Using artificial intelligence to predict cyberattacks

UDK 004.4

Anton Shantyr[1], Vyacheslav Zinchenko[2]

State University of Information and Communication Technologies,
[1]anton.shantyr@gmail.com, [2]zinchenkovv86@gmail.com

The rapid development of technology has opened a new era in which artificial intelligence (AI), big data, and the Internet of Things are key forces in improving service intelligence. However, these advancements have increased the risk of cyber threats. These require innovative defense strategies to counter potential attacks.

Recent literature has highlighted the key role of AI in predicting and mitigating cyberattacks in various domains. AI models potential attack scenarios and develops proactive defenses using large and specific data sets. Support vector machines (SVMs) and naive Bayes classifiers are critical for analyzing vulnerabilities and predicting attacks in reliable way. Cognitive AI systems such as knowledge growth systems (KGS) use real-world data to predict the timing and types of cyber threats, offering effective countermeasures. [1-3]

Proposed a security architecture that surpasses traditional security approaches and includes several key components, including a data collection module that aggregates real-time data from various sources, such as network logs, system events, and user activity logs. The AI-based analysis engine uses specialized machine learning algorithms such as support vector machines (SVMs) and Naive Bayes to detect suspicious patterns that indicate risk of cyber threats. The architecture includes a vulnerability assessment module that matches data against a continuously updated database of known vulnerabilities to identify potential threats. The threat engine then takes appropriate action, from blocking malicious traffic to isolating affected systems. It also alerts security personnel. Complemented by continuous learning that improves threat detection capabilities and Security Operations Center (SOC) integration. This robust system can detect threats in real-time. It uses predictive analytics, strengthening the organization’s cybersecurity.

This architecture leverages cutting-edge technology to enable real-time threat detection, predictive analytics, and automated responses, improving an organization's cybersecurity. By continuously improving and adapting AI models and frameworks, and deepening understanding of tactics, system can stay ahead of cybercriminals.

1. Deepak, N. S., Hanitha, T., Tanniru, K., Kiran, L. R., Sai, N. R., & Kumar, M. J. (2023). Analyze and Forecast the Cyber Attack Detection Process using Machine Learning Techniques. In 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 1732-1738). Coimbatore, India.
2. Ryu, S., Kim, J., Park, N., & Seo, Y. (2021). Preemptive Prediction-Based Automated Cyberattack Framework Modeling. Symmetry, 13(5), 793.
3. Sumari, A. D. W., & et al. (2020). Cognitive artificial intelligence application to cyber defense. In IOP Conference Series: Materials Science and Engineering, 732(1), 012037.