CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. PRASHANT SANJEEV KAMAGOND-ACHARYA INSTITUTE OF TECHNOLOGY- Artificial Intelligence and Machine Learning

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

Create a robust network intrusion detection system (NIDS) using machine learning. The system should be capable of analyzing network traffic data to identify and classify various types of cyber-attacks (e.g., DoS, Probe, R2L, U2R) and distinguish them from normal network activity. The goal is to build a model that can effectively secure communication networks by providing an early warning of malicious activities.

PROPOSED SOLUTION

- To develop a machine learning-based Network Intrusion Detection System (NIDS) that analyzes network traffic to accurately detect and classify cyberattacks (e.g., DoS, Probe, R2L, U2R), enabling early warnings and enhanced network security. The solution will consist of the following components:
- Data Collection:
  - Utilize the Kaggle Network Intrusion Detection Dataset (https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection), which includes labeled instances of normal and malicious traffic.
  - Gather features such as duration, protocol type, service, flag, src_bytes, dst_bytes, and more, that represent various aspects of network connections.
- Data Preprocessing:
  - Preprocess the data by cleaning missing values, removing duplicates, encoding categorical features, and normalizing numerical values.
  - Handle class imbalance using techniques like undersampling to improve detection of rare attack types such as R2L and U2R.
- Machine Learning Algorithm:
  - Implement classification algorithms such as Random Forest, Support Vector Machine (SVM), K-Nearest Neighbors (KNN) to improve detection accuracy across diverse attack types.
  - Train the models to classify traffic into multiple categories: Normal, DoS, Probe, R2L, U2R.
- Deployment:
  - Deploy the trained classification model on IBM watsonx.ai to provide real-time predictions through a cloud-based, secure, and scalable environment.
- Evaluation:
  - Assess the model using metrics like Accuracy, Precision, Recall, and F1-score to measure classification performance.

SYSTEM APPROACH

The "System Approach" section outlines the overall strategy and methodology for developing and implementing the rental bike prediction system. Here's a suggested structure for this section:

- **System requirements :**

- **IBM Cloud** – Platform used for model deployment and cloud resources
- **IBM Watson Studio** – Used to build, train, and deploy the machine learning model
- **IBM Cloud Object Storage** – For storing and accessing the intrusion detection dataset *(Example: Cloud Object Storage-zv)*

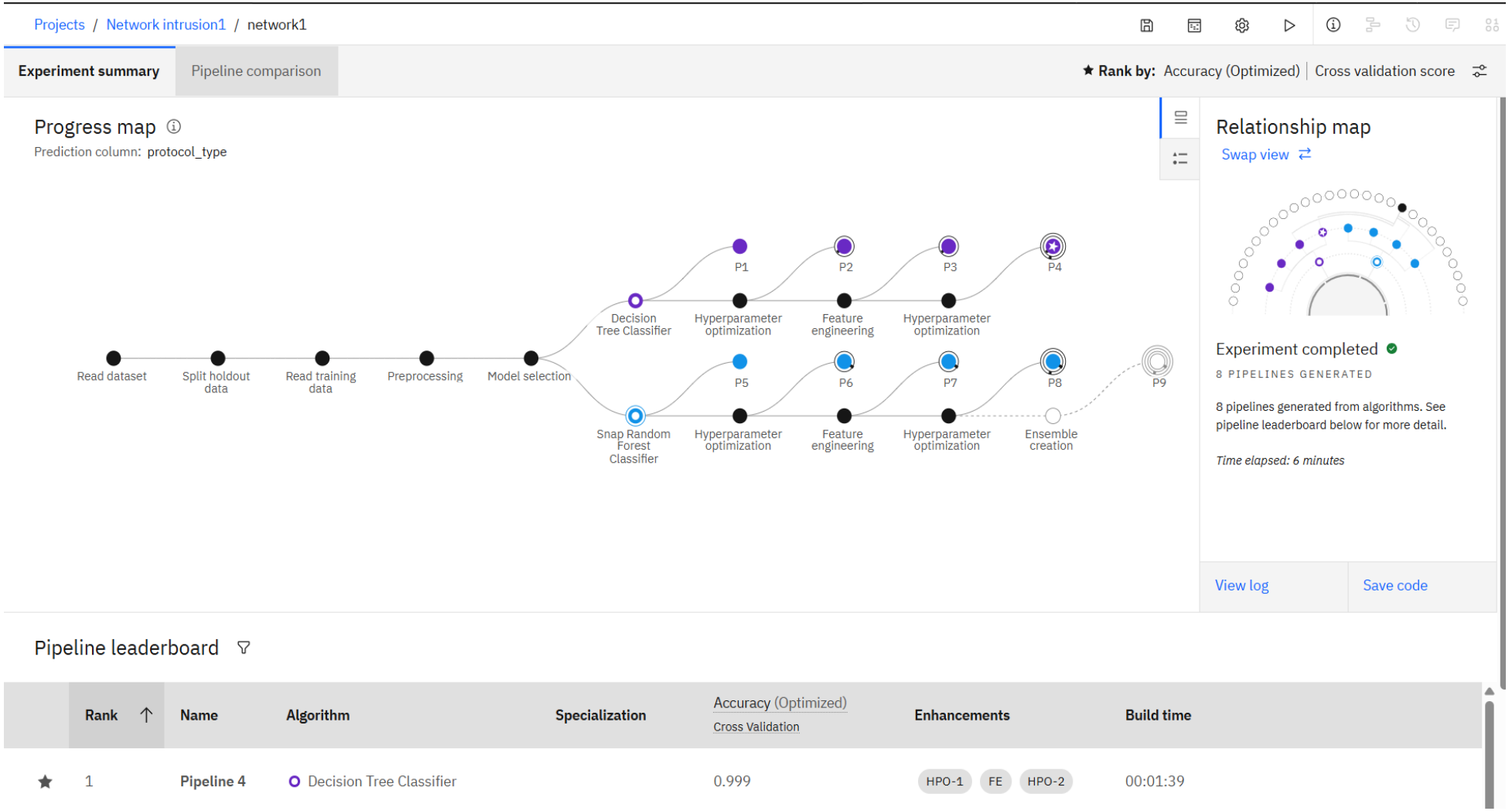
- **AI / ML Services:**

- watsonx.ai Studio
- watsonx.ai Runtime

ALGORITHM & DEPLOYMENT

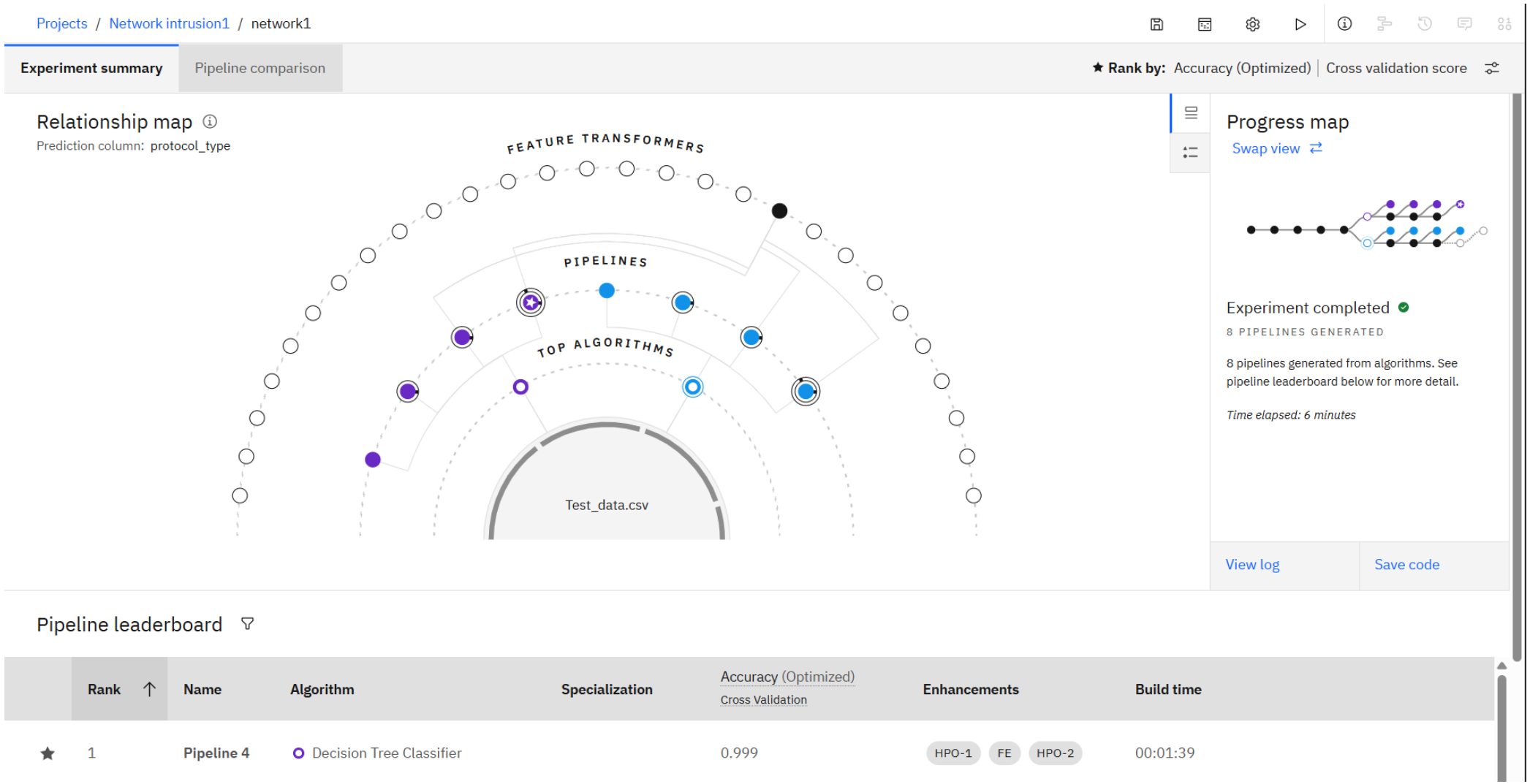
- **Algorithm Selection:**
  - Decision Tree Classifier(chosen for high accuracy on multi-class network attack detection) & Random Forest Classifier
- **Data Input:**
  - Network traffic features: duration, protocol, service, flag, source/destination bytes, and host-based statistical features.
- **Training Process:**
  - Supervised learning on labeled network traffic data with preprocessing, train-test split, and Random Forest model optimized via hyperparameter tuning.
- **Prediction Process:**
  - Deployed on IBM Watson Studio API for real-time traffic classification and early warning alerts.

RESULT



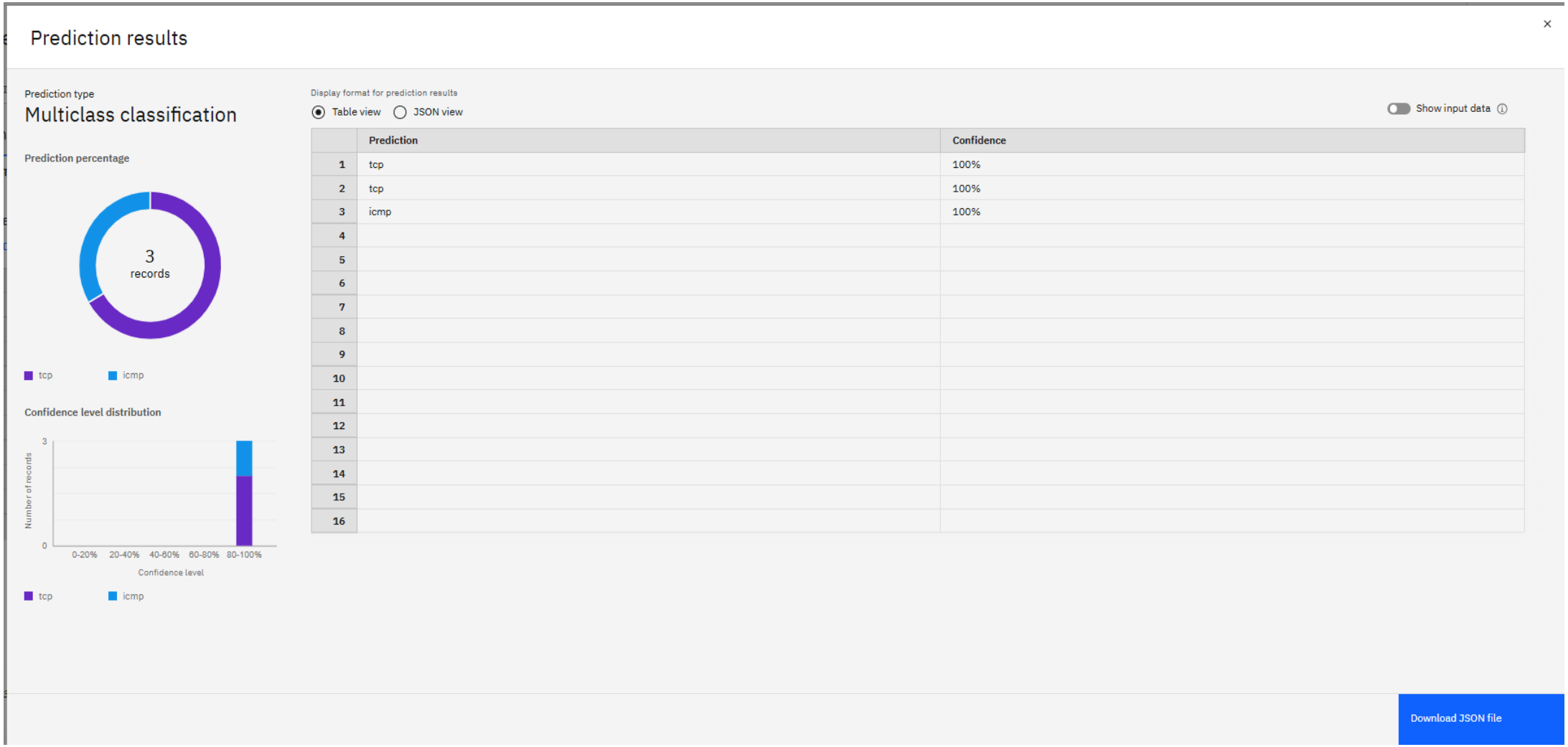
edunet foundation

RESULT



edunet foundation

RESULT



edunet foundation

CONCLUSION

- In this project, we developed a Network Intrusion Detection System (NIDS) using machine learning to secure communication networks by detecting and classifying cyber-attacks.
- Using IBM AutoAI, we trained a model on network traffic data. The best-performing pipeline, a Decision Tree Classifier, achieved 99.9% accuracy and effectively predicted the Protocol_type(TCP, UDP, ICMP), helping identify unusual traffic behavior.
- While the model currently focuses on protocol types, it provides a solid base for detecting suspicious activity. With future enhancements like attack-type labeling, this system can offer reliable early warnings against intrusions.

FUTURE SCOPE

- This project demonstrates the potential of using IBM Cloud and AutoAI to build an effective Network Intrusion Detection System (NIDS). Going forward, the system can be extended in several impactful ways:
- **Wider Attack Coverage**: By incorporating labeled attack categories (e.g., DoS, R2L, Probe), the system can evolve from protocol detection to full cyber threat classification.
- **Scalability Across Regions**: IBM Cloud's global infrastructure allows for deployment across multiple cities or networks, making the system suitable for large-scale enterprise or government use.
- **Integration with Live Systems**: The model can be integrated with real-time network monitoring tools and IBM services (like Event Streams or QRadar) to provide live intrusion alerts.
- **Support for Encrypted Traffic**: The future system could analyze encrypted traffic using privacy-preserving machine learning, enabling safer and smarter intrusion detection.
- **Continuous Model Improvement**: Leveraging AutoAI and Watson pipelines, the system can automatically retrain with new data, keeping pace with evolving cyber threats.

REFERENCES

- Used the **KDD Cup 1999 dataset** from Kaggle for training and testing the intrusion detection system.
  https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection
- Used **IBM AutoAI** platform to build, train, and evaluate machine learning models with minimal manual effort.
- Studied *"A detailed analysis of the KDD Cup 99 dataset"* by **Mahbod Tavallaee et al. (2009)** to understand dataset limitations and improvements.
- **IBM AutoAI** – Used for model automation, training, and evaluation in IBM Cloud.
  https://www.ibm.com/cloud/autoai

IBM CERTIFICATIONS (Getting Started with Artificial Intelligence)

In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence
IBM SkillsBuild

Prashant Kamagond

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

Issued on: Jul 19, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/b45102eb-9236-4aae-8b8d-90c09c978e0c

IBM

edunet foundation

IBM CERTIFICATIONS (Journey to Cloud)

edunet foundation

IBM CERTIFICATIONS (Lab : RAG with Langchain)

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Prashant Kamagond

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 24 Jul 2025 (GMT) **Learning hours:** 20 mins

edunet foundation

THANK YOU

edunet foundation