Smart Intrusion Detection with AI and Deep Learning for Enhanced Network Security

Abstract:

The Intrusion Detection System (IDS) project aims to develop a sophisticated and robust IDS leveraging modern machine learning (ML) and deep learning (DL) techniques. The primary goal is to enhance detection accuracy and minimize latency in identifying network intrusions, especially within complex environments like IoT and wireless networks. This system will utilize contemporary datasets such as CICIDS 2017, UNSW-NB15, IoT Network Traffic, and Wireless Network Traffic.

The project encompasses several key modules:

1. Data Collection and Preprocessing: This includes the collection of network traffic data, data cleaning, normalization, transformation, and feature extraction.
2. Model Training and Validation: It involves training ML models (e.g., SVM, Random Forest) and DL models (e.g., CNN, RNN, LSTM) using both traditional and modern datasets. Validation is performed using cross-validation and performance metrics such as accuracy, precision, recall, and F1-score.
3. Real-time Detection: This module implements real-time network traffic monitoring, integrating trained models for live intrusion detection, and generating alerts and logs.
4. Evaluation and Comparison: It focuses on evaluating model performance across different datasets and comparing traditional ML techniques with modern DL approaches.
5. User Interface: The development of a user-friendly dashboard for monitoring and managing alerts, visualizing network traffic, and reporting tools for analysis and decision-making.

The project utilizes Python for data processing and model development, JavaScript (Node.js) for real-time data handling, Scikit-learn for traditional ML models, TensorFlow/ Keras for DL models, and React.js for the user interface. By adopting these advanced technologies and datasets, the proposed IDS aims to be more adaptable and responsive to new and evolving cyber threats, ultimately contributing to improved network security.