CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. TANISHA CHOPRA – SG. BALEKUNDRI INSTITUTE OF TECHNOLOGY

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

- The proposed system uses machine learning to detect and classify network intrusions in real time. It analyzes TCP/IP connection data to identify abnormal activities such as DoS attacks, unauthorized access, or probing.
- **Data Collection:**
  - Use datasets like **KDD Cup 1999** with labeled traffic as normal or specific attack types.
- **Data Preprocessing:**
  - Encode categorical features, normalize numeric data, and split into training/testing sets.
- **Machine Learning Algorithm:**
  - Train classification models like **Random Forest** to detect and classify intrusions.
- **Predition:**
  - Train classification models like **Random Forest** or **SVM** to detect and classify intrusions.
- **Deployment:**
  - Deploy on **IBM Cloud** using Watson Studio and Machine Learning.
  - Expose the model as a **REST API** for real-time predictions.

SYSTEM APPROACH

System Requirements:

❑ Hardware:

- 4 GB RAM or higher (locally)
- Stable internet connection

❑ IBM Cloud:

- IBM Cloud account (Lite plan)
- Watson Studio
- Cloud Object Storage

ALGORITHM & DEPLOYMENT

Algorithm

- **Algorithm Selection:**
- The Random Forest Classifier is used due to its high accuracy, ability to handle large datasets, and effectiveness in multiclass classification (normal vs. different attack types).
- **Data Input:**
- The model uses 41 features from the network connection records (e.g., protocol_type, src_bytes, flag) and predicts the class (normal or specific attack).
- **Training Process:**
- Preprocess the dataset (encode, scale, split into train/test).
- Train the model using cross-validation and fine-tune it for better accuracy.
- **Prediction:**
- The trained model predicts whether new incoming network traffic is normal or an intrusion type, with a confidence score.

ALGORITHM & DEPLOYMENT

Deployment

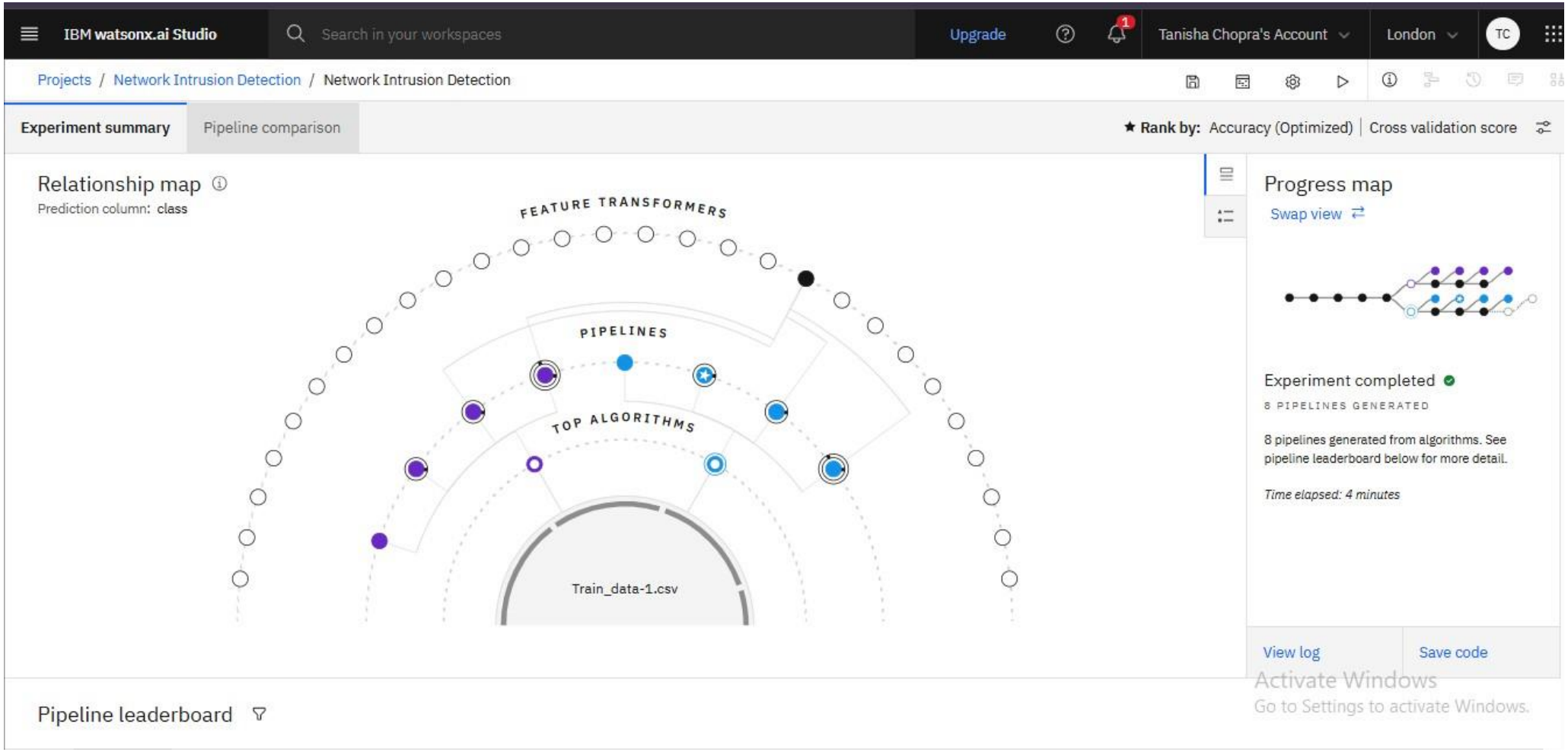
- **Platform:**

- The model is deployed on IBM Cloud using:
- Watson Studio for training and development
- Watson Machine Learning (WML) for deployment
- Cloud Object Storage for data storage

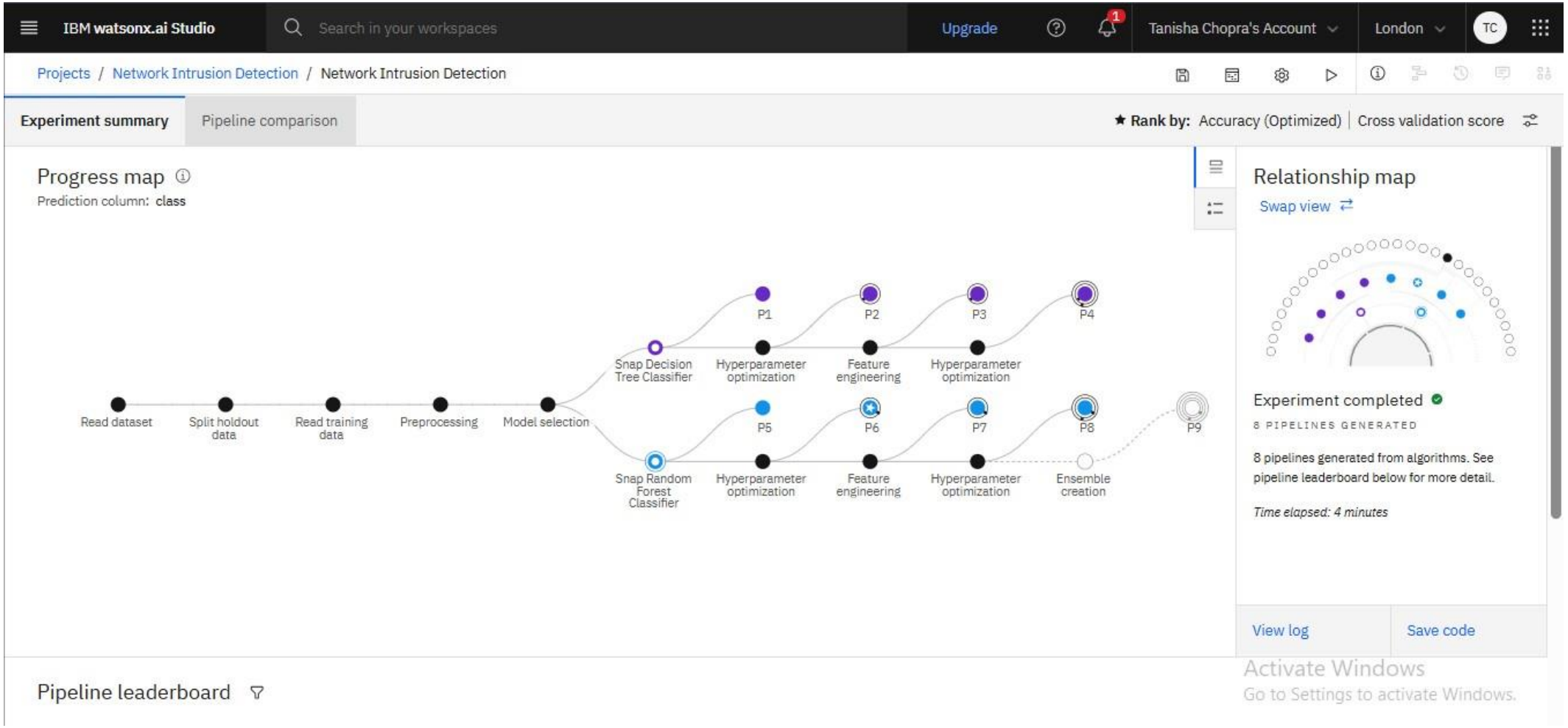
- **Deployment Steps:**

- Upload dataset and train model in Watson Studio.
- Save and deploy the model using WML.
- Generate a REST API endpoint for the deployed model.
- Use this API to classify live or test data for intrusion detection.

RESULT

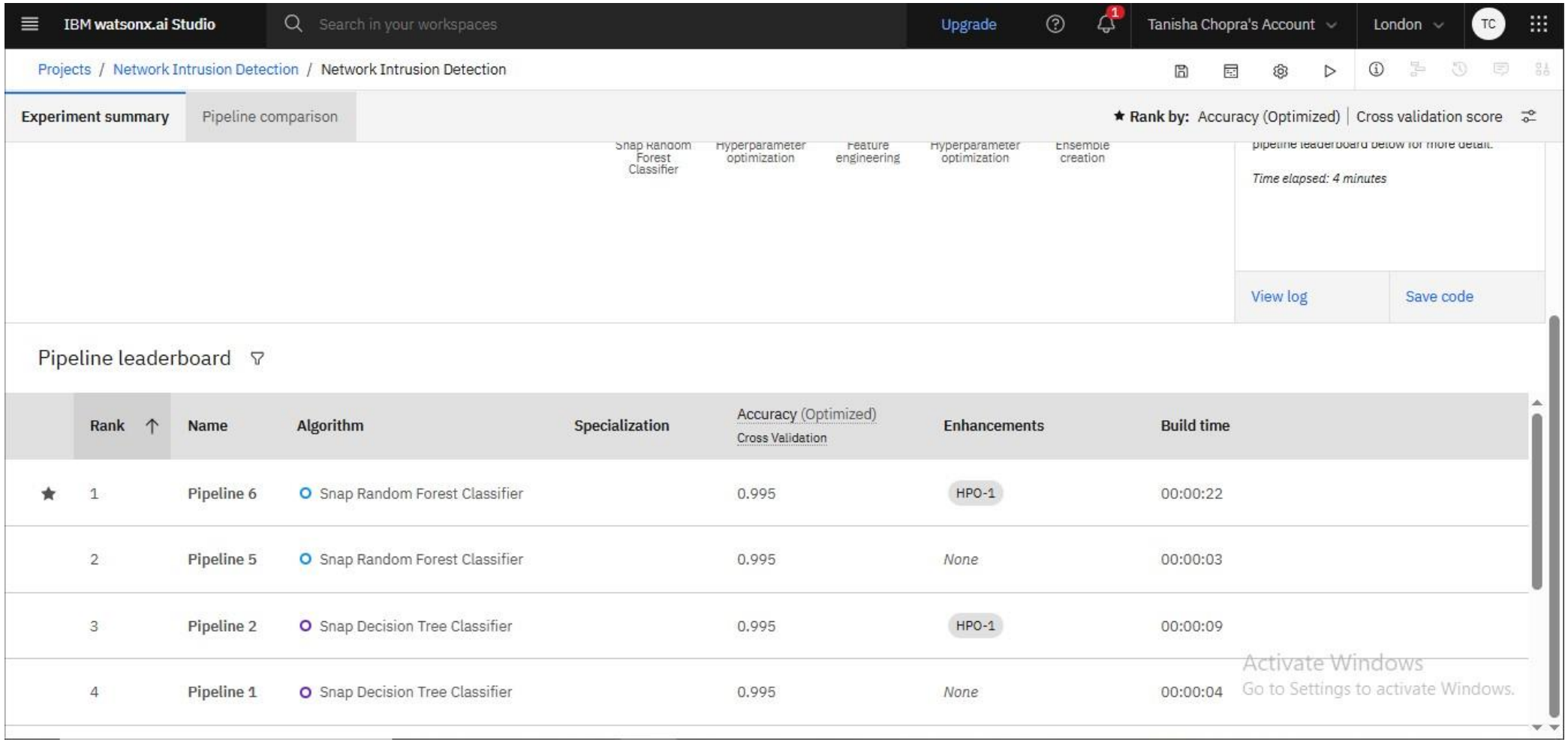


RESULT



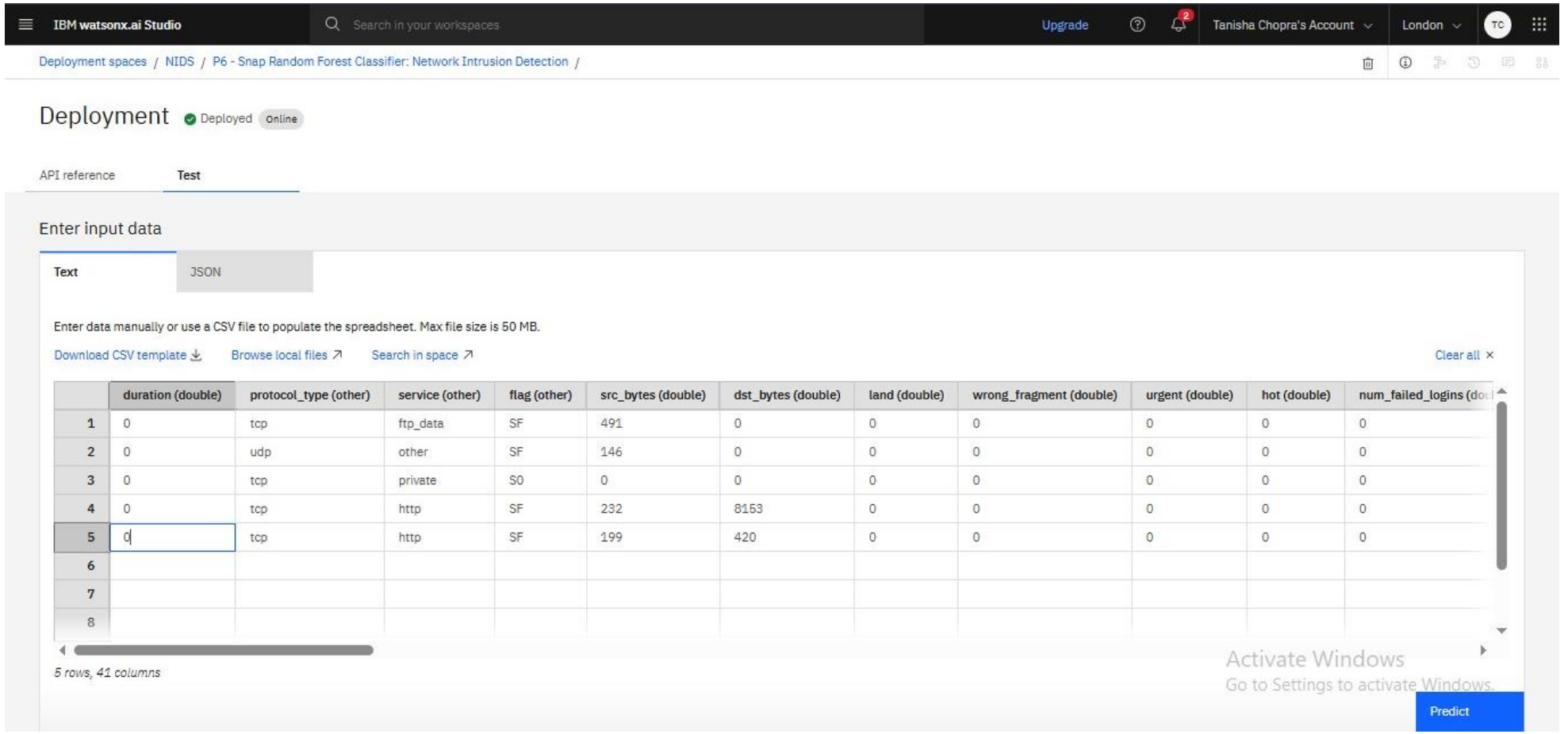
edunet foundation

RESULT

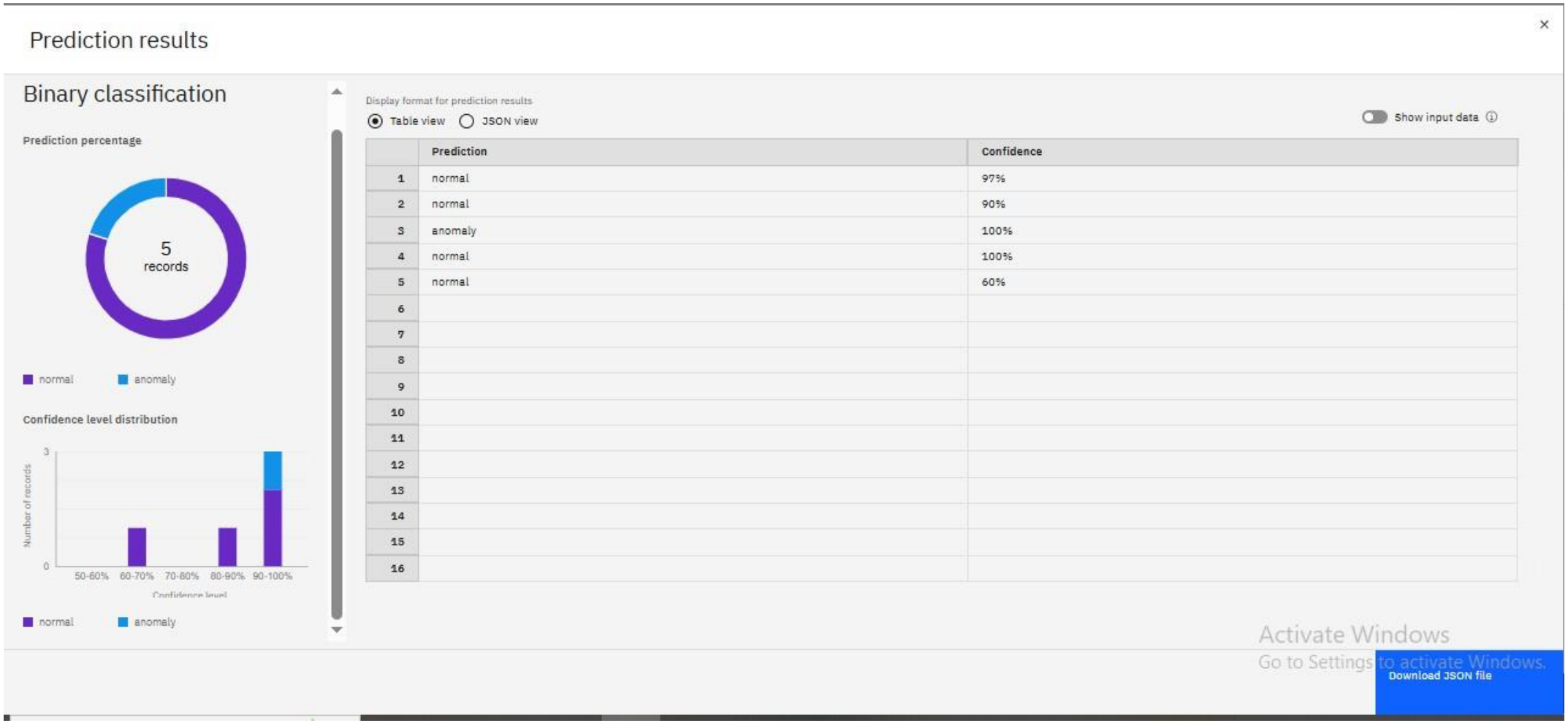


edunet foundation

RESULT


IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Tanisha Chopra's Account
London
Deployment spaces / NIDS / P6 - Snap Random Forest Classifier: Network Intrusion Detection /
Deployment
Deployed
Online
API reference
Test
Enter input data
Text
JSON
Enter data manually or use a CSV file to populate the spreadsheet. Max file size is 50 MB.
Download CSV template
Browse local files
Search in space
Clear all
duration (double) protocol_type (other) service (other) flag (other) src_bytes (double) dst_bytes (double) land (double) wrong_fragment (double) urgent (double) hot (double) num_failed_logins (dou
1 0 tcp ftp_data SF 491 0 0 0 0 0 0
2 0 udp other SF 146 0 0 0 0 0 0
3 0 tcp private S0 0 0 0 0 0 0 0
4 0 tcp http SF 232 8153 0 0 0 0 0
5 0 tcp http SF 199 420 0 0 0 0 0
6
7
8
5 rows, 41 columns
Activate Windows
Go to Settings to activate Windows.
Predict

RESULT



CONCLUSION

- The proposed machine learning-based intrusion detection system effectively identifies and classifies network attacks using historical connection data. By using algorithms like Random Forest and deploying the solution on IBM Cloud, the system ensures accurate, fast, and scalable intrusion detection. This enhances network security by enabling early threat detection and real-time response to potential cyberattacks.

FUTURE SCOPE

- **Real-time Monitoring**: Integrate the model with live network streams for real-time intrusion alerts.
- **Deep Learning Models**: Explore advanced models like LSTM or CNNs for better pattern detection.
- **Hybrid Systems**: Combine anomaly-based and signature-based methods for improved accuracy.
- **Automated Response**: Implement auto-blocking or alert systems for critical intrusions.
- **Wider Dataset Usage**: Use newer datasets like CICIDS2017 to improve model robustness across attack types.

REFERENCES

- KDD Cup 1999 Dataset – http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html
- IBM Cloud – Watson Studio Documentation – https://www.ibm.com/cloud/watson-studio
- Scikit-learn Documentation – https://scikit-learn.org/stable/
- IBM Cloud - Watson Studio https://www.ibm.com/cloud/watson-studio
- IBM Cloud - Watson Machine Learning https://www.ibm.com/cloud/machine-learning

IBM CERTIFICATIONS

edunet foundation

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

TANISHA DHIRAJ CHOPRA

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/9c7422d1-b274-444e-8658-2a94d97cea67

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild**

Completion Certificate

This certificate is presented to

TANISHA DHIRAJ CHOPRA

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 23 Jul 2025 (GMT)

Learning hours: 20 mins

edunet foundation

THANK YOU

edunet foundation