

---

# **CAPSTONE PROJECT**

## **NETWORK INTRUSION DETECTION SYSTEM USING AUTOAI**

**Presented By:**  
**Mohd Faizan**  
**Nawab Shah Alam Khan College of Engineering and Technology**  
**CSE(AI/ML)**

# OUTLINE

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

---

# Problem Statement

With the exponential growth of internet-connected systems, cybersecurity threats have become more sophisticated, targeting networks with diverse attack vectors. Traditional intrusion detection systems often rely on predefined signatures and cannot adapt to new or evolving attack patterns.

This results in undetected breaches, data theft, and potential damage to critical infrastructure.

There is a pressing need for an intelligent, automated system capable of detecting multiple types of attacks in real-time and differentiating them from normal network activity.

---

# Proposed Solution

The proposed solution is an AI-powered Network Intrusion Detection System (NIDS) built using IBM Watson Studio's AutoAI service.

The system is designed to automatically train and optimize machine learning models to classify network traffic as either Normal or Anomalous.

Key features of the solution include:

- Automated data preprocessing and feature engineering.
- Evaluation of multiple algorithms to select the best-performing model.
  - Deployment as a cloud-based API for real-time prediction.
- Scalability to handle large-scale network traffic data and evolving attack patterns.

---

# System Approach

## **System Requirements:**

- IBM Cloud Lite account with Watson Studio and Watson Machine Learning services.
  - AutoAI experiment setup in Watson Studio.
- Dataset: KDD-based intrusion detection dataset with Normal and Anomalous labels.

## **Libraries/Technologies Used:**

- IBM Watson Studio AutoAI
  - Python for API testing
- Pandas, Requests for data handling and integration
  - Cloud Object Storage for data and model storage

# System Approach

## Approach

### 1. Data Preparation

- Upload Train\_data.csv to Watson Studio project assets
- Ensure target column class is correctly labeled

### 2. Model Building with AutoAI

- Create AutoAI experiment and select dataset
- Set problem type to Classification
- Enable automated preprocessing, feature engineering, and pipeline generation

### 3. Model Selection & Deployment

- Review leaderboard and select top-performing pipeline
- Save as model and deploy as an Online Deployment
- Obtain Scoring URL and API Key

### 4. Testing & Validation

- Send sample input data via Python script using requests
- Verify predictions and probabilities returned by API

# Algorithm & Deployment

## **Algorithm Selection:**

- AutoAI automatically evaluates multiple models (Random Forest, Gradient Boosting, XGBoost, Logistic Regression, etc.) and selects the one with the highest F1-score for optimal classification.

## **Data Input:**

- 41 features per network connection, including 3 categorical and 38 numerical attributes.

## **Training Process:**

- AutoAI performs automated preprocessing, feature engineering, model training, and hyperparameter tuning.
  - Pipelines are ranked based on evaluation metrics.

## **Deployment:**

- The best pipeline is saved as a model in Watson Machine Learning.
- Deployed as an Online API endpoint for real-time intrusion detection.

# Result

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

🔔

Mohd Faizan's Account

Dallas

MF

Projects / Network\_Intrusion\_Detection / NIDS\_AutoAI

Configure AutoAI experiment

NIDS\_AutoAI

Autosaved: 9:26:27 PM

Add data source

Add files such as tabular data (CSV).

Browse

Select from project

Train\_data.csv

Size: 2.74 MB

Columns: 42

Configure details

Enable this option to predict future activity over a specified date/time range. Data must be structured and sequential. [Learn more](#)

Yes

No

💡

What do you want to predict?

Prediction column ⓘ

class

Prediction column: class

CUH remaining: 1.2 CUH ⚠️

PREDICTION TYPE

Binary Classification

POSITIVE CLASS

Normal

OPTIMIZED FOR

Accuracy & run time

Experiment settings

Run experiment

26°C

Mostly cloudy

Search

🔍

ENG

IN

9:28 PM

8/4/2025

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

🔔

Mohd Faizan's Account

London

MF

Projects / Network\_Intrusion\_Detection / NIDS\_AutoAI

Experiment summary

Pipeline comparison

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

Progress map ⓘ

Prediction column: class

Read dataset

Split holdout data

Read training data

Preprocessing

Model selection

Snap Decision Tree Classifier

Hyperparameter optimization

Feature engineering

Hyperparameter optimization

P1

P2

P3

P4

Decision Tree Classifier

Hyperparameter optimization

Feature engineering

Hyperparameter optimization

P5

P6

P7

P8

Relationship 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	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★ 1		Pipeline 2	🟡 Snap Decision Tree Classifier	0.995	HPO-1	00:00:08

24°C

Mostly cloudy

Search

🔍

ENG

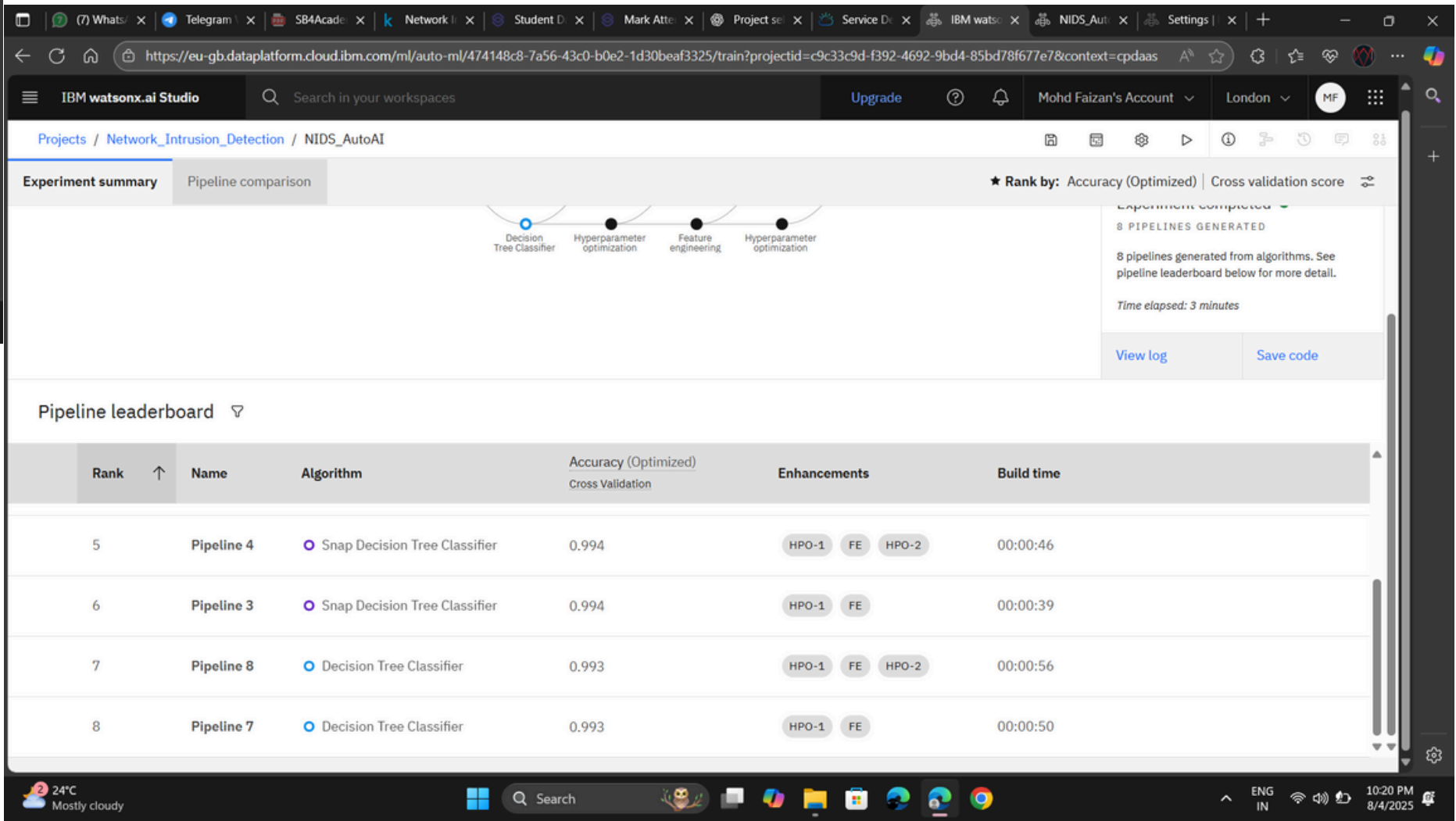
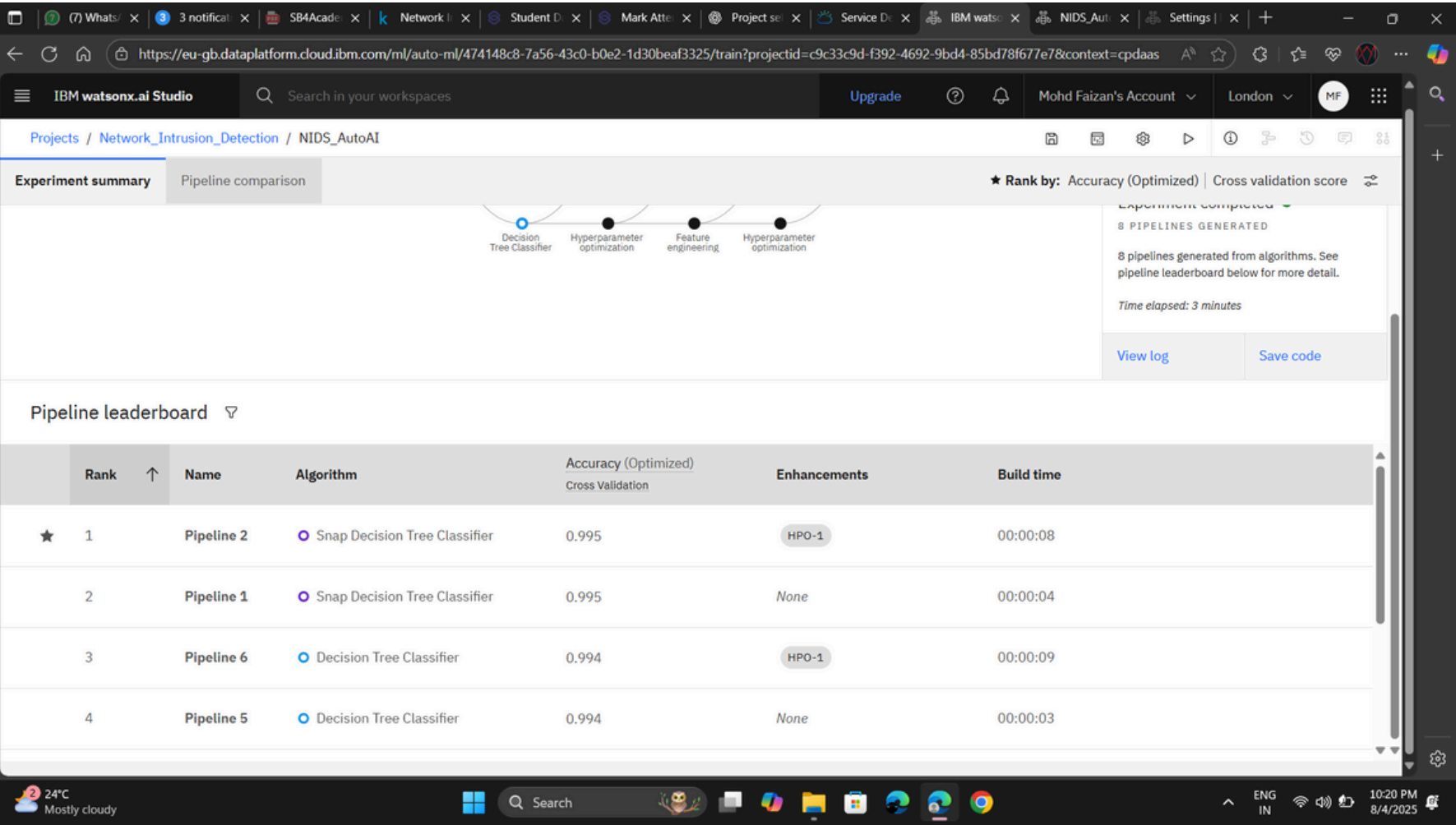
IN

10:18 PM

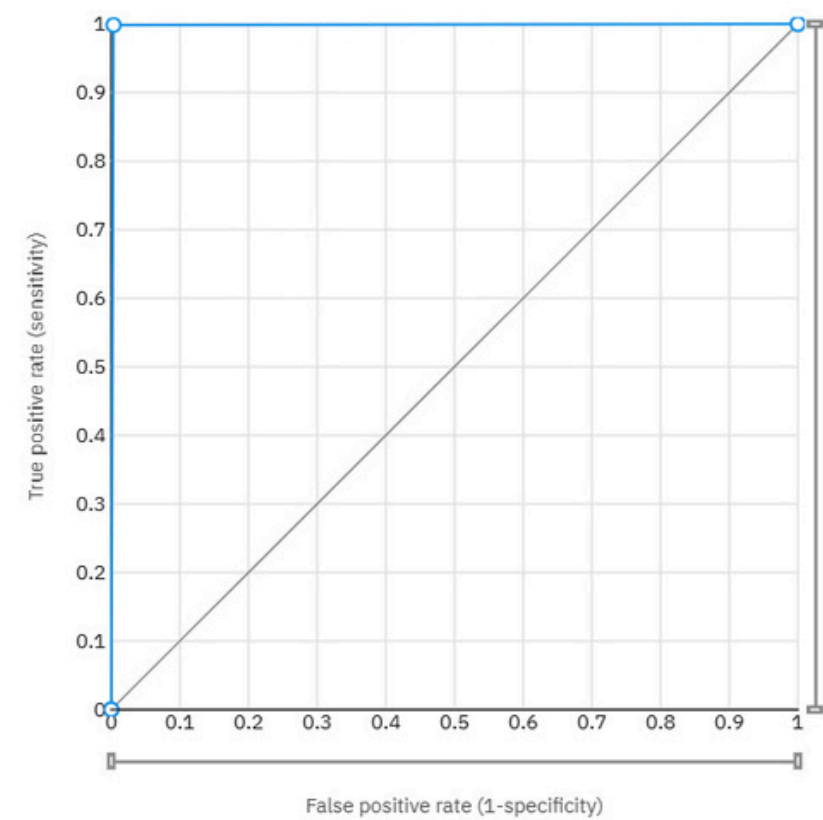
8/4/2025



# Result



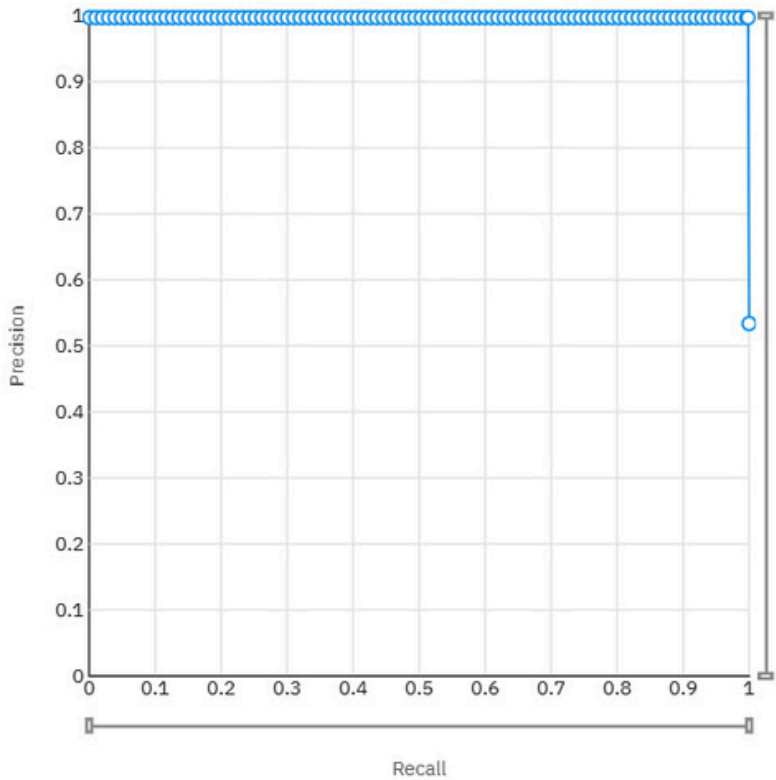
# Result



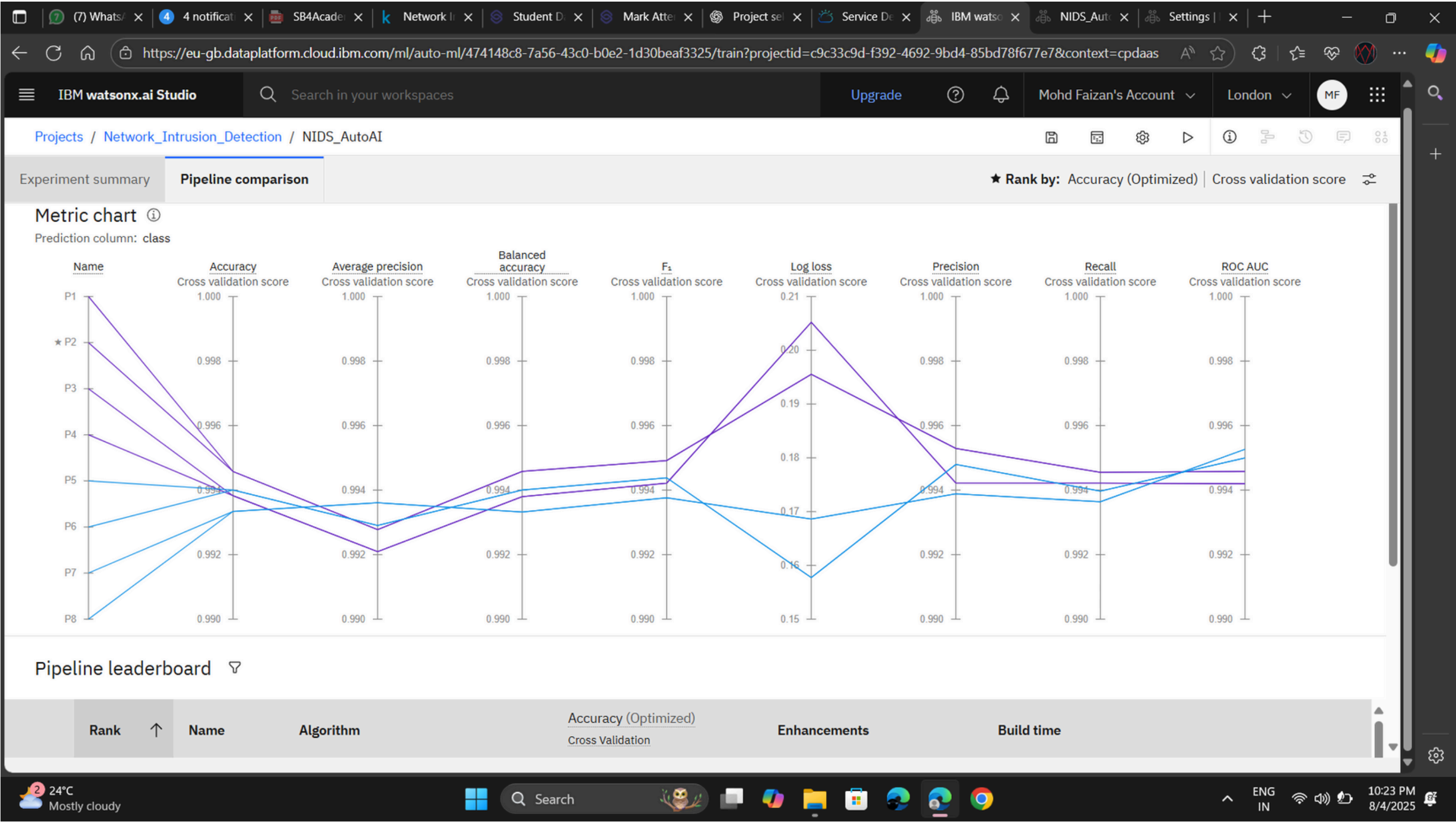
Model evaluation measure		
Measures	Holdout score	Cross validation score
Accuracy	0.998	0.995
Area under ROC	0.998	0.995
Precision	0.997	0.995
Recall	0.999	0.995
F1	0.998	0.995
Average precision	0.996	0.993
Log loss	0.086	0.196

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%



# Result



PIPELINE Comparison

# Result

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

Mohd Faizan's Account

London

MF

Deployment spaces / NIDS\_Deploy / P2 - Snap Decision Tree Classifier: NIDS\_AutoAI

Deployments

Model details

Search

New deployment

Name	Type	Status	Tags	Last modified
NIDS_Deploy	Online	Deployed		47 seconds ago Mohd Faizan (You)

Items per page: 20 1-1 of 1 items 1 of 1 pages

About this asset

NameP2 - Snap Decision Tree Classifier: NIDS\_AutoAI

DescriptionNo description provided.

Asset DetailsType: wml-hybrid\_0.1Model ID: c60dbc08-0f44-49...Software specification: hybrid\_0.1Hybrid pipeline software specifications: autoai-kb\_rt24.1-py3.11

TagsAdd tags to make assets easier to find.

Source asset details

Last modified2 minutes ago by Mohd Faizan

Created onAug 4, 2025 by Mohd Faizan

# DEPLOYMENT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

Mohd Faizan's Account

London

MF

Deployment spaces / NIDS\_Deploy / P2 - Snap Decision Tree Classifier: NIDS\_AutoAI

NIDS\_Deploy

Deployed

Online

API reference

Test

Endpoints for scoring

Private endpointhttps://private.eu-gb.ml.cloud.ibm.com/ml/v4/deployments/d59c7aef-1420-45ed-9369-0461e4da69f8/predictionsIAM

Public endpointhttps://eu-gb.ml.cloud.ibm.com/ml/v4/deployments/d59c7aef-1420-45ed-9369-0461e4da69f8/predictions

Learn more about the 2021-05-01 version query parameter

Code snippets

cURLJavaJavaScriptPythonScala

# NOTE: you must set \$API\_KEY below using information retrieved from your IBM Cloud account (https://eu-gb.dataplatform.cloud.ibm.com)export API\_KEY=<your API key>export IAM\_TOKEN=\$(curl --insecure -X POST --location "https://iam.cloud.ibm.com/identity/token" \--header "Content-Type: application/x-www-form-urlencoded" \

About this deployment

NameNIDS\_Deploy

DescriptionNo description provided.

Deployment DetailsDeployment ID: d59c7aef-1420-45...Serving name: No serving name.Software specification: hybrid\_0.1Hybrid pipeline software specifications: autoai-kb\_rt24.1-py3.11Copies: 1

TagsAdd tags to make assets easier to find.

Associated assetP2 - Snap Decision Tree Classifier: NIDS\_AutoAI

Last modified



# Result

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

Mohd Faizan's Account

London

MF

Deployment spaces / NIDS\_Deploy / P2 - Snap Decision Tree Classifier: NIDS\_AutoAI /

NIDS\_Deploy 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.

9 rows, 41 columns

Predict

# TESTING

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

Mohd Faizan's Account

London

MF

Deployment spaces / NIDS\_Deploy / P2 - Snap Decision Tree Classifier: NIDS\_AutoAI /

Prediction results

Prediction type

Binary classification

Prediction percentage

9 records

normal

anomaly

Confidence level distribution

Display format for prediction results

Table view

JSON view

Show input data

	Prediction	Confidence
1	normal	100%
2	normal	100%
3	anomaly	100%
4	normal	100%
5	anomaly	100%
6	normal	100%
7	anomaly	100%
8	anomaly	100%
9	anomaly	100%
10		
11		

Download JSON file

---

# Conclusion

- The AI-powered Network Intrusion Detection System successfully demonstrates the application of AutoAI for cybersecurity.
- By automating the process of model selection, training, and deployment, the system achieved high accuracy and adaptability against diverse network attacks.
- The deployment as a cloud API enables real-time threat detection without manual intervention.
- This approach reduces the dependency on static rule-based systems and improves resilience against evolving cyber threats.

---

## Future scope

- Integrate real-time streaming data analysis for live network monitoring. Expand the system to multi-class classification for identifying specific attack types (DoS, Probe, R2L, U2R).
- Incorporate anomaly detection techniques for zero-day threats. Enhance explainability to provide detailed reasons for flagged anomalies.
- Deploy on edge devices for local, low-latency detection in IoT and critical systems.

---

# References

- Dataset: <https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection>
- IBM Watson Studio Documentation: <https://dataplatform.cloud.ibm.com/docs>
- “A Detailed Analysis of the KDD Cup 99 Dataset” – Research Paper
- IBM AutoAI Overview: <https://www.ibm.com/cloud/watson-studio/autoai>



# IBM Certifications

In recognition of the commitment to achieve  
professional excellence



## Mohd Faizan

Has successfully satisfied the requirements for:

### Getting Started with Artificial Intelligence



Issued on: Jul 23, 2025  
Issued by: IBM SkillsBuild

Verify: <https://www.credly.com/badges/4d8f9ce3-98d1-4a05-a684-65bc45d49519>



# IBM Certifications

In recognition of the commitment to achieve  
professional excellence



## Mohd Faizan

Has successfully satisfied the requirements for:

---

### Journey to Cloud: Envisioning Your Solution

---

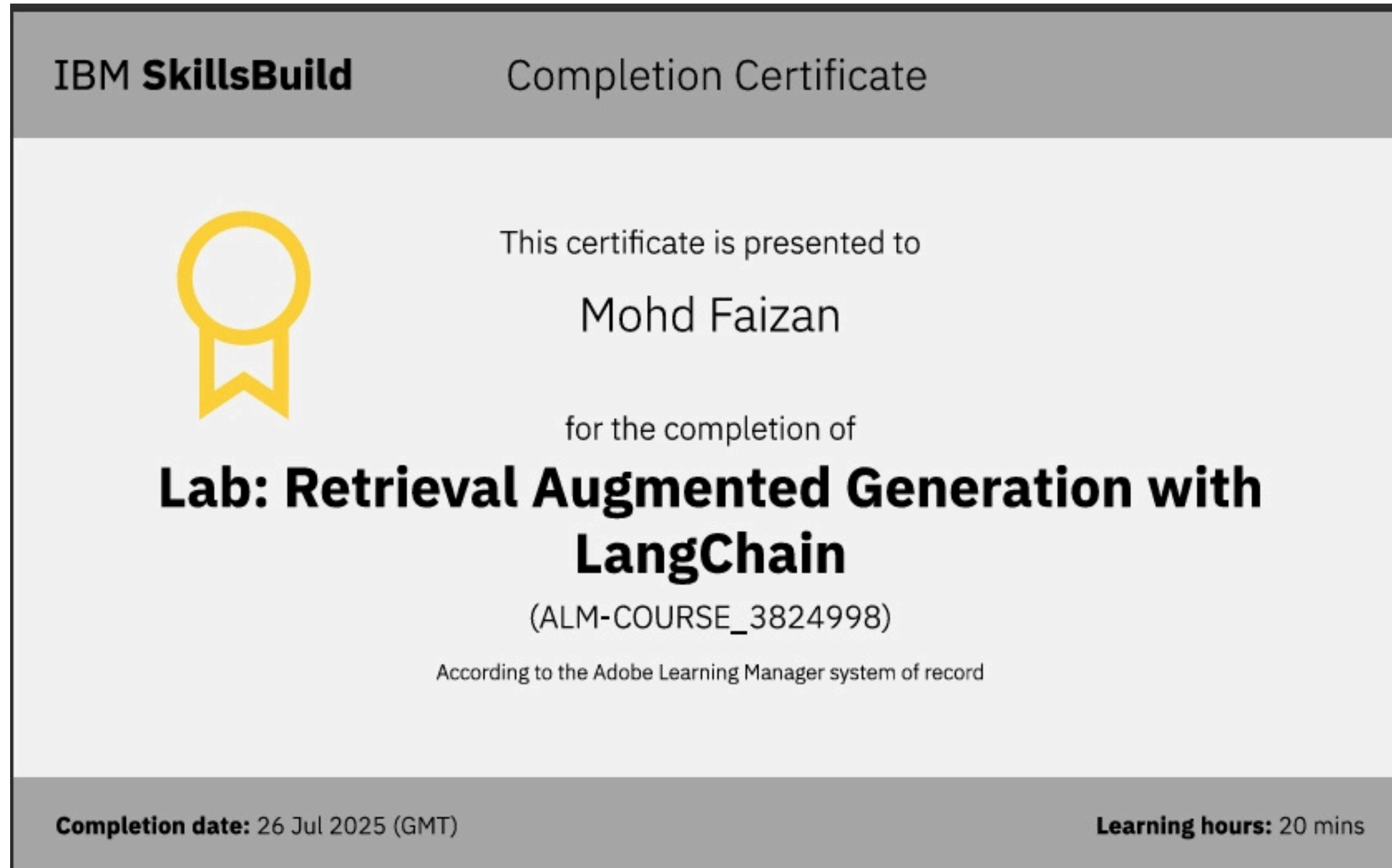


Issued on: Jul 23, 2025  
Issued by: IBM SkillsBuild

Verify: <https://www.credly.com/badges/a8774713-06c1-47bb-be12-436b2ac57a9e>



# IBM Certifications





**THANK YOU**