ISSN: 2053-3578 I.F. 12.34

THEORETICAL APPROACHES TO THE APPLICATION OF ARTIFICIAL INTELLIGENCE ALGORITHMS IN CYBERSECURITY SYSTEMS

Nurbek Nasrullayev Bakhtiyorovich
Dean of the Faculty of Cybersecurity, DSc, Associate Professor
Abrorxon Maxmudov Narzulla ogli
Independent Researcher, Muhammad al-Khwarizmi
Tashkent University of Information Technologies

Abstract: This article examines the theoretical approaches to applying artificial intelligence algorithms in cybersecurity systems. The study focuses on the role of AI technologies in threat detection, monitoring network attacks, identifying malware, and analyzing anomalies. In addition, the research highlights the importance of modern approaches such as machine learning, deep learning, and neural networks in improving the effectiveness of cybersecurity systems.

Keywords: cybersecurity, artificial intelligence, machine learning, deep learning, neural networks, network monitoring, threat detection.

Annotatsiya: Ushbu maqolada sun’iy intellekt (AI) algoritmlarining kiberxavfsizlik tizimlarida qo‘llanilishi nazariy jihatdan tahlil qilinadi. Tadqiqot davomida tahdidlarni aniqlash, tarmoq hujumlarini monitoring qilish, zararli dasturlarni aniqlash hamda anomaliyalarni tahlil qilish jarayonlarida AI texnologiyalarining ahamiyati ko‘rib chiqiladi. Shuningdek, mashinali o‘rganish, chuqur o‘rganish va neyron tarmoqlar kabi zamonaviy usullarning kiberxavfsizlik tizimlaridagi o‘rni ilmiy jihatdan yoritiladi.

Kalit so‘zlar: kiberxavfsizlik, sun’iy intellekt, mashinali o‘rganish, chuqur o‘rganish, neyron tarmoqlar, tarmoq monitoringi, tahdidlarni aniqlash.

Аннотация: В данной статье рассматриваются теоретические подходы к применению алгоритмов искусственного интеллекта в системах кибербезопасности. Анализируется использование методов ИИ для выявления угроз, мониторинга сетевых атак, обнаружения вредоносных программ и анализа аномалий. Особое внимание уделяется научным моделям и подходам, направленным на повышение эффективности систем кибербезопасности, включая машинное обучение, глубокое обучение и нейронные сети.

Ключевые слова: кибербезопасность, искусственный интеллект, машинное обучение, глубокое обучение, нейронные сети, мониторинг сети, обнаружение угроз.

INTRODUCTION

With the rapid development of digital technologies, threats in the field of cybersecurity are also becoming increasingly complex. Traditional security methods are sometimes no longer sufficient to protect modern information systems. Therefore, the use of artificial intelligence algorithms makes it possible to improve the effectiveness of cybersecurity systems. AI technologies are capable of quickly analyzing large volumes of data, detecting suspicious activities, and identifying potential attacks in advance. This plays an important role in ensuring the security of organizations and information systems.

MAIN BODY

Artificial intelligence algorithms are applied in several key areas within cybersecurity systems:

Threat detection. Machine learning algorithms analyze network traffic, system logs, and user activity to identify unusual behavior. Such systems are capable of processing large volumes of data quickly and can automate the process of detecting malicious activities. By using anomaly detection techniques, even previously unknown cyberattacks can be identified. For example, artificial intelligence–based systems learn users' typical behavior patterns and detect activities that significantly differ from them, marking these as potential threats. This enables cybersecurity systems to respond quickly and effectively.

Examples of such threats include:

- Phishing attacks – attacks aimed at obtaining passwords or banking information by deceiving users.
- DDoS (Distributed Denial of Service) attacks – attacks that overload a server or network with excessive requests in order to disrupt its normal functioning.
- Brute-force attacks – attempts to gain access to a system by automatically trying many password combinations.
- Ransomware attacks – malicious software that encrypts a user's data and demands payment to restore access.
- Insider threats – security risks caused intentionally or unintentionally by employees within an organization.

Artificial intelligence–based systems play a crucial role in quickly detecting and preventing these kinds of threats.

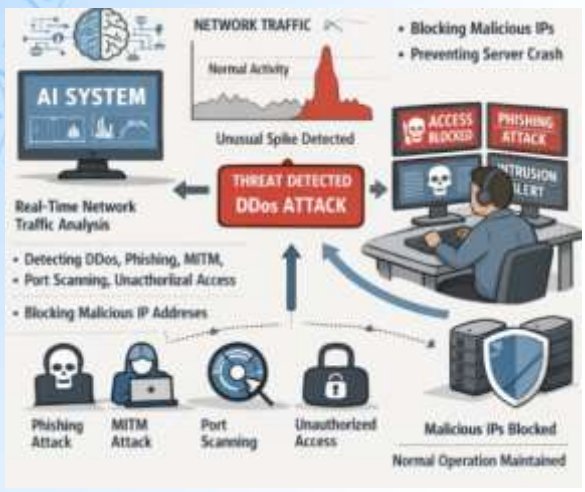
ISSN: 2053-3578 I.F. 12.34

Pic 1. Threat detection

For example, in an organization's information system, users typically log in during working hours (between 9:00 and 18:00). If an AI system detects a login attempt at 03:00 AM from an unknown IP address, this activity may be considered an anomaly. The AI system can label it as a potential cyberattack and automatically notify the administrator or temporarily block the login attempt.

Through this process, artificial intelligence helps ensure cybersecurity by identifying threats at an early stage.

Network attack monitoring. AI-based systems monitor network traffic in real time and continuously analyze network activity. Such systems make it possible to quickly detect cyberattacks such as DDoS attacks, phishing attacks, man-in-the-middle (MITM) attacks, port scanning, and unauthorized access attempts. These systems often operate using a combination of signature-based and behavior-based monitoring methods. As a result, they achieve a much higher level of accuracy compared to traditional security systems. Additionally, AI systems can analyze attack trends and predict potential future threats.



Pic 2. AI-Based network attack monitoring system

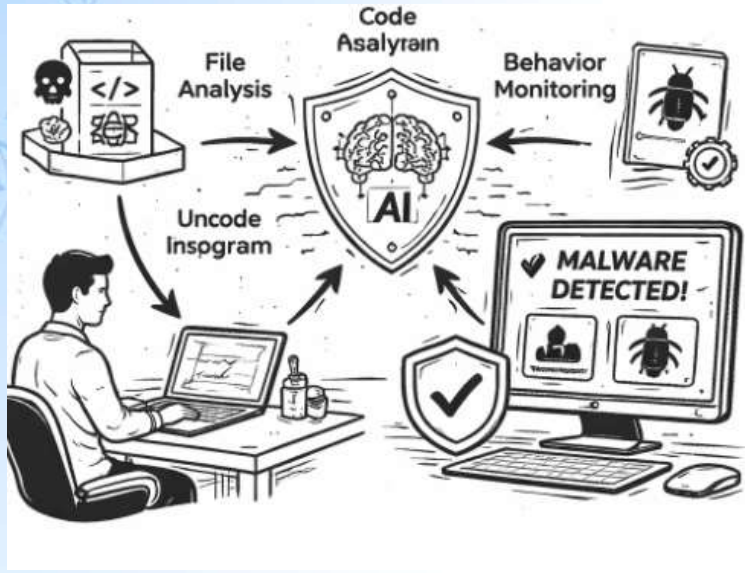
ISSN: 2053-3578 I.F. 12.34

This image shows how an artificial intelligence–based system analyzes network traffic in real time and detects cyberattacks such as DDoS, phishing, MITM, port scanning, and unauthorized access attempts. After identifying suspicious activity, the system blocks malicious IP addresses and protects the server, ensuring the normal operation of the system.

For instance, if thousands of requests are sent to a website server at the same time, it may indicate a DDoS attack. An AI system can detect the unusual spike in network traffic, classify it as an attack, and automatically block the malicious IP addresses. In this way, the system can prevent the server from crashing and maintain its normal operation.

Malware detection. Malicious software can be automatically detected using deep learning and neural networks. AI algorithms analyze file structure, program code, system activity, and the behavioral patterns of programs during execution to identify malware. This approach makes it possible to detect new and previously unknown types of viruses, trojans, or ransomware. In addition, artificial intelligence can classify malicious software and determine how it operates, which helps security systems function more effectively.

For instance, a user downloads an unknown program from the internet onto their computer. From the outside, the program may appear to be a normal file, but it may contain malicious code. An AI-based security system analyzes the file's structure, its program code, and how it behaves within the system. If the program attempts to secretly encrypt the user's files or send data from the system, the AI system identifies it as ransomware or a trojan and immediately blocks or deletes it. In this way, the system prevents the spread of malicious software.



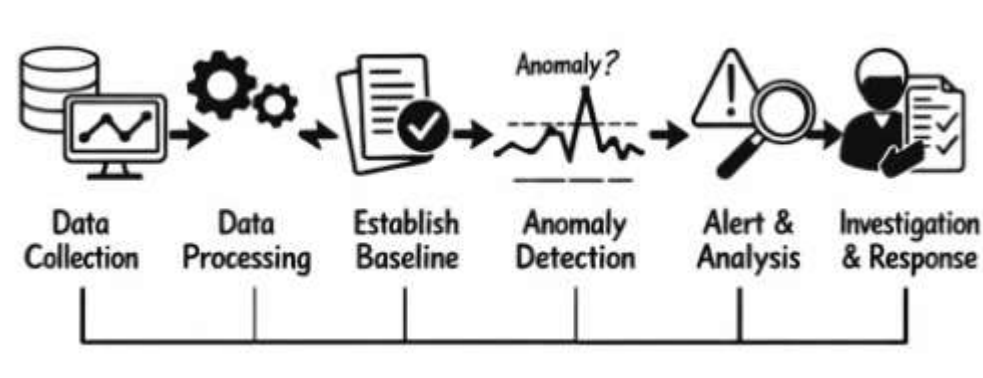
Pic 3. AI-Based Malware detection system

ISSN: 2053-3578 I.F. 12.34

This image illustrates the process of detecting malicious software using artificial intelligence. The AI system identifies viruses, trojans, or other malicious programs by analyzing files, examining program code, and monitoring program behavior. Once detected, the malicious software is blocked, ensuring the security of the system.

Anomaly analysis. Anomaly analysis helps identify unusual activities in user behavior or system operations. In this process, artificial intelligence algorithms learn the normal behavioral patterns of users and detect activities that deviate from them. For example, logging into a system at an unusual time, using unknown devices, or sending an excessive number of requests to a database may be considered anomalies. This method helps detect cyberattacks at an early stage and significantly improves the effectiveness of security systems.

In addition, during anomaly analysis AI systems can also detect sudden changes in network traffic, unusual file download activities by users, or abnormal usage of system resources. Artificial intelligence analyzes large volumes of data and identifies activities that may potentially pose a security risk. As a result, administrators can quickly detect threats and take the necessary measures.



Pic 4. Anomaly analysis

For instance, an employee in a company normally works with 10–20 files per day. If this user suddenly attempts to download 500 files in a single day, the AI system will identify this as an anomaly. This situation may indicate possible data theft or an insider cyberattack. In response, the security system may send an alert to the administrator or temporarily block the suspicious activity.

ANALYSIS AND RESULTS

The application of AI algorithms in cybersecurity systems provides a number of important advantages. First of all, such systems make it possible to detect threats quickly and accurately. In addition, the ability to perform automatic monitoring and real-time analysis increases the overall level of security.

ISSN: 2053-3578 I.F. 12.34

Furthermore, AI technologies make it possible to detect previously unknown attacks. This significantly improves the effectiveness of cybersecurity systems.

Table 1.

Analysis of artificial intelligence methods used in cybersecurity systems

Method	Main function	How It works	Detected threats	AI technology	Advantages	Limitations
Threat detection	Identifying suspicious or malicious activities in a system	Analyzes network traffic, system logs, and user activity patterns	Phishing, DDoS, brute-force, ransomware, insider threats	Machine Learning	Processes large volumes of data quickly and detects threats automatically	May generate false positives in some situations
Network attack monitoring	Monitoring network traffic to detect attacks in real time	Continuously analyzes network packets and traffic behavior	DDoS, MITM, port scanning, unauthorized access	AI with behavioral analysis	Enables real-time detection and improves security accuracy	Requires significant computational resources
Malware detection	Identifying malicious software in systems	Examines file structure, program code, and runtime behavior	Viruses, trojans, ransomware	Deep Learning, Neural Networks	Capable of detecting new and previously unknown malware	Some advanced malware may evade detection
Anomaly analysis	Detecting unusual user or system behavior	Learns normal activity patterns and identifies deviations	Insider attacks, data theft, unauthorized access	Machine Learning, Behavioral analysis	Can detect previously unknown attacks	Requires large datasets to build accurate behavioral models

At the same time, AI-based systems also have some disadvantages. For example, implementing such systems requires a highly advanced technological infrastructure. In addition, in some cases false alerts (false positives) may occur.

CONCLUSION

The study shows that the application of artificial intelligence algorithms plays an important role in improving the effectiveness of modern cybersecurity systems. AI technologies enable security systems to analyze large volumes of data, detect suspicious activities, and respond to potential cyber threats more quickly and accurately than traditional security methods.

The research demonstrates that artificial intelligence can be effectively applied in several key areas of cybersecurity, including threat detection, network attack monitoring, malware detection, and anomaly analysis. By using technologies such as machine learning, deep learning, and neural networks, cybersecurity systems are able to identify both known and previously unknown cyberattacks.

At the same time, despite the significant advantages of AI-based security systems, some limitations still exist. These include the need for advanced technological infrastructure, high computational resources, and the possibility of false positive alerts in certain situations.

Overall, the integration of artificial intelligence into cybersecurity systems significantly enhances the ability of organizations to protect their information systems and digital resources. In the future, further development of AI technologies and improvement of intelligent security models will play a key role in strengthening cybersecurity and ensuring more reliable protection against evolving cyber threats.

REFERENCES

1. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. *Information Fusion, 97*, 101804. https://doi.org/10.1016/j.inffus.2023.101804

2. Sowmya, T., & Somasundaram, K. (2023). A comprehensive review of AI-based intrusion detection systems for cybersecurity. *Array, 18*, 100304. https://doi.org/10.1016/j.array.2023.100304

3. Mohamed, N. (2023). Current trends in artificial intelligence and machine learning for cybersecurity: A state-of-the-art review. *Cogent Engineering, 10*(1). https://doi.org/10.1080/23311916.2023.2272358

4. Ofusori, L. (2024). Artificial intelligence in cybersecurity: A comprehensive review and future directions. *Journal of Intelligent & Fuzzy Systems*. https://doi.org/10.1080/08839514.2024.2439609

5. Mohamed, N., & Al-Jaroodi, J. (2025). Artificial intelligence and machine learning in cybersecurity. *Knowledge and Information Systems*. https://doi.org/10.1007/s10115-025-02429-y

6. Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). A comprehensive survey on intrusion detection systems with advances in machine learning and deep learning. *Discover Artificial Intelligence*, *5*(1). https://doi.org/10.1007/s44163-025-00578-1

7. Al-Shidi, M. A. (2025). Artificial intelligence in cybersecurity: Review and future prospects. *World Journal of Advanced Engineering and Technology*.

8. Hana, M., Aouraghe, I., El Haouari, O., Khaissidi, G., & Mrabti, M. (2025). A survey of artificial intelligence techniques in intrusion detection for the Internet of Things. *Journal of Cybersecurity and Information Systems*.