished data transmission resulting from local processing. Furthermore, it supports the deployment of lightweight artificial intelligence (AI) models directly on devices and improves resilience against network attacks via decentralization [1, 4].

Conclusions. The cybersecurity of edge and IoT devices presents a prominent challenge within the context of Industry 4.0. The integration of artificial intelligence, edge computing, contemporary cryptographic techniques, and intrusion detection systems holds the potential to significantly enhance the resilience of industrial networks. For practical implementation, a standardized approach regarding software updates, network segmentation, and routine penetration testing is indispensable. Future research should focus on optimizing lightweight AI models suitable for resource-constrained devices and incorporating encryption algorithms resistant to quantum computing attacks.

ЛІТЕРАТУРА / REFERENCE

1. Alotaibi B. A Survey on Industrial Internet of Things Security: Requirements, Attacks, AI-Based Solutions, and Edge Computing Opportunities. Sensors. – 2023. 23(17):7470. doi:10.3390/s23177470 [in English].
2. Liebl S, Lathrop L, Raithel U, Söllner M, Aßmuth A. Threat Analysis of Industrial Internet of Things Devices. arXiv preprint arXiv:2405.16314. 2024 [in English].
3. Rathi B. Realizing the potential of Internet of Things (IoT) in Industrial applications. Discover Internet of Things. – 2025. doi:10.1007/s43926-025-00141-5 [in English].
4. Kumar A. Securing IoT devices in edge computing through reinforcement learning. Computers & Security. – 2025. doi:10.1016/j.cose.2025.104474 [in English].
5. Orman A. Cyberattack Detection Systems in Industrial Internet of Things (IIoT) Networks in Big Data Environments. Applied Sciences. – 2025. 15(6):3121. doi:10.3390/app15063121 [in English].
6. Krzysztoń E. Review of Fuzzy Methods Application in IIoT Security-Challenges and Perspectives. Electronics. – 2025. 14(17):3475. doi:10.3390/electronics14173475 [in English].

КІБЕРБЕЗПЕКА НА EDGE-ПРИСТРОЯХ

Р.М. Сизоненко, С.В. Клименко

Анотація. *У сучасних системах Індустрії 4.0 інтеграція периферійних пристроїв та пристроїв Інтернету речей (IoT) полегшує збір даних у реальному часі, їх локальну обробку та подальшу передачу, тим самим значно підвищуючи ефективність автоматизованих процесів. Водночас їх широке взаємоз'єднання в мережах породжує суттєві проблеми кібербезпеки, включаючи порушення*

конфіденційності, цілісності та доступності даних, а також відчутні фізичні наслідки, що виникають у результаті успішних вторгнень. У цій статті розглядаються вимоги до безпеки промислового Інтернету речей (IIoT), класифікуються загрози за архітектурними рівнями (сприйняття, мережа, застосування), визначаються основні джерела загроз та аналізуються типові вразливості пристроїв. Крім того, надається комплексний аналіз потенційних застосувань штучного інтелекту для виявлення аномалій та ідентифікації кібератак. Також досліджуються переваги периферійних обчислень для вдосконалення децентралізованих механізмів захисту. Крім того, в дослідженні вивчаються методи підвищення стійкості, включаючи методи шифрування, системи виявлення вторгнень, федеративне навчання та інтеграцію блокчейну. Дослідження підкреслює необхідність комплексного підходу до захисту пристроїв з обмеженими ресурсами, що забезпечує надійну роботу критично важливих інформаційних та контрольних систем.

Ключові слова: *кібербезпека, edge computing, IoT пристрої, IIoT, промислові загрози, AI-рішення, вразливості, Industry 4.0, виявлення вторгнень, децентралізований захист.*