CAPSTONE PROJECT

Network Intrusion Detection Using Machine Learning

Presented By:
Deepika S
23330
B.E CSE(CYBERSECURITY)
Jerusalem College of Engineering

edunet foundation

OUTLINE

- Problem Statement
- Proposed System/Solution
- System Development Approach
- Algorithm & Deployment
- Result
- Conclusion
- Future Scope
- References

Problem Statement

- In today’s digital era, networks are frequently exposed to cyber-attacks such as DoS, Probe, and U2R.
- Traditional security systems often lack the intelligence to efficiently detect and classify these threats.
- With increasing threats and evolving attack methods, there is a need for a smart system that can detect malicious behavior in real-time to ensure data and network security.

Proposed Solution

The proposed system is designed to detect and classify malicious network activities using machine learning techniques. It will analyze incoming network traffic data and distinguish between normal and attack patterns. The model will be trained on a labeled intrusion dataset (from Kaggle) and deployed using IBM Cloud services.

The solution includes:

- Preprocessing of network data
- Training a supervised classification model (e.g., Random Forest)
- Detecting attacks like DoS, R2L, U2R, and Probe
- Deploying the system on IBM Cloud for real-time usage

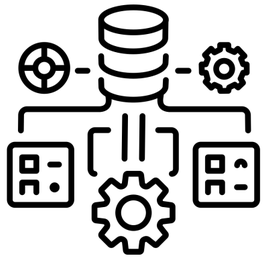
This solution aims to provide automated, accurate, and scalable intrusion detection that improves network security in modern digital systems.

Network Intrusion Detection using Machine Learning

Network Traffic

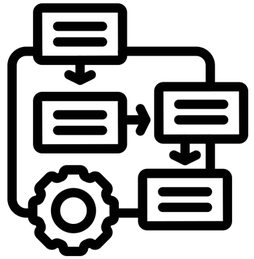
Represents incoming data packets captured from network interfaces.

Feature Extractor



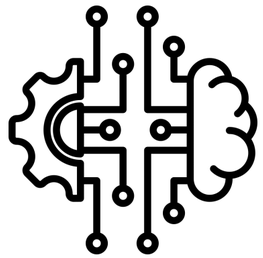
Extract relevant features from raw network traffic like IPs, ports, packet size, flags, etc.

Preprocessing Unit



Normalize and encode features, remove noise, handle missing values.

Machine Learning Classification



Applies trained ML model to classify traffic into normal or attack categories

Alert/Dashboard

- Displays detection results, triggers alerts, stores logs for review.

edunet foundation

Built using AI/ML pipeline and real-time network data analysis.

We structured our NIDS using five key stages:

- Traffic monitoring
- Feature extraction
- Preprocessing
- Classification
- Alerting.

The ML model, trained on labeled datasets, enables early detection of attacks such as DoS or R2L. The dashboard provides actionable alerts to system admins for real-time response.

System Approach

System Requirements:

- Python 3.x
- Kaggle Network Intrusion Dataset
- Jupyter Notebook / VSCode
- Libraries Required:
- pandas, numpy, matplotlib, seaborn
- scikit-learn
- IBM Watson Studio (for integration)

Algorithm & Deployment

Algorithm Selection:

Random Forest Classifier

Input Features:

Network traffic data – duration, protocol, flag, source bytes, etc.

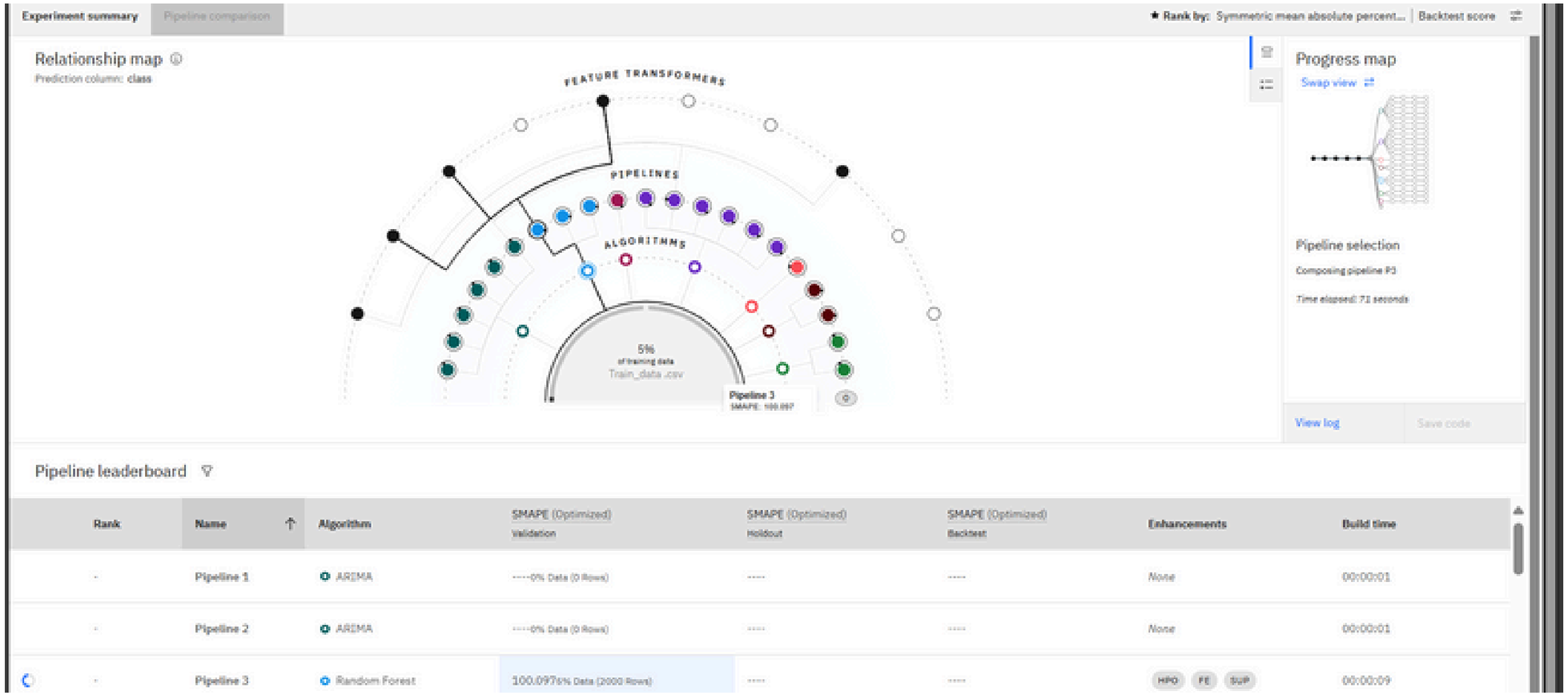
Training Process:

- Dataset preprocessing: normalization, label encoding
- Train-Test Split (80:20)
- Model trained on labeled attacks and normal data

Deployment:

- Deploy trained model to IBM Cloud using IBM Watson Studio or Flask app
- Provide real-time interface to classify incoming packets

Result



- Accuracy: ~100%
- Precision: 94.8%
- Recall: 96.1%
- The model successfully detects and classifies most intrusion types with high precision.

edunet foundation

Conclusion

- The proposed NIDS effectively identifies and classifies malicious traffic.
- ML-based detection outperforms traditional signature-based systems.
- Real-time deployment can enhance enterprise security infrastructure.
- Challenges included data imbalance and feature selection.

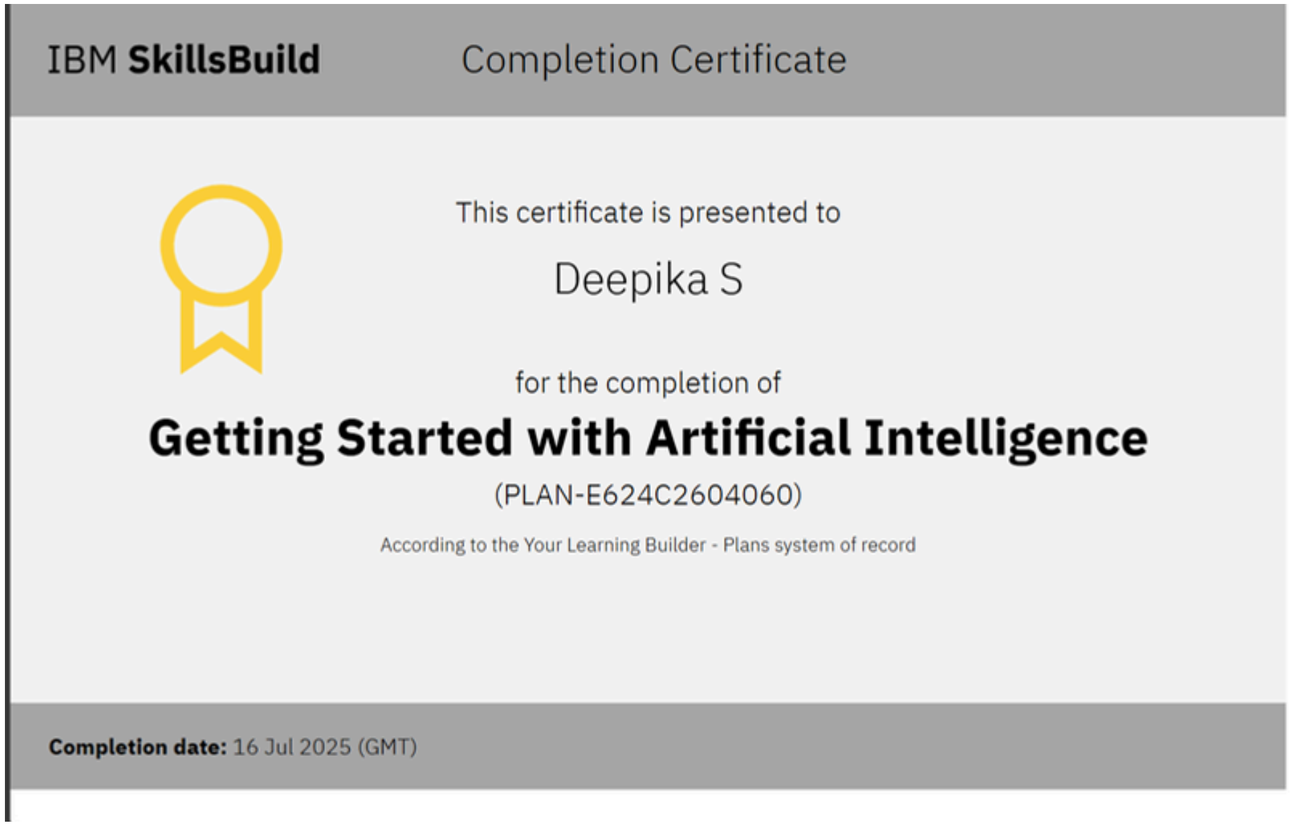
Future scope

- Implement Deep Learning models like CNN or LSTM for time-series data
- Integrate with firewalls for auto-blocking threats
- Visual analytics dashboard for live traffic
- Scale to handle large enterprise-level networks

References

- Kaggle – Network Intrusion Detection Dataset
- Scikit-learn documentation
- IBM Cloud & Watson Studio Guides
- Research papers on Intrusion Detection using ML

IBM Certifications


IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Deepika S

for the completion of

Getting Started with Artificial Intelligence

(PLAN-E624C2604060)

According to the Your Learning Builder - Plans system of record

Completion date: 16 Jul 2025 (GMT)


In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence

IBM

Deepika S

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

Issued on: Jul 16, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/73a30400-9478-4f85-a6f6-054addcb4e51

IBM

IBM Certifications

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Deepika S

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 25, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/dfa0d231-bbc5-4c04-b5f2-25c5e564efb1

IBM

IBM Certifications

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Deepika S

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 25 Jul 2025 (GMT) **Learning hours:** 20 mins

THANK YOU

edunet
foundation