GAN Models for Malware Detection: A Survey

Ankita Ghosh
Department of Computer Science and Engineering, Indira Gandhi Delhi Technical University for Women, Delhi, Tamil Nadu, India

Anisha Das
Department of Information Technology, Indira Gandhi Delhi Technical University for Women, Delhi, Tamil Nadu, India

Abstract

This survey paper covers the application of Generative Adversarial Networks (GANs) to malware detection, focusing on how these networks can enhance detection capabilities by producing artificial malware samples. Traditional signature-based detection has become less effective due to the ongoing evolution of cyberthreats, particularly when identifying new or polymorphic malware. The study examines the advantages and disadvantages of various GAN architectures for malware detection, including DCGAN, AC-GAN, CycleGAN, and WGAN. The necessity of large and varied datasets such as VirusShare and EMBER, as well as the potential of GANs to address issues with data imbalance in malware detection systems, are also mentioned in the paper. Despite their impressive improvements in detection performance and resilience, GANs also present challenges such as computational cost, training instability, and ethical concerns when used to create evasive malware. The current survey provides a thorough overview of malware detection with GANs, outlining its advantages, disadvantages, and potential research directions.

Keywords

Malware Detection, GANs, Dataset, Malware Generation.