APPLICATIONS OF GENERATIVE AI AND LARGE LANGUAGE MODELS IN NETWORK AND CLOUD SECURITY

Nadtochyi M.M., Balagura D.S.
Kharkiv National University of Radioelectronics, Kharkiv, Ukraine

The cybersecurity landscape is undergoing a significant transformation with the emergence of generative artificial intelligence (AI) and Large Language Models (LLMs). These technologies present a dual-edged sword, offering unprecedented opportunities to enhance network and cloud security while simultaneously introducing new and sophisticated threats. Scientific research indicates that generative AI can bolster defenses through advanced intrusion and anomaly detection, proactive vulnerability testing, and the simulation of complex attack scenarios [1]. LLMs, with their proficiency in natural language processing, are proving invaluable in areas such as phishing detection, malware analysis, and automated threat intelligence gathering [2]. The commercial sector is rapidly integrating these AI innovations into security products, promising enhanced threat detection, automated response capabilities, and more intuitive security operations.

The aim of the paper is to analyze theory and practice of GenAI and LLM applications in network and cloud security.

The scientific exploration of generative AI in network security consistently reveals its dual potential. While it significantly enhances defensive capabilities, it also presents a powerful tool that can be leveraged by attackers. This creates a continuous cycle of innovation, often referred to as a cybersecurity "arms race", where advancements in defensive AI are met by increasingly sophisticated AI-driven attacks

Generative AI, using models like Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), enhances intrusion detection by simulating attacks and identifying anomalies. LLMs are used in detecting phishing attempts, analyzing malware, and automating threat intelligence. They offer sophisticated analysis and automate responses, improving security posture. In cloud environments, generative AI automates security controls and enhances threat detection.

The future of cybersecurity will be shaped by the ongoing interplay between AI-powered threats and defenses, and organizations that embrace a forward-thinking and adaptive security strategy will be best positioned to thrive in this dynamic environment.

References

1. Generative AI in cybersecurity, Capgemini Research Institute (2024) https://www.capgemini.com/insights/research-library/generative-ai-in-cybersecurity/

2. Kasri, W., Himeur, Y., Alkhazaleh, H. A., Tarapiah, S., Atalla, S., Mansoor, W., Al-Ahmad, H. (2025) From Vulnerability to Defense: The Role of Large Language Models in Enhancing Cybersecurity DOI: https://doi.org/10.3390/computation13020030