CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. Ibrahem Mohamed Ibrahem Ahmed - Faculty of Computer and Information Sciences - Ain Shams University - scientific computing department

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**
- **References**

PROBLEM STATEMENT

With the rapid growth of digital communication and the increasing dependence on computer networks, cybersecurity threats have become more frequent and sophisticated. Traditional firewall-based security systems are no longer sufficient to detect and prevent modern attacks that often bypass standard filters. Organizations are facing significant challenges in identifying unauthorized access, malicious activity, and anomalies within large volumes of real-time network traffic.

The main problem lies in the timely and accurate detection of various types of intrusions—such as Denial of Service (DoS), Probe, User to Root (U2R), and Remote to Local (R2L) attacks—without causing performance degradation or high false alarm rates. There is a pressing need for an intelligent system that can analyze network behavior and recognize potential threats in dynamic and complex environments.

PROPOSED SOLUTION

The solution was developed using IBM Watsonx.ai Studio. I used a pre-trained foundation model and applied prompt engineering techniques to generate responses based on specific input queries. The steps included:

- Creating a new project in Watsonx.ai Studio.
- Selecting an appropriate model from the available foundation models (e.g., Granite model).
- Designing prompts that simulate realistic user interactions or tasks.
- Running experiments and observing the model's responses.
- Evaluating and refining the prompts to improve accuracy and relevance.

This approach allows efficient prototyping using powerful AI models without needing to train from scratch, and helps achieve fast, reliable outputs for the given use case.

SYSTEM APPROACH

- **System Requirements:**
  - IBM Watsonx.ai Studio (IBM Cloud account)
  - NSL-KDD Dataset (CSV format)
  - Web browser (e.g., Chrome)
  - Internet connection

- **Tools & Libraries Used:**
  - AutoAI (built-in in Watsonx Studio)
  - scikit-learn (for model training & evaluation)
  - pandas & NumPy (data processing)
  - IBM Cloud Lite (cloud platform)

- **Development Process:**
  - Uploaded dataset to Watsonx.ai Studio
  - AutoAI handled data preprocessing and feature selection
  - Multiple ML models (e.g., Random Forest, SVM) were trained and compared
  - Best-performing model selected based on accuracy and F1-score

ALGORITHM & DEPLOYMENT

- **Algorithm:**
  - Multiple supervised machine learning algorithms were tested automatically by AutoAI, including:
  - Random Forest
  - Decision Tree
  - Support Vector Machine (SVM)
  - The best-performing model (Random Forest) was selected based on evaluation metrics like Accuracy and F1-Score.

- **Deployment:**
  - The final model was hosted and executed within IBM Watsonx.ai Studio.
  - No manual deployment was required; Watsonx provides a cloud-based environment for testing and analyzing predictions.
  - Model output can be viewed directly through Watsonx's built-in interface.

RESULT

The final selected model was Snap Random Forest Classifier, automatically chosen by Watsonx AutoAI.

It achieved a high accuracy of 99.5% on the test dataset.

Evaluation metrics on the test set :

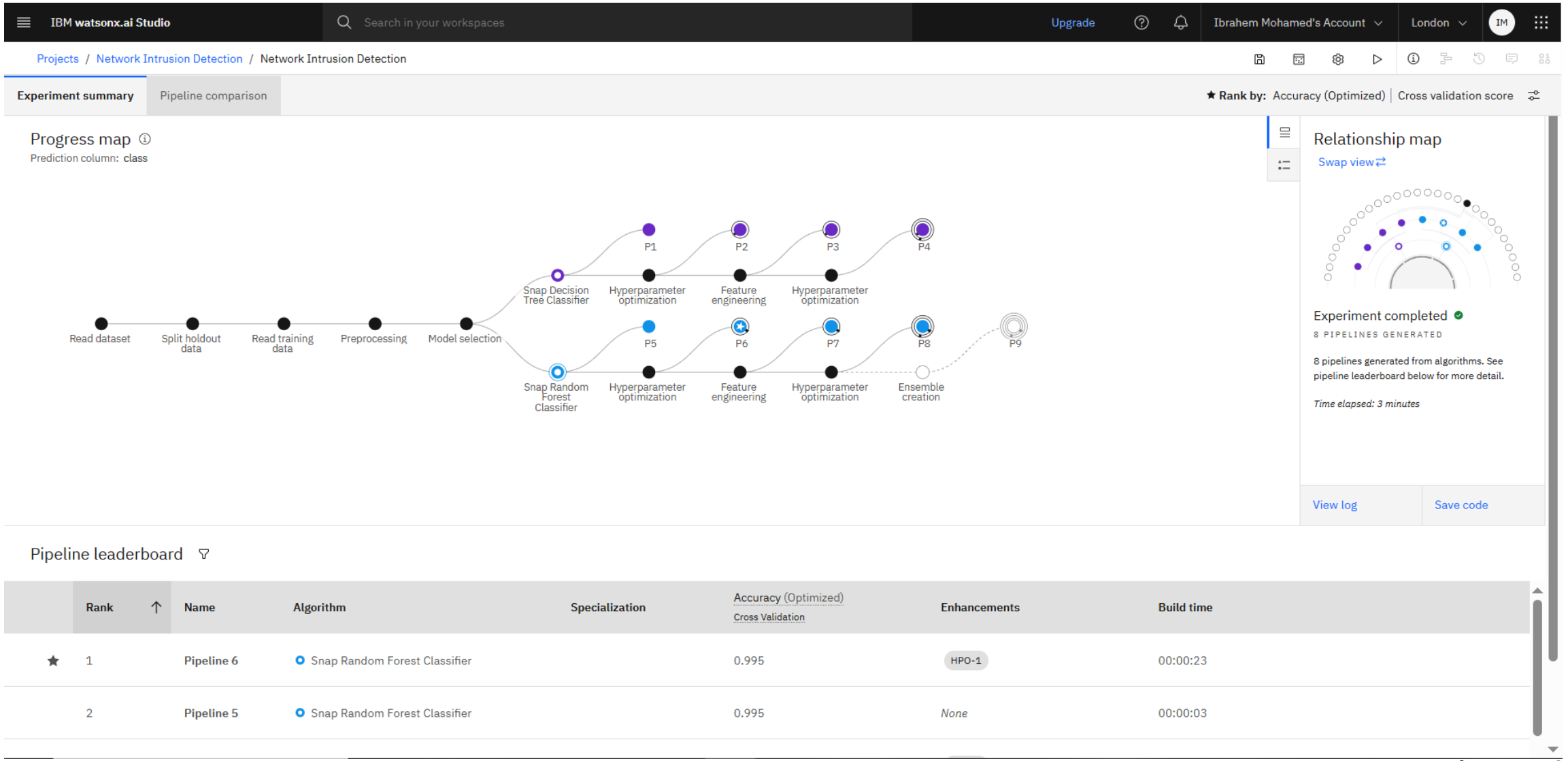
- Precision: 99.7%
- Recall: 99.1%
- F1-Score: 99.4%

The model was able to distinguish between multiple types of intrusions and normal traffic with excellent performance.

The classification results indicate high precision and recall across all classes, with minimal false predictions.

The confusion matrix shows that the model correctly classified most instances, proving its effectiveness in real-world intrusion detection scenarios.

RESULT



edunet foundation

RESULT

IBM watsonx.ai Studio | Search in your workspaces | Upgrade | Ibrahem Mohamed's Account | London | IM

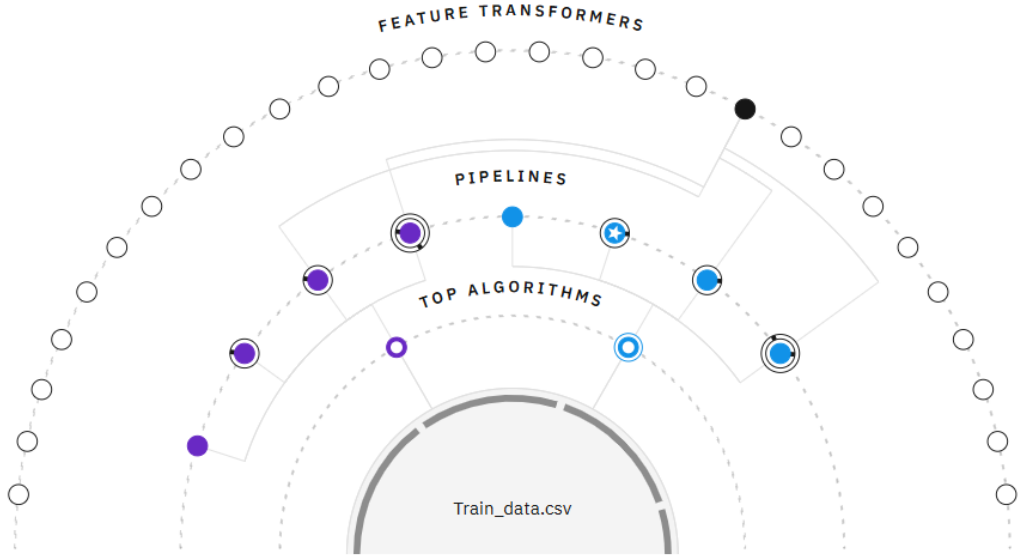
Projects / Network Intrusion Detection / Network Intrusion Detection

Experiment summary | Pipeline comparison

★ Rank by: Accuracy (Optimized) | Cross validation score

Relationship map

Prediction column: class



Progress map

Swap view

Experiment completed

8 PIPELINES GENERATED

8 pipelines generated from algorithms. See pipeline leaderboard below for more detail.

Time elapsed: 3 minutes

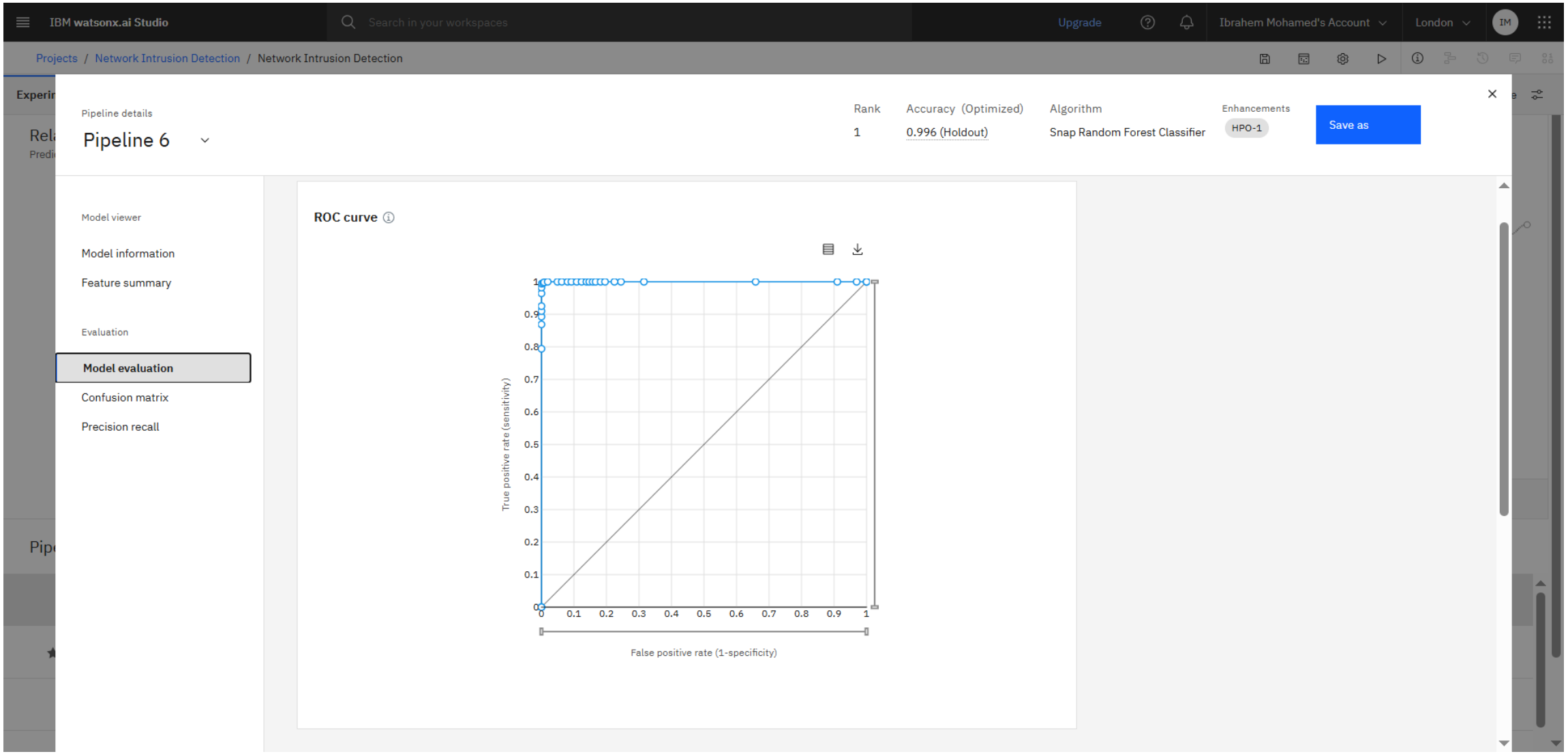
View log | Save code

Pipeline leaderboard

	Rank	Name	Algorithm	Specialization	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	Pipeline 6	Snap Random Forest Classifier		0.995	HPO-1	00:00:23

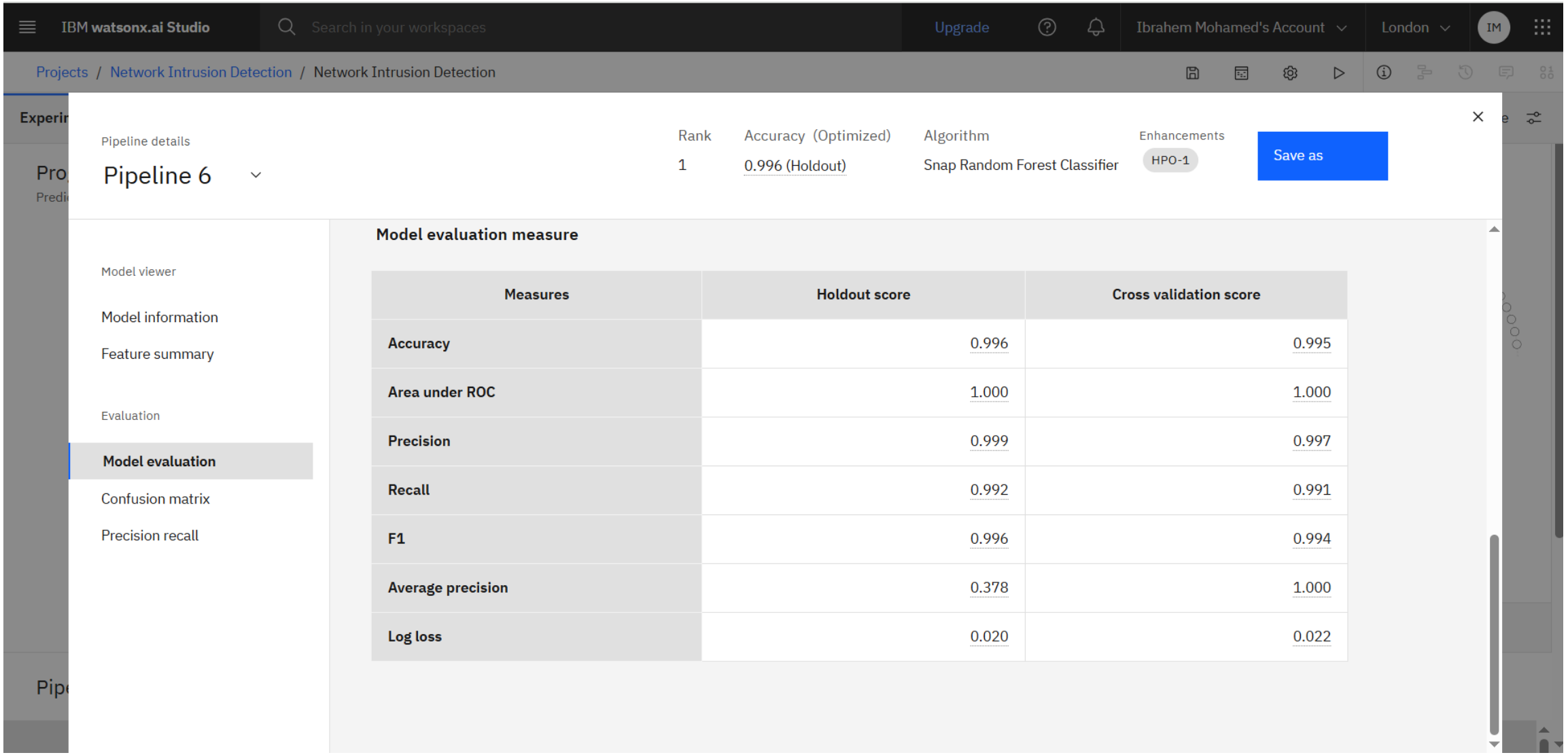
edunet foundation

RESULT



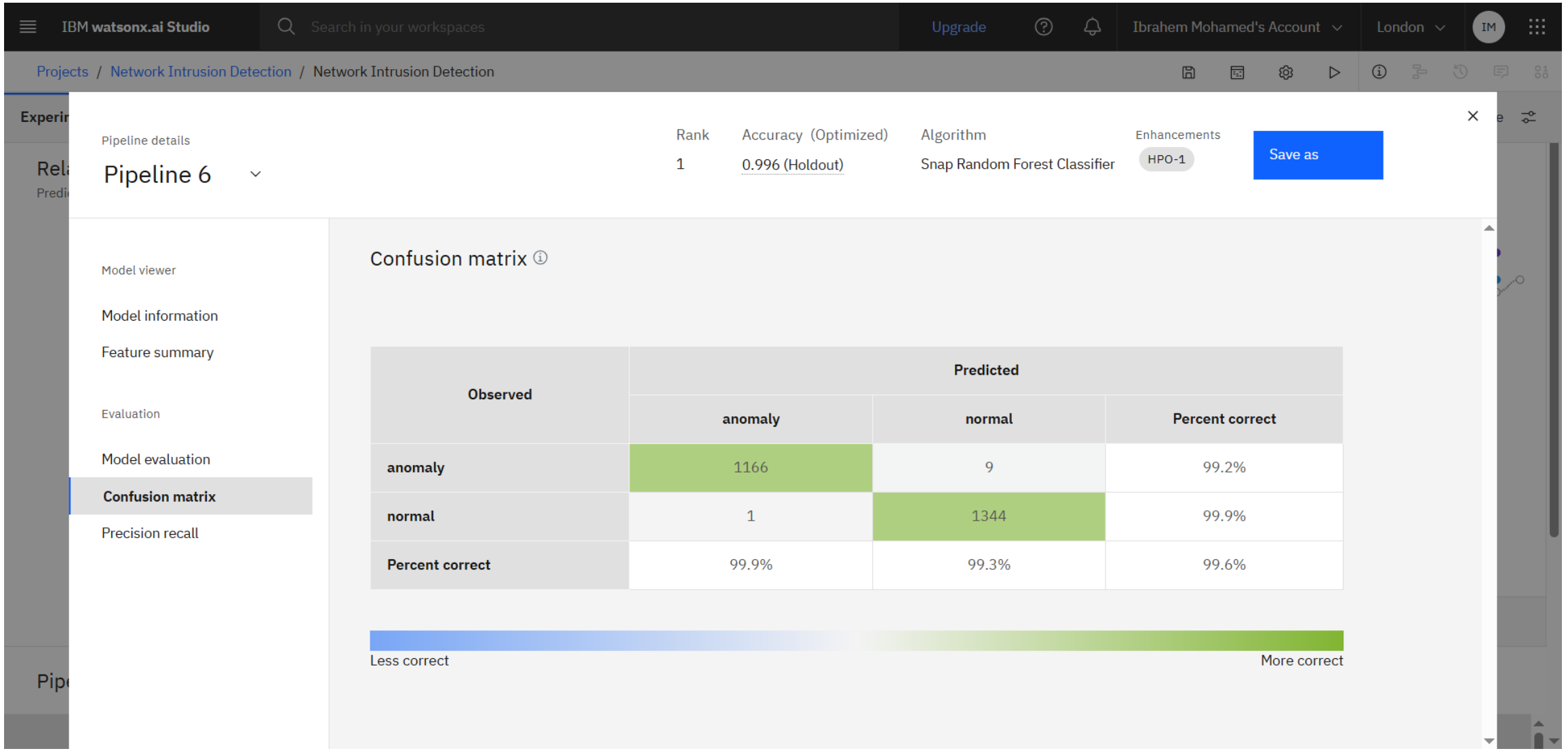
edunet foundation

RESULT

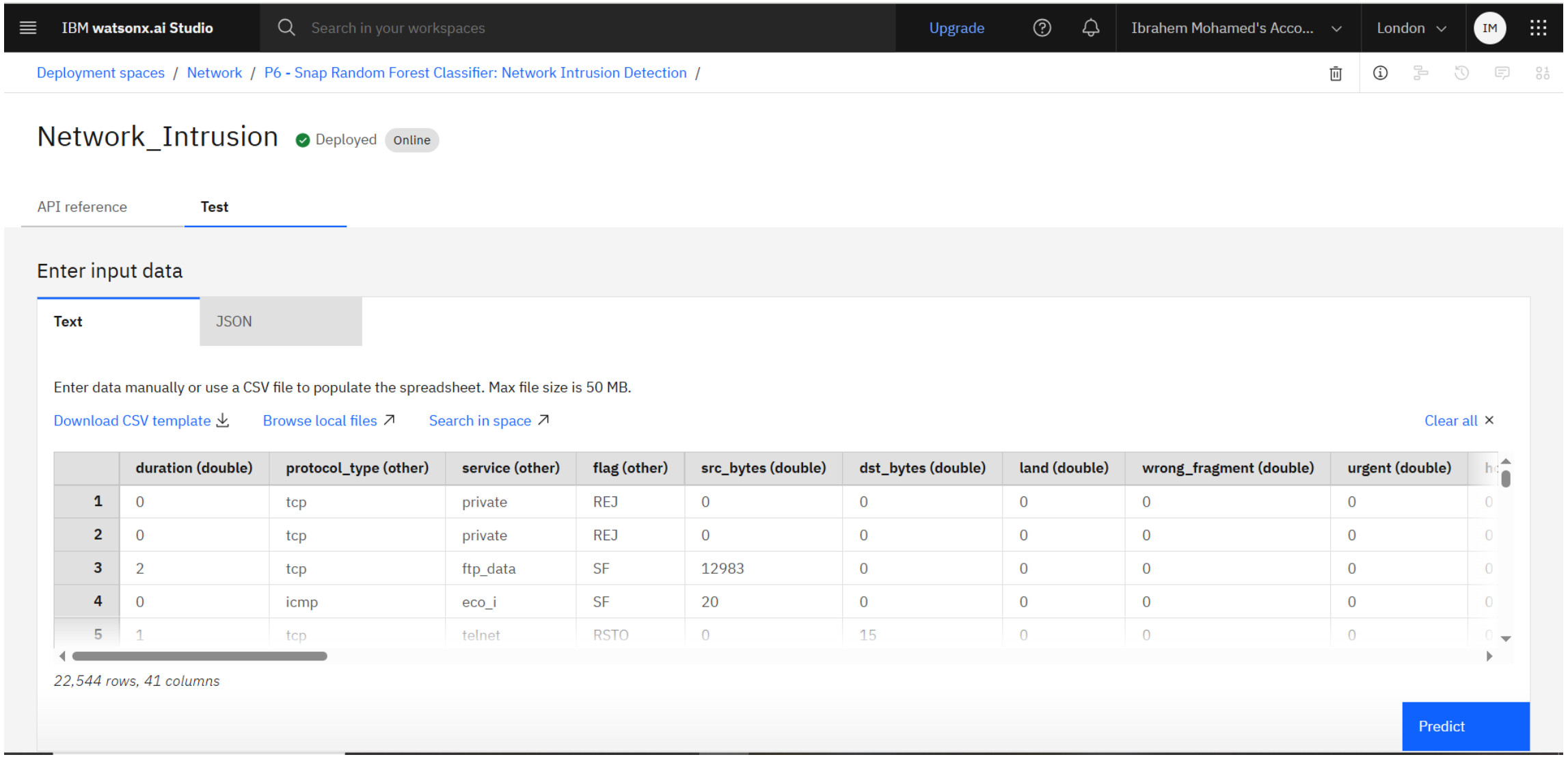


Measures	Holdout score	Cross validation score
Accuracy	0.996	0.995
Area under ROC	1.000	1.000
Precision	0.999	0.997
Recall	0.992	0.991
F1	0.996	0.994
Average precision	0.378	1.000
Log loss	0.020	0.022

RESULT

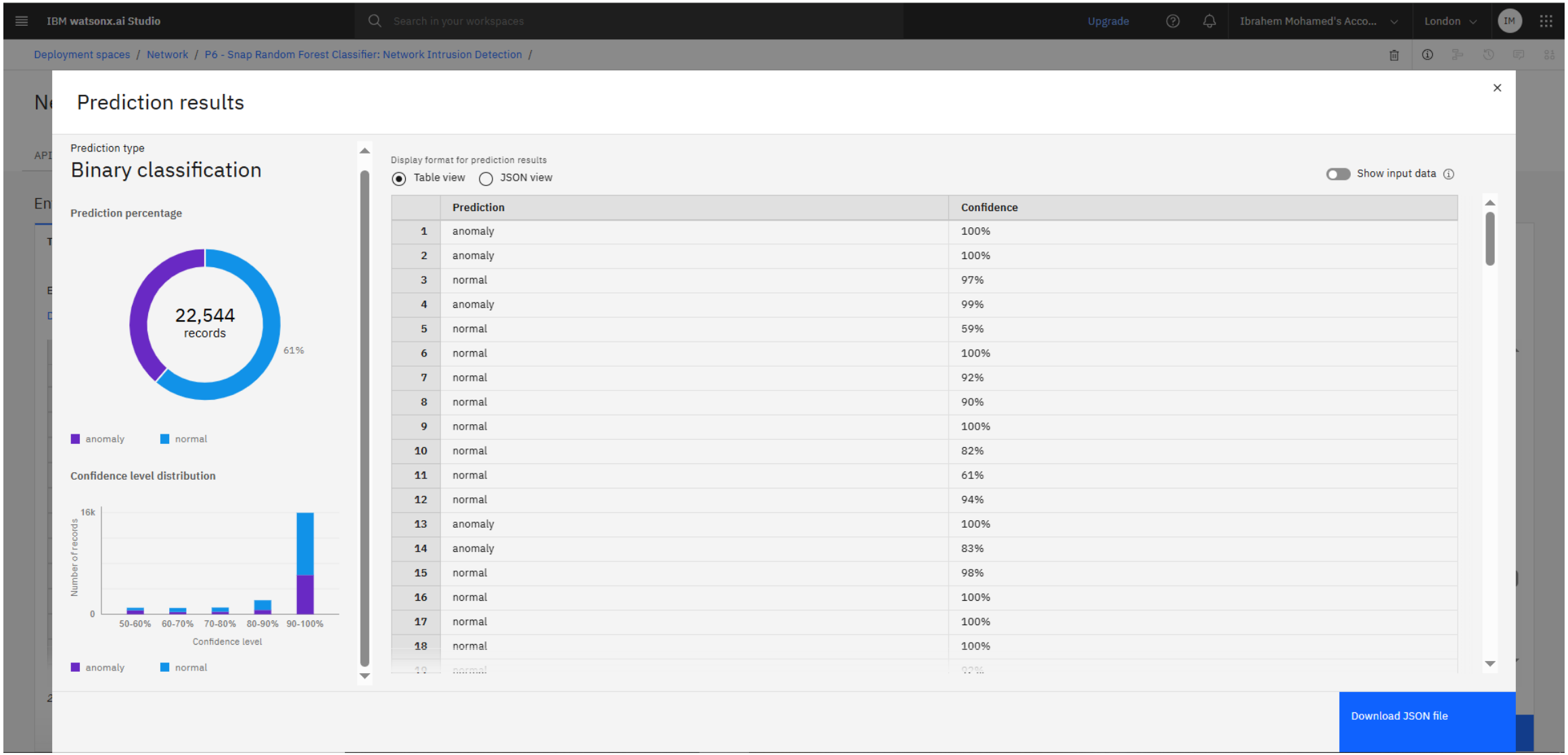


RESULT



edunet foundation

RESULT



	Prediction	Confidence
1	anomaly	100%
2	anomaly	100%
3	normal	97%
4	anomaly	99%
5	normal	59%
6	normal	100%
7	normal	92%
8	normal	90%
9	normal	100%
10	normal	82%
11	normal	61%
12	normal	94%
13	anomaly	100%
14	anomaly	83%
15	normal	98%
16	normal	100%
17	normal	100%
18	normal	100%

CONCLUSION

- The project successfully developed a machine learning-based system to detect and classify network intrusions using IBM Watsonx.ai Studio. The final model (Snap Random Forest Classifier) achieved 99.5% accuracy, demonstrating the effectiveness of the proposed solution in identifying various types of cyber-attacks.

- During the implementation, minimal manual effort was required due to the AutoAI pipeline, but understanding the model's behavior and evaluating results was essential. A key challenge was interpreting multi-class classification outputs and ensuring balanced detection across all intrusion types.

- This system highlights the importance of using intelligent, automated tools to enhance cybersecurity and proactively respond to network threats in real time. Future improvements could include real-time deployment and retraining with updated data to handle zero-day attacks.

FUTURE SCOPE

- Real-time Integration:

  Extend the system to monitor live network traffic for real-time intrusion detection and response.

- Improved Data Sources:

  Incorporate more diverse and updated datasets from real-world network environments to improve model generalization and detect zero-day attacks.

- Model Optimization:

  Apply advanced techniques like ensemble learning or deep learning models (e.g., LSTM, CNN) for higher detection accuracy and handling sequential data.

- False Positive Reduction:

  Fine-tune the model to reduce false positives, ensuring that normal traffic is not incorrectly flagged.

- Edge Deployment:

  Explore deploying the model at the edge (e.g., on routers/firewalls) for low-latency, distributed protection.

- Continuous Learning:

  Enable the system to retrain automatically with new data to stay updated with evolving attack patterns.

REFERENCES

1. Recorded Zoom sessions and training materials provided during the IBM SkillsBuild Internship Program – 2025.

2. PDF documents and resources shared via the official Telegram channel of the internship program.

3. IBM SkillsBuild Courses:

   - Introduction to Machine Learning
   - AI Fundamentals
   - Getting Started with IBM Cloud

4. IBM Watsonx.ai Documentation and Platform

   https://www.ibm.com/cloud/watsonx-ai

5. GPT-based assistance (OpenAI ChatGPT) for clarification and explanation of technical concepts during implementation.

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence
IBM SkillsBuild

Ibrahem Mohamed

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

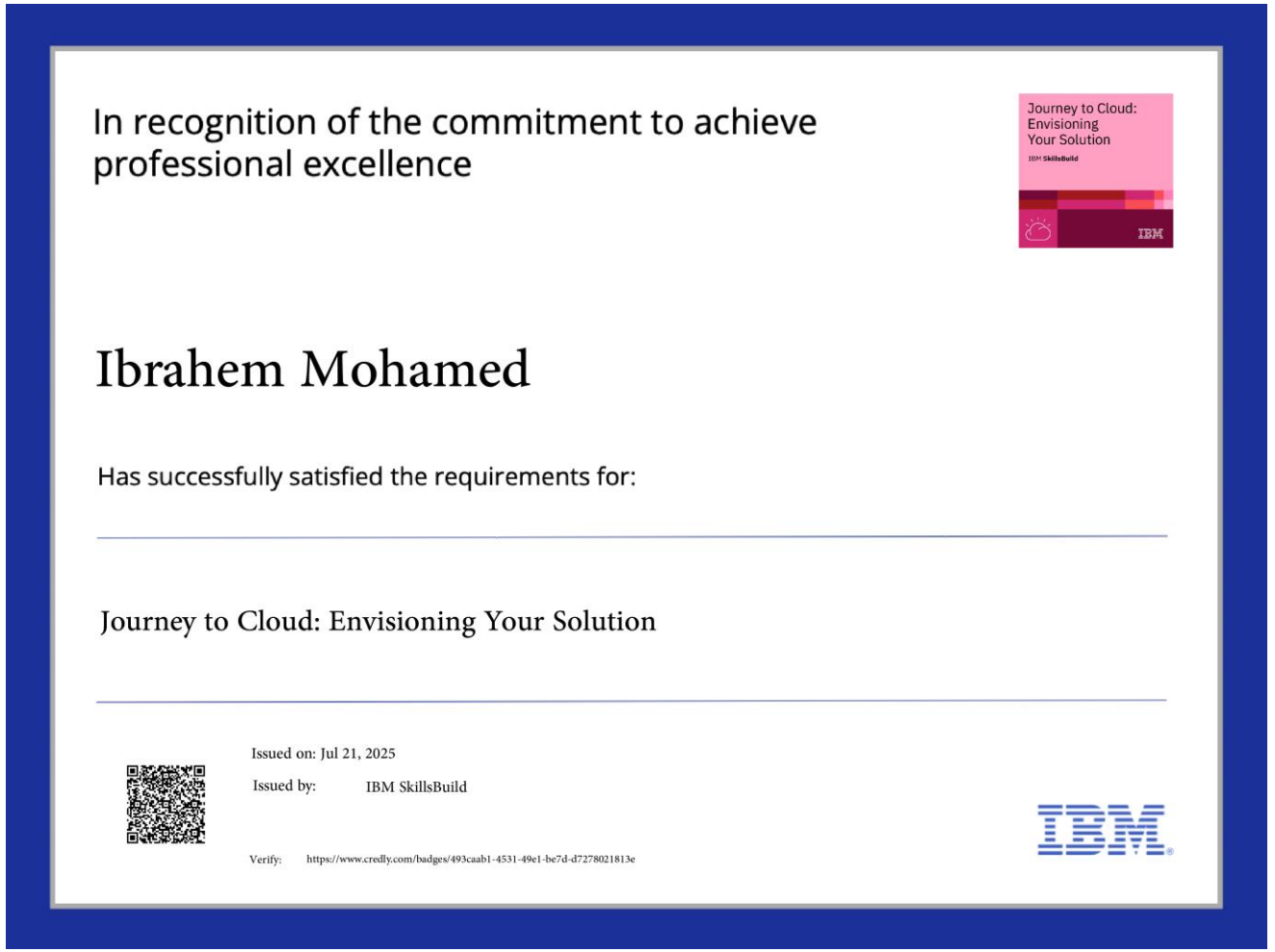
Issued on: Jul 20, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/cdcec169-bb87-4c43-a153-b356998c212d

IBM

IBM CERTIFICATIONS



In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution
IBM SkillsBuild

Ibrahem Mohamed

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 21, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/493caab1-4531-49e1-be7d-d7278021813e

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Ibrahem Mohamed Ibrahem Ahmed

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

THANK YOU

edunet foundation