Chapter 18
Harnessing Deep Learning for Enhancing Security for Social Empowerment

T. Venkat Narayana Rao
https://orcid.org/0000-0002-1996-1819
Jawaharlal Nehru Technological University, India

Ananya Seeta
Jawaharlal Nehru Technological University, India

J. V. P. Udaya Deepika
Jawaharlal Nehru Technological University, India

Kumari G. Seshu
Jawaharlal Nehru Technological University, India

ABSTRACT

Critical structures are increasingly susceptible to cyber threats, leading to the inadequacy of traditional security measures. This study explores the application of deep learning tools aimed specifically at enhancing the security of vital systems, such as power grids and transportation networks. By employing convolutional neural networks and recurrent neural networks, the research conducts an analysis of network traffic data to identify security anomalies. An inclusive dataset, which includes simulated attack scenarios, with workable models. Preliminary findings indicate that the convolutional neural network model achieved a high level of anomaly detection accuracy, ominously surpassing the performance of conventional

DOI: 10.4018/979-8-3373-0954-5.ch018

methods. Furthermore, the recurrent neural network model demonstrated enhanced capabilities in detecting time-sensitive threats, resulting in an extensive reduction in false positives. This chapter focus on future research should focus on examining the integration of deep learning models with security frameworks to fortify resilience against evolving threats

1. INTRODUCTION

The increasing complexity of cyber threats targeting critical infrastructure has necessitated the development of more sophisticated security measures, with deep learning emerging as a transformative approach. Traditional cybersecurity methods, such as signature-based detection and rule-based analysis, have proven inadequate against modern adversarial attacks, particularly zero-day exploits and adaptive threats. As a result, deep learning, with its ability to autonomously detect patterns and anomalies in large datasets, has gained prominence in cybersecurity research (Aldhaheri et al., 2024). However, while many studies highlight the potential of deep learning, its integration into cybersecurity frameworks remains an evolving challenge that requires a critical review of existing methodologies, theoretical underpinnings, and practical applications. Furthermore, the effectiveness of deep learning techniques depends on their adaptability to different cybersecurity domains, necessitating a broader discussion of their implementation across various sectors of critical infrastructure.

Deep learning's relevance in cybersecurity has grown significantly due to the increasing sophistication of AI-powered cyberattacks. Attackers now leverage artificial intelligence to bypass traditional security defenses, creating an arms race between cybercriminals and security professionals. Real-world incidents, such as AI-generated phishing schemes and adversarial attacks on machine learning models, illustrate the urgency of advancing AI-driven security mechanisms (Goodfellow et al., 2015). For instance, adversarial malware can subtly modify its code to evade detection, tricking AI-based security systems into classifying it as benign software (Kurakin et al., 2017). These developments present significant challenges for conventional security frameworks, which often rely on predefined patterns and static rule-based mechanisms. The ability of deep learning models to detect emerging threats in real time has therefore become essential in mitigating risks before they escalate into large-scale cyber incidents.

While the advantages of deep learning in cybersecurity are widely acknowledged, its deployment in critical infrastructure security poses unique challenges. One of the primary concerns is the computational intensity required to train and deploy deep learning models, which may not always be feasible for resource-constrained