Euromed University of Fez (UEMF)

Faculty of Engineering

AI-Enhanced Intrusion Detection System

for Network Security

Academic Project Report

Module: Fundamentals of Cybersecurity

Class: 1st Year of Engineering Cycle – Artificial Intelligence

Professor: Zineddine Mhamed

Academic Year: 2024 – 2025

Prepared by:

Anas Touzi — Student ID: 2301174

Touimi Benjelloun Mohamed Abdelaziz — Student ID: 2300562

Abstract

With the continuous expansion of computer networks, cybersecurity threats have become increasingly complex and difficult to detect using traditional security mechanisms. Classical Intrusion Detection Systems (IDS) rely primarily on predefined rules and signatures, which limits their ability to identify new or evolving attacks. This project presents an AI-enhanced Intrusion Detection System based on machine learning techniques. Using the CICIDS2017 dataset, a neural network model is trained to classify network traffic as normal or malicious. The system includes data preprocessing, model training, evaluation, real-time detection simulation, and a visualization dashboard. Experimental results demonstrate very high detection accuracy, highlighting the effectiveness of artificial intelligence in modern network security.

1 Introduction

Cybersecurity has become a major concern due to the rapid growth of networked systems and the increasing sophistication of cyberattacks. Modern networks are exposed to threats such as Distributed Denial of Service (DDoS), brute-force attacks, and malware propagation.

Traditional Intrusion Detection Systems rely on rule-based or signature-based mechanisms, which are effective only for known attacks. These systems fail to adapt to new attack patterns, making them insufficient for modern security requirements.

Artificial Intelligence and Machine Learning provide adaptive solutions capable of learning network behavior. This project aims to design and implement an AI-based IDS capable of detecting malicious network traffic automatically.

2 Related Work

Signature-based IDS such as Snort and Suricata are widely deployed in real networks. However, they require constant rule updates and are ineffective against zero-day attacks.

Recent studies have demonstrated the effectiveness of machine learning algorithms, including Support Vector Machines, Random Forests, and Neural Networks, in intrusion detection tasks. Deep learning models are particularly suitable for analyzing complex and high-dimensional network traffic data.

3 Dataset Description

The CICIDS2017 dataset, developed by the Canadian Institute for Cybersecurity, was used in this project. It contains realistic network traffic captured under controlled conditions and includes both normal traffic and multiple attack types.

Each network flow is represented by statistical features such as flow duration, packet size, and packet rate, along with a corresponding class label.

4 System Architecture

The proposed IDS consists of the following components:

- Data preprocessing and cleaning
- Feature normalization
- Neural network training
- Model evaluation

- Real-time detection simulation
- Visualization dashboard

5 Data Preprocessing

Raw data preprocessing is essential to ensure reliable model performance. The preprocessing phase involved removing duplicates, handling missing and infinite values, normalizing numerical features, and encoding class labels.

The cleaned dataset was split into training and testing subsets to evaluate the generalization ability of the model.

6 Model Design and Training

A feedforward Artificial Neural Network was implemented using TensorFlow and Keras. The network consists of two hidden layers with ReLU activation functions and an output layer using Softmax activation.

The model was trained using the Adam optimizer and sparse categorical cross-entropy loss function.

7 Evaluation and Results

The trained model achieved excellent performance on the test dataset, with near-perfect accuracy, precision, recall, and F1-score. The confusion matrix confirmed a very low number of misclassifications.

These results demonstrate the effectiveness of AI-based intrusion detection systems when trained on high-quality data.

8 Real-Time Detection and Dashboard

A real-time detection simulation was implemented to validate practical applicability. Additionally, a Streamlit-based dashboard was developed to visualize detection results and provide real-time alerts.

9 Conclusion and Future Work

This project successfully demonstrated the use of artificial intelligence in intrusion detection. The AI-enhanced IDS outperformed traditional rule-based approaches and provided real-time monitoring capabilities.

Future work includes integration with real packet capture tools, deployment in operational networks, and hybrid integration with traditional IDS systems.