IBM HACKATHON PROJECT

NETWORK INTRUSION DETECTION

Problem statement No.40

Presented By
Faculty name : Dr. Diana Earshia
College Name & Department : Vel Tech & ECE

edunet foundation

OUTLINE

- Problem Statement
- Technology used
- Wow factor
- End users
- Result
- Conclusion
- Git-hub Link
- Future scope
- IBM Certifications

edunet foundation

PROBLEM STATEMENT

Modern communication networks face a growing volume and diversity of cyber-attacks that can disrupt services, exfiltrate data, and compromise critical infrastructure.

Proposed Solution:

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.

TECHNOLOGY USED

IBM cloud lite services

IBM Granite model

IBM CLOUD SERVICES USED

- IBM Cloud Watsonx AI Studio
- IBM Cloud Watsonx AI runtime and Associates

WOW FACTORS

This agent will provide **Accurate Classification of Network Traffic** by distinguishing between normal activity and multiple types of cyber-attacks (DoS, Probe, R2L, U2R).

Unique features:

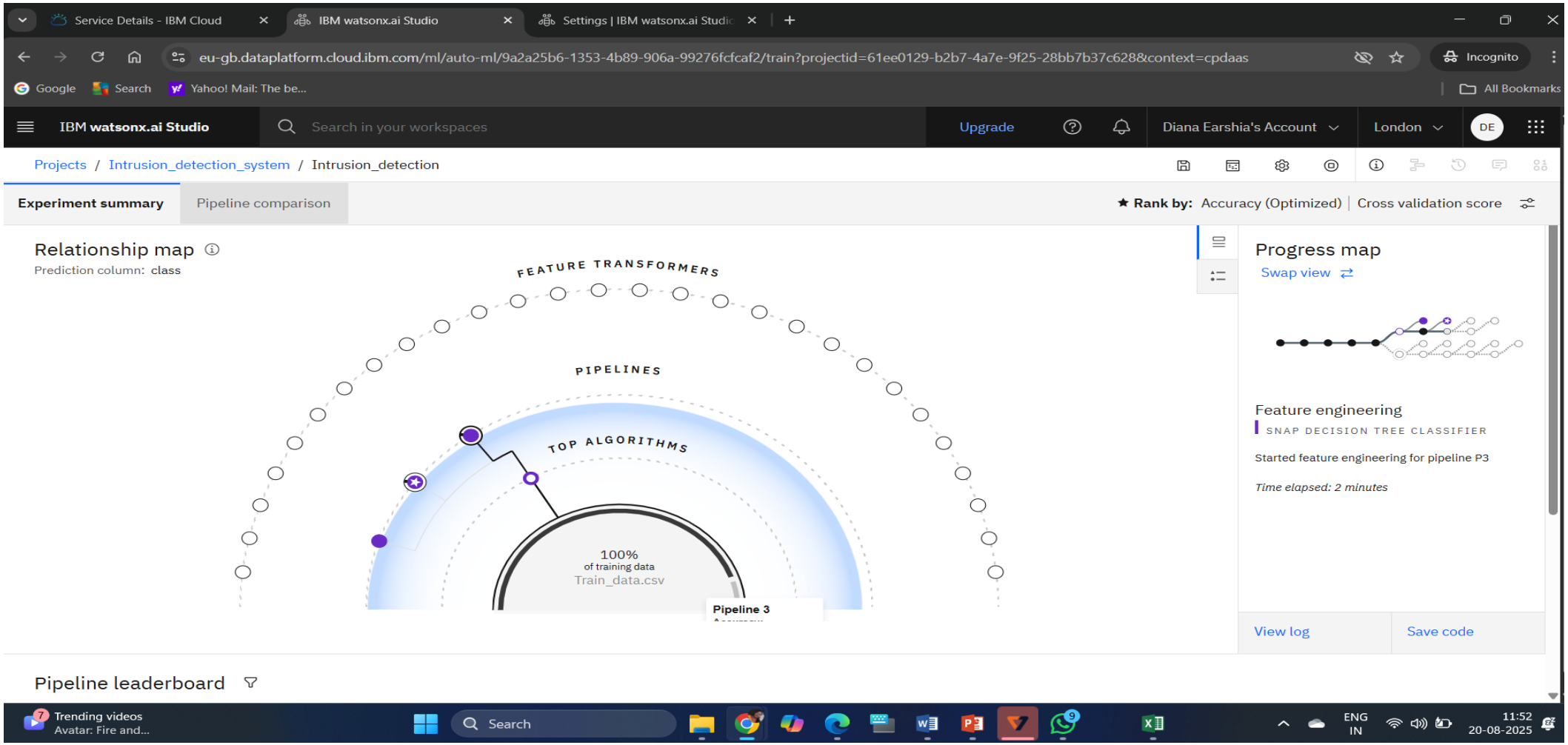
- Real-Time Detection with Low Latency
- Adaptive Learning Against Evolving Threats
- High Accuracy on Rare Attack Types (R2L & U2R)
- Hybrid Detection
- Privacy-Preserving Traffic Analysis

END USERS

- Network Administrators
- Security Analysts
- Cloud Service Providers
- Enterprise Organizations
- Internet Service Providers
- Regulatory & Compliance Officers

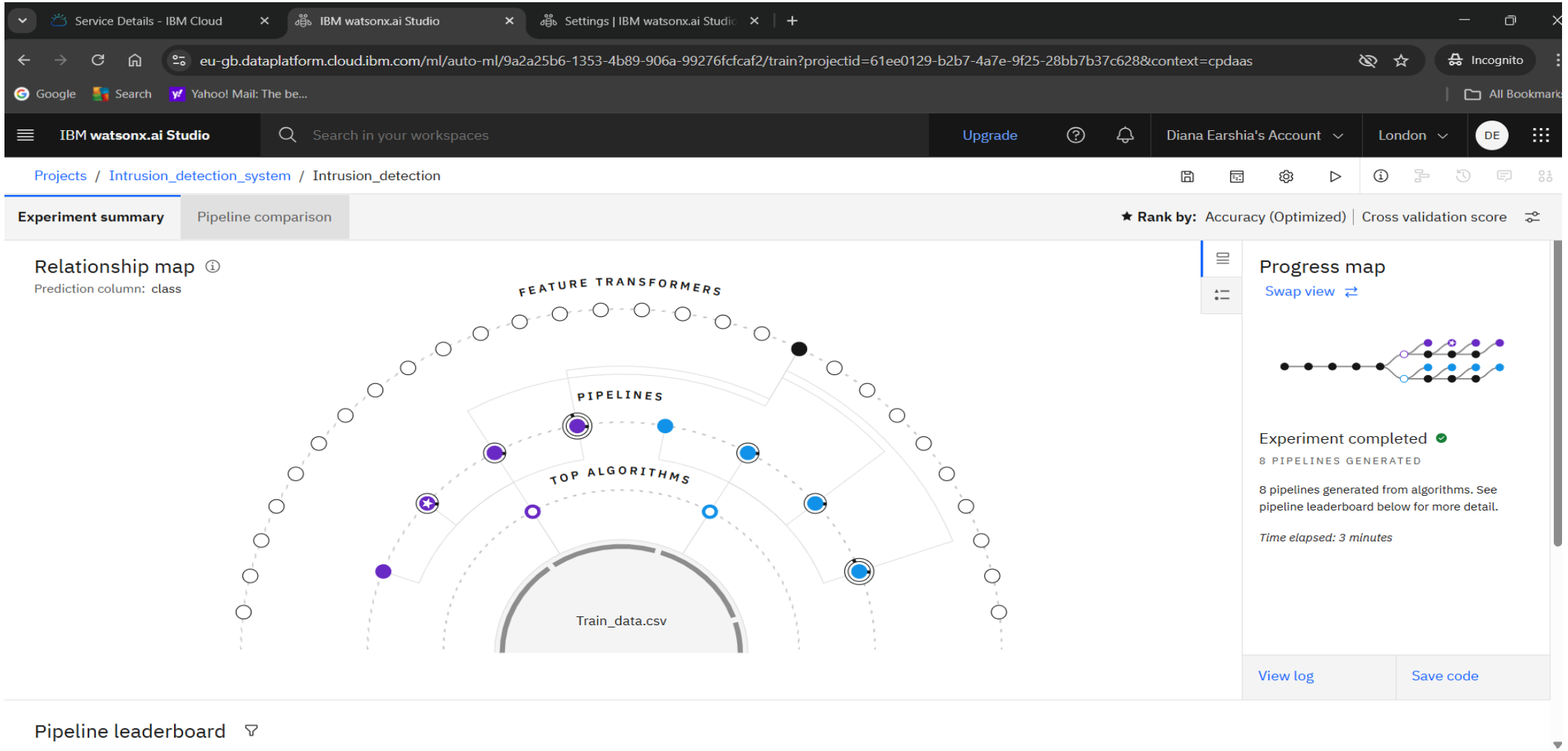
RESULTS

Dataset - Kaggle dataset link –
https://www.kaggle.com/datasets/sampadab17/network intrusion-detection

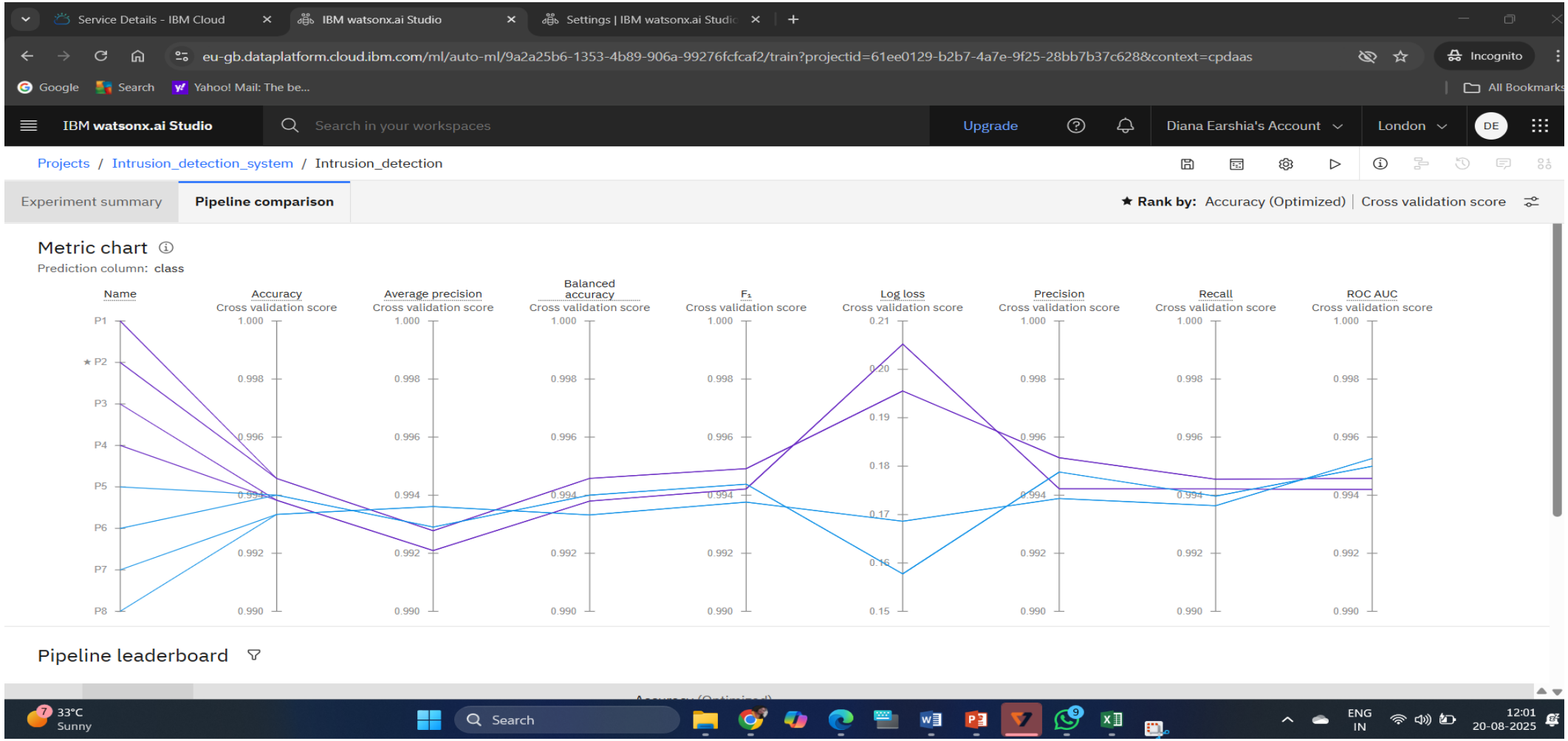


edunet foundation

RESULTS



RESULTS



edunet foundation

RESULTS

Pipeline leaderboard

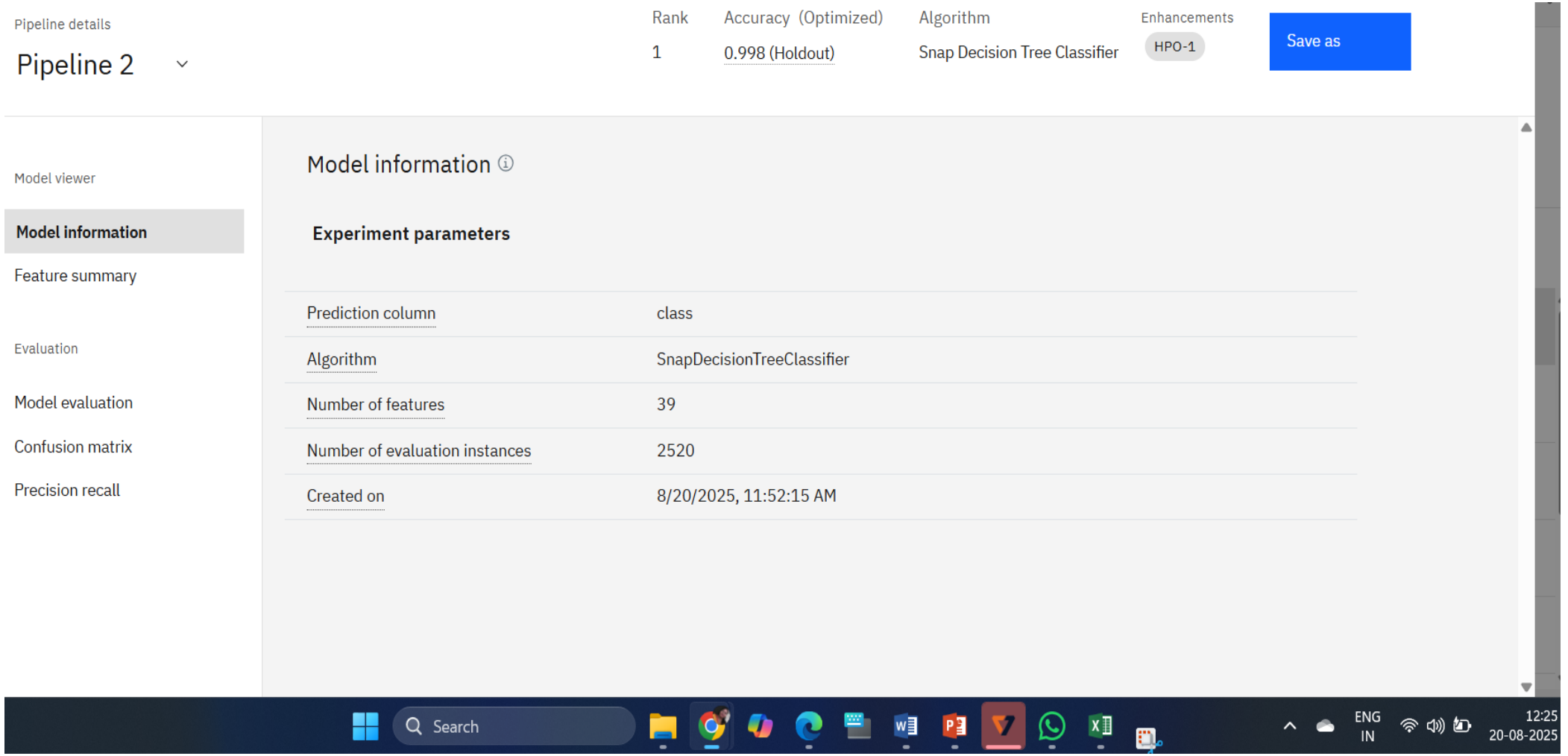
	Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	**Pipeline 2**	Snap Decision Tree Classifier	0.995	HPO-1	00:00:10
	2	**Pipeline 1**	Snap Decision Tree Classifier	0.995	*None*	00:00:03
	3	**Pipeline 6**	Decision Tree Classifier	0.994	HPO-1	00:00:09
	4	**Pipeline 5**	Decision Tree Classifier	0.994	*None*	00:00:03

Pipeline leaderboard

	Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
	5	**Pipeline 4**	Snap Decision Tree Classifier	0.994	HPO-1 FE HPO-2	00:00:47
	6	**Pipeline 3**	Snap Decision Tree Classifier	0.994	HPO-1 FE	00:00:41
	7	**Pipeline 8**	Decision Tree Classifier	0.993	HPO-1 FE HPO-2	00:00:56
	8	**Pipeline 7**	Decision Tree Classifier	0.993	HPO-1 FE	00:00:50

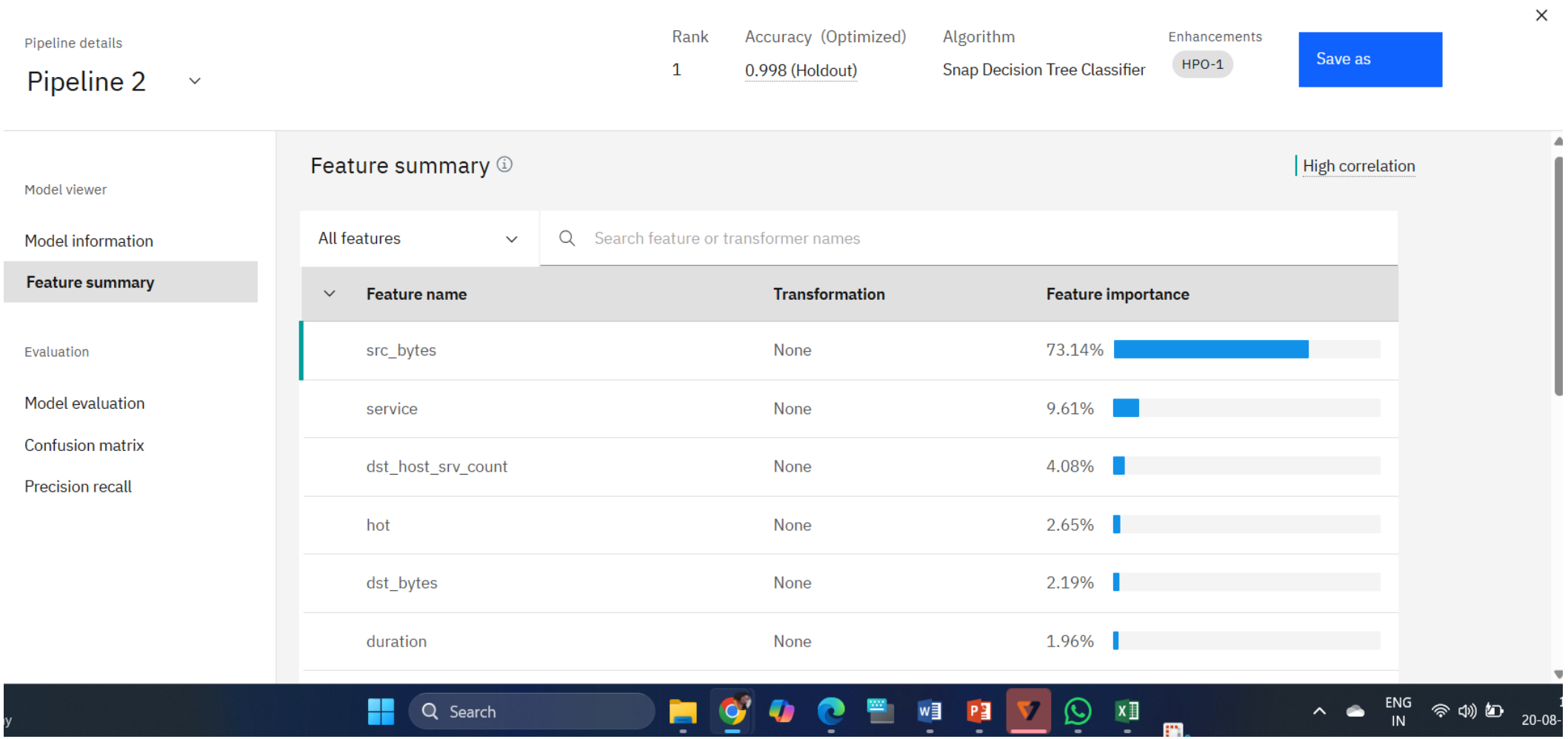
edunet foundation

RESULTS



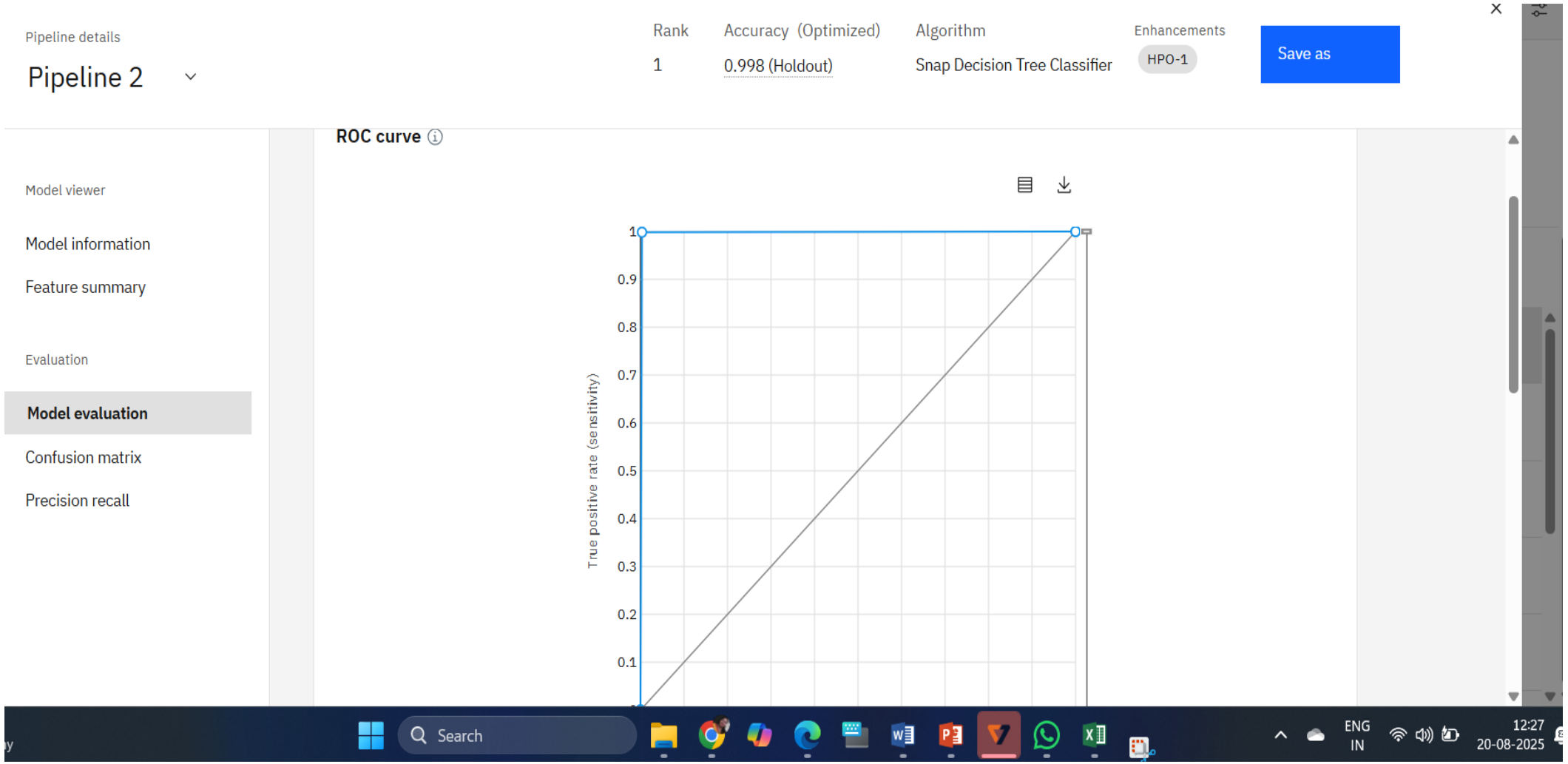
edunet foundation

RESULTS



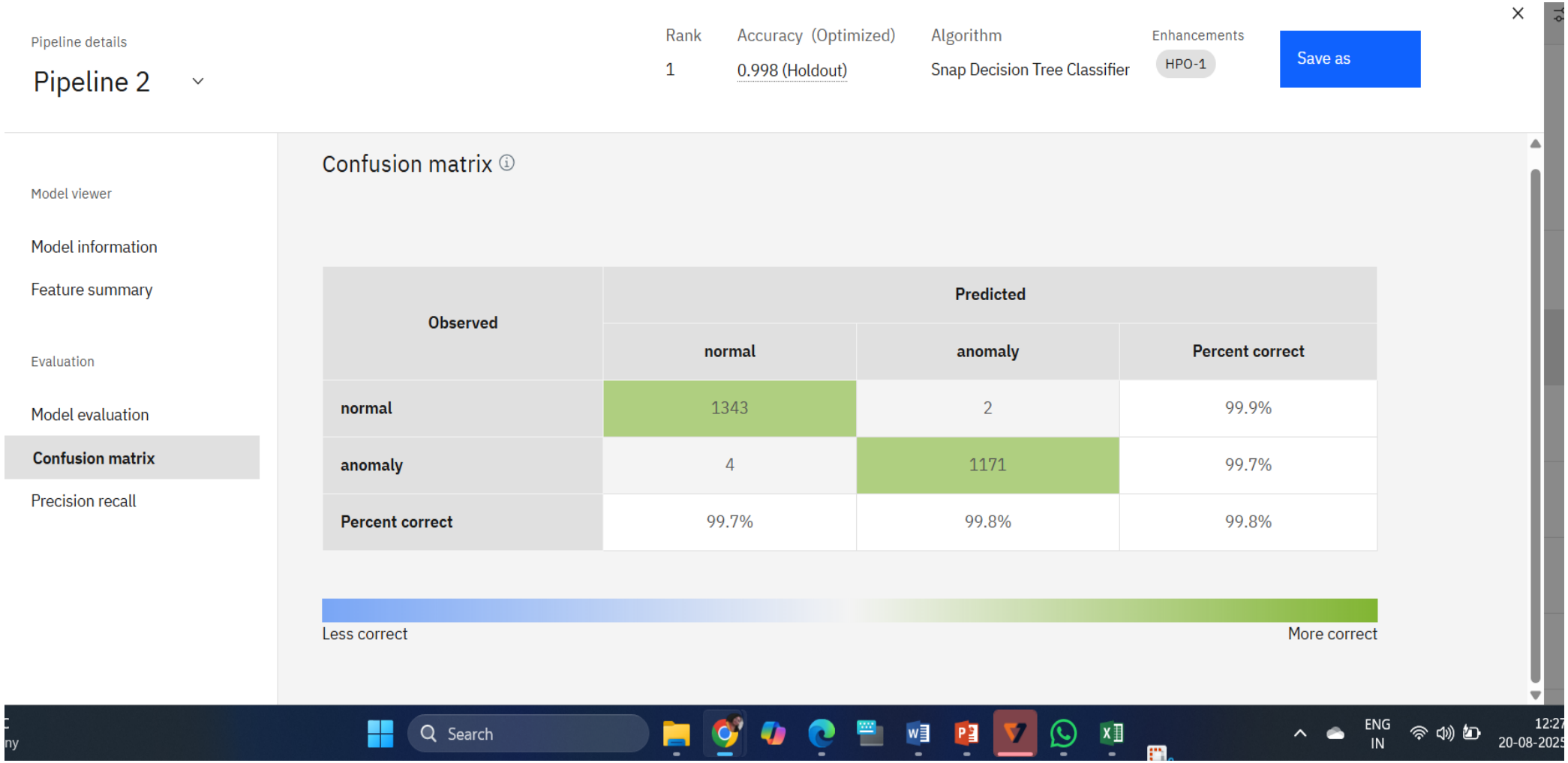
edunet foundation

RESULTS



edunet foundation

RESULTS



edunet foundation

RESULTS

Pipeline details

Pipeline 2

Rank	Accuracy (Optimized)	Algorithm	Enhancements
1	0.998 (Holdout)	Snap Decision Tree Classifier	HPO-1

Save as

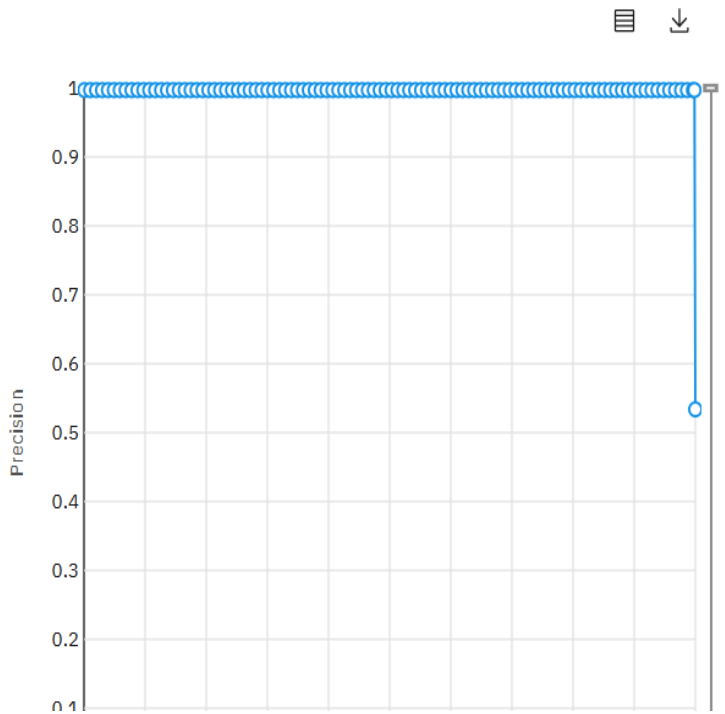
Model viewer

- Model information
- Feature summary

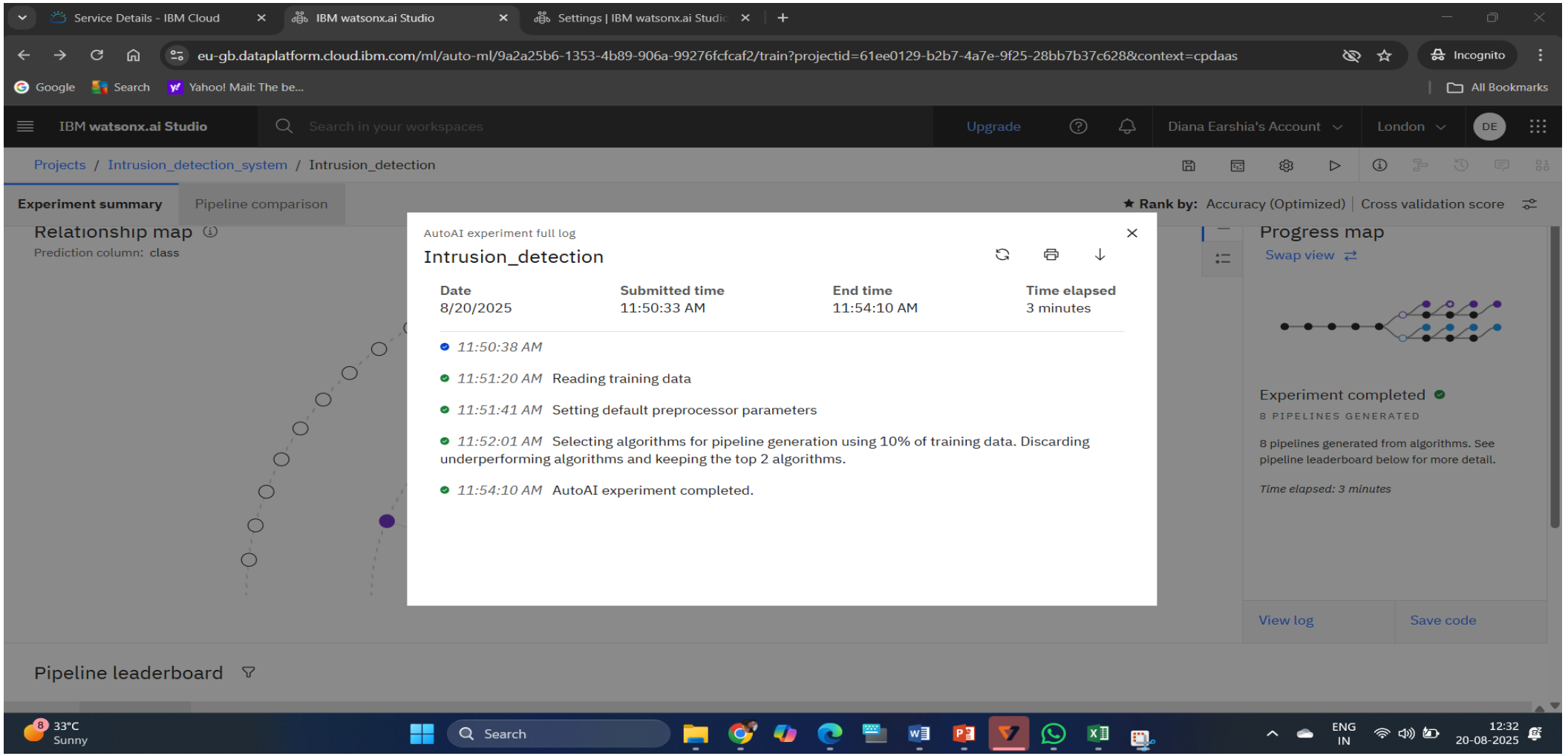
Evaluation

- Model evaluation
- Confusion matrix
- **Precision recall**

Precision recall curve

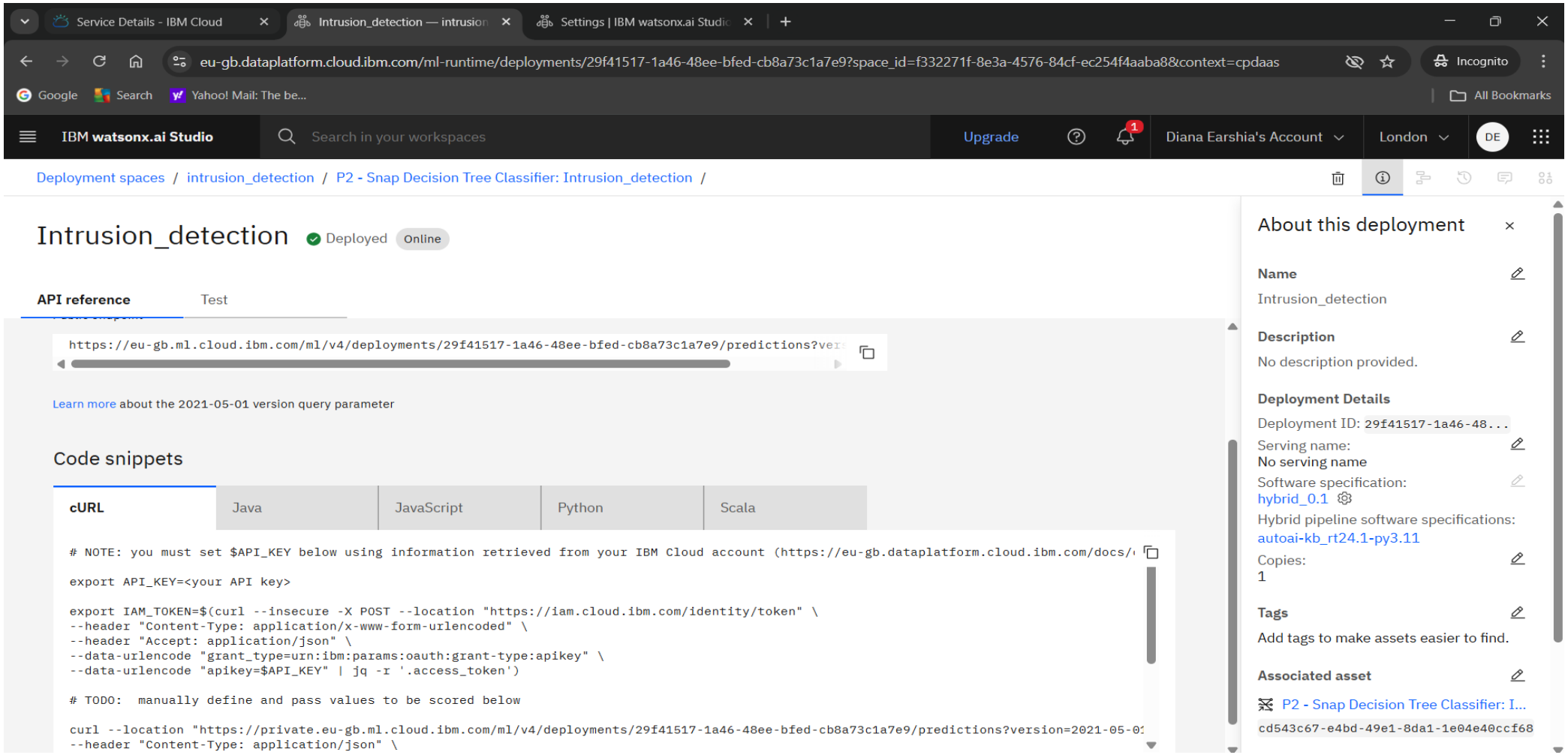


RESULTS



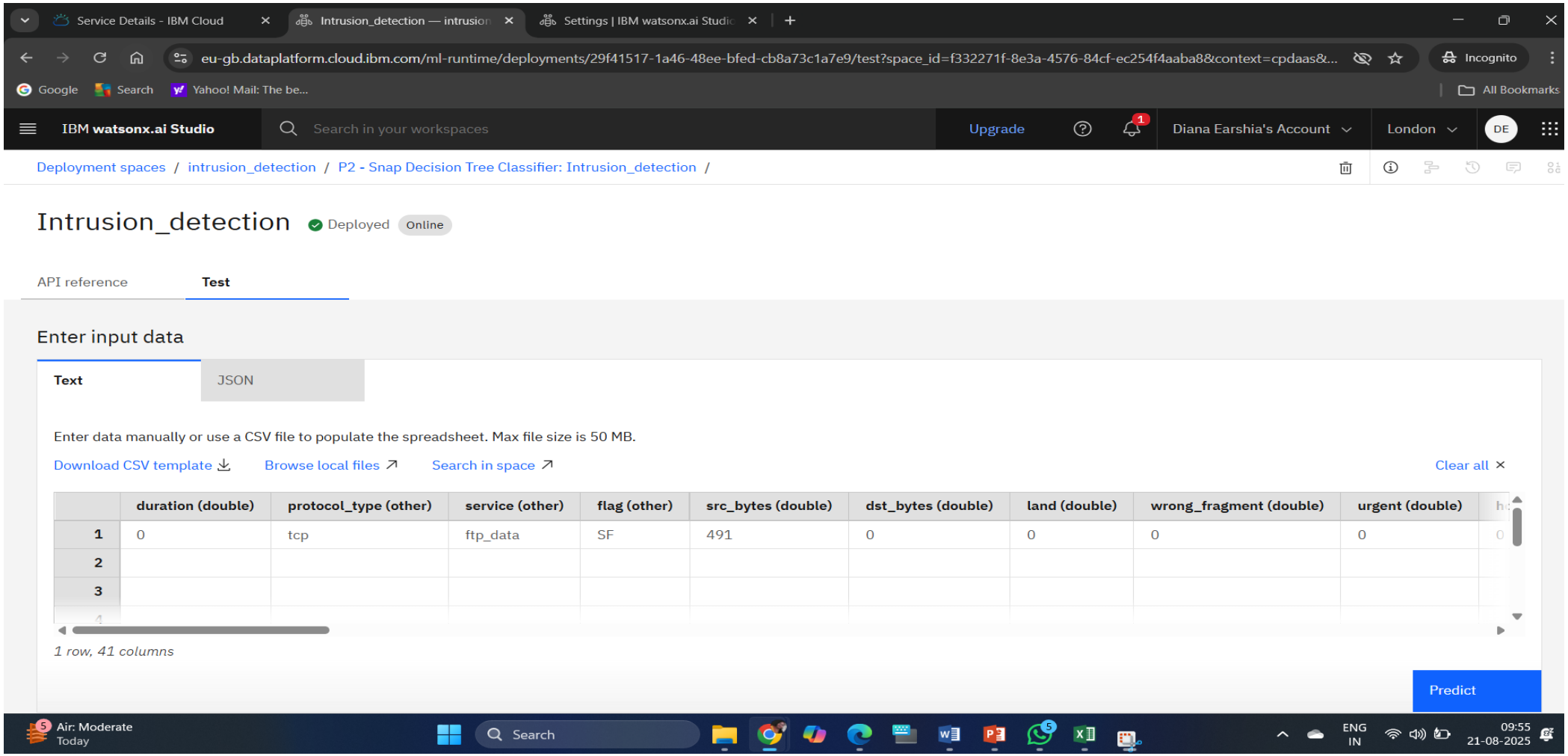
edunet foundation

RESULTS



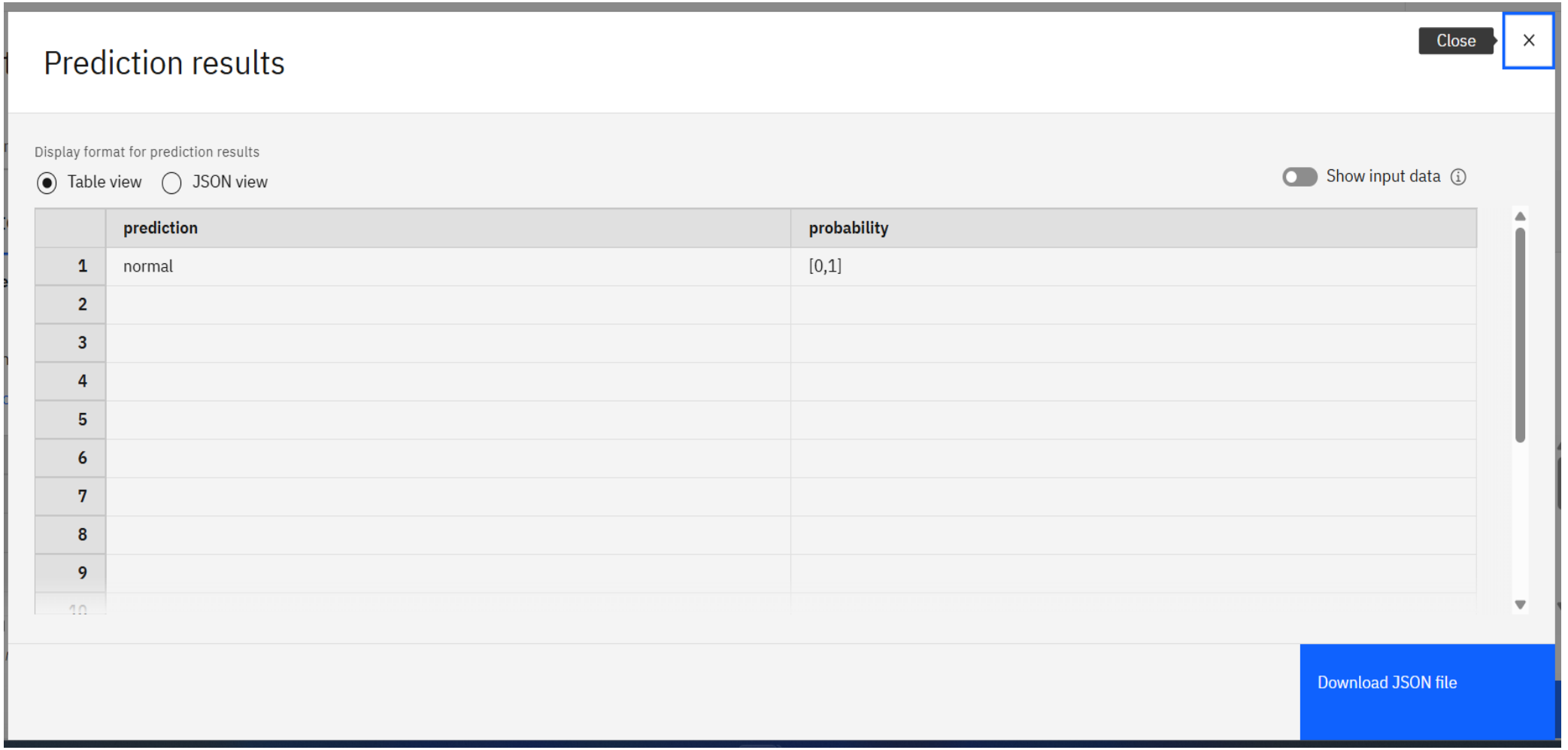
edunet foundation

RESULTS



edunet foundation

RESULTS


Prediction results
Close
Display format for prediction results
Table view
JSON view
Show input data
prediction
probability
1
normal
[0,1]
2
3
4
5
6
7
8
9
Download JSON file

CONCLUSION

- The system strengthens network defenses by delivering **alerts**, that safeguards sensitive data, and enable proactive responses to cyber threats.
- It distinguishes normal traffic from malicious activities effectively and classifies diverse attack types such as **DoS, Probe, R2L, and U2R** with high accuracy.
- It delivers accurate alerts with low false positives and offering explainable insights.

GITHUB LINK

- https://github.com/dianaearshia/IBM-FDP.git

FUTURE SCOPE

- Semi-/self-supervised learning for unknown attacks.
- Online learning with human-in-the-loop labeling.
- Federated/privacy-preserving training across organizations.

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Generative AI in Action
IBM SkillsBuild

Diana Earshia

Has successfully satisfied the requirements for:

Generative AI in Action

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

Verify: https://www.credly.com/badges/66ab53ff-9948-443f-a368-ef7143903c83

IBM

edunet foundation

IBM CERTIFICATIONS

edunet foundation

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Diana Earshia

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 20 Aug 2025 (GMT)

Learning hours: 20 mins

edunet foundation

THANK YOU

edunet foundation