

Chapter 13

Enhancing Cyber Security Through Generative Adversarial Networks


Varkha Kumarlal Jewani

Sant Gadge Baba Amravati University, India

Prafulla E. Ajmre

Sant Gadge Baba Amravati University, India

Mohammad Atique

 <https://orcid.org/0000-0001-6976-9895>

Sant Gadge Baba Amravati University, India

Suhashini Chaurasia

 <https://orcid.org/0000-0002-7443-0105>

S.S. Maniar College of Computer and Management, India

ABSTRACT

GANs, or generative adversarial networks, are becoming a very useful tool in many fields, such as data generation, natural language processing, and computer vision. They still have untapped potential to strengthen cyber security protocols, nevertheless. The uses and ramifications of using GANs to improve cyber security are explored in this abstract. First, by using GANs for data augmentation, realistic and varied datasets that are essential for training malware classifiers, anomaly detection models, and intrusion detection systems can be created. Through the generation of synthetic data that closely mimics real-world cyber threats, GANs enable more thorough and efficient training, strengthening security mechanisms against emerging cyber-attacks in the process. GANs help with security testing and password cracking. This helps security experts assess how strong passwords are and strengthen authentication procedures to fend off possible intrusions.

DOI: 10.4018/979-8-3693-3597-0.ch013

INTRODUCTION

Safeguarding personal information and impeding malicious actors have become essential in the highly interconnected digital world of today when cyber-attacks and data breaches happen often. It has been demonstrated that traditional cyber security techniques are unable to stop fraudsters' ever-evolving tactics. To address these problems, new approaches are required. Using Generative Adversarial Networks (GANs) to strengthen cyber security measures is one such approach. Because they can generate realistic data samples, Generative Adversarial Networks have gained significant momentum in a few disciplines since they were introduced by Ian Goodfellow and colleagues in 2014. The discriminator and the generator are the two neural networks that make up a GAN. They compete with one another. It is the discriminator's responsibility to distinguish between real and fake. While the generator's objective is to produce synthetic data samples that are exact replicas of real data, the discriminator's task is to distinguish between real and fake data.

GANs produce samples and iteratively improve their quality through this adversarial process. GANs have a wide range of uses in cyber security, from adversarial training and data anonymization to threat detection and intrusion prevention. Generating synthetic data to train robust intrusion detection systems (IDS) is one of the main uses of GANs in cyber security. With the help of GANs, a variety of realistic datasets can be produced, allowing IDS models to be trained more successfully to identify unusual activity and more accurately identify possible cyber threats.

GANs can also be used in the field of adversarial machine learning, where they can be used to strengthen cyber security defenses powered by AI against hostile attacks. Adversarial assaults are when input data is manipulated to trick machine learning algorithms and produce inaccurate results. Cyber security algorithms can be strengthened against adversarial cases by exposing them to a wide variety of examples during the training phase by using GANs.

Furthermore, by creating synthetic data that maintains the statistical characteristics of the original dataset while guaranteeing privacy and secrecy, GANs help data anonymization approaches. This is especially important in situations where exchanging sensitive data for joint research or analysis is required yet puts personal privacy at risk. (Goodfellow, et.al 2014).

Finally, Generative Adversarial Networks offer an attractive paradigm for improving cyber security on several fronts. Organizations may usher in a new era of cyber resilience in an increasingly digital environment by utilizing GANs to strengthen defense mechanisms, increase threat detection accuracy, limit adversarial risks, and preserve critical data. To ensure responsible and ethical usage of GANs in cyber security, it is crucial to recognize and handle the ethical issues and potential misuse related to their deployment.

LITERATURE SURVEY

- (Arora and Shantanu, 2022) reviewed uses for Generative Adversarial Networks in the cyber security domain. The paper also places a lot of emphasis on a case study of anomaly detection and generation using the KDD-NSL dataset. While it offers a good overview of some of the different GAN models.
- (Cai et al .2022) have produced a comprehensive and in-depth analysis of the security and privacy aspects where GAN can be used. This paper fiercely presents the opposing views of GAN

14 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/enhancing-cyber-security-through-generative-adversarial-networks/347467

Related Content

The Neglect of Technology in Theories of Policy Change

Albert Meijer and Karl Löfgren (2015). *International Journal of Public Administration in the Digital Age* (pp. 75-88).

www.irma-international.org/article/the-neglect-of-technology-in-theories-of-policy-change/121525

Investigating Factors Influencing the Quality of Crowdsourced Work Under Different Incentives: Some Empirical Results

Evangelos Mourelatos and Manolis Tzagarakis (2019). *Crowdsourcing: Concepts, Methodologies, Tools, and Applications* (pp. 1263-1281).

www.irma-international.org/chapter/investigating-factors-influencing-the-quality-of-crowdsourced-work-under-different-incentives/226790

Family and Care Work Facing Social Change and Globalization: Conjunction between Family, Care Work and Immigration in Japan

Reiko Ogawa (2012). *International Journal of Public and Private Healthcare Management and Economics* (pp. 41-53).

www.irma-international.org/article/family-care-work-facing-social/76380

Factors Affecting the Adoption of Self-Service Technology (SST) in the Public Sector: An Empirical Examination of Housing Corporations

Guido Ongena, Sanne Staat and Pascal Ravesteijn (2020). *International Journal of Public Administration in the Digital Age* (pp. 32-46).

www.irma-international.org/article/factors-affecting-the-adoption-of-self-service-technology-sst-in-the-public-sector/264240

"Zeropay": The Simple Payment Service for Small Businesses – The Strategic FinTech Policy in Seoul Metropolitan Government

June-Suh Cho (2020). *International Journal of Public Administration in the Digital Age* (pp. 47-69).

www.irma-international.org/article/zeropay/264241