Chapter 6
Enhancing Network Security on a Hybrid LSTM–Gradient Boosting Framework for Intrusion Detection

R. Saranya
https://orcid.org/0009-0005-2415-4930
Bharath Institute of Higher Education and Research, India

S. Silvia Priscila
https://orcid.org/0000-0002-6040-3149
Bharath Institute of Higher Education and Research, India

ABSTRACT

The chapter presents a new hybrid intrusion detection framework that combines LSTM networks with gradient-boosting techniques. The approach presented in this study utilizes two prominent datasets, namely CICIDS2018 and CICIDS2017. The main objective is to improve the precision and reliability of intrusion detection in systems. This is achieved by capturing temporal dependencies in network traffic data and improving predictive performance by implementing boosting algorithms. The datasets are subjected to a thorough preprocessing process involving cleaning, normalization, and feature selection. This guarantees that the input for the model is of the highest quality. The LSTM component functions as the central element, extracting complex patterns and relationships from sequential data. The predictions generated by the LSTM model are refined by gradient boosting algorithms, which utilize their ensemble learning capabilities to improve overall performance.

DOI: 10.4018/979-8-3373-4672-4.ch006

INTRODUCTION

In today's rapidly evolving digital landscape, the prevalence of cyber threats continues to rise and presents a formidable obstacle to the security of networked systems (Admass et al., 2024). The growing dependence on interconnected technologies in diverse sectors, such as finance and healthcare, has significantly amplified the potential consequences of cyber-attacks (Cremer et al., 2022). The attacks carried out by individuals with bad intentions aiming to exploit vulnerabilities in network security cover a wide range of tactics, including advanced malware and specific infiltration methods (Reaves and Morris, 2009; Sudar et al., 2020; Ahmad et al., 2021). As a result, organizations are increasingly under pressure to enhance their cybersecurity measures and protect sensitive data from unauthorized access and manipulation. One of the key challenges in addressing cyber threats is the need for effective intrusion detection (Kumar and Sharma, 2018). Efforts are made to detect and counteract unauthorized access attempts and fraudulent activities within network environments (Renjith, 2024). Within the area of detection of attacks, conventional methods have traditionally leaned on rule techniques and signature techniques detection mechanisms to pinpoint familiar hazards (Kalra et al., 2020).

Nevertheless, the ever-changing landscape of cyber-attacks, known for their elusive and adaptable characteristics, has made traditional approaches progressively less successful (Van Houdt et al., 2020). Network traffic data's vast amount and complexities pose significant obstacles in promptly and accurately detecting every possible risk (Jeba et al., 2023). As organizations face the challenge of analyzing vast amounts of data generated by their interconnected systems, differentiating between real threats and harmless network activity becomes increasingly difficult (Pranav et al., 2024). Within this particular context, there is an urgent requirement for sophisticated detection mechanisms that can identify nuanced patterns and irregularities that may suggest malicious intentions amidst the overwhelming volume of network traffic (Boye, 2024). To effectively combat the constantly evolving cyber threats, intrusion detection solutions must be able to adapt and withstand the ever-changing attack strategies and tactics (Raja et al., 2024).

In the ever-evolving world of cybercrime, criminals always find innovative ways to avoid detection and take advantage of weaknesses, making traditional detection methods ineffective (Dhinakaran et al., 2023). Therefore, it is crucial to develop intrusion detection frameworks that can quickly adapt to emerging threats and rapidly evolving attack vectors (Varmann et al., 2023). Given the previous scenario, this work addresses the pressing need for robust and adaptable detection systems that can successfully fend off the growing flood of cyberattacks. The primary objective is to improve the efficiency of the detection mechanisms by utilizing machine learning and deep learning techniques, particularly Long Short-Term Memory networks, in