CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. VECHALAPU VARSHINI - CVR COLLEGE OF ENGINEERING - CSE(CYBERSECURITY)

edunet foundation

OUTLINE

- **Problem Statement** (Should not include solution)
- **Proposed System/Solution**
- **System Development Approach** (Technology Used)
- **Algorithm & Deployment**
- **Result (Output Image)**
- **Conclusion**
- **Future Scope**

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

- The proposed solution is a **machine learning-based NIDS** that processes raw network traffic data and accurately classifies malicious vs. benign activities.
- Key Features:

1. Preprocess network traffic dataset (KDD/NSL-KDD or Kaggle NIDS dataset)
2. Train multiple ML models (Random Forest, SVM, KNN, etc.)
3. Evaluate performance using metrics like Accuracy, Precision, Recall, and F1-score
4. Deploy in a simulated environment or as a dashboard for alerts

SYSTEM APPROACH

Technology Used:

- Python (NumPy, Pandas, Scikit-learn, Matplotlib, Seaborn)
- IBM Cloud Lite Services
- Jupyter Notebook for model building and visualization
- IBM Granite / Watson Studio (if applicable)

System Requirements:

- 8GB+ RAM, Python 3.8+, Internet
- Kaggle dataset

ALGORITHM & DEPLOYMENT

- **Algorithm Chosen:** Random Forest Classifier (also tried Logistic Regression, Decision Tree)
- **Data Input:**

-> Network features like duration, protocol_type, service, src_bytes, dst_bytes, etc.

- **Training:**

-> Dataset split into 80:20 train-test

-> Feature selection & normalization

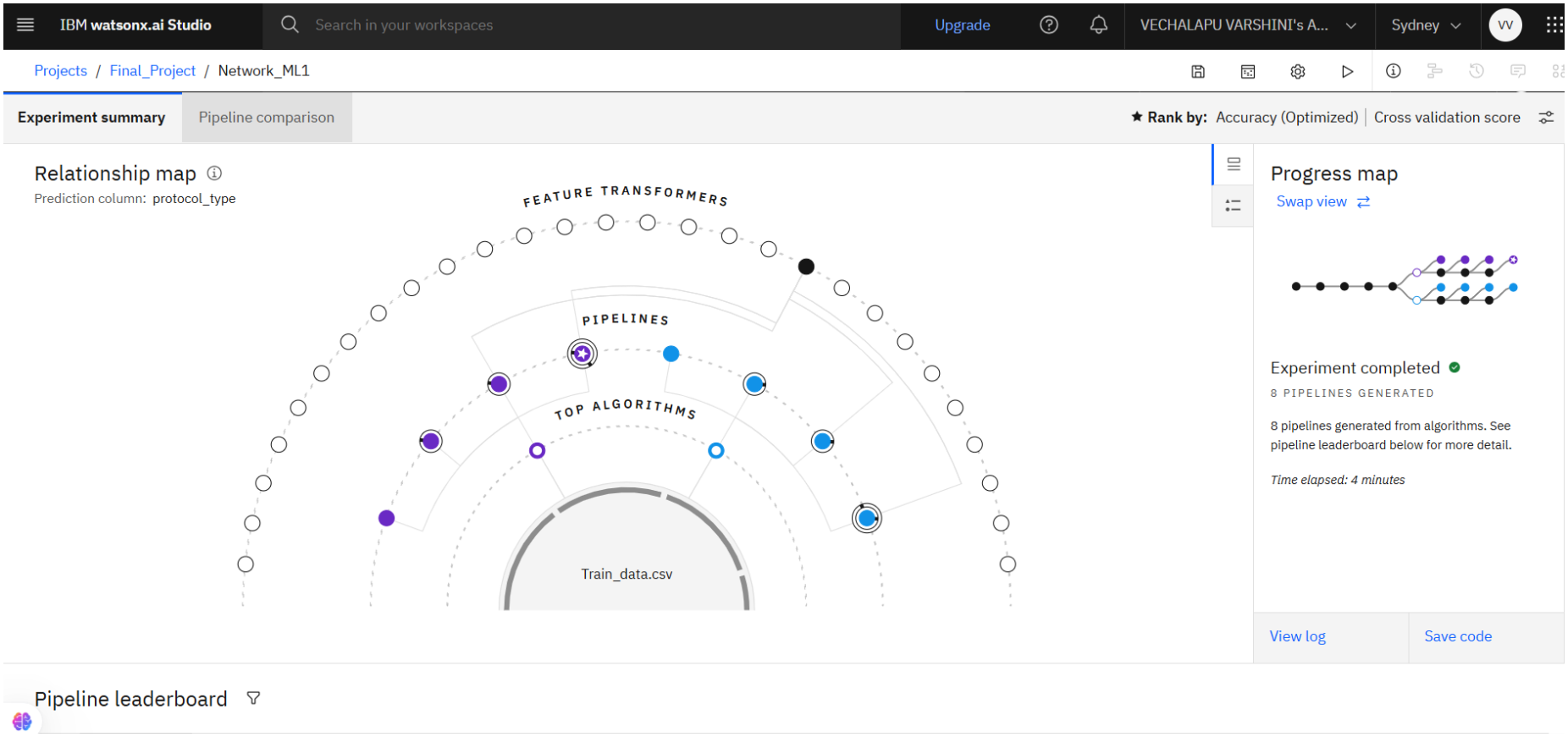
-> Trained using cross-validation

- **Prediction:**

-> Predicts class label: 'normal' or type of attack (DoS, Probe, etc.)

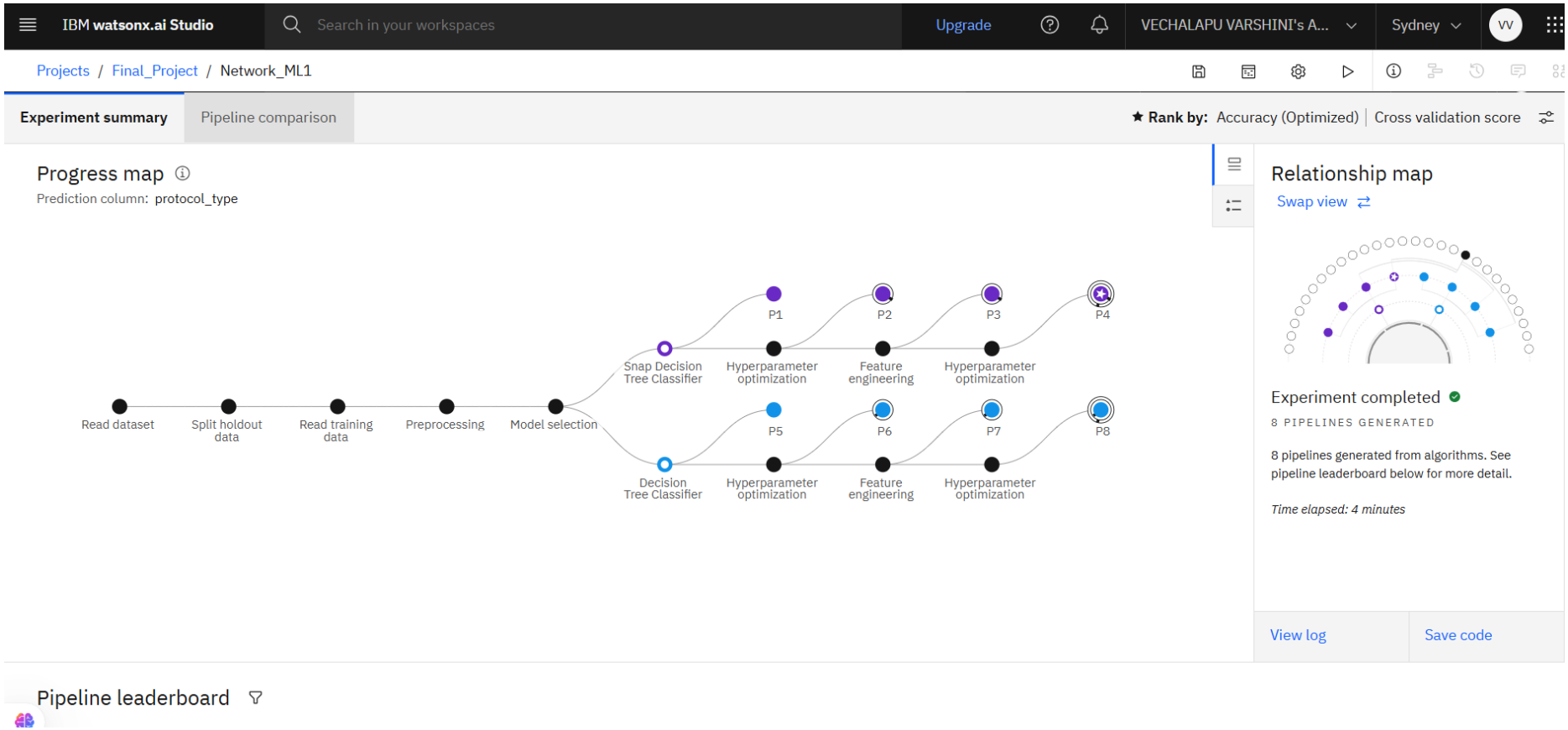
-> Can be integrated into IBM Cloud for real-time alert system

RESULT



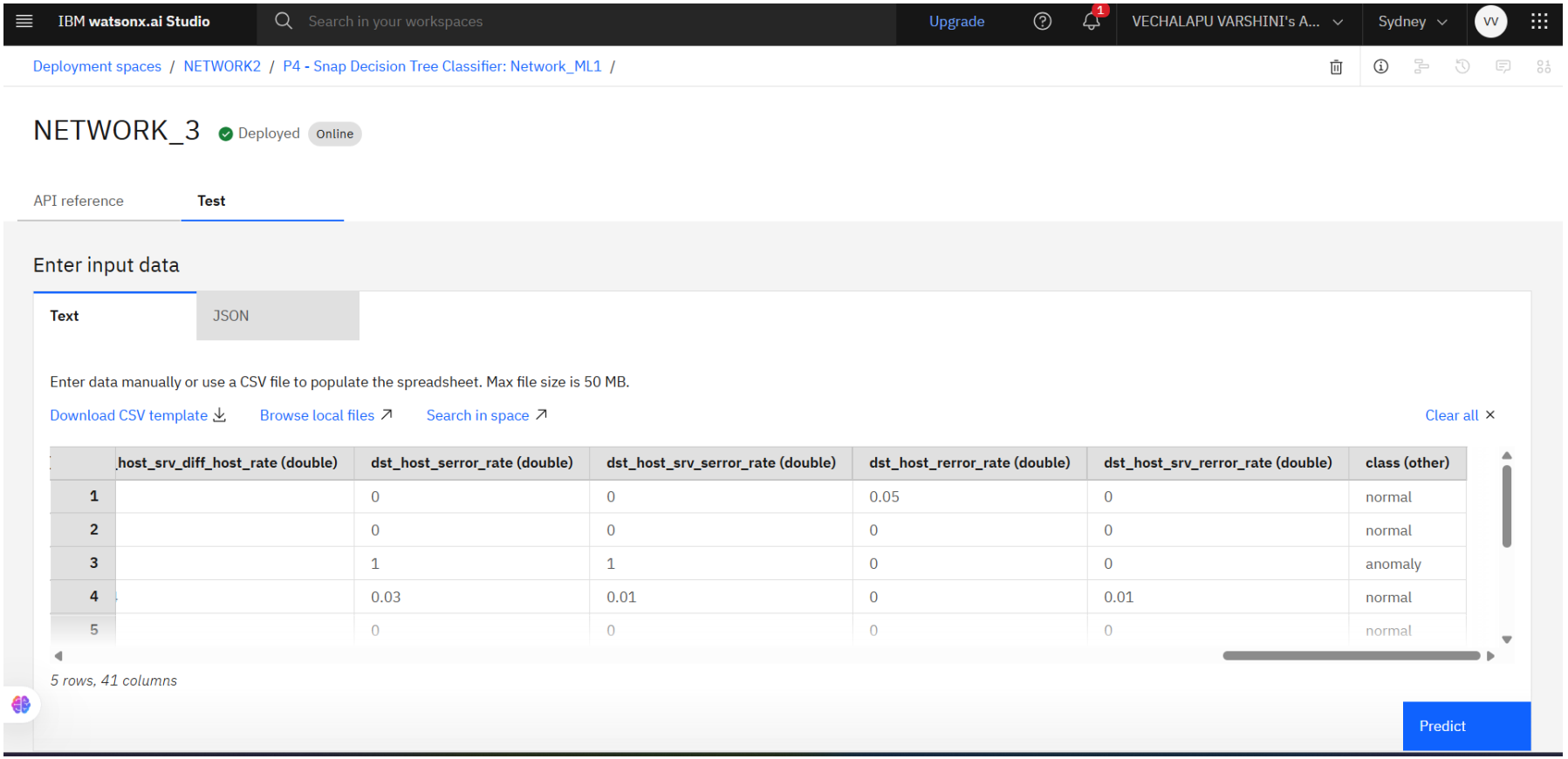
edunet foundation

RESULT



edunet foundation

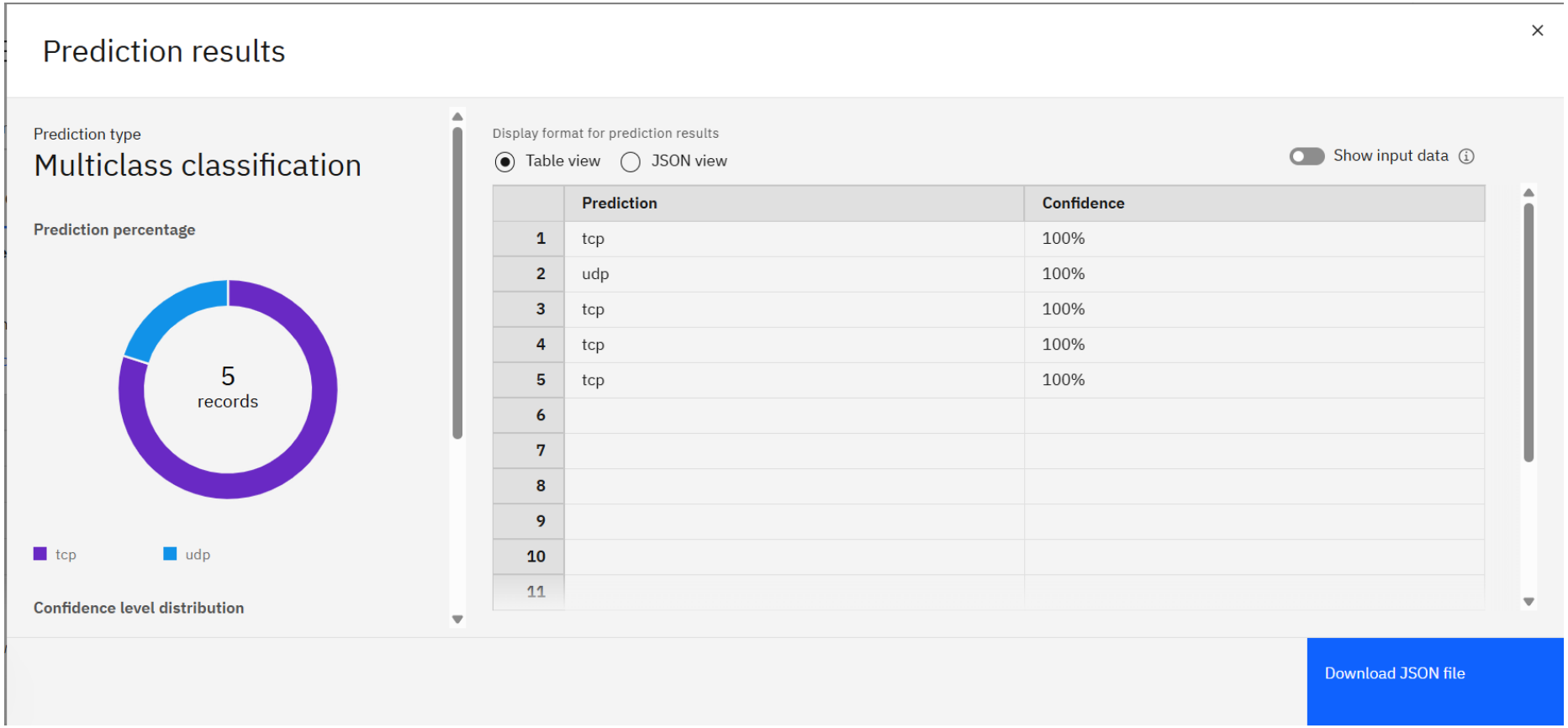
RESULT



	host_srv_diff_host_rate (double)	dst_host_serror_rate (double)	dst_host_srv_serror_rate (double)	dst_host_rerror_rate (double)	dst_host_srv_rerror_rate (double)	class (other)
1		0	0	0.05	0	normal
2		0	0	0	0	normal
3		1	1	0	0	anomaly
4		0.03	0.01	0	0.01	normal
5		0	0	0	0	normal

edunet foundation

RESULT



edunet foundation

CONCLUSION

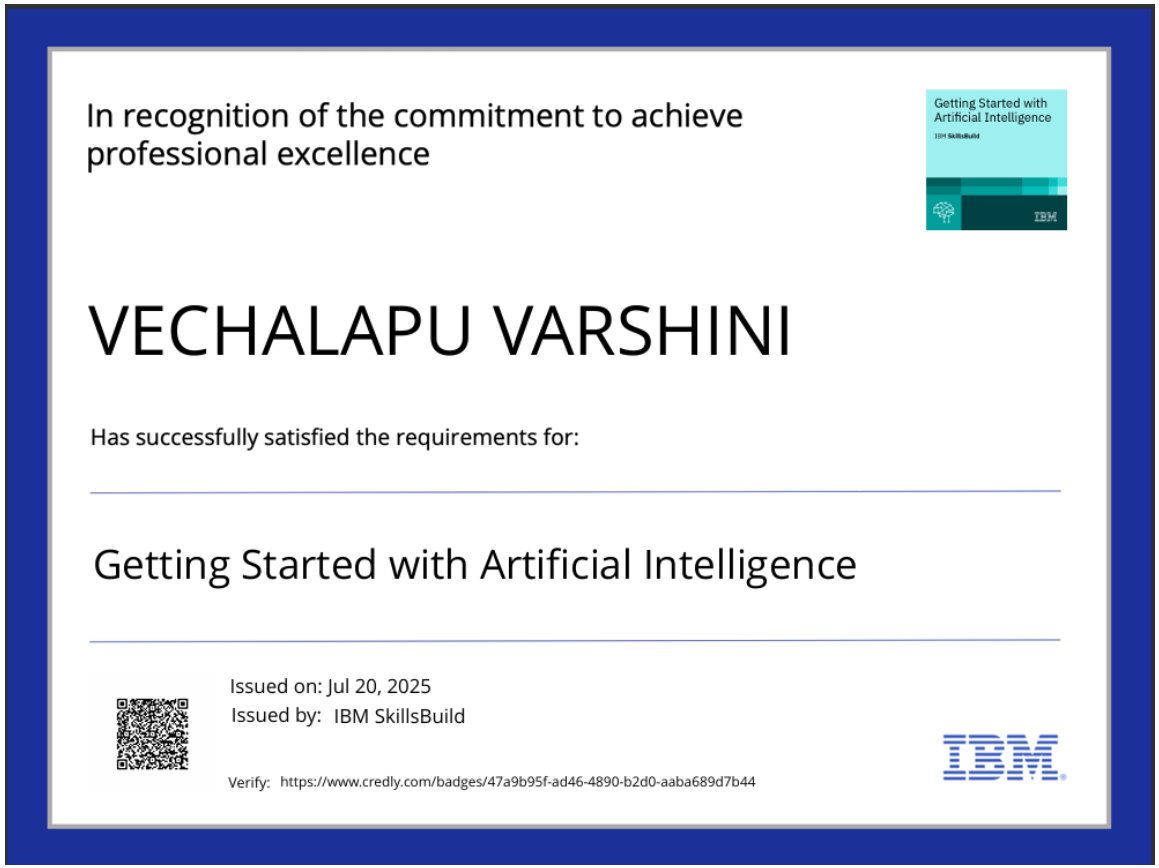
- Random Forest Successfully built and tested a ML-based NIDS
- outperformed others in accuracy and generalization
- Identified and classified network attacks effectively using labeled data
- Demonstrated potential to enhance security in real-time environments

edunet foundation

FUTURE SCOPE

- Extend to deep learning models (e.g., LSTM for sequential data)
- Real-time traffic monitoring & alerts
- Integration with firewalls and SIEM tools
- Use updated datasets like CIC-IDS2017 or UNSW-NB15
- Support for encrypted traffic analysis

IBM CERTIFICATIONS



edunet foundation

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM SkillsBuild

IBM

VECHALAPU VARSHINI

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 20, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/e79afca5-0bfb-45db-ac5f-afaccbba2e99

IBM

edunet foundation

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

V Varshini

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