Chapter 17

Exploring the Role of Generative Adversarial Networks in Cybersecurity:

Techniques, Applications, and Advancements

Ambika S. Jaiswal
https://orcid.org/0000-0003-4517-0786
Sant Gadge Baba Amravati University, India

Dipak V. Bhavsagar
Seth Kesarimal Porwal College of Arts and Science and Commerce, India

Sonali Ravindra Chavan
https://orcid.org/0009-0001-0712-1572
Bharatiya Mahavidyalaya, Amravati, India

Priyanka C. Tikekar
Bharatiya Mahavidyalaya, Amravati, India

Suhashini Chaurasia
https://orcid.org/0000-0002-7443-0105
S.S. Maniar College of Computer and Management, Nagpur, India

ABSTRACT

To protect the vast amounts of data being stored on computers and transported over networks, cybersecurity is crucial. To prevent increasingly complex assaults in the future, methods for identifying threats must be regularly updated. Experts in security are using GAN to accomplish results in password cracking, anomaly generation, and intrusion detection. The creative use of GANs in cybersecurity is explored in this chapter. An overview of GANs and their importance in strengthening cyber defense mechanisms is presented in the introduction. An extensive literature analysis to clarify the current state of knowledge is provided after a detailed examination of traditional GAN techniques. The chapter clarifies the GAN's architectural subtleties and highlights its applicability to cybersecurity scenarios. Additionally, study of variety of GAN applications in cybersecurity. It classifies different kinds of GANs and frameworks used in their application. It studied the intrusion detection-based GAN model with its parameters results compared with the existing study.

DOI: 10.4018/979-8-3693-3597-0.ch017

INTRODUCTION

Generative Adversarial Network is an example of an artificial intelligence (AI) system or technique that made up of two neural networks i.e. a discriminator & generator. Created data is compared with the dataset is the basic concept behind a GAN. Generator produces samples, means it generates new data. For instance, the generator would produce images that resemble human faces if you wanted to create realistic faces.

In contrast, the discriminator assesses the generated data and attempts to determine if it is authentic (drawn from the genuine dataset) or synthetic (made by the generator). In essence, it plays the role of a detective, attempting to determine whether the data is created or real. In order to protect private networks, data, hardware, and software from cyberattacks, a set of guidelines and practices known as cybersecurity is put in place. The many attack types include malware/virus-based software deployment, dos, phishing & man in the middle. Because to the interconnectivity IoT for short, and the huge volume of information produced by the machines, gadgets, apps, and websites utilized in cloud-based services, there has been a notable increase in cyberthreats in recent times. (Tasneem & Gupta 2022) The increasingly sophisticated and cunning cyberattacks are beyond the detection and prevention of the security mechanisms. To address these challenges, deep learning techniques are commonly applied in the cybersecurity field.

Conventional Approaches: The conventional and widely-used approaches for intrusion detection and password-cracking software are covered in this section. To prevent advanced attacks, a number of strong and novel intrusion detection systems are being developed. These methods fall within the categories of anomaly- and signature-based intrusion detection systems. Signature based IDS discovers assaults by analyzing the patterns and comparing the event patterns with previous signature & attack.

Anamoly based intrusion detection system records & patterns of different attack types & identify latest types of well-known attacks by utilizing a variety of methodologies like ML based, statistical Anamoly based, different IDs are listed & classified in (Figure 1). Many companies and industries, including the banking, military, the stock market, social media, and telecommunications, place a strong premium on password security. It was possible to break these passwords with brute force attack, dictionary attack, rainbow table etc. A few of the frequently used password cracking programs are THC Hydra, Brutus and John the Ripper.

LITERATURE REVIEW

The study “Detecting Adversarial Examples for Network Intrusion Detection System with GAN” by Ye Peng, Guobin Fu, addresses how machine learning models can be vulnerable in an adversarial environment. To enhanced the accuracy of NIDs authors suggest a defense algorithm that uses a bidirectional GAN. Metrics such as accuracy, precision, recall & f1 score significantly decline when study assesses the effects of Fast Gradient Sign Method, Projected Gradient Descent, and Momentum Iterative Fast Gradient Sign Method attacks on functionality of DNN-based NIDS. hostile Sample Detection (ASD), the suggested defense algorithm, successfully enhances NIDS performance in the hostile setting. The robustness of NIDS is increased by the ASD technology’s better parameter results in identifying adversarial samples produced by FGSM, PGD, and MI-FGSM attacks.

Related Content