

Enhancing Network Intrusion Detection Systems Using Machine Learning Techniques

Student Name: Keval Mahendra Motivaras

Student ID: 2515743

Module: ACFA7004

MSc Cybersecurity & Digital Forensics

Research Context / Background

Cyber-attacks grow rapidly (DDoS, ransomware, zero-day attacks)

Signature-based systems for IDS (like Snort):

- Recognize known cyber-attacks only.
- Cannot detect new types of cyber-attacks [1].

Growth of network complexity (IoT, Cloud, BYOD).

Machine Learning (ML) allows for:

- Pattern recognition.
- Anomaly detection.

Real-time cyber-attack detection.

“Modern cybersecurity needs intelligent and adaptive detection systems.”

Research Problem

Limitations of IDS based on tradition:

- Generation of high false positives
- Unable to detect attacks known as zero day attack

ML based IDS problems include:

- Poor real time performance.
- Issues related to imbalanced datasets.
- Limited generalization capability [1].

Problem statement:

“Present Intrusion Detection Systems have low detection accuracy and are not adaptable enough to detect new threats to cybersecurity.”

Aim & Objectives

Aim :

Develop an intrusion detection system using Machine Learning techniques that is more accurate and effective than present systems.

Project Objectives :

- Analysing IDS and ML techniques
- Selecting appropriate ML techniques (Random Forest, SVM, Deep Learning)
- Applying IDS using NSL-KDD/CICIDS2017 datasets
- Performance evaluation using Accuracy/Precision/Recall indicators
- Compare results with traditional IDS approaches

Literature Review

ML-based intrusion detection systems are more efficient than traditional IDS [1].

The use of deep learning enhances the efficiency of detecting attacks [2].

The Random Forest is an effective approach to classify data [3].

Challenges in the area:

- Imbalance of dataset
- Overfitting
- Real-time implementation

Research Gap:

- No optimized machine learning algorithm for real-time application

Network Traffic



Data Preprocessing



Feature Selection



ML Model



Detection Output

Proposed System

Data collected from network traffic

Preprocessing (cleaning, normalization)

Feature extraction

ML model classification:

Normal vs Attack

Output alerts

Research Methodology

Type:

Quantitative Analysis & Experimental Study

Datasets used:

- NSL-KDD & CICIDS2017[2].

Software:

- Python
- Scikit-learn
- Wireshark (if necessary)

Techniques used:

- Random Forest
- Support Vector Machine (SVM)
- Neural Networks

ML enables automatic detection of intrusions and higher scalability in comparison to rule-based approaches.

Data Collection & Evaluation

Data Collection:

Publicly available:

- NSL-KDD
- CICIDS2017

Evaluation Metrics:

- Accuracy
- Precision
- Recall
- F1-score
- Confusion Matrix

“Evaluation ensures reliability and effectiveness of the proposed IDS model.”

Project Timeline

PhaseDuration:

Week 1–2

- Literature Review

Week 3

- Data Collection

Week 4–6

- Model Development

Week 7

- Testing & Evaluation

Week 8

- Final Report

Resources

Tools:

- Python
- Jupyter Notebook
- Scikit-learn
- Kaggle datasets

Hardware:

- Laptop (8GB+ RAM)

Other:

- Academic papers
- Internet access

Impact & Limitations

Effects:

Increase in accuracy in cyber threat detection

Reduction in false positives

Beneficial for:

Organisations

Cloud security

IoT environment

Limitations:

Dependence on dataset

High computational complexity

Challenges in implementation in practical scenarios

Conclusion

- Machine Learning improves intruder detection through enhanced accuracy and flexibility
- Some disadvantages of IDS can be overcome using data-driven methods
- The above-proposed IDS is designed to lower the number of false positives
- Future work involves practical implementation

References

- [1] R. Sommer and V. Paxson, “Outside the Closed World: On Using Machine Learning for Network Intrusion Detection,” IEEE Symposium on Security and Privacy, 2010.
- [2] I. Sharafaldin, A. Habibi Lashkari and A. A. Ghorbani, “Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization,” ICISSP, 2018.
- [3] M. Ring et al., “A Survey of Network-Based Intrusion Detection Data Sets,” Computers & Security, 2019.

Thank You