Chapter 14
Convolution Neural Network-Based Efficient Development of Intrusion Detection Using Various Deep Learning Approaches

G. Gowthami
Bharath Institute of Higher Education and Research, India

S. Silvia Priscila
Bharath Institute of Higher Education and Research, India

ABSTRACT

As internet usage has increased, firewalls and antiviruses are not alone enough to overcome the attacks and assure the privacy of information in a computer network, which needs to be a security system with multiple layers. Security layers are a must for protecting the network system from any potential threats through regular monitoring, which is provided with the help of IDS. The main objective of implementing intrusion detection is to monitor and identify the possible violation of the security policies of the computer system. Working preventively rather than finding a solution after the problem is essential. Threat prevention is done using intrusion detection systems development based on security policies concerning integrity, confidentiality, availability of resources, and system data that need to be preserved from attacks. In this research, three algorithms, namely Artificial Neural Network (ANN), Multi-Layer Perceptron (MLP), and Convolution Neural Network (CNN), have been used. From the results obtained, the proposed Convolution Neural Network (CNN)produces an Accuracy of 90.94%, MSE of 0.000242, Log Loss of 0.4079 and Mathews Coefficient of 0.9177. The tool used is Jupyter Notebook, and the language used is Python.

DOI: 10.4018/979-8-3693-1355-8.ch014

INTRODUCTION

Intrusion detection is a critical component of cybersecurity, aiming to identify and respond to unauthorized activities or security breaches within a computer system or network. Traditional intrusion detection systems (IDS) often rely on rule-based or signature-based approaches, which may struggle to adapt to the evolving nature of cyber threats (Jafar et al., 2019). Deep learning, a subset of machine learning, has emerged as a powerful tool for enhancing intrusion detection capabilities by leveraging complex neural network architectures to learn and recognize patterns indicative of intrusions automatically. Here, we delve into the application of deep learning in intrusion detection and its key aspects (AlAjmi et al., 2013). Deep learning algorithms, particularly deep neural networks, are designed to mimic the structure and functionality of the human brain (Alfaifi & Khan, 2022). They consist of multiple layers of interconnected nodes (neurons), each extracting hierarchical features from the input data (Francis & Sheeja, 2023). The deep architecture enables the model to automatically learn intricate representations of complex patterns and relationships within the data (Gaayathri et al., 2023).

APPLICATION OF DEEP LEARNING IN INTRUSION DETECTION

Anomaly Detection: Deep learning excels in anomaly detection, a crucial aspect of intrusion detection. Unlike signature-based systems that rely on predefined rules, deep learning models can learn normal behaviour patterns from the data. Deviations from these learned patterns are flagged as anomalies, potentially indicating unauthorized or malicious activities (Chunduri et al., 2023). This approach is particularly effective in identifying novel and previously unseen threats.

Feature Extraction: Deep learning models automatically extract relevant features from raw input data, eliminating the need for manual feature engineering (Francis & Sheeja, 2024). In intrusion detection, these features may include network traffic patterns, user behaviour, or system log data (Dwivedi, Pankaj & Sharma, 2023). The ability of deep learning to discern intricate and abstract features contributes to detecting subtle anomalies indicative of intrusions (Goswami et al., 2022).

Adaptability to Evolving Threats: Deep learning models exhibit adaptability to evolving threats, making them well-suited for dynamic cybersecurity environments (Haider et al., 2024). As cyber threats continuously evolve, traditional IDS may struggle to keep pace with new attack vectors. Deep learning, however, can continuously learn from new data, enabling the system to adapt and recognize emerging patterns associated with novel threats (Alzubi et al., 2023a).

Network Traffic Analysis: Deep learning is particularly effective in analyzing network traffic, a common source of information for intrusion detection (Manoj et al., 2023). Models can learn normal traffic patterns and identify deviations, such as unusual communication patterns, data exfiltration attempts, or malicious network activities (Alzubi et al., 2023). This capability enhances the detection of known and unknown threats within network traffic.

Behavioural Analysis: Deep learning facilitates behavioural analysis by learning patterns associated with normal user or system behaviour (Alzubi et al., 2023b). Deviations from these learned behaviours, such as unexpected access attempts or privilege escalations, can trigger alerts for potential intrusions. This approach is valuable in detecting insider threats or attacks that involve compromised user credentials (Kaliyaperumal et al., 2021).