CAPSTONE PROJECT

ML-BASED NETWORK INTRUSION DETECTION SYSTEM (NIDS) USING IBM CLOUD

Presented By:
Vivank Tyagi–Dayalbagh Educational Institute –Electrical Engineering

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

- With the rapid growth of the internet and digital communication, computer networks are increasingly exposed to a wide range of cyber-attacks. Traditional firewall and rule-based systems often fail to detect new and evolving threats in real time.
- It becomes critical to build a system that can **predict and classify potential intrusions or attacks** in network traffic before serious damage is done.
- The major challenge lies in identifying different types of attacks such as **DoS, Probe, R2L, and U2R** with high accuracy from large volumes of network data.
- A machine learning-based Network Intrusion Detection System (NIDS) is required to **analyze traffic patterns**, detect malicious behavior, and provide early warnings to ensure a **secure communication environment**.

PROPOSED SOLUTION

- The proposed system aims to detect and classify network intrusions using machine learning and IBM Cloud services. It includes the following components:
- **Data Collection:** Use the Kaggle dataset containing labeled network traffic, including normal and attack types (DoS, Probe, R2L, U2R).
- **Data Preprocessing:** Clean the data, handle missing values, and perform feature engineering and encoding.
- **Machine Learning Algorithm:** Train models like Random Forest, SVM, or Neural Networks to classify network behavior.
- **Deployment:** Use IBM Watson Machine Learning for model deployment, Cloud Object Storage for data, and Cloud Functions for alerts.
- **Evaluation:** Evaluate model performance using accuracy, precision, recall, and F1-score, and fine-tune as needed.
- **Result:** A smart, cloud-based NIDS capable of real-time threat detection and improved network security.

SYSTEM APPROACH

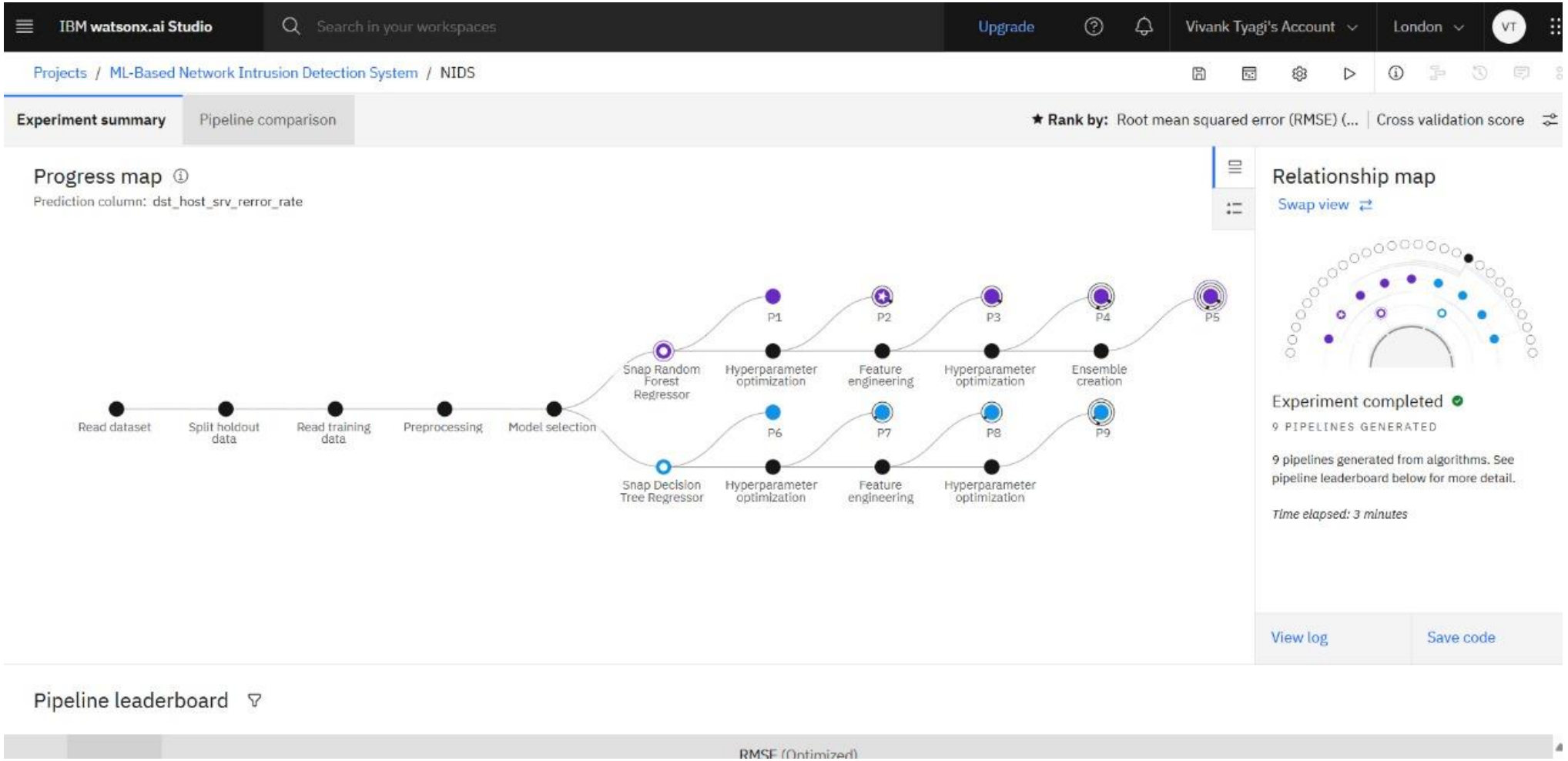
- The system approach for the Network Intrusion Detection System includes the following:
- **System Requirements:** A minimum Intel i5 processor, 8 GB RAM, 10 GB free disk space, any OS (Windows/Linux/Mac), and a stable internet connection.
- **Programming Language:** Python 3.8 or higher.
- **Libraries Required:**

  NumPy and Pandas for data processing,
  Matplotlib and Seaborn for data visualization,
  Scikit-learn for building and evaluating machine learning models,
  Imbalanced-learn for handling class imbalance (e.g., SMOTE),
  IBM Watson Machine Learning SDK for deploying models to IBM Cloud,
  Flask or Streamlit (optional) for building a user interface,
  IBM Cloud CLI for cloud service management.

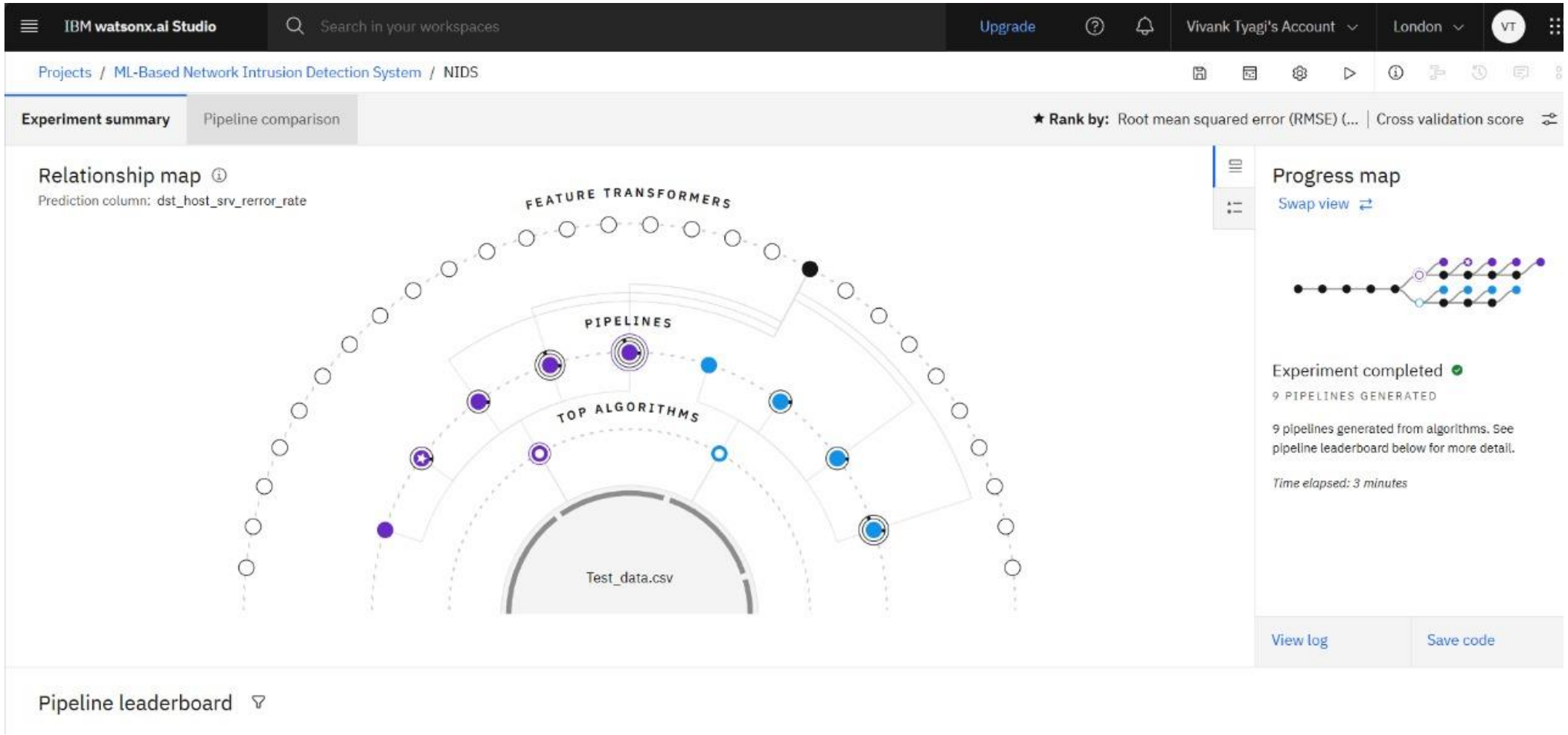
ALGORITHM & DEPLOYMENT

- **Algorithms Used:** Random Forest, Support Vector Machine (SVM), and Neural Networks for classifying network traffic.
- **Model Training:** Dataset is split into training and testing sets; models are trained and optimized using cross-validation and hyperparameter tuning.
- **Evaluation Metrics:** Accuracy, Precision, Recall, and F1-score are used to select the best-performing model.
- **Deployment Platform:** The selected model is deployed on **IBM Watson Machine Learning**.
- **Cloud Services Used:**
  - **IBM Cloud Object Storage** for storing datasets and results.
  - **IBM Cloud Functions** for real-time alert generation.
- **Optional UI:** A simple dashboard can be built using **Flask** or **Streamlit** to display predictions and alerts.

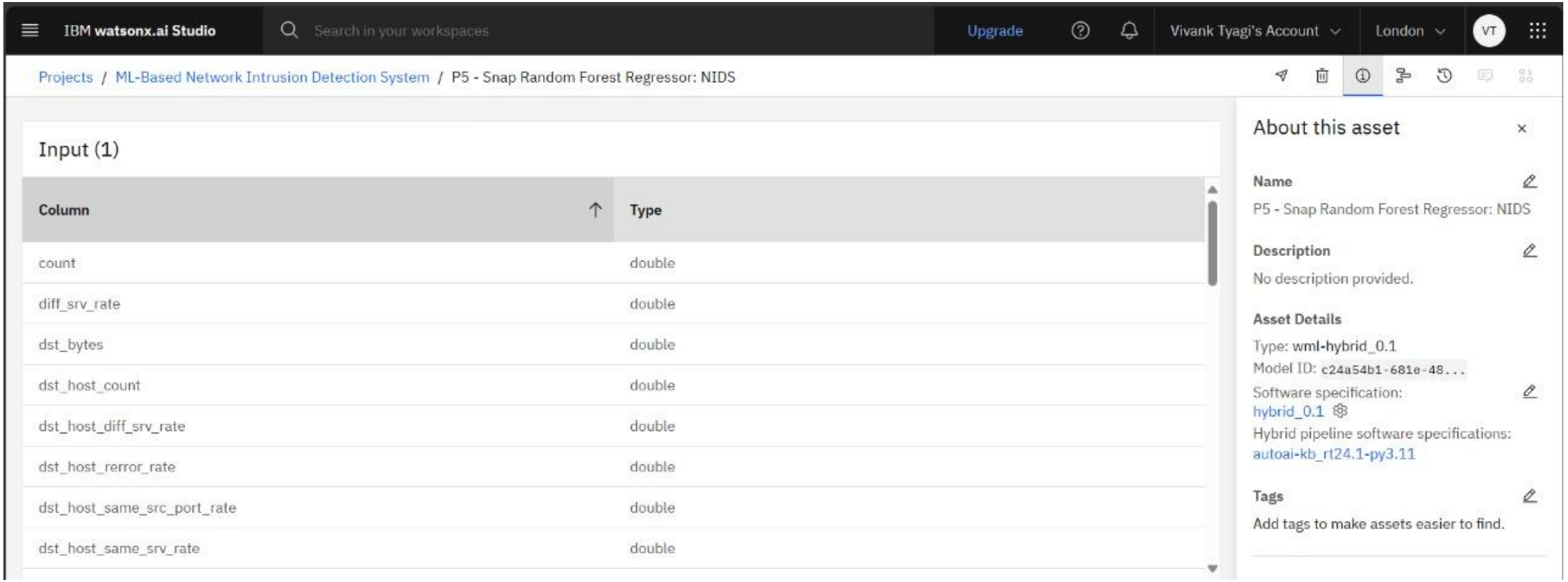
RESULT



RESULT



RESULT


IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Vivank Tyagi's Account
London
VT
Projects / ML-Based Network Intrusion Detection System / P5 - Snap Random Forest Regressor: NIDS
Input (1)
Column
Type
count
double
diff_srv_rate
double
dst_bytes
double
dst_host_count
double
dst_host_diff_srv_rate
double
dst_host_rerror_rate
double
dst_host_same_src_port_rate
double
dst_host_same_srv_rate
double
About this asset
Name
P5 - Snap Random Forest Regressor: NIDS
Description
No description provided.
Asset Details
Type: wml-hybrid_0.1
Model ID: c24a54b1-681e-48...
Software specification:
hybrid_0.1
Hybrid pipeline software specifications:
autoai-kb_rt24.1-py3.11
Tags
Add tags to make assets easier to find.

RESULT

Prediction results

Close

Prediction type

Regression

Prediction distribution

Display format for prediction results

Table view JSON view

Show input data

	Prediction
1	0.0017654526665864978
2	
3	
4	
5	
6	
7	
8	
9	

edunet foundation

CONCLUSION

- The project successfully developed a machine learning-based **Network Intrusion Detection System** capable of identifying and classifying various cyber-attacks.
- The use of **IBM Cloud services** enabled efficient deployment, real-time alerting, and scalable storage.
- The selected ML model (e.g., Random Forest) achieved **high accuracy and reliability**, demonstrating its effectiveness in securing network environments.
- The system provides an **early warning mechanism**, helping reduce the risk of data breaches and unauthorized access.
- With continuous monitoring and updates, the model can adapt to **new threats** and improve over time.

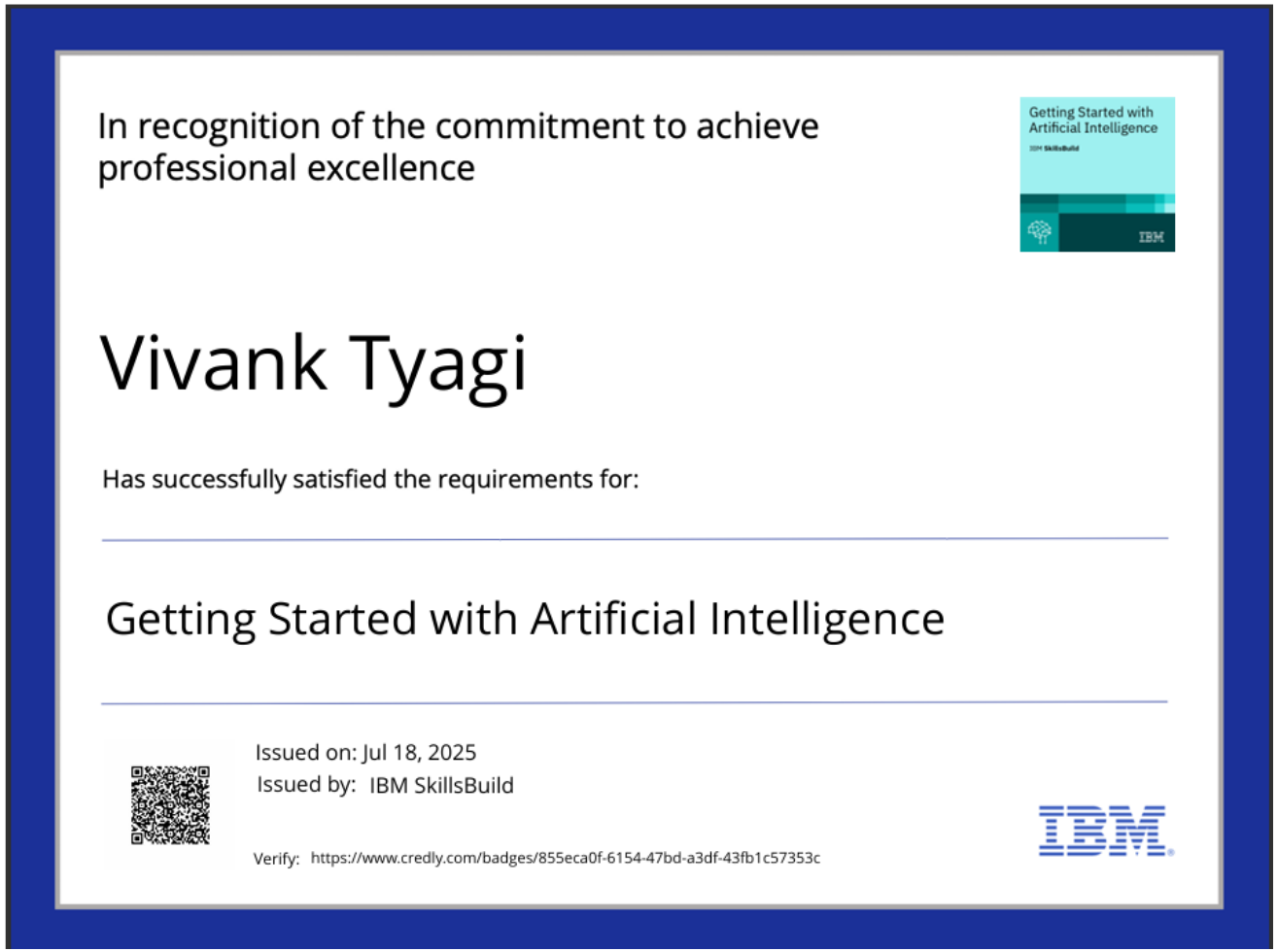
FUTURE SCOPE

- Integrate with real-time traffic monitoring tools for live detection.
- Use deep learning models like LSTM or CNN for better accuracy.
- Enable adaptive learning to update the model with new data.
- Expand to detect advanced and zero-day attacks.
- Connect with firewall or SIEM tools for auto-response.
- Develop a mobile-friendly dashboard for remote monitoring.
- Combine with host-based systems for layered security.

REFERENCES

- **Kaggle Dataset** – Network Intrusion Detection Dataset
  https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection
- **IBM Cloud Documentation** – IBM Watson Machine Learning
  https://cloud.ibm.com/docs/watson-machine-learning
- Scikit-learn: Machine Learning in Python
  https://scikit-learn.org/
- Imbalanced-learn Documentation
  https://imbalanced-learn.org/
- Panda's Documentation – Data Analysis Library
  https://pandas.pydata.org/
- Research papers and articles on intrusion detection systems (IDS) and machine learning
- applications in cybersecurity (IEEE, Springer, etc.)

IBM CERTIFICATIONS



IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Vivank Tyagi

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 18, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/0d1b3ebb-ac93-4c9d-bd25-a61802e437b9

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Vivank Tyagi

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