RADemics

Generative Adversarial Networks (GANs) for Augmenting Cyber Threat Intelligence and Enhancing Detection of Evasive Malware

Krishna Kumar, Jothi.P , Senthil Kumar Dhandapani
RVS COLLEGE OF ARTS AND SCIENCE, ST. JOSEPH'S COLLEGE OF ENGINEERING

Generative Adversarial Networks (GANs) for Augmenting Cyber Threat Intelligence and Enhancing Detection of Evasive Malware

[1]Krishna Kumar, AI Expert & Data Scientist, Artificial Intelligence, nitcseac@gmail.com

[2]Jothi.P, Assistant Professor, School of Computer Studies-BSC IT, RVS college of Arts and science, jothip_scsug@rvsgroup.com

[3]Senthil Kumar Dhandapani, Assistant Professor, Artificial Intelligence and Data Science, St. Joseph's College of Engineering, OMR, Chennai 600119. sentencruze@gmail.com

Abstract

The rapid expansion of digital infrastructures has led to an unprecedented increase in cyber threats, necessitating advanced techniques for real-time anomaly detection in network traffic. Traditional rule-based and statistical methods often fail to detect sophisticated attacks due to their reliance on predefined signatures and limited adaptability to evolving threats. Deep learning has emerged as a promising alternative, leveraging data-driven approaches to enhance detection accuracy. Convolutional Neural Networks (CNNs) have demonstrated efficiency in extracting spatial-temporal patterns from network traffic, while Transformer-based architectures excel in capturing long-range dependencies and sequential anomalies. However, existing solutions face challenges related to scalability, computational overhead, imbalanced datasets, and adversarial robustness. This chapter provides a comprehensive analysis of CNN and Transformer-based deep learning architectures for real-time anomaly detection, highlighting their strengths, limitations, and practical deployment challenges. A hybrid approach integrating CNNs and Transformers is explored to enhance detection performance by combining local feature extraction with global sequence modeling. the role of synthetic data augmentation, adaptive learning techniques, and adversarial defense mechanisms in improving model generalization and resilience is examined. Future research directions focus on explainable AI, lightweight models for real-time applications, and self-supervised learning for mitigating data scarcity. The insights presented in this chapter contribute to the advancement of AI-driven cybersecurity solutions, enabling proactive threat detection and risk mitigation in dynamic network environments.

Keywords: Deep Learning, Anomaly Detection, Network Security, Convolutional Neural Networks, Transformers, Cyber Threats

Introduction

The cybersecurity landscape has experienced a significant transformation with the increasing sophistication of cyber threats, particularly in the form of evasive malware. Traditional malware detection systems, such as signature-based detection and heuristic methods, have long been the cornerstone of cybersecurity strategies. However, these conventional methods are increasingly ineffective against advanced forms of malware that employ evasion techniques like polymorphism, metamorphism, and obfuscation. Evasive malware is specifically designed to bypass detection

systems by altering its behavior or appearance, making it difficult for traditional methods to recognize and counteract it. As cybercriminals continue to innovate, the existing defenses are often left unable to keep up with the dynamic nature of new attacks. This evolving challenge demands innovative solutions capable of detecting previously unknown threats in real-time, and one promising approach is the integration of deep learning models, particularly Generative Adversarial Networks (GANs).

Generative Adversarial Networks (GANs), introduced in 2014 by Ian Goodfellow, have emerged as a powerful tool for a range of applications, including cybersecurity. A GAN consists of two neural networks: a generator and a discriminator, which are trained together in a process that can be likened to a game. The generator attempts to create data that resembles real-world data, while the discriminator works to distinguish between real and generated data. This adversarial setup leads to a model that can generate high-quality data, making it particularly useful for anomaly detection and creating synthetic datasets for training machine learning models. In the context of cybersecurity, GANs are being explored as a method for detecting evasive malware, as their ability to generate new data points allows them to simulate novel attack scenarios that may not yet be present in threat intelligence databases. This characteristic is vital for identifying zero-day attacks or polymorphic malware, which are designed to elude traditional detection methods.

Incorporating GANs into cybersecurity frameworks can significantly enhance the detection of evasive malware and improve the overall security posture. One of the primary applications of GANs in this domain is anomaly detection, where the goal is to distinguish between normal system behavior and malicious activities. By training GANs on legitimate network traffic or system operations, the generator learns to simulate expected behaviors, and the discriminator identifies any deviations from this norm. These deviations may signify an intrusion or malware infection. GANs can be used to generate synthetic attack data, which can augment existing threat intelligence datasets. This synthetic data can include novel attack vectors, enabling security systems to better prepare for new and unknown threats. By generating adversarial examples, GANs can also be used to enhance other machine learning models for malware detection, making them more robust and adaptive to new evasion techniques employed by attackers.