Chapter 1
Overview of Generative AI Techniques for Cybersecurity

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

Krishna Raj V. Prabagaran
Universiti Malaysia Sarawak, Malaysia

Rehan Akbar
https://orcid.org/0000-0002-3703-5974
Florida International University, USA

Manzoor Hussain
Indus University, Pakistan

Nazir Ahmed Malik
https://orcid.org/0000-0002-0118-4601
Bahria University, Islamabad, Pakistan

ABSTRACT

Generative AI techniques have been popular since they can generate data or content that could be hardly distinguished from genuine ones. This chapter comprehensively reviews generative AI for cybersecurity and its definition, history, and applications in different fields. It covers basic ideas such as generative models, probability distributions, and latent spaces. Also, it goes into more detail on some of the more popular approaches like GANs, VAEs, and the combination of RL. The chapter explores the structure and training processes of GANs and VAEs and demonstrates

DOI: 10.4018/979-8-3693-5415-5.ch001

their application in tasks such as image synthesis, data enhancement, and novelty detection. Also, it explores the interaction between RL and generative models and the challenges, including the exploration-exploitation trade-off. The chapter focuses on the development of generative AI with the help of DL and analyses the benefits of deep generative models and their usage in various fields. Evaluation measures and the problems with measuring generative models are discussed, focusing on the methods of improving the measurement accuracy. Finally, the chapter focuses on new directions, like transformer-based models and self-supervised learning, to look at the future of generative AI. The emphasis is made on understanding these techniques due to their versatility, and some ideas about the possible further developments of the findings for other fields and future studies and applications are provided.

INTRODUCTION TO GENERATIVE AI

Definition of Generative AI

Generative AI stands out as a form of intelligence setting itself apart from conventional approaches that focus on analyzing data to draw conclusions and make decisions. Unlike its counterparts generative AI is geared towards creating content, like text, images or music. These sophisticated algorithms are crafted to recognize patterns and characteristics within a dataset and generate data resembling it. Operating at a level of Machine Learning (ML) techniques such as learning generative AI excels at approximating probabilistic distributions to yield remarkably lifelike outcomes. Its ability to spark creativity and produce works across domains has garnered significant attention and acclaim. Generative AI models function by learning from datasets to grasp the structure and features of the information. Effectively trained these models can generate samples that rival the quality of the original dataset. Among the employed techniques in AI is GANs as described by Dash et al. (2023). GANs comprise two networks. The generator and the discriminator. That train harmoniously in tandem. While the generator focuses on creating data samples the discriminator strives to differentiate between generated data driving a continuous enhancement, in the quality of generated outputs. In AI there is another known technique called VAEs, which was introduced by Ye and Borş in 2023. VAEs can create a representation of the input data and produce samples using this hidden space. These models are commonly applied in tasks like generating images or detecting anomalies. The components of AI can be seen in Figure 1 provided below.