INNOVATIONS IN TECHNOLOGY AND SCIENCE EDUCATION
ISSN 2181-371X
https://science-research.org.uz/index.php/ITSE

ARTIFICIAL INTELLIGENCE BASED NETWORK TRAFFIC ANOMALY DETECTION

Jalolov Mirzolim Saloxiddin o'g'li,
Toshkent Axborot Texnologiyalari Universiteti,
2-kurs magistranti , email: mirzolimhacker2001@gmail.com
Janxojaev Asqar Ayxoja uli,
Toshkent Axborot Texnologiyalari Universiteti,
2-kurs magistranti , email: askarjankhojaev02@gmail.com

Abstract: This paper explores the use of artificial intelligence to detect anomalies in network traffic and strengthen cybersecurity. The study analyzes AI methods that automate and enhance the identification of abnormal patterns indicating possible threats. Using intelligent algorithms to process network data, the research aims to increase detection accuracy, reduce false positives, and improve response speed. Results show that AI-based solutions outperform traditional approaches in adaptability and efficiency. The findings highlight the importance of integrating advanced AI techniques into network monitoring to address growing cybersecurity challenges.

Keywords: network security, anomaly detection, artificial intelligence, machine learning, generative adversarial network, principal component analysis

Аннотация: В статье рассматривается использование искусственного интеллекта для обнаружения аномалий в сетевом трафике и усиления кибербезопасности. Исследование анализирует методы ИИ, которые автоматизируют и улучшают выявление ненормальных шаблонов, указывающих на возможные угрозы. С помощью интеллектуальных алгоритмов анализируются сетевые данные с целью повышения точности, снижения ложных срабатываний и ускорения реакции. Результаты показывают, что решения на основе ИИ превосходят традиционные подходы по адаптивности и эффективности. Полученные данные подчеркивают важность интеграции передовых технологий ИИ в системы мониторинга сети для решения растущих задач кибербезопасности.

Ключевые слова: сетевая безопасность, обнаружение аномалий, искусственный интеллект, машинное обучение, генеративно-состязательная сеть, метод главных компонент

Annotatsiya: Ushbu maqolada tarmoq trafikidagi anomaliyalarni aniqlash va kiberxavfsizlikni kuchaytirish uchun sun'iy intellektdan foydalanish o'rganiladi. Tadqiqot AI usullarini tahlil qilib, xavf belgilarini avtomatik aniqlash va yaxshilashga qaratilgan. Aqlli algoritmlar yordamida tarmoq ma'lumotlari tahlil qilinib, aniqlikni oshirish, soxta ogohlantirishlarni kamaytirish va javob tezligini oshirish maqsad qilingan. Natijalar shuni ko'rsatadiki, AI asosidagi yechimlar moslashuvchanlik va samaradorlikda an'anaviy yondashuvlardan ustun. Xulosalar ilg'or AI texnologiyalarini tarmoq monitoringiga integratsiya qilishning kiberxavfsizlik muammolarini hal etishda muhimligini ta'kidlaydi.

Kalit so'zlar: tarmoq xavfsizligi, anomaliyani aniqlash, sun'iy intellekt, mashinaviy o'rganish, generativ raqobatlashuvchi tarmoq, asosiy komponentlar tahlili

Introduction. Detecting attacks is a critical stage in ensuring network security. Today, two main approaches are primarily used for this task: **signature-based** and **anomaly-based** methods. In the signature-based approach, the system stores signatures of known attack types in a database and inspects incoming traffic by comparing it against those signatures. This approach is precise and fast, but its main limitation is that it can only detect attacks that are already known. New, unknown, or modified (polymorphic) attack types may go undetected by such systems.

The anomaly-based approach, on the other hand, relies on artificial intelligence and machine learning tools. This method learns the network's notion of "normal" behavior and flags deviations — such as unusual traffic, abnormal port activity, or unexpected data flows — as potential attacks. Its primary advantages are:

- The ability to detect new attacks — it can identify zero-day and previously unknown threats;
- Self-learning — it adapts to the network environment over time;
- Broad analysis scope — it can detect complex, multi-stage attacks.

Moreover, the anomaly-based method reduces the need for manual updates to signature databases and can operate in real time. Therefore, combining signature-based and anomaly-based approaches in modern network security systems yields the optimal result. This combination enables networks to be protected not only against existing threats but also effectively against emerging ones.

Research Methodology. To systematically investigate AI methods for network traffic anomaly detection, this study adopted a structured research approach comprising several key phases. Initially, relevant network traffic datasets were collected from controlled environments to provide a representative basis for model development and evaluation. The gathered data underwent extensive preprocessing, including normalization and the removal of artifacts, to ensure that features used for analysis accurately reflected genuine network activity rather than noise or inconsistencies. Following preprocessing, multiple AI algorithms were selected for comparative assessment, prioritizing models recognized for their automation and self-learning capacities that align with current advances in the field[1]. Throughout these stages, particular attention was paid to designing experiments that would meaningfully capture the diverse and dynamic characteristics of modern network environments while adhering to best practices in anomaly detection research[1].

Related Works (Literature Review). Recently, several studies have concentrated on the application of artificial intelligence methods to network traffic anomaly detection, offering comparative perspectives on their respective methodologies and outcomes. Notably, machine learning and deep learning models such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) have received considerable attention for their capacity to recognize complex temporal and spatial patterns within network data, demonstrating marked improvements over conventional approaches[4]. Additionally, contemporary research in the telecommunications domain has underscored that traditional techniques are frequently inadequate for the rapidly changing threat landscape, prompting the adoption of more adaptive AI-driven models. Emerging techniques involving Generative Adversarial Networks (GANs) and Reinforcement Learning (RL) are also being explored, offering new capabilities in both anomaly prediction and real-time response[3]. Taken together, the literature indicates a decisive trend toward hybrid and self-adaptive AI systems that continually refine their performance to address evolving cybersecurity requirements.

Fundamentals of Network Traffic Anomaly Detection. At the core of network traffic anomaly detection lies the identification of deviations from established patterns that may indicate malicious activity or operational disruptions. Network anomalies commonly manifest as unusual spikes in bandwidth usage, sudden changes in communication protocols, or irregular packet flows, all of which can signal the presence of attacks or faults. Artificial intelligence, particularly through architectures such as hybrid Convolutional Neural Networks (CNNs) combined with Generative Adversarial Networks (GANs), has transformed detection capabilities by enabling models to learn complex feature representations and simulate normal traffic behavior. In this approach, CNNs efficiently capture subtleties in real traffic, while GANs generate synthetic baseline data, allowing the system to distinguish between legitimate variability and potentially harmful anomalies. As a result, AI-driven methods have shown superior performance over traditional techniques, providing heightened accuracy and reducing false alarms in diverse network conditions[5].

Results and Discussion. Moreover, the experimental evaluation highlighted that integrating Principal Component Analysis (PCA) with Generative Adversarial Networks (GANs) yielded high levels of accuracy in diagnosing network anomalies. The PCA-GAN approach demonstrated an

accuracy rate of approximately 99.12%, surpassing several established models such as CNN-GRU, CNN-LSTM, and Conv-LSTM by 1.49%(Figure 1). This performance gain can be attributed to the selective extraction of essential network features via PCA, which streamlined the detection process and minimized the risk of overlooking subtle irregularities. Beyond accuracy, the method's robust anomaly identification under various network conditions suggests promising potential for application in protecting dynamic environments against sophisticated threats[2]. These favorable outcomes emphasize the relevance of advanced AI-based techniques, reinforcing the necessity for continuous methodological innovation as network infrastructures and attack strategies evolve.

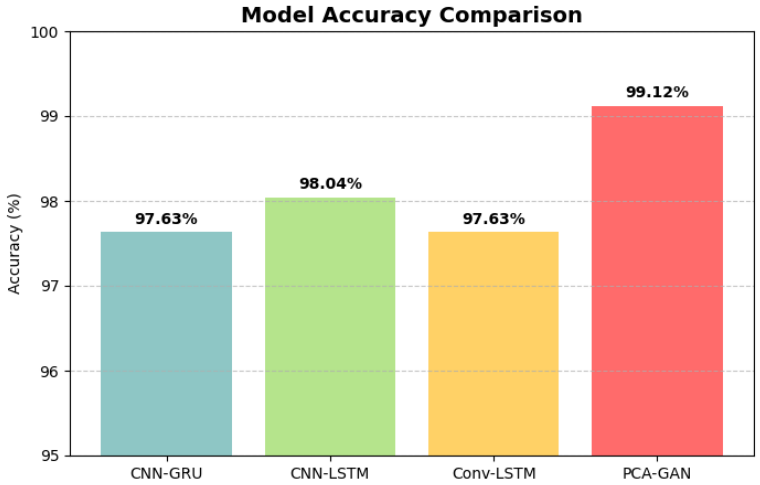


Figure 1. Comparison of model accuracy for different AI-based anomaly detection approaches.

Conclusion. In summary, this study has demonstrated that artificial intelligence offers considerable promise in enhancing network traffic anomaly detection, particularly by improving accuracy and adaptability in identifying abnormal patterns. The experimental results affirm that AI-driven approaches not only outperform conventional techniques but also exhibit strengths in minimizing false alarms and adapting to changing network environments. Furthermore, the integration of advanced models, such as those combining dimensionality reduction and generative frameworks, points toward the feasibility of deploying intelligent monitoring systems in real-world, large-scale networks. Despite these advancements, ongoing research remains essential to address new threat vectors and to refine models for efficiency and real-time applicability. Continued innovation in AI-based solutions can further secure critical infrastructures, making the exploration of hybrid architectures and unsupervised methods a promising direction for future investigation.

References:

[1]. Abdiyeva-Aliyeva, G., & Hematyar, M. (2023). AI-based network security anomaly prediction and detection in future network. In *4th International Conference on Artificial Intelligence and Applied Mathematics in Engineering* (Vol. 7, pp. 149–159). Springer. https://doi.org/10.1007/978-3-031-31956-3_13

[2]. Changala, R., Kayalvili, S., Farooq, M., Rao, L. M., Rao, V. S., & Muthuperumal, S. (2024). Using Generative Adversarial Networks for Anomaly Detection in Network Traffic: Advancements in AI Cybersecurity. *Ieeexplore.Ieee.Org*. https://doi.org/10.1109/ICDSNS62112.2024.10690857

[3]. Edozie, E., Shuaibu, A. N., Sadiq, B. O., & John, U. K. (2025). Artificial intelligence advances in anomaly detection for telecom networks. *Artificial Intelligence Review*, *58*, 100. https://doi.org/10.1007/s10462-025-11108-x

[4]. P M, V. P., & S, S. (2024). Advancements in anomaly detection techniques in network traffic: The role of artificial intelligence and machine learning. *Jsrtjournal.Com*, *2*(6), 38–48. https://doi.org/10.61808/jsrt114

[5]. Rao, V. S., Balakrishna, R., El-Ebiary, Y. A. B., Thapar, P., Saravanan, K. A., & Godla, S. R. (2024). AI driven anomaly detection in network traffic using hybrid CNN-GAN. *Journal of Advances in Information Technology*, *15*(7), 886–895. https://doi.org/10.12720/jait.15.7.886-895