

EDGE COMPUTING IN CYBERSECURITY: REAL-TIME THREAT DETECTION IN IOT NETWORKS

Vinnitsia National Technical University

Анотація

Публікація досліджує критичну роль периферійних обчислень (*edge computing*) у підвищенні рівня кібербезпеки децентралізованих мереж Інтернету речей (IoT). Завдяки перенесенню процесів виявлення загроз та обробки даних безпосередньо на периферію мережі, системи досягають майже миттєвого часу реагування для нейтралізації швидких кібератак, таких як DDoS та вразливості нульового дня. У дослідженні висвітлюється впровадження легких моделей машинного навчання для поведінкового аналізу в реальному часі, а також використання федеративного навчання для забезпечення конфіденційності даних. Крім того, розглядається, як мікросегментація запобігає горизонтальному поширенню ботнетів у локальній мережі. Також робота звертає увагу на технічні виклики, пов'язані з обмеженими ресурсами периферійних пристроїв, наголошуючи на необхідності застосування методів оптимізації нейронних мереж, таких як квантування та прунінг.

Ключові слова: периферійні обчислення, кібербезпека, Інтернет речей (IoT), машинне навчання, федеративне навчання, виявлення загроз, мікросегментація.

Abstract

This paper explores the critical role of edge computing in enhancing the cybersecurity of decentralized Internet of Things (IoT) networks. By shifting threat detection and data processing directly to the network edge, systems achieve near-instantaneous response times to mitigate rapid cyber threats, such as DDoS attacks and zero-day exploits. The study highlights the implementation of lightweight machine learning models for real-time behavioural analysis and the use of federated learning to ensure robust data privacy. Furthermore, it examines how micro-segmentation prevents lateral botnet propagation within local networks. Finally, the paper addresses the technical challenges associated with resource-constrained edge devices, emphasizing the necessity of neural network optimization techniques, such as quantization and pruning, to balance performance and security.

Keywords: edge computing, cybersecurity, Internet of Things (IoT), machine learning, federated learning, threat detection, micro-segmentation.

Introduction

The rapid expansion of the Internet of Things (IoT) has exponentially increased the attack surface for cyber threats. Traditionally, cybersecurity frameworks have relied on centralized cloud architectures to monitor traffic, detect anomalies, and mitigate attacks. However, this centralized approach introduces significant latency. In the context of modern cyberattacks, even a delay of a few milliseconds can result in a massive data breach or system compromise. To address this, edge computing proposes a decentralized security model where data processing and threat analysis occur at the edge of the network, closer to the data source.

Research results

Integrating cybersecurity protocols directly into edge computing architectures is fundamentally transforming approaches to threat detection and mitigation. One of the key benefits of this approach is a significant reduction in response time to potential threats. By analysing network traffic directly at the gateway or edge server, the system can instantly identify and block anomalous activity, such as sudden traffic spikes associated with DDoS attacks, before these threats can penetrate the core network or overload the core infrastructure.

In addition, the implementation of lightweight machine learning models on edge devices opens up the possibility of real-time behavioural analysis. Traditional signature-based security approaches become less effective in the case of attacks using zero-day exploits. Instead, edge AI allows you to continuously monitor the typical behavioural pattern of connected IoT devices, such as smart cameras or industrial sensors. If a device starts to exhibit unusual activity, such as trying to connect to an unfamiliar external IP address or transferring excessive amounts of data, the edge system quickly flags this as suspicious and blocks the dangerous activity.

Another important element of edge-level protection is ensuring data privacy and securely training algorithms. Instead of sending raw data to the cloud for analysis, which potentially exposes it to interception, such data is analysed locally. Federated learning is widely used today to improve cyber threat detection methods without compromising privacy. This approach allows edge devices to train a shared model directly on-site and send only updated model parameters to a central server instead of the user data itself.

The decentralized organization of the system also significantly increases its resilience to cyberattacks. IoT devices are often targeted for botnet integration, as was the case with the notorious Mirai malware. If an edge node identifies malicious activity, such as horizontal movement of a threat or illegal communication with a command and control (C2) server, it can quickly isolate the infected device in quarantine. Thanks to micro-segmentation technology, this isolation prevents the threat from spreading further within the local network.

However, implementing cybersecurity at the edge level comes with serious technical challenges. Edge devices have limited resources, both computational and energy. Therefore, the use of optimized cryptographic methods and lightweight intrusion detection systems is critical. To ensure stable operation of security protocols without negatively impacting the performance of the IoT environment, quantization and pruning techniques of neural networks are widely used, which allow for an effective balance between performance and security.

Conclusion

The integration of edge computing into cybersecurity frameworks marks a critical paradigm shift in securing IoT networks. By decentralizing threat detection and deploying lightweight machine learning models directly at the network edge, systems can achieve near-instantaneous response times, effectively mitigating rapid threats like DDoS attacks and zero-day exploits. Furthermore, the adoption of federated learning and micro-segmentation significantly enhances data privacy and network resilience, successfully isolating compromised nodes and preventing lateral botnet propagation. While the inherent resource constraints of edge devices necessitate advanced optimization techniques – such as neural network quantization and pruning – the transition to edge-based, localized security architectures is essential for building robust, scalable, and secure modern IoT infrastructures.

REFERENCES

1. Roman, R., Lopez, J., & Mambo, M. (2018). Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges. *Future Generation Computer Systems*, 78, 680-698.
2. Nguyen, D. C., Ding, M., Pathirana, P. N., Seneviratne, A., Li, J., & Poor, H. V. (2021). Federated learning for internet of things: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3), 1622-1658.
3. Xiao, Y., Jia, Y., Liu, C., Cheng, X., Yu, J., & Lv, W. (2019). Edge computing security: State of the art and challenges. *Proceedings of the IEEE*, 107(8), 1608-1631.
4. What is Edge Security? – https://www.hpe.com/emea_europe/en/what-is/edge-security.html – date of application 16.03.2026

Павловська Анастасія Вячеславівна – студентка групи ІБС-24б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: nastyapav2006@gmail.com.

Науковий керівник: **Чопляк Вікторія Володимирівна** – викладач англійської мови, кафедра іноземних мов, Вінницький національний технічний університет, м. Вінниця, e-mail: nikavnuchkova@gmail.com.

Pavlovska Anastasiia Vyacheslavovna – student group 1SS-24b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nastyapav2006@gmail.com.

Scientific Supervisor: **Victoriia V. Chopliak** – teacher of English, Foreign Languages Department, Vinnytsia National Technical University, Vinnytsia, e-mail: nikavnuchkova@gmail.com.