

IBM HACKATHON PROJECT

NETWORK INTRUSION DETECTION

Problem statement No.40

Presented By

Faculty name : Dr. Diana Earshia

College Name & Department : Vel Tech & ECE

OUTLINE

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

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

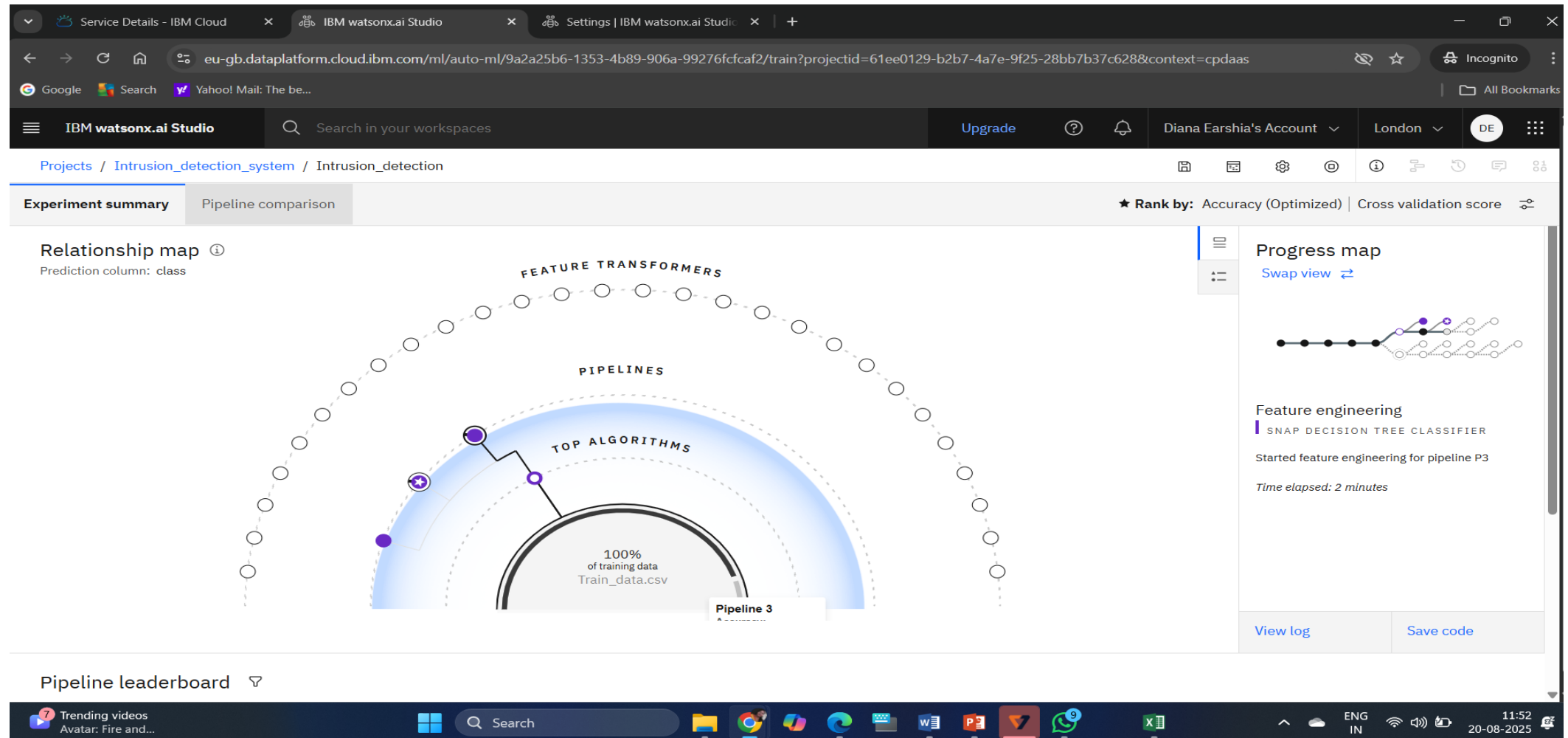
END USERS

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

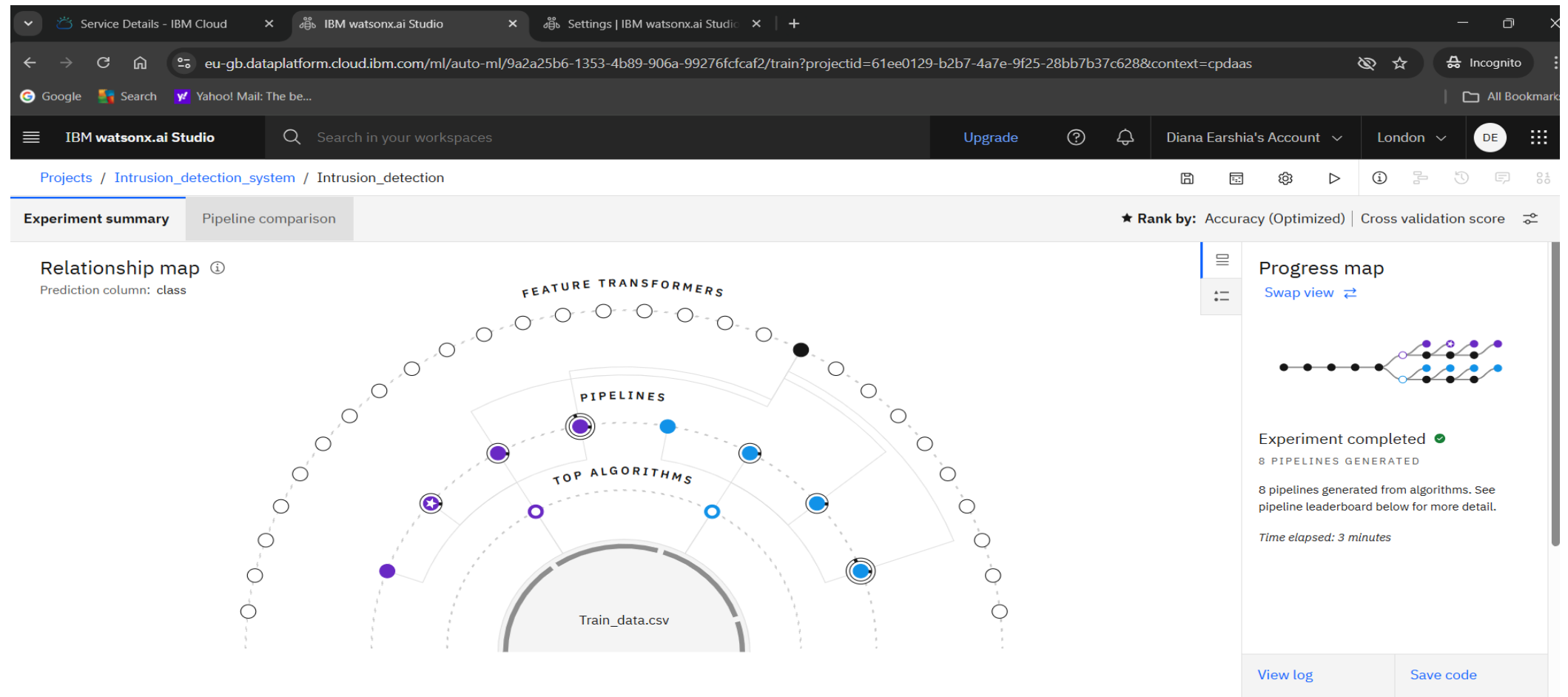
RESULTS

Dataset - Kaggle dataset link -

<https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection>

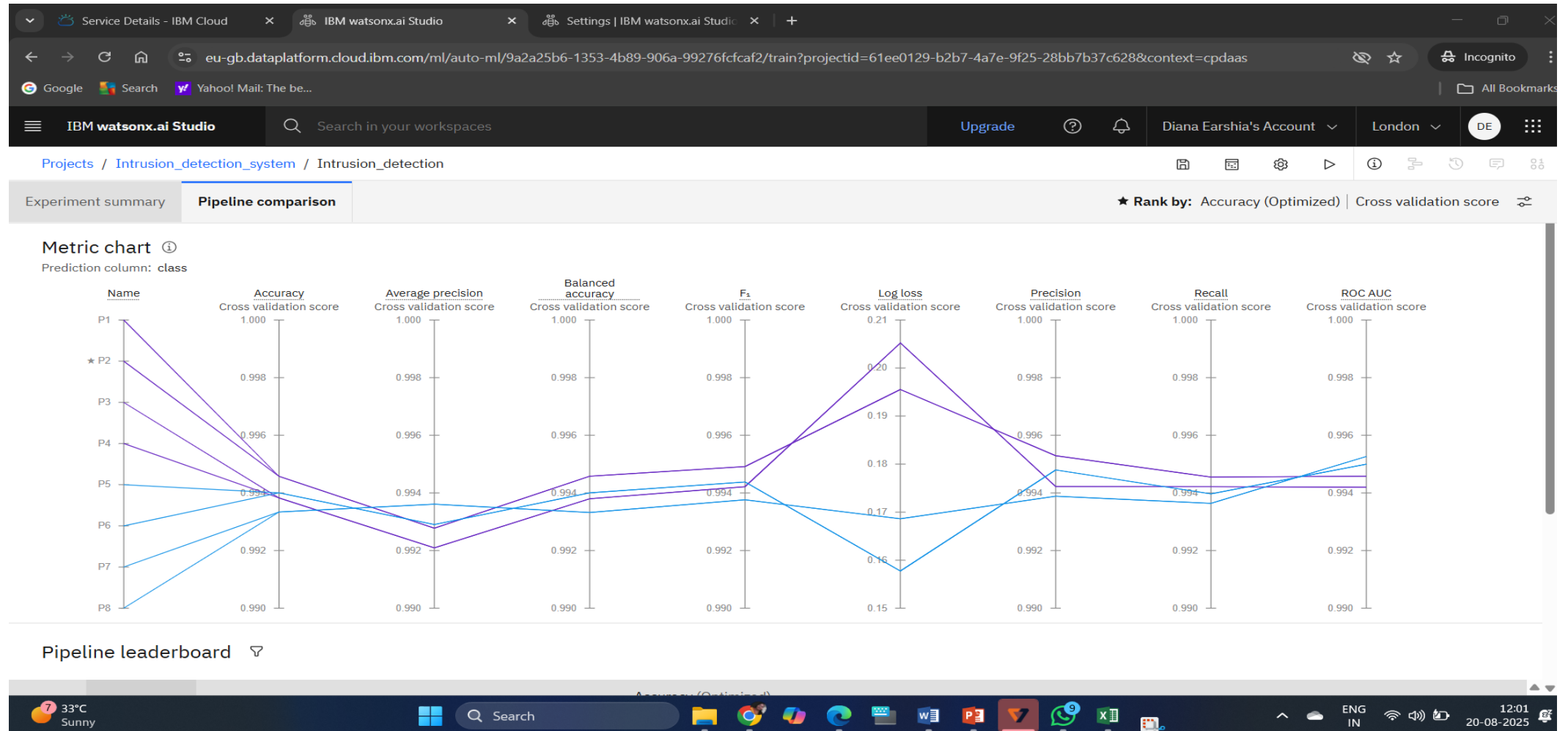


RESULTS



Pipeline leaderboard

RESULTS



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

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

Model information ⓘ

Experiment parameters

<u>Prediction column</u>	class
<u>Algorithm</u>	SnapDecisionTreeClassifier
<u>Number of features</u>	39
<u>Number of evaluation instances</u>	2520
<u>Created on</u>	8/20/2025, 11:52:15 AM



Search



ENG
IN



12:25
20-08-2025

RESULTS

Pipeline details

Pipeline 2

Rank

1

Accuracy (Optimized)

0.998 (Holdout)

Algorithm

Snap Decision Tree Classifier

Enhancements

HPO-1

Save as

×

Model viewer

Model information

Feature summary

Evaluation

Model evaluation

Confusion matrix

Precision recall

Feature summary ⓘ

High correlation

All features

Search feature or transformer names

Feature name	Transformation	Feature importance
src_bytes	None	73.14%
service	None	9.61%
dst_host_srv_count	None	4.08%
hot	None	2.65%
dst_bytes	None	2.19%
duration	None	1.96%

RESULTS

Pipeline details

Pipeline 2 ▾

Rank

1

Accuracy (Optimized)

0.998 (Holdout)

Algorithm

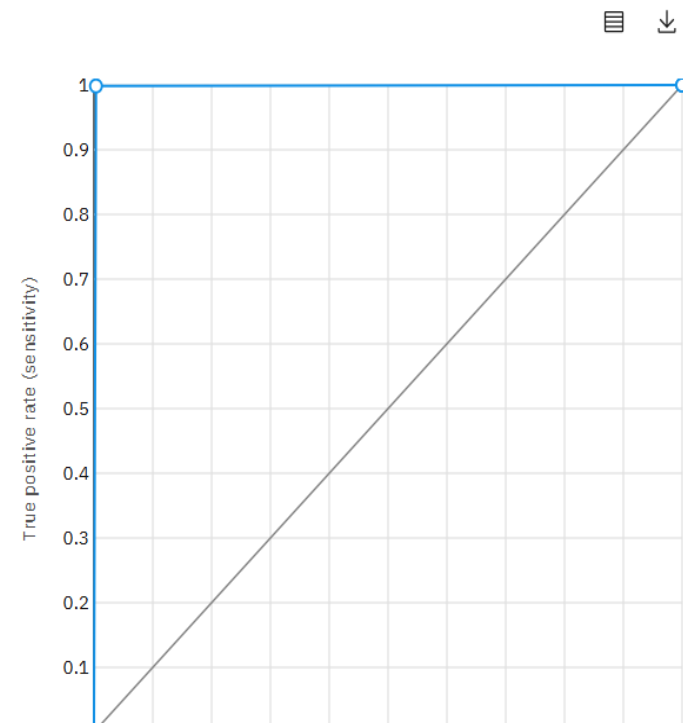
Snap Decision Tree Classifier

Enhancements

HPO-1

Save as

ROC curve ⓘ



Model viewer

Model information

Feature summary

Evaluation

Model evaluation

Confusion matrix

Precision recall



Search



ENG
IN



12:27
20-08-2025

RESULTS

Pipeline details

Pipeline 2

Rank

1

Accuracy (Optimized)

0.998 (Holdout)

Algorithm

Snap Decision Tree Classifier

Enhancements

HPO-1

Save as

Model viewer

Model information

Feature summary

Evaluation

Model evaluation

Confusion matrix

Precision recall

Confusion matrix

Observed	Predicted		
	normal	anomaly	Percent correct
normal	1343	2	99.9%
anomaly	4	1171	99.7%
Percent correct	99.7%	99.8%	99.8%

Less correct

More correct

RESULTS

Pipeline details

Pipeline 2 ▾

Rank

1

Accuracy (Optimized)

0.998 (Holdout)

Algorithm

Snap Decision Tree Classifier

Enhancements

HPO-1

Save as

Model viewer

Model information

Feature summary

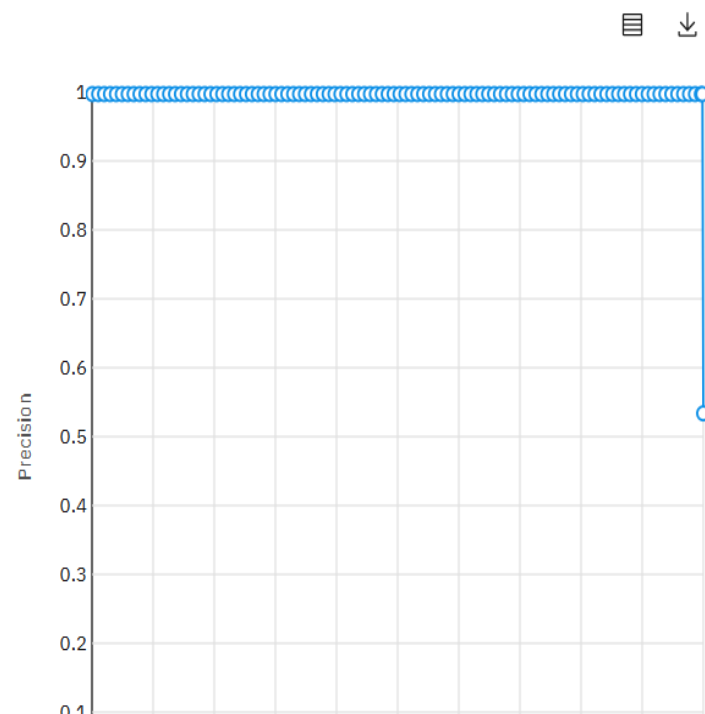
Evaluation

Model evaluation

Confusion matrix

Precision recall

Precision recall curve



RESULTS

The screenshot displays the IBM watsonx.ai Studio interface. The browser address bar shows the URL: `eu-gb.dataplatform.cloud.ibm.com/ml/auto-ml/9a2a25b6-1353-4b89-906a-99276fcfaf2/train?projectId=61ee0129-b2b7-4a7e-9f25-28bb7b37c628&context=cpdaas`. The interface includes a top navigation bar with 'IBM watsonx.ai Studio' and a search bar. The main content area is titled 'Projects / Intrusion_detection_system / Intrusion_detection'. A modal window titled 'AutoAI experiment full log' is open, showing the following details:

Date	Submitted time	End time	Time elapsed
8/20/2025	11:50:33 AM	11:54:10 AM	3 minutes

The log entries are as follows:

- 11:50:38 AM
- 11:51:20 AM Reading training data
- 11:51:41 AM Setting default preprocessor parameters
- 11:52:01 AM Selecting algorithms for pipeline generation using 10% of training data. Discarding underperforming algorithms and keeping the top 2 algorithms.
- 11:54:10 AM AutoAI experiment completed.

The background interface shows a 'Relationship map' with a prediction column of 'class', a 'Progress map' with a 'Swap view' button, and a 'Pipeline leaderboard' section. The right sidebar indicates 'Experiment completed' with 8 pipelines generated and a time elapsed of 3 minutes. The bottom status bar shows the system temperature as 33°C and the date as 20-08-2025.

RESULTS

The screenshot displays the IBM watsonx.ai Studio interface. The browser address bar shows the URL: `eu-gb.dataplatform.cloud.ibm.com/ml-runtime/deployments/29f41517-1a46-48ee-bfed-cb8a73c1a7e9?space_id=f332271f-8e3a-4576-84cf-ec254f4aaba8&context=cpdaas`. The page title is "Intrusion_detection" with a green checkmark and "Deployed" status, and a "Test" button. Below the title, there is a "Code snippets" section with tabs for cURL, Java, JavaScript, Python, and Scala. The cURL tab is active, showing a cURL command for making a prediction. The right sidebar, titled "About this deployment", contains details such as Name (Intrusion_detection), Description (No description provided), Deployment Details (Deployment ID: 29f41517-1a46-48...), Serving name (No serving name), Software specification (hybrid_0.1), Hybrid pipeline software specifications (autoai-kb_rt24.1-py3.11), Copies (1), Tags (Add tags to make assets easier to find), and Associated asset (P2 - Snap Decision Tree Classifier: Intrusion_detection).

Service Details - IBM Cloud x Intrusion_detection — intrusion x Settings | IBM watsonx.ai Studio x +

eu-gb.dataplatform.cloud.ibm.com/ml-runtime/deployments/29f41517-1a46-48ee-bfed-cb8a73c1a7e9?space_id=f332271f-8e3a-4576-84cf-ec254f4aaba8&context=cpdaas

Google Search Yahoo! Mail: The be... All Bookmarks

IBM watsonx.ai Studio Search in your workspaces Upgrade ? 1 Diana Earshia's Account London DE

Deployment spaces / intrusion_detection / P2 - Snap Decision Tree Classifier: Intrusion_detection /

Intrusion_detection

Deployed Online

API reference Test

`https://eu-gb.ml.cloud.ibm.com/ml/v4/deployments/29f41517-1a46-48ee-bfed-cb8a73c1a7e9/predictions?version=2021-05-01`

[Learn more](#) about the 2021-05-01 version query parameter

Code snippets

cURL	Java	JavaScript	Python	Scala
------	------	------------	--------	-------

```
# NOTE: you must set $API_KEY below using information retrieved from your IBM Cloud account (https://eu-gb.dataplatform.cloud.ibm.com/docs/)\nexport API_KEY=<your API key>\n\nexport IAM_TOKEN=$(curl --insecure -X POST --location "https://iam.cloud.ibm.com/identity/token" \\\n--header "Content-Type: application/x-www-form-urlencoded" \\\n--header "Accept: application/json" \\\n--data-urlencode "grant_type=urn:ibm:params:oauth:grant-type:apikey" \\\n--data-urlencode "apikey=$API_KEY" | jq -r '.access_token')\n\n# TODO: manually define and pass values to be scored below\n\ncurl --location "https://private.eu-gb.ml.cloud.ibm.com/ml/v4/deployments/29f41517-1a46-48ee-bfed-cb8a73c1a7e9/predictions?version=2021-05-01"\n--header "Content-Type: application/json" \
```

About this deployment

Name [Intrusion_detection](#)

Description [No description provided.](#)

Deployment Details

Deployment ID: [29f41517-1a46-48...](#)

Serving name: [No serving name](#)

Software specification: [hybrid_0.1](#)

Hybrid pipeline software specifications: [autoai-kb_rt24.1-py3.11](#)

Copies: [1](#)

Tags [Add tags to make assets easier to find.](#)

Associated asset [P2 - Snap Decision Tree Classifier: Intrusion_detection](#)

[cd543c67-e4bd-49e1-8da1-1e04e40ccf68](#)

Air: Moderate Today

Search

ENG IN

09:55 21-08-2025

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		
10		

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/dianaeearshia/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



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 CERTIFICATIONS

In recognition of the commitment to achieve
professional excellence



Diana Earshia

Has successfully satisfied the requirements for:

Code Generation and Optimization Using IBM Granite



Issued on: Aug 19, 2025
Issued by: IBM SkillsBuild

Verify: <https://www.credly.com/badges/6e338c01-3f65-40c5-bac2-928ad819309f>



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



THANK YOU