



Deep Learning-Based Network Intrusion Detection Using a Hybrid
CNN-LSTM Framework

Prepared By

Name: Megern Qaisse

ID No.: 253001866

Submitted in fulfillment of the requirements for the degree Master of
Science in Artificial Intelligence

At

Collage of Informatics

Midocean University

UAE

Supervisor Name: **Dr. Amjad Qtaish**

Collage of Informatics, Midocean University, Comoros

Email:.....

Acknowledgements

Special thanks to **Dr. Amjad Qtaish**

Abstract

List of Publications

Table of Contents

List of Abbreviations.....	xiv
List of Figures.....	xvi
List of Tables	xviii

Chapter 1: Introduction and

Overview.....	
1.2 Problem Definition	
1.3 Thesis Objectives	
1.4 Thesis Contribution	
1.5 Thesis Organization.....	

Chapter 2: Background and Related Work

2.1 Introduction	
2.2 Intrusion Detection Systems (IDS)	
2.3 Types of Intrusion Detection Approaches	
2.4 Machine Learning in Intrusion Detection	
2.5 Deep Learning for Intrusion Detection	
2.6 Related Work	
2.7 Research Gap	

Chapter 3: Proposed Framework and Methodology

4.1 Introduction	
------------------------	--

Chapter 4: Experimental Results and Discussion

Chapter 5: Conclusion and Future Work

7.1 Important Features	
7.3 Future Work	

References	
------------------	--

List of Abbreviations

Acc.: Accuracy
ANN: Artificial Neural Network
CNN: Convolutional Neural Network
LSTM: Long Short-Term Memory
DL: Deep Learning
ML: Machine Learning
IDS: Intrusion Detection System
DoS: Denial of Service
ROC: Receiver Operating Characteristic
AUC: Area Under the Curve
TP: True Positive
FP: False Positive
TN: True Negative
FN: False Negative

List of Figures

- 2.1 General Architecture of Intrusion Detection Systems
- 2.2 Types of Network Attacks in IDS
- 2.3 Overview of Deep Learning in Cybersecurity
- 3.1 Proposed Hybrid CNN-LSTM Framework
- 3.2 Data Preprocessing Pipeline
- 4.1 Confusion Matrix of the Proposed Model
- 4.2 ROC Curve of the Proposed Model

List of Tables

- 2.1 Summary of Related Work in Deep Learning-based IDS
- 3.1 NSL-KDD Dataset Description
- 4.1 Performance Comparison Between Proposed Model and Traditional ML Models
- 4.2 Evaluation Metrics Results (Accuracy, Precision, Recall, F1-score)

Chapter 1 Introduction

1.1 Overview

The rapid growth of digital communication and internet-based services has significantly increased the exposure of computer networks to various cybersecurity threats. Organizations across sectors rely heavily on networked systems to store, process, and transmit sensitive information. As a result, cyberattacks such as denial-of-service (DoS), probing, unauthorized access, and malware-based intrusions have become more frequent and sophisticated.

Intrusion Detection Systems (IDS) play a crucial role in identifying malicious activities within network environments. Traditional IDS approaches typically rely on rule-based detection mechanisms or classical machine learning algorithms. However, these approaches often struggle to detect complex and previously unseen attack patterns. Additionally, high false positive rates remain a persistent challenge, leading to inefficient security monitoring.

Recent advancements in artificial intelligence, particularly deep learning, have demonstrated promising results in pattern recognition and anomaly detection tasks. Deep learning models are capable of automatically extracting complex representations from large datasets, making them suitable for cybersecurity applications. This research focuses on leveraging deep learning techniques to enhance network intrusion detection performance.

Specifically, this thesis proposes a hybrid deep learning framework that integrates Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks to improve detection accuracy and reduce false alarms in network intrusion detection systems.

1.2 Problem Definition

Despite continuous advancements in cybersecurity technologies, existing intrusion detection systems face several limitations. Traditional signature-based systems can only detect known attacks and fail to identify new or evolving threats. On the other hand, anomaly-based systems may generate a high number of false positives due to difficulty in modeling complex network behavior.

Machine learning-based IDS have improved detection performance; however, many models struggle to capture both spatial relationships among network features and temporal dependencies within traffic sequences. As cyberattacks become increasingly sophisticated,

there is a need for more intelligent detection models capable of learning complex patterns from network data.

Therefore, the main problem addressed in this research is:

How can a hybrid deep learning model combining CNN and LSTM improve the accuracy and reliability of network intrusion detection compared to traditional machine learning approaches?

1.3 Thesis Objectives

The primary objectives of this thesis are:

- To design and implement a hybrid CNN-LSTM deep learning model for network intrusion detection.
- To preprocess and prepare the NSL-KDD dataset for effective model training.
- To evaluate the performance of the proposed model using standard evaluation metrics such as Accuracy, Precision, Recall, and F1-score.
- To compare the proposed deep learning model with selected traditional machine learning classifiers.
- To analyze the impact of hybrid modeling on reducing false positives in intrusion detection systems.

1.4 Thesis Contribution

The main contributions of this thesis are summarized as follows:

- Proposing a hybrid deep learning framework that integrates CNN for spatial feature extraction and LSTM for temporal pattern learning in network intrusion detection.
- Providing a comprehensive experimental evaluation using a benchmark dataset (NSL-KDD).
- Conducting a comparative analysis between the proposed hybrid model and conventional machine learning approaches.
- Demonstrating the effectiveness of deep learning in improving intrusion detection performance and minimizing false alarm rates.

1.5 Thesis Organization

The remainder of this thesis is organized as follows:

Chapter 2 presents the background and related work in intrusion detection systems and deep learning techniques. It reviews existing studies and identifies research gaps in current IDS approaches.

Chapter 3 describes the proposed hybrid CNN-LSTM framework and explains the methodology adopted in this research, including dataset preprocessing, model design, and implementation details.

Chapter 4 presents the experimental results and performance evaluation of the proposed model, along with a comparative analysis against traditional machine learning classifiers.

Finally, Chapter 5 concludes the thesis by summarizing the key findings and discussing potential directions for future research.

Chapter 2 Background and Related Work

2.1 Introduction

Cybersecurity has become a critical concern for modern information systems due to the increasing reliance on digital infrastructures and network-based services. Organizations depend heavily on computer networks to store, process, and transmit sensitive information, which makes these systems attractive targets for cyber attackers. Consequently, detecting and preventing malicious network activities has become an essential requirement for maintaining secure information systems.

Intrusion Detection Systems (IDS) are widely used to monitor network traffic and identify suspicious or malicious behavior. These systems analyze network activities in order to detect attacks such as denial-of-service (DoS), unauthorized access attempts, probing attacks, and other forms of cyber intrusions. Over the years, various approaches have been proposed to improve the effectiveness of IDS technologies.

Traditional IDS solutions mainly rely on signature-based detection or rule-based systems. While these approaches are effective in identifying known attacks, they often fail to detect new or previously unseen threats. In addition, anomaly-based detection systems may produce a high number of false positives due to the complexity of modeling normal network behavior.

Recent advances in machine learning and deep learning have introduced new opportunities for improving intrusion detection performance. Deep learning models have demonstrated strong capabilities in identifying complex patterns in large datasets. As a result, researchers have increasingly explored the application of deep learning techniques in cybersecurity and network intrusion detection.

This chapter provides the theoretical background necessary for understanding intrusion detection systems and the role of machine learning and deep learning

in this domain. It also reviews related studies that have applied artificial intelligence techniques to improve IDS performance.

2.2 Intrusion Detection Systems (IDS)

Intrusion Detection Systems are security tools designed to monitor network traffic and detect malicious activities or policy violations. IDS technologies play an important role in protecting computer networks from cyber threats by identifying abnormal behavior that may indicate an ongoing attack.

An IDS typically analyzes network packets, system logs, or host activities to determine whether a particular action represents normal behavior or a potential intrusion. Once suspicious activity is detected, the system generates alerts to notify security administrators.

IDS can generally be classified into two main categories: Host-Based Intrusion Detection Systems (HIDS) and Network-Based Intrusion Detection Systems (NIDS).

Host-Based IDS operates on individual devices or hosts and monitors internal system activities such as file changes, system calls, and log entries. In contrast, Network-Based IDS monitors network traffic across the entire network infrastructure, analyzing packets that travel between devices in order to detect malicious behavior.

2.3 Types of Intrusion Detection Approaches

Intrusion detection methods can be categorized into two primary approaches: signature-based detection and anomaly-based detection.

Signature-based detection identifies attacks by comparing network activity against a database of known attack signatures. When a match is found, the system flags the activity as malicious. Although this method is effective for detecting previously known attacks, it cannot identify new or unknown threats.

Anomaly-based detection, on the other hand, attempts to identify abnormal behavior by modeling normal network activity. Any deviation from the established normal behavior is considered suspicious. This approach is capable of detecting previously unknown attacks; however, it often suffers from high false positive rates.

With the advancement of artificial intelligence technologies, machine learning and deep learning approaches have been introduced to enhance anomaly detection capabilities in IDS systems.

2.4 Machine Learning in Intrusion Detection

Machine learning techniques have been widely applied in intrusion detection systems to automatically learn patterns from network data. Unlike traditional rule-based systems, machine learning algorithms can analyze large volumes of data and identify complex relationships between features.

Common machine learning algorithms used in IDS include Decision Trees, Support Vector Machines (SVM), Random Forest, and K-Nearest Neighbors (KNN). These algorithms are trained using labeled datasets that contain examples of both normal and malicious network activities.

Although machine learning models have shown improved performance in many intrusion detection tasks, they still face several limitations. Feature engineering often requires significant manual effort, and traditional algorithms may struggle to capture complex relationships in large and high-dimensional datasets.

2.5 Deep Learning for Intrusion Detection

Deep learning has recently emerged as a powerful technique for analyzing complex datasets and extracting high-level representations from raw data. Deep

neural networks can automatically learn relevant features from data without requiring extensive manual feature engineering.

Several deep learning architectures have been applied to intrusion detection systems, including Artificial Neural Networks (ANN), Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN). CNN models are particularly effective in extracting spatial patterns from structured data, while RNN models such as Long Short-Term Memory (LSTM) networks are capable of capturing temporal dependencies within sequential data.

Combining multiple deep learning architectures has also become a promising approach for improving detection performance. Hybrid models that integrate CNN and LSTM networks can benefit from both spatial feature extraction and temporal pattern recognition. This hybrid approach is expected to improve the accuracy and reliability of network intrusion detection systems.

2.6 Related Work

Recent research has extensively explored the use of machine learning and deep learning techniques for improving intrusion detection systems. Various approaches have been proposed to enhance detection accuracy and reduce false positive rates.

Tavallae et al. (2009) introduced the NSL-KDD dataset as an improved version of the KDD'99 dataset, addressing issues such as redundancy and imbalance. This dataset has since become a benchmark for evaluating intrusion detection models.

Kim et al. (2016) applied deep neural networks (DNN) for intrusion detection and demonstrated improved classification performance compared to traditional machine learning models. However, their model required extensive feature engineering.

Yin et al. (2017) proposed an LSTM-based intrusion detection system to capture temporal dependencies in network traffic. Their results showed that LSTM outperformed conventional machine learning algorithms, particularly in detecting sequential attack patterns.

Shone et al. (2018) introduced a deep autoencoder-based intrusion detection model combined with Random Forest. Their approach achieved high detection accuracy while reducing feature dimensionality.

Vinayakumar et al. (2019) evaluated the performance of deep learning models such as CNN and DNN on large-scale intrusion detection datasets. Their results indicated that deep learning models significantly outperform traditional methods in handling large datasets.

Alrawashdeh and Purdy (2016) utilized deep belief networks (DBN) for intrusion detection, demonstrating improved performance in detecting complex attack patterns.

Zhang et al. (2019) proposed a CNN-based intrusion detection model that effectively extracted spatial features from network traffic data. Their model showed improved performance over traditional classifiers.

Khan et al. (2020) developed a hybrid deep learning model combining CNN and LSTM for intrusion detection. Their study demonstrated that hybrid models can achieve higher accuracy by capturing both spatial and temporal patterns.

Li et al. (2020) proposed a deep learning-based intrusion detection system using bidirectional LSTM, achieving improved detection rates for complex attacks.

Ferrag et al. (2020) provided a comprehensive survey of deep learning-based intrusion detection systems, highlighting the advantages of hybrid models and identifying key research challenges.

Moustafa and Slay (2015) introduced the UNSW-NB15 dataset, which includes modern attack scenarios and has been widely used in IDS research.

Sohi et al. (2021) evaluated deep learning models for intrusion detection in IoT environments and demonstrated improved performance in detecting advanced threats.

Bedi et al. (2021) proposed a deep learning-based framework for anomaly detection, achieving high accuracy in identifying unknown attacks.

Verma and Ranga (2020) used ensemble learning techniques combined with deep learning for intrusion detection, improving classification performance.

Recent studies have shown that hybrid models combining CNN and LSTM provide better performance compared to single models, as they leverage both spatial and temporal feature extraction capabilities.

2.7 Research Gap

Despite the significant advancements in intrusion detection systems using machine learning and deep learning techniques, several challenges still remain.

Many traditional machine learning models rely heavily on manual feature engineering and struggle to capture complex patterns in network traffic data. Although deep learning approaches have improved detection accuracy, some models focus only on either spatial or temporal features, limiting their effectiveness.

Furthermore, some existing models suffer from high false positive rates, which can reduce the efficiency of intrusion detection systems in real-world environments. Additionally, there is still a need for models that can effectively handle both feature relationships and sequential dependencies in network traffic data.

Therefore, this research aims to address these limitations by proposing a hybrid CNN-LSTM model that combines spatial and temporal feature learning to improve intrusion detection performance.

Chapter 4 Proposed Approach (Methodology)

Chapter 5 :Experimental Results and Discussion

Chapter 6 Conclusion and Future Work

References

Tavallae et al., 2009 – NSL-KDD Dataset

Yin et al., 2017 – LSTM-based IDS

Shone et al., 2018 – Deep Autoencoder IDS

Vinayakumar et al., 2019 – Deep Learning IDS

Khan et al., 2020 – CNN-LSTM IDS

Ferrag et al., 2020 – Survey on DL IDS

Moustafa & Slay, 2015 – UNSW-NB15 Dataset