Chapter 3
Generative AI in Network Security and Intrusion Detection

Siva Raja Sindiramutty
https://orcid.org/0009-0006-0310-8721
Taylor's University, Malaysia

Raja Kumar Murugesan
https://orcid.org/0000-0001-9500-1361
Taylor's University, Malaysia

Krishna Raj V. Prabagaran
Universiti Malaysia Sarawak, Malaysia

Sarfraz Nawaz Brohi
University of the West of England, UK

N. Z. Jhanjhi
https://orcid.org/0000-0001-8116-4733
Taylor's University, Malaysia

Mehdi Masud
https://orcid.org/0000-0001-6019-7245
Taif University, Saudi Arabia

ABSTRACT

Protecting virtual assets from cyber threats is essential as we live in a digitally advanced world. Providing a responsible emphasis on proper network security and intrusion detection is imperative. On the other hand, traditional strategies need a supportive tool to adapt to the transforming threat space. New generative AI techniques like generative adversarial networks (GANs) and variational autoencoders (VAEs) are the mainstream technologies required to meet the gap. This chapter deals with how these models can enhance network security by inspecting the network traffic for anomalies and malicious behaviors detected through unsupervised learning, which considers strange or emerging phenomena. This survey features innovations in fault detection, behavior control, deep packet inspection, traffic classification, and examples of real-world intrusions detected by GAN-based systems. Furthermore, the chapter focuses on the challenges of adversarial attacks on models that require the

DOI: 10.4018/979-8-3693-5415-5.ch003

development of solid defense mechanisms, such as generative adversarial networks. Ethics becomes the following matter on our list of discussions, given that privacy transparency and accountability are to be observed when working with generative AI technologies in network security. Finally, the authors examine trends that determine how cyber-attacks are dealt with comprehensively.

INTRODUCTION

Overview of the Significance of Network Security and Intrusion Detection in Protecting Digital Assets

Securing networks and monitoring intrusions is essential because this is one of the most vital parts of cyber protection. Digital networks' security concerns have become necessary because they are the core of modern business communications. Confidential information and operational stability will derange if the networks are unprotected (Kumar & Khan, 2024). The network security protocols govern pro-active approaches to disallow unauthorized access, damaging intrusions, or other malicious activities that may affect reliability, confidentiality, and data availability (Rachakonda et al., 2024).

Employment of Intrusion Detection Systems (IDS), which continuously work to detect and stop abnormal traffic, is an imperative part of network security as these devices monitor and identify any possible penetrations in traffic flow within the organization's infrastructure. As sophisticated as IDS might be, it can be used to conduct real-time analysis, thus providing a platform in which it is possible to detect malware attacks, unauthorized access attempts, and denial-of-service attacks before any serious harm can be done to the business, hence giving the businesses enough time to take corrective action before it is too late. Monitoring the activity patterns of a particular company's digital assets may be accomplished by this technology. In so doing, the concerns will easily be in the position to proactively deal with any vulnerability that the hackers may be trying to utilize, which in turn will prevent data or financial loss that unlawful activities like cyber-attacks may cause (Ali et al., 2024; Konar et al.,2023). The application of sound techniques used in protecting networks from intrusions aids organizations in the legal compliance department when they deal with critical information, such as customer details, by protecting people's rights regarding security. Having a complex and high-security framework presents the unequivocal message of treating as sacred client content, which in turn promotes the client's trust in the service, and the service provider reduces this risk of reputation being tarnished due to downtimes induced by the laxity of information security (Alalmaie et al., 2024; Khalil et al., 2021).