RADemics

Real Time Anomaly Detection in Cybersecurity Using Generative Adversarial Networks and Autoencoders

Sudhanshu Kumar Jha, M. Kavitha,
UNIVERSITY OF ALLAHABAD, UNIVERSITY OF ALLAHABAD.

13. Real Time Anomaly Detection in Cybersecurity Using Generative Adversarial Networks and Autoencoders

1Sudhanshu Kumar Jha, Assistant Professor, Department of Electronics and Communication, University of Allahabad, Prayagraj, Uttar Pradesh, India. sudhanshukumarjha@gmail.com

2M. Kavitha,, Assistant Professor, Department of Electronics and Communication, University of Allahabad, Prayagraj, Uttar Pradesh, India. sudhanshukumarjha@gmail.com

Abstract

Anomaly detection was a critical aspect of cybersecurity, with the increasing complexity and volume of data posing significant challenges for traditional methods. This chapter explores the application of advanced deep learning techniques, specifically Autoencoders and Generative Adversarial Networks (GANs), for real-time anomaly detection in cybersecurity. Autoencoders are employed for their ability to learn a compact representation of normal system behavior, enabling the identification of outliers based on reconstruction errors. GANs, through their adversarial training approach, enhance anomaly detection by generating synthetic data that improves model robustness. The chapter delves into the fundamental principles of these models, their training processes, and how they effectively balance sensitivity and specificity in detecting anomalies. Challenges such as dataset quality, noise handling, and the trade-off between false positives and negatives are addressed. Through the integration of Autoencoders and GANs, this chapter offers innovative insights into enhancing cybersecurity defense systems.

Keywords:

Anomaly Detection, Autoencoders, Generative Adversarial Networks, Cybersecurity, Deep Learning, Real-Time Detection

Introduction

As the digital landscape evolves, so do the tactics and sophistication of cyber threats [1]. Traditional security mechanisms, such as signature-based intrusion detection systems (IDS), often fail to identify novel or zero-day attacks that deviate from known patterns [2-4]. With the rapid increase in the volume and variety of data generated within enterprise networks, detecting subtle anomalies, whichindicate a breach, has become increasingly difficult [5-7]. Conventional approaches rely on predefined patterns of malicious behavior, making them inadequate against sophisticated and previously unseen cyberattacks [8,9]. As cyber threats grow more complex and elusive, there was a pressing need for more adaptive and scalable solutions [10]. Advanced machine learning techniques, including Autoencoders and Generative Adversarial Networks (GANs), offer promising alternatives, capable of detecting anomalies in real-time without the need for extensive labeled datasets [11,12]. These methods leverage unsupervised learning and

generative capabilities, which makes them highly effective in identifying anomalies, even those previously unknown [13,14].

Autoencoders have gained significant attention in anomaly detection due to their ability to learn compressed representations of normal data and identify deviations from these patterns [15,16]. By reconstructing input data through a bottleneck architecture, Autoencoders minimize the difference between the input and output, effectively learning the underlying features of normal data [17,18]. When exposed to an anomaly, the reconstruction error increases, signaling a deviation from the learned norm [19,20]. This unsupervised learning approach allows Autoencoders to detect outliers without needing labeled anomaly data, making them ideal for applications where anomalies are rare or unknown [21,22]. The ability to identify anomalies based on the reconstruction error makes Autoencoders particularly useful in detecting intrusions, fraudulent activities, and other malicious actions in cybersecurity [23,24]. Their application in network security, for example, allows systems to identify unusual patterns of behavior, whichindicate unauthorized access or abnormal network traffic that could point to an attack [25].

Generative Adversarial Networks (GANs) represent another breakthrough in machine learning that has shown promise for anomaly detection. GANs consist of two networks: a generator and a discriminator, which work in opposition to each other. The generator creates synthetic data samples, while the discriminator attempts to differentiate between real and fake data. This adversarial training process enables GANs to model complex data distributions, making them effective at detecting anomalies that do not conform to established patterns. GANs can generate realistic samples of normal behavior, and anomalies can be identified as instances that deviate from this generated data. The capacity of GANs to capture intricate patterns within data makes them an ideal solution for detecting novel or evolving threats in real-time, such as zero-day attacks. By modeling the distribution of normal data, GANs can effectively spot deviations that represent previously unseen threats, enhancing the overall detection accuracy and robustness of cybersecurity systems.