Design and Implementation of an Intelligent Intrusion Detection System Using Machine Learning

Sawaira Haq , Rukhma Noor
Supervisor: Ihsan ul Haq
Department of Computer System Engineering
UET Peshawar

June 3, 2025

Abstract

This project proposes the design and implementation of an intelligent Intrusion Detection System (IDS) using machine learning techniques. It will utilize supervised learning to analyze network traffic and classify malicious behavior in real-time, addressing limitations of traditional signature-based systems.

Introduction

Cybersecurity threats are evolving as digital reliance increases. Traditional security systems often fail to detect unknown attacks. This project investigates a machine learning-based IDS for improved network protection.

Literature Review

- Traditional IDS: Signature-based (e.g., Snort) — limited to known threats.
- Anomaly-based IDS using ML: Detects unknown patterns.
- Datasets used: NSL-KDD, CIC-IDS2017, UNSW-NB15.
- Algorithms: Decision Trees, SVM, Random Forest, Deep Neural Networks.

Problem Statement

Current IDS systems:

- Cannot detect zero-day attacks effectively.
- Suffer from high false positive rates.
- Lack adaptability to evolving attack patterns.

Hypothesis

A machine learning-based IDS can outperform traditional systems by:

- Learning from historical network data.
- Adapting to new threats dynamically.
- Reducing false positives and enhancing detection accuracy.

Motivation

- Growing cyber threats necessitate intelligent security systems.
- Traditional IDS lacks real-time adaptability.
- Machine learning offers scalable and accurate intrusion detection capabilities.

Methodology

- **Literature Review**: Understand IDS and ML models.
- **Data Collection**: NSL-KDD, CIC-IDS2017.
- **Preprocessing**: Clean, normalize, label datasets.
- **Model Training**: SVM, Random Forest, DNN.
- **Evaluation**: Accuracy, Precision, Recall, F1-score.
- **Implementation**: Real-time IDS using Scapy/Wireshark.

Results and Discussion

- Algorithms will be compared on:
  - Accuracy
  - False Positive Rate
  - F1-Score
- Real-time testing on live traffic to assess robustness.

Conclusion and Future Work

- ML-based IDS shows promise in enhancing detection accuracy.
- Future enhancements:
  - Cloud deployment
  - Real-time adaptive learning
  - Automated threat response

Acknowledgement

Special thanks to:

- Supervisor: Ihsan ul Haq
- Department of Computer System Engineering, UET Peshawar

References

1. Tavallaee, M., et al. "A detailed analysis of the KDD CUP 99 data set."
2. Moustafa, N., & Slay, J. "UNSW-NB15: A comprehensive dataset for network intrusion detection systems."
3. Ali, S. S., et al. "Machine Learning Based Intrusion Detection for 5G Networks."

Gantt Chart

Phase	**Tasks**	**Duration**
Phase 1	Research and Literature Review	2 weeks
Phase 2	Data Collection and Preprocessing	2 weeks
Phase 3	Model Training and Evaluation	3 weeks
Phase 4	System Integration and Development	3 weeks
Phase 5	Testing and Analysis	2 weeks
Phase 6	Report Writing and Submission	2 weeks