AMERICAN JOURNALS
Open Access, Peer Reviewed Journals

American Journal of Technology and Applied Sciences
ISSN (E): 2832-1766 Volume 30, November - 2024

APPLICATION OF GENERATIVE AI IN CYBERSECURITY DETECTION AND PREVENTION OF NEXT-GENERATION ATTACKS

Aram Andreasyan
IT Specialist, Los Angeles, USA

ABSTRACT

This article examines modern approaches to applying generative artificial intelligence (Generative AI) to cybersecurity problems. Particular attention is paid to the use of generative adversarial networks (GANs), large-scale language models (LLMs), and transformer architectures to detect, model, and prevent next-generation attacks, including zero - day attacks, polymorphic malware, and phishing.

KEYWORDS

Generative AI, cybersecurity, GAN, LLM, intrusion detection, adversarial attacks, zero-day.

Introduction

The scientific novelty of the study lies in the justification of the use of generative artificial intelligence as a proactive cyber defense tool capable of modeling unknown attacks, generating synthetic training data and increasing the effectiveness of detecting new generation threats (zero-day, polymorphic software, APT).

Swift The digitalization of the economy, public administration, and critical infrastructure is accompanied by a steady increase in the number and complexity of cyber threats. Modern information systems are becoming increasingly distributed, dynamic, and heterogeneous, significantly expanding the attack surface. As a result, traditional information security methods based on signature analysis and static rules demonstrate limited effectiveness in countering new-generation attacks, including zero-day exploits, polymorphic malware, targeted APT campaigns, and artificial intelligence-enabled attacks [1].

Classic intrusion detection and prevention systems (IDS/IPS) typically focus on identifying known attack patterns and require regular signature updates. This reduces their effectiveness in the face of a rapidly evolving threat landscape and the emergence of previously unknown attack scenarios [2]. Therefore, the scientific community is actively researching intelligent and adaptive approaches capable of detecting anomalous behavior and predicting potential threats.

In recent years, artificial intelligence and machine learning methods have become an integral part of modern cybersecurity systems. However, most traditional ML approaches fall into the category of discriminative models focused on classification and requiring large volumes of labeled data. The lack of high-quality datasets , as well as the imbalance of attack classes, significantly limit the capabilities of such models, especially when detecting rare and new types of threats [3].

In this context, generative artificial intelligence (Generative AI), including generative adversarial networks (GANs), variational autoencoders, and large-scale language models, is of particular interest. Generative methods are capable of not only analyzing input data but also synthesizing new patterns that mimic real-world network traffic distributions, malicious code, or user behavior. This allows them to be used to generate synthetic training samples, model attacks, and improve the resilience of security systems to unknown threats [1, 4].

Generative adversarial networks, proposed by I. Goodfellow and co-authors, have gained widespread acceptance in cybersecurity due to their ability to generate realistic and diverse data. Current research shows that GAN models are effectively used for intrusion detection, adversarial example generation, and polymorphic malware analysis [4]. Their use improves the generalization ability of IDS systems and reduces the number of false positives.

In parallel, the use of large language models and transformer architectures is developing in log analysis, vulnerability detection, and threat automation tasks. intelligence and phishing attack detection. According to several reviews, LLMs can significantly improve the speed of incident handling and the quality of analytical solutions in security operations centers (SOCs) [5].

However, generative AI has a dual nature. On the one hand, it strengthens defense mechanisms, but on the other, it is actively used by attackers to automatically generate malicious code and create highly realistic phishing messages and deepfake content. This creates a new paradigm of confrontation, in which both offensive and defensive tools rely on the same artificial intelligence technologies [6].

Thus, the relevance of this study is due to the need for a comprehensive analysis of the capabilities of generative artificial intelligence in the tasks of detecting and preventing new generation attacks, as well as assessing the risks and limitations of its practical application in modern cybersecurity systems.

Generative artificial intelligence encompasses a class of models capable of synthesizing new data based on learned distributions. In cybersecurity, such technologies are used for intrusion detection, attack modeling, training data generation, and automated threat analysis. The most significant are generative adversarial networks, large-scale language models, variational autoencoders, and transformer architectures.

Generative adversarial networks (Generative Adversarial Networks) are an architecture consisting of two neural networks - a generator and a discriminator -trained in an adversarial fashion. The generator synthesizes data, and the discriminator evaluates its authenticity.

In cybersecurity, GANs are used for: generating synthetic network traffic; modeling zero - day attacks; detecting anomalies; and creating polymorphic malware for IDS testing.

Research shows that using GANs improves intrusion detection accuracy and reduces dependence on unbalanced datasets [7]. Furthermore, GANs are actively used for generating adversarial examples and stress testing security systems [4].

Large language models are based on a transformer architecture and trained on massive text data corpora. In cybersecurity, LLMs are used for: event and incident log analysis; threat automation intelligence; phishing message detection; source code audit; vulnerability analysis.

Modern research demonstrates the high efficiency of LLM in the tasks of automated response and support of SOC center analysts [5].

Variational Autoencoders are used for probabilistic modeling of data distributions. In cybersecurity, they are used for: detecting anomalies in network traffic; compressing and reconstructing logs; and

generating synthetic samples. VAEs are particularly effective at detecting deviations from normal system behavior, which is important for detecting covert attacks [3].

Transformers and hybrid generative models (GAN + Transformer, GAN + Autoencoder) provide deeper analysis of network event sequences. Their applications include user experience analysis (UEBA); detection of complex APT attacks; and event correlation in SIEM systems. Hybrid architectures demonstrate improved accuracy and resilience to noise compared to classical ML models [1].

Table 1 - Comparative characteristics of generative AI technologies in cybersecurity

Technology	Operating principle	Key Challenges in Cybersecurity	Advantages	Restrictions
GAN	Adversarial training of generator and discriminator	Attack generation, IDS training, adversarial testing	High data realism	Difficulty of learning, instability
LLM	Transformer language model	Analysis logs, phishing, threat intelligence	Contextual analysis, SOC automation	Risk of abuse, resource intensity
VAE	Probabilistic autoencoder	Anomaly detection, data generation	It detects deviations well.	Less realistic than GAN
Hybrid models	Combination of architectures	APT detection, UEBA, SIEM analytics	Increased accuracy	High computational cost

Next-generation attacks are characterized by a high degree of automation, adaptability, and the ability to evade traditional defenses. These include zero-day exploits, polymorphic malware, targeted APT campaigns, and attacks generated using artificial intelligence. Unlike signature-based threats, they lack predetermined patterns, significantly complicating their detection by traditional IDS/IPS systems [2].

The use of generative artificial intelligence enables the transition from a reactive to a proactive defense model. Generative models are trained on normal and malicious system behavior and are then capable of identifying statistical and behavioral deviations that indicate an attack [7].

Zero - day attacks exploit previously unknown vulnerabilities and are therefore undetectable by signature-based methods. Generative adversarial networks and variational autoencoders are used to model normal network behavior and detect anomalies.

The use of GANs in attack detection tasks is based on the generation of variable threat scenarios and the expansion of IDS training samples, which increases the detection of previously unknown intrusions.

Polymorphic Malware changes its structure each time it spreads, while maintaining its functionality. Generative models are used to: identify hidden behavioral patterns; generate mutations in malicious code; and train detectors on variable samples.

Research shows that GAN approaches improve the classification accuracy of polymorphic threats compared to traditional ML algorithms [7].

Large language models are used for semantic text analysis, identifying anomalies in writing styles, and detecting AI-generated messages. LLMs are capable of analyzing the structure of phishing emails, fake domains, and behavioral communication patterns. This enables automated threat filtering and increased detection accuracy for complex phishing campaigns [5].

Advanced Persistent APTs are characterized by a long-term, hidden presence within infrastructure. Their detection uses hybrid generative architectures that analyze event sequences, network flows, and user behavior.

Transformer models and GANs allow the detection of correlated anomalies that are not noticeable in traditional log analysis, which significantly increases the efficiency of SOC analytics [1].

Consequently, generative artificial intelligence provides a qualitatively new level of detection for next-generation attacks by: modeling unknown threats; identifying behavioral anomalies; generating training data; and analyzing complex multi-stage attacks. This makes generative technologies a key element of proactive cyberdefense systems.

Modern cyber threats require a shift from a reactive security model to a proactive one, based on predicting and preventing attacks before they occur. Generative artificial intelligence plays a key role in developing such defense mechanisms due to its ability to model potential threats, generate attack scenarios, and identify vulnerabilities at early stages [1]. Proactive Cyber defense using generative models is focused not only on detection, but also on proactive response, automation of protection measures and increasing the resilience of infrastructure to unknown threats [5].

Generative models, primarily GANs, are used for synthetic simulation of cyberattacks in a controlled environment. This allows for: testing infrastructure resilience; identifying vulnerabilities in security architecture; training IDS/IPS on expanded samples; and conducting automated red Teaming . Synthetic attack generation increases system readiness for new threats and reduces dependence on real incidents.

Generative AI is used to improve the effectiveness of IDS/IPS by: generating rare classes of attacks; balancing training datasets ; reducing false positive ; adaptation to changing threat patterns. Research shows that generative approaches improve detection accuracy and system resilience to adversarial attacks [1].

One of the key challenges in cybersecurity is the lack of representative datasets . Generative models allow for the creation of realistic samples of network traffic, logs, and malicious activity. This is especially important for IoT environments , cloud infrastructures, and critical information systems. Synthetic data improves the generalization ability of models and accelerates the training of security systems.

Integration of Generative AI with SOAR (Security) platforms Orchestration, Automation and Response) allows you to: automatically generate response scenarios; generate playbooks; predict incident development; and optimize the actions of SOC analysts. LLM and transformer models are used to intelligently automate response and incident management processes.

Table 2 - Application of generative AI in proactive cyber defense

Direction of application	**Technologies used**	**Main functions**	**Effect on security**
Attack modeling	GAN, Diffusion Models	Generating exploit scenarios, red teaming	Improving threat preparedness
IDS/IPS Enhancement	GAN, VAE	Data balancing, attack generation	detection accuracy
Synthetic datasets	GAN, Autoencoders	Traffic and log generation	Improving model training
SOAR automation	LLM, Transformers	Playbook generation , response	Reducing response time
Vulnerability analysis	LLM, Hybrid AI	Finding weaknesses, code audit	Preventing exploit attacks

Generative artificial intelligence enables a transition to a proactive cybersecurity paradigm, in which threat modeling, synthetic learning, and automated response are key. This not only prevents known attacks but also increases infrastructure resilience to previously unknown scenarios.

Despite the significant potential of generative artificial intelligence for enhancing cybersecurity, its use is associated with a number of technological and applied risks. However, generative AI can be used not only in defensive but also in offensive scenarios, creating a new paradigm for cyberspace conflict.

First, generative AI is used by attackers to automatically develop malware, including polymorphic and obfuscated code. This lowers the barrier to entry for cybercrime and accelerates exploit creation . Second, large language models allow for the generation of highly realistic Phishing messages, deepfake content, and social engineering scenarios increase the success of attacks on users and organizations. Third, there's the risk of confidential data leaks through trained models, as well as the possibility of adversarial manipulations aimed at evading detection systems .

Additional limitations include high computational costs, low interpretability of generative models, and the lack of standardized regulatory mechanisms. Therefore, the effective use of generative AI in cybersecurity requires the development of oversight mechanisms, ethical regulation, and protection of the AI systems themselves from abuse.

Thus, the analysis showed that integrating generative models into cyberdefense systems improves the adaptability, predictability , and resilience of security systems. Despite existing risks, further development of generative models, hybrid architectures, and explainable approaches will enable the creation of adaptive and proactive defense systems capable of countering evolving cyberthreats.

References

1. The impact of generative AI on cybersecurity // Neurocomputing . – URL: https://www.sciencedirect.com/science/article/pii/S0925231225000785
2. Generative AI-based intrusion detection for vehicular networks // Pervasive and Mobile Computing. – URL: https://www.sciencedirect.com/science/article/pii/S1570870525002793
3. Enhanced intrusion detection system using hybrid techniques // Alexandria Engineering Journal. – URL: https://www.sciencedirect.com/science/article/pii/S1110866525001562
4. A survey on GAN applications in cybersecurity // arXiv preprint. – URL: https://arxiv.org/pdf/2407.08839
5. Generative AI in cybersecurity: a comprehensive review of large language models // Internet of Things. – URL: https://www.sciencedirect.com/science/article/pii/S2667345225000082
6. The Impact of Generative AI on Cybersecurity // Securelist . – URL: https://securelist.ru/story-of-the-year-2023-ai-impact-on-cybersecurity/108558
7. A comprehensive survey of GANs in cybersecurity intrusion detection // ResearchGate . – URL: https://www.researchgate.net/publication/372404301