CAPSTONE PROJECT

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

Presented By:
1. **Amit Kumar Bhardwaj-Ignou-**Bachelor of Computer Applications.

edunet
foundation

OUTLINE

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

PROBLEM STATEMENT

Network traffic is constantly under threat from various cyberattacks. Manual intrusion detection is not scalable or effective for large-scale networks. The problem is to identify malicious activity (e.g., DoS, Probe, R2L, U2R) from legitimate network traffic in real time.

PROPOSED SOLUTION

- To address the challenge of detecting and classifying cyberattacks in real-time, the proposed solution is to build an intelligent, cloud-based **Network Intrusion Detection System (NIDS)** using **machine learning** techniques, deployed on **IBM Watsonx.ai** using AutoAI.
- The solution consists of the following components:

Data Collection:

- Source: Kaggle Network Intrusion Detection Dataset (NSL-KDD-based)
- Contains labeled examples of network traffic: normal and various attack types.
- **Data Preprocessing:**
- Encode categorical features (e.g., protocol_type, flag) using label or one-hot encoding. Normalize numerical features for better model performance.
- Remove irrelevant or redundant columns. Handle class imbalance using techniques like **SMOTE** or **undersampling.**
- **Machine Learning Algorithm:**
- **Input:** Preprocessed dataset with labeled examples.
- AutoAI automatically performs: Train/test data splitting, Feature selection and transformation, Algorithm evaluation (e.g., Random Forest, XGBoost, Logistic Regression), Hyperparameter tuning
- Output: Best-performing ML pipeline based on metrics like accuracy.
- **Model Deployment:**
- Deploy the optimized model as a **web service** using **Watson Machine Learning**.

SYSTEM APPROACH

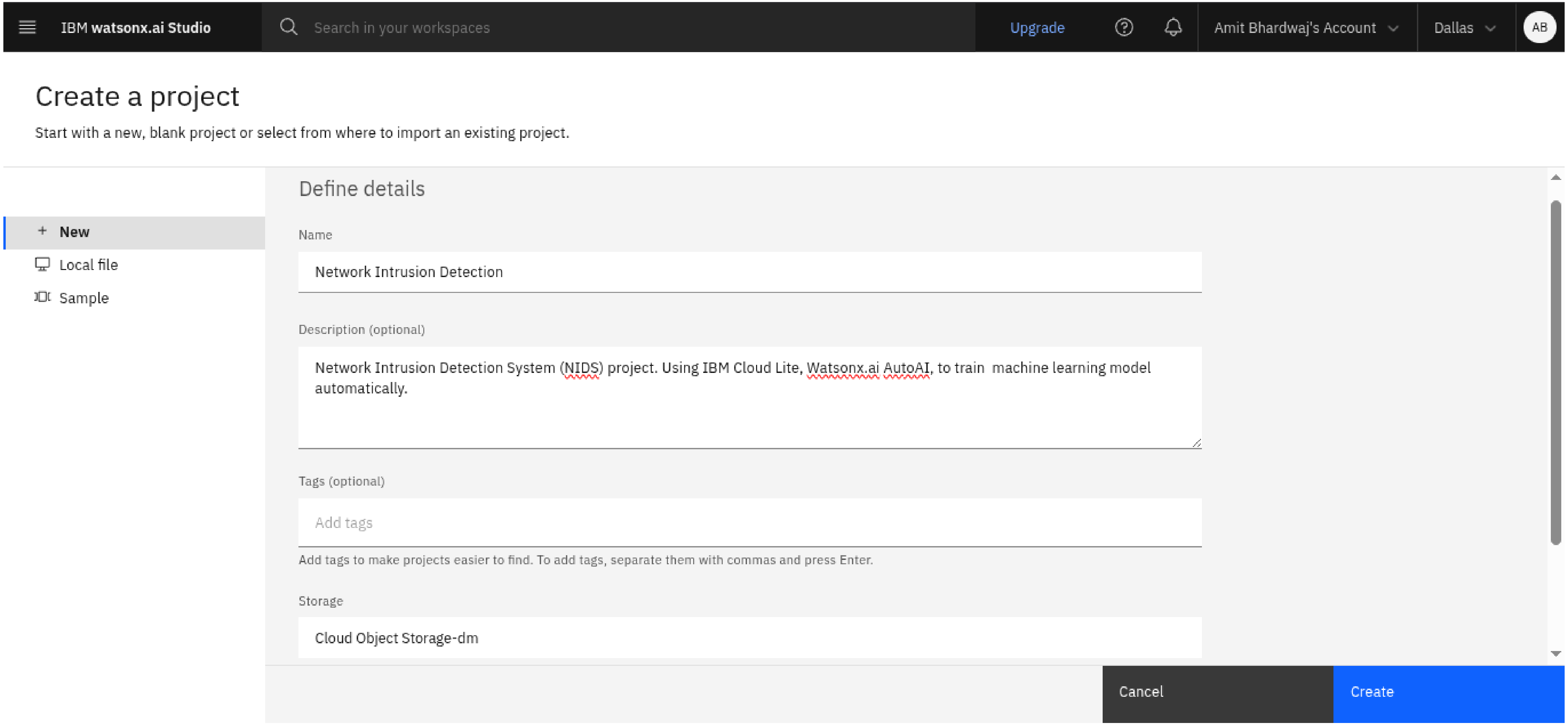
The "System Approach" section outlines the overall strategy and methodology for developing and implementing the Network Intrusion Detection System (NIDS) . Here's a suggested structure for this section:

- System requirements:
- Dataset: Kaggle NIDS dataset.
- https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection?resource=download
- Platform: IBM Watsonx.ai, Cloud Object Storage.
- Tooling: AutoAI, Watson Studio.

ALGORITHM & DEPLOYMENT

- In the Algorithm section, describe the machine learning algorithm chosen for predicting Network attacks. Here's an example structure for this section:
- Algorithm Selection and Training:
- IBM Watsonx.ai AutoAI automates the full ML pipeline: from preprocessing to model optimization.
- AutoAI automatically: Splits data into training and testing sets, Performs feature encoding and scaling, Tunes hyperparameters for each algorithm. The best model pipeline is selected based on the highest performance score.
- Model Input Features:
- Models trained on 41 network traffic features, including:
  - **Protocol attributes, Connection metrics, Host-level statistics, Flags and binary indicators.**
  - AutoAI normalizes numerical values and encodes categorical fields automatically.
- Prediction Process:
- Real-time or batch network traffic records are formatted into JSON.
- Each record must contain 41 feature values, matching the training dataset structure.
- Example input fields include: `duration`, `protocol_type`, `service`, `src_bytes`, `dst_bytes`, etc.

RESULT



Create a project

Start with a new, blank project or select from where to import an existing project.

Define details

Name

Network Intrusion Detection

Description (optional)

Network Intrusion Detection System (NIDS) project. Using IBM Cloud Lite, Watsonx.ai AutoAI, to train machine learning model automatically.

Tags (optional)

Add tags

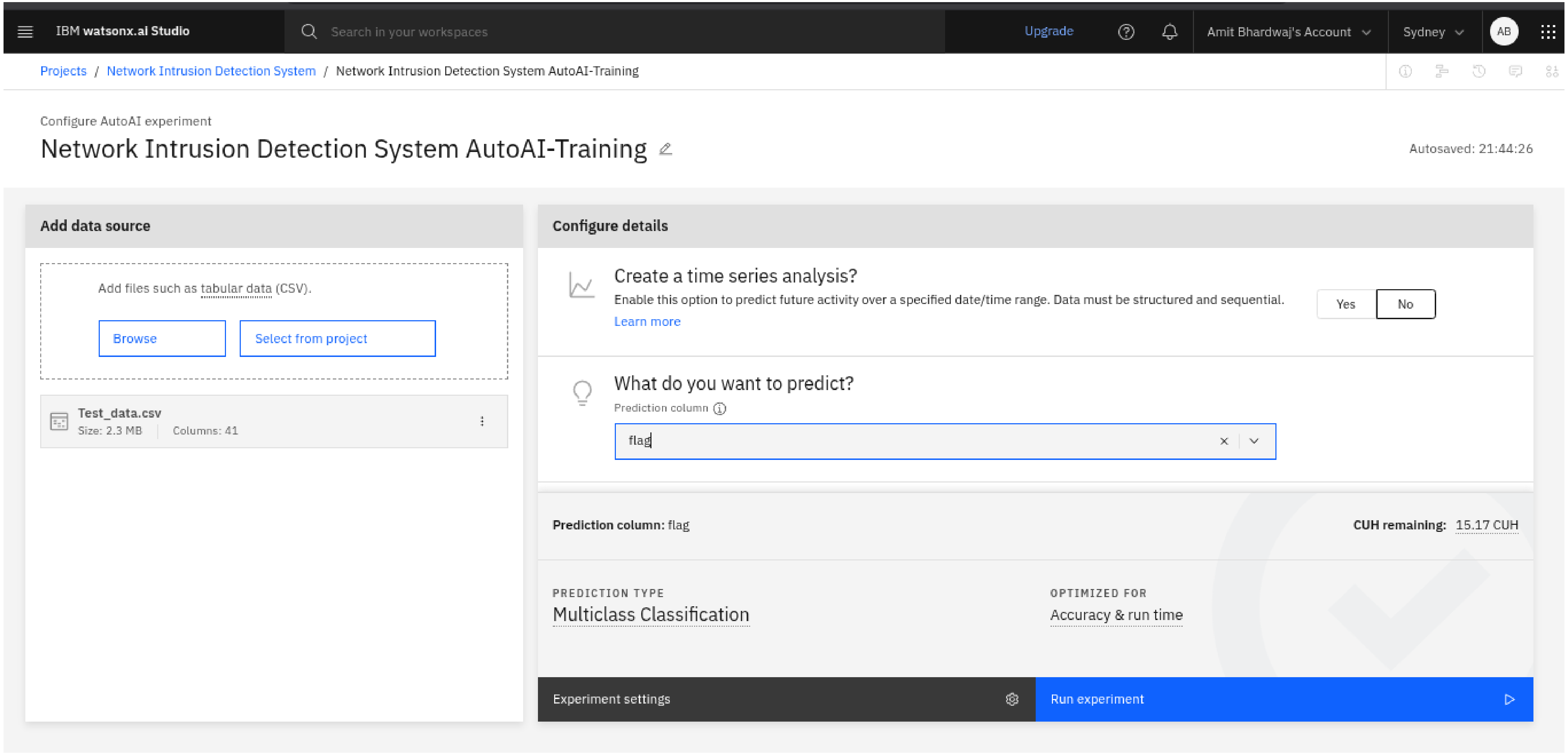
Add tags to make projects easier to find. To add tags, separate them with commas and press Enter.

Storage

Cloud Object Storage-dm

edunet foundation

RESULT



Projects / Network Intrusion Detection System / Network Intrusion Detection System AutoAI-Training

Configure AutoAI experiment

Network Intrusion Detection System AutoAI-Training

Autosaved: 21:44:26

Add data source

Add files such as tabular data (CSV).

Test_data.csv
Size: 2.3 MB | Columns: 41

Configure details

Create a time series analysis?
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
flag

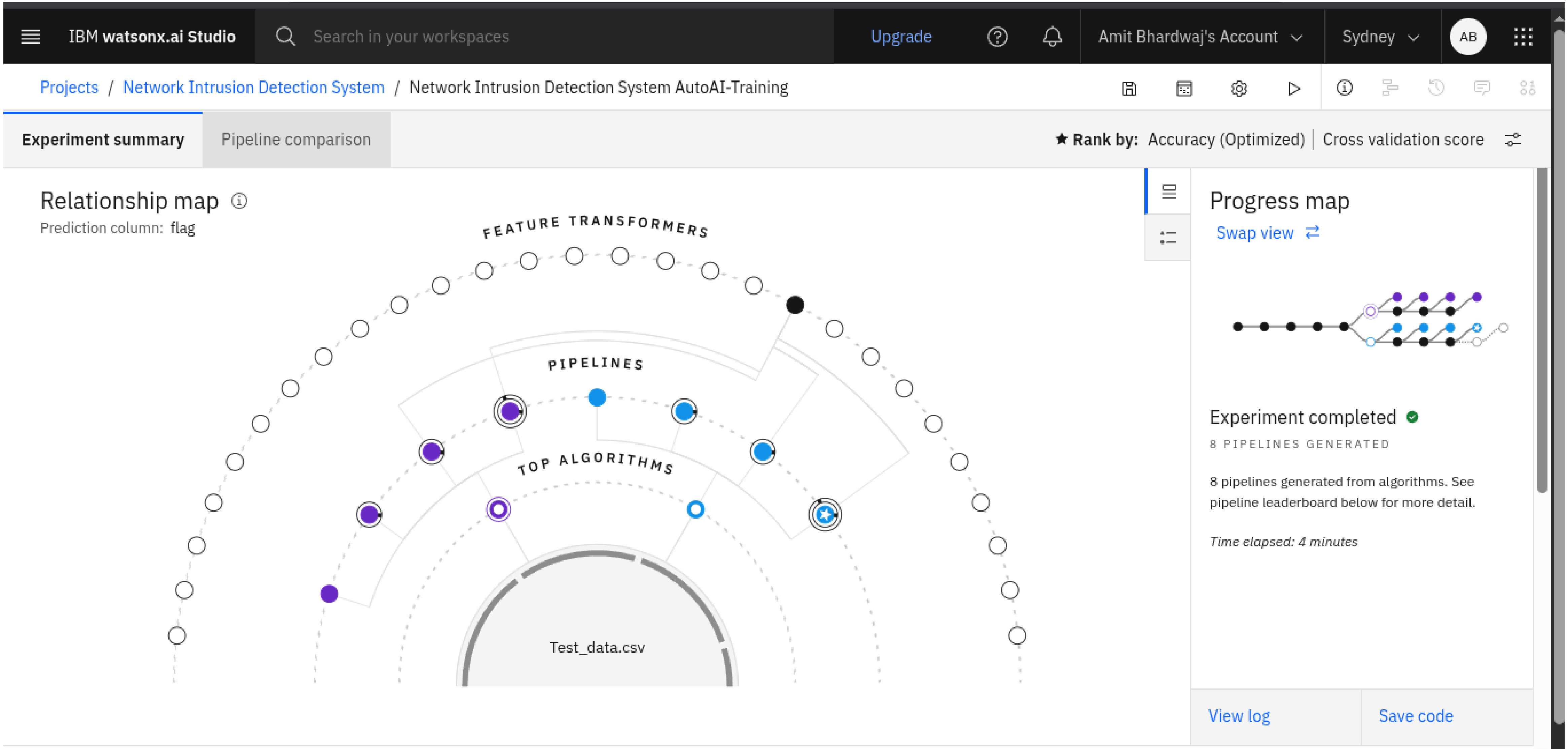
Prediction column: flag

CUH remaining: 15.17 CUH

PREDICTION TYPE
Multiclass Classification

OPTIMIZED FOR
Accuracy & run time

RESULT



Projects / Network Intrusion Detection System / Network Intrusion Detection System AutoAI-Training

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

Relationship map

Prediction column: flag

Progress map

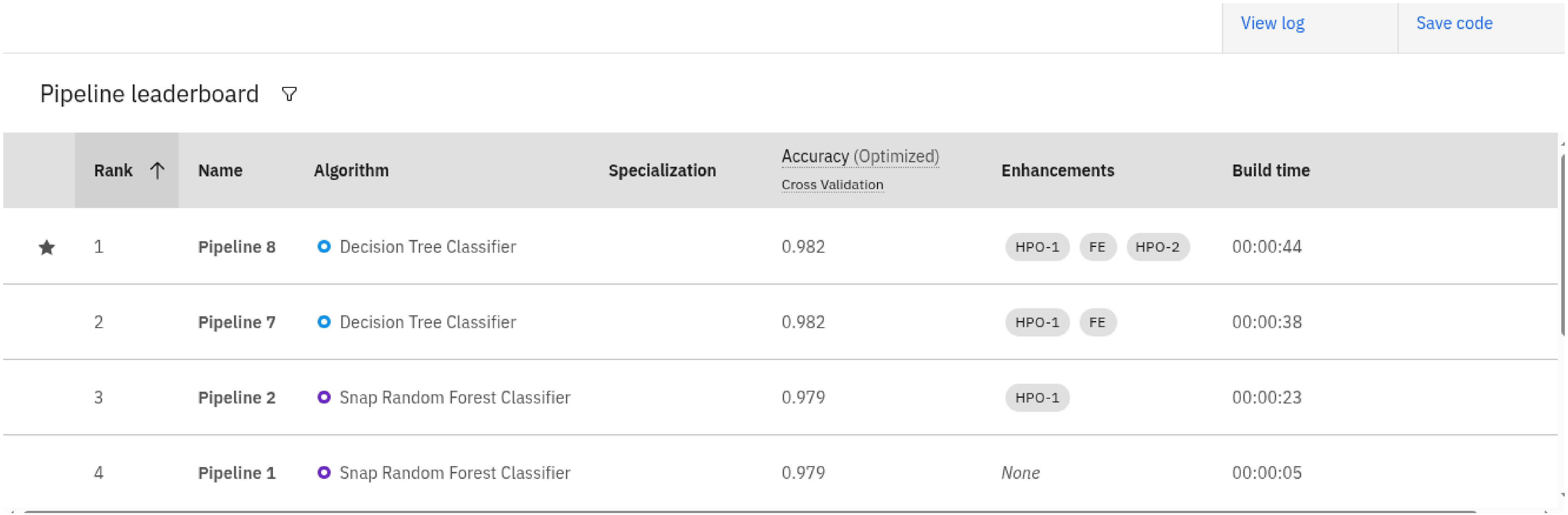
Experiment completed

8 PIPELINES GENERATED

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

Time elapsed: 4 minutes

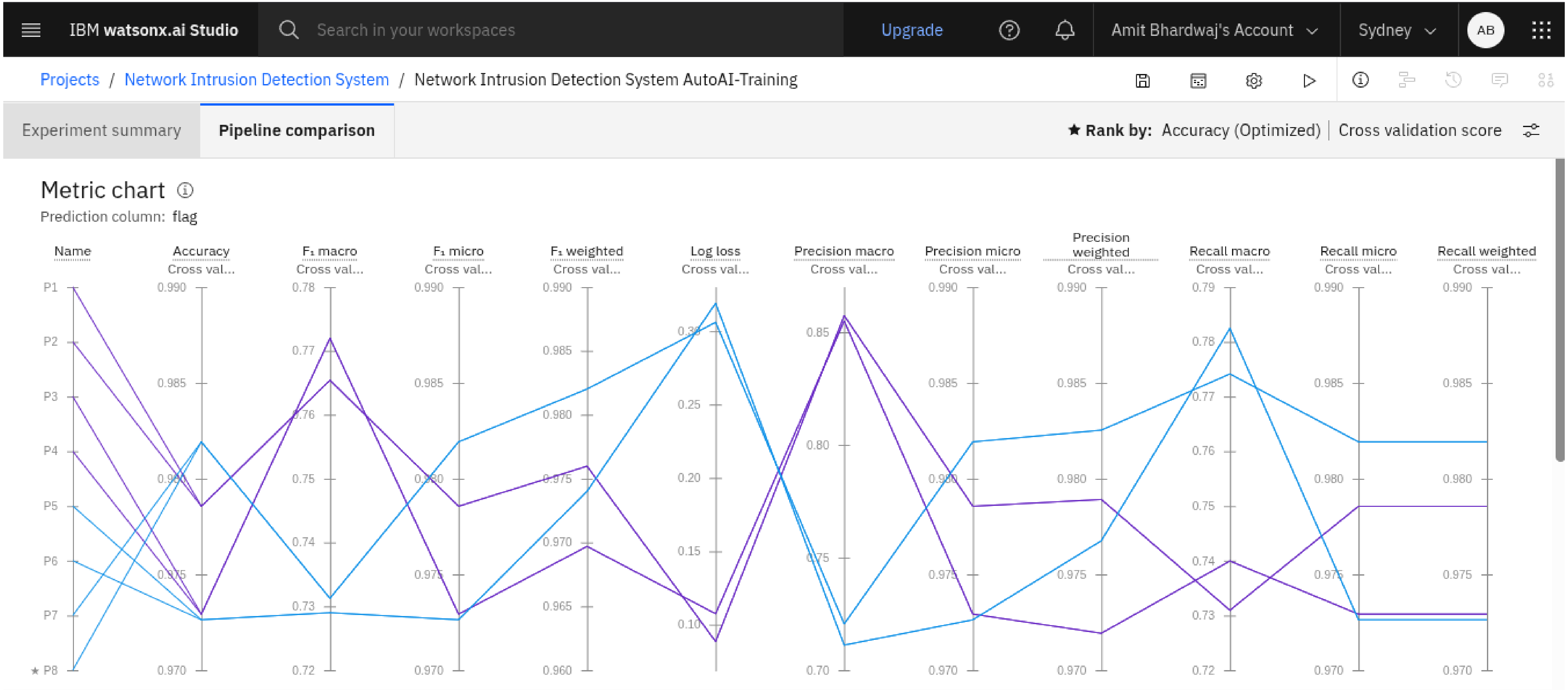
RESULT



Pipeline leaderboard

	Rank ↑	Name	Algorithm	Specialization	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	**Pipeline 8**	○ Decision Tree Classifier		0.982	HPO-1 FE HPO-2	00:00:44
	2	**Pipeline 7**	○ Decision Tree Classifier		0.982	HPO-1 FE	00:00:38
	3	**Pipeline 2**	○ Snap Random Forest Classifier		0.979	HPO-1	00:00:23
	4	**Pipeline 1**	○ Snap Random Forest Classifier		0.979	*None*	00:00:05

RESULT



IBM **watsonx.ai Studio**

Search in your workspaces

Upgrade

Amit Bhardwaj's Account

Sydney

AB

Projects / Network Intrusion Detection System / Network Intrusion Detection System AutoAI-Training

Experiment summary

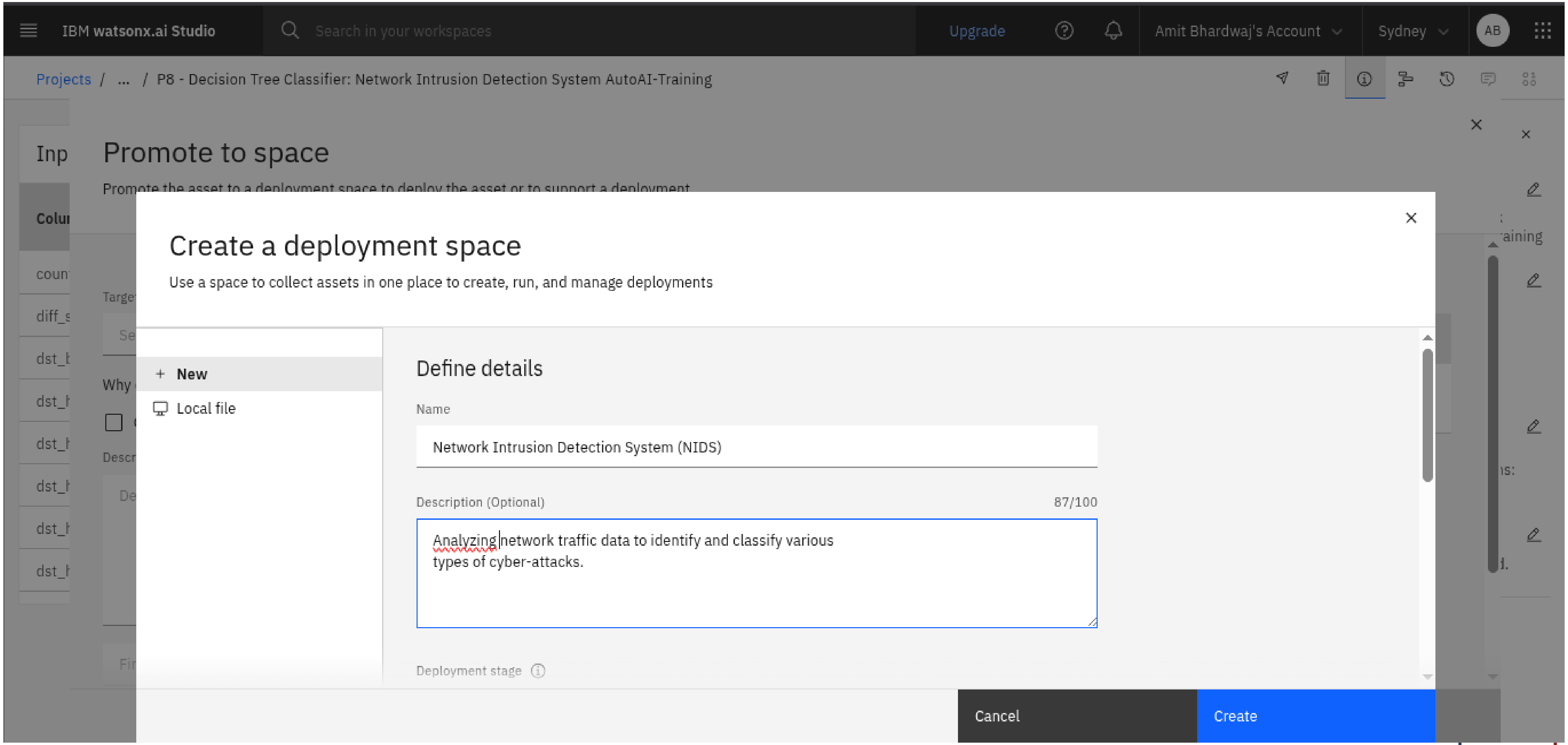
Pipeline comparison

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

Metric chart

Prediction column: flag

RESULT



IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Amit Bhardwaj's Account
Sydney
AB
Projects / ... / P8 - Decision Tree Classifier: Network Intrusion Detection System AutoAI-Training
Promote to space
Promote the asset to a deployment space to deploy the asset or to support a deployment

Create a deployment space

Use a space to collect assets in one place to create, run, and manage deployments

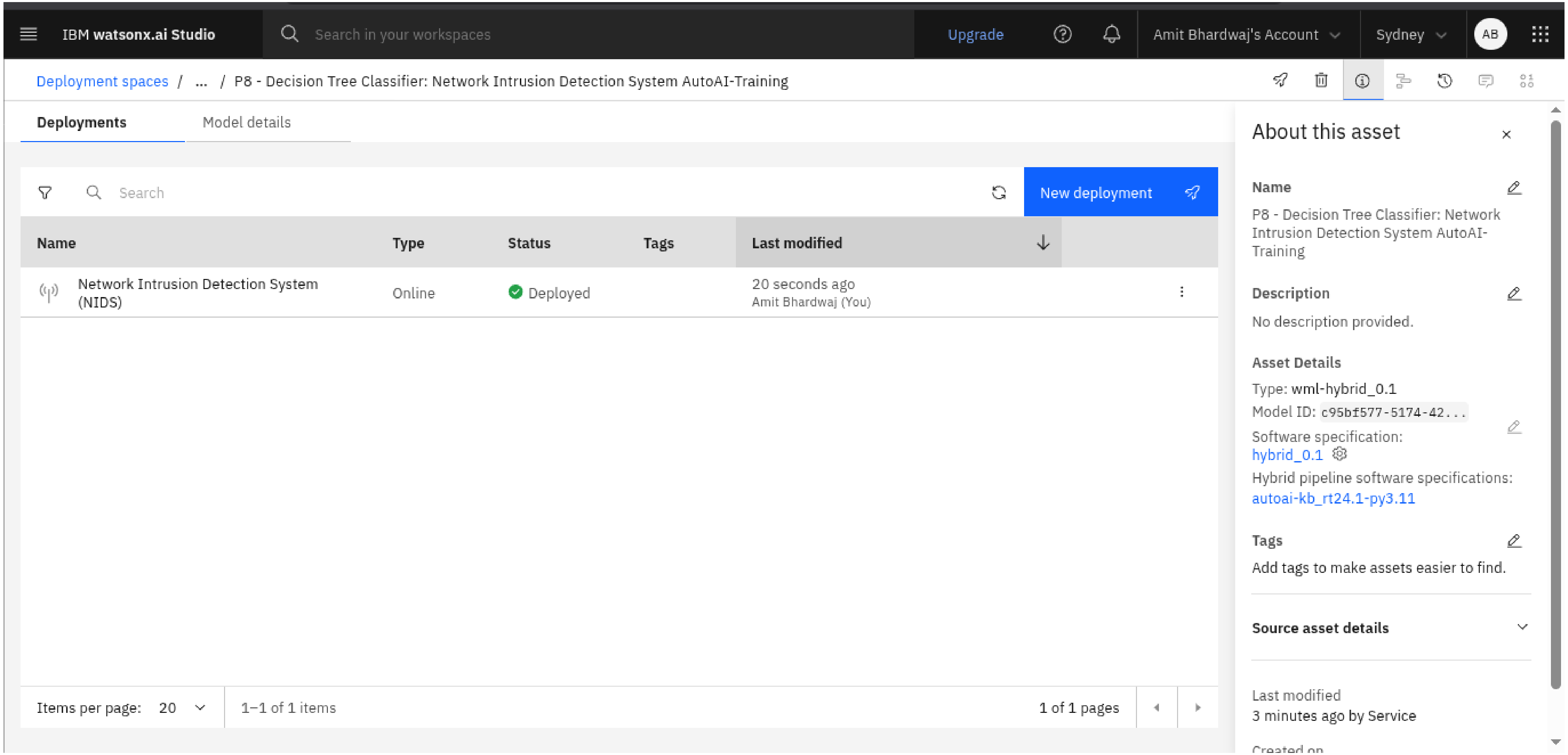
Define details

Name: Network Intrusion Detection System (NIDS)

Description (Optional) 87/100: Analyzing network traffic data to identify and classify various types of cyber-attacks.

Deployment stage
Cancel
Create

RESULT



Name	Type	Status	Tags	Last modified
Network Intrusion Detection System (NIDS)	Online	✓ Deployed		20 seconds ago Amit Bhardwaj (You)

About this asset

Name

P8 - Decision Tree Classifier: Network Intrusion Detection System AutoAI-Training

Description

No description provided.

Asset Details

Type: wml-hybrid_0.1

Model ID: `c95bf577-5174-42...`

Software specification: hybrid_0.1

Hybrid pipeline software specifications: autoai-kb_rt24.1-py3.11

Tags

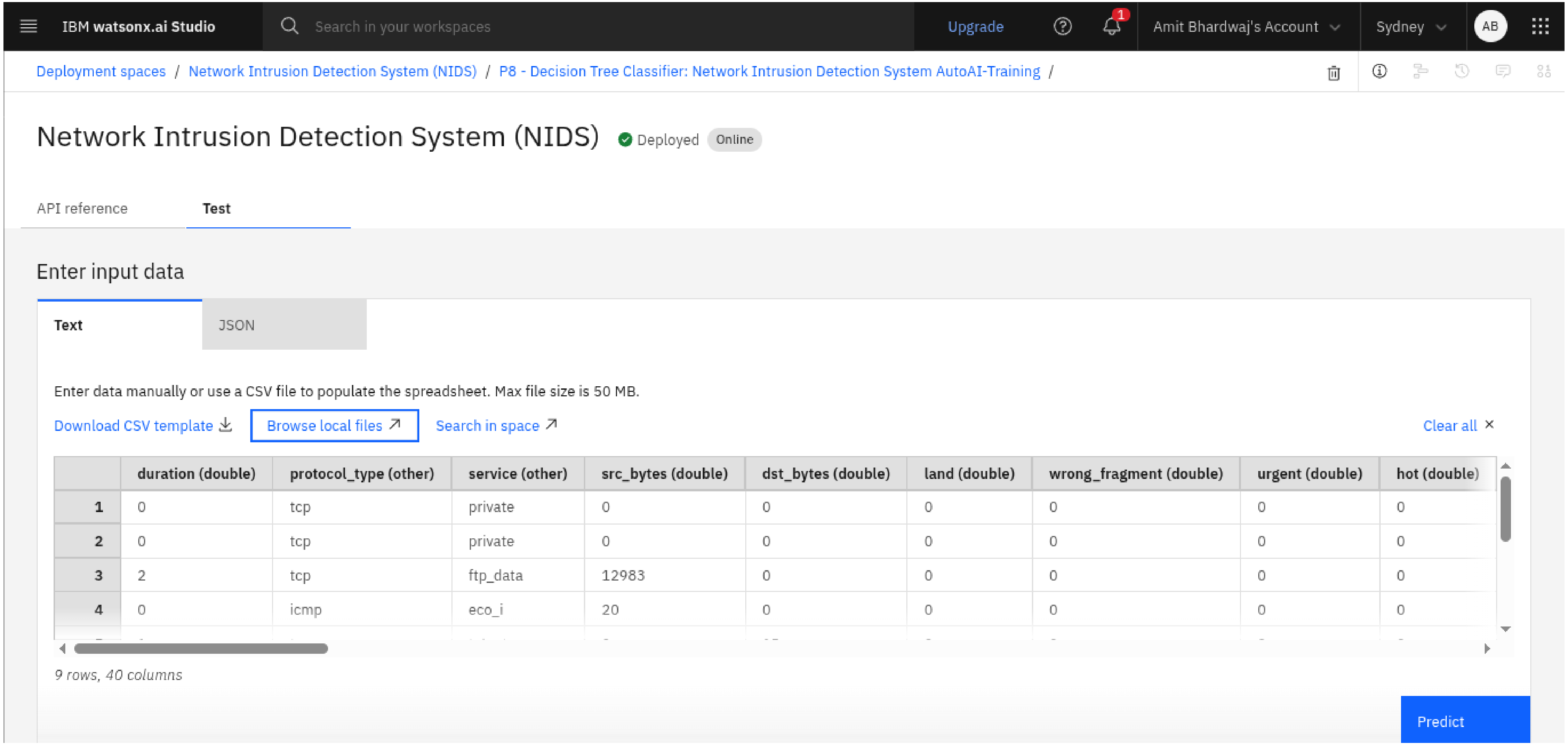
Add tags to make assets easier to find.

Source asset details

Last modified
3 minutes ago by Service

Created on

RESULT



Deployment spaces / Network Intrusion Detection System (NIDS) / P8 - Decision Tree Classifier: Network Intrusion Detection System AutoAI-Training /

Network Intrusion Detection System (NIDS) Deployed Online

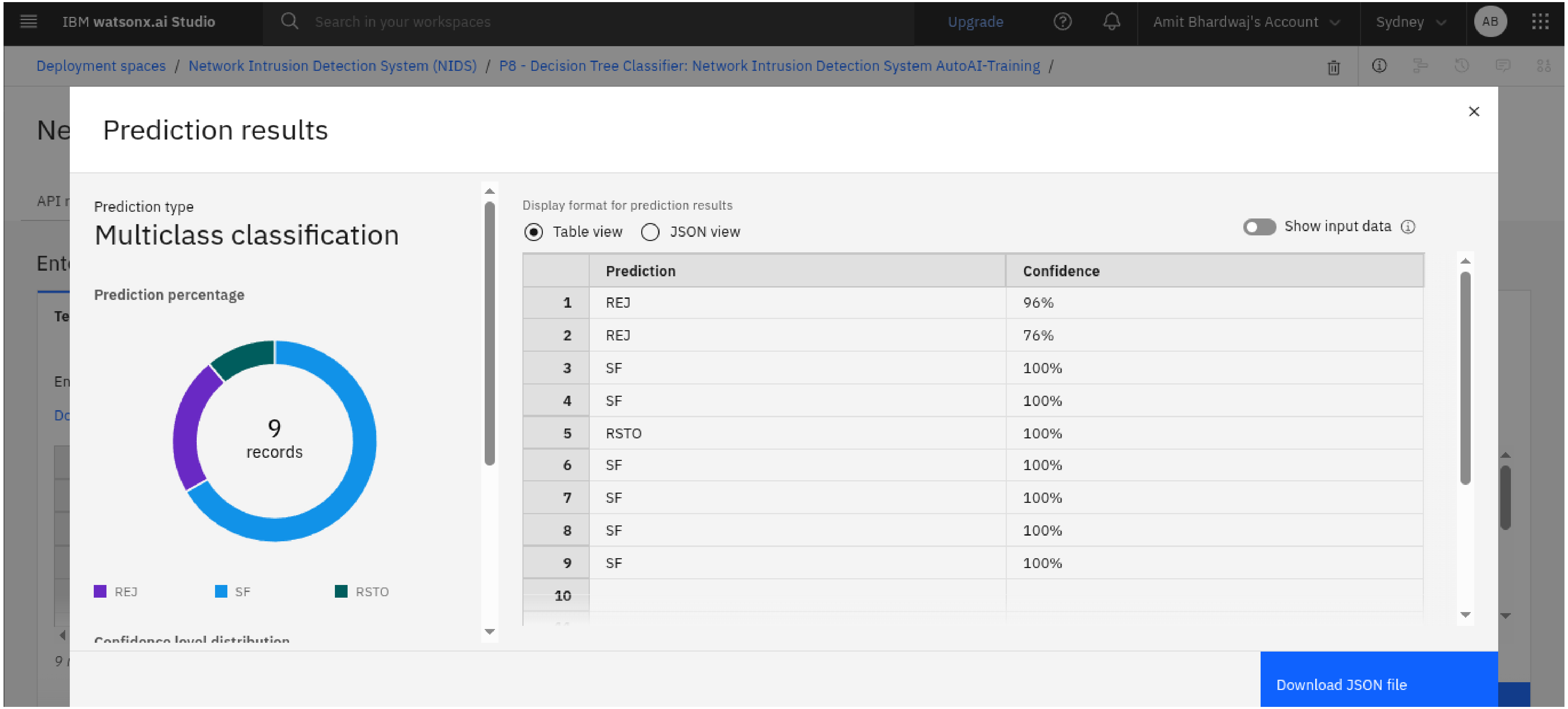
Enter input data

Enter data manually or use a CSV file to populate the spreadsheet. Max file size is 50 MB.

	duration (double)	protocol_type (other)	service (other)	src_bytes (double)	dst_bytes (double)	land (double)	wrong_fragment (double)	urgent (double)	hot (double)
1	0	tcp	private	0	0	0	0	0	0
2	0	tcp	private	0	0	0	0	0	0
3	2	tcp	ftp_data	12983	0	0	0	0	0
4	0	icmp	eco_i	20	0	0	0	0	0

9 rows, 40 columns

RESULT



IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Amit Bhardwaj's Account
Sydney
AB
Deployment spaces / Network Intrusion Detection System (NIDS) / P8 - Decision Tree Classifier: Network Intrusion Detection System AutoAI-Training /

Prediction results

Prediction type

Multiclass classification

Prediction percentage

Confidence level distribution

Display format for prediction results

● Table view ○ JSON view

Show input data

	Prediction	Confidence
1	REJ	96%
2	REJ	76%
3	SF	100%
4	SF	100%
5	RSTO	100%
6	SF	100%
7	SF	100%
8	SF	100%
9	SF	100%
10		

CONCLUSION

- Successfully developed a **cloud-based Network Intrusion Detection System (NIDS)** using machine learning.
- Leveraged **IBM Watsonx.ai AutoAI** to automate model training, evaluation, and selection.
- Achieved high accuracy in classifying network traffic into **normal** and multiple **attack categories** (DoS, Probe, R2L, U2R).
- The project demonstrates the **effectiveness of AutoAI** in building secure, scalable, and automated NIDS solutions suitable for modern cyber defense.

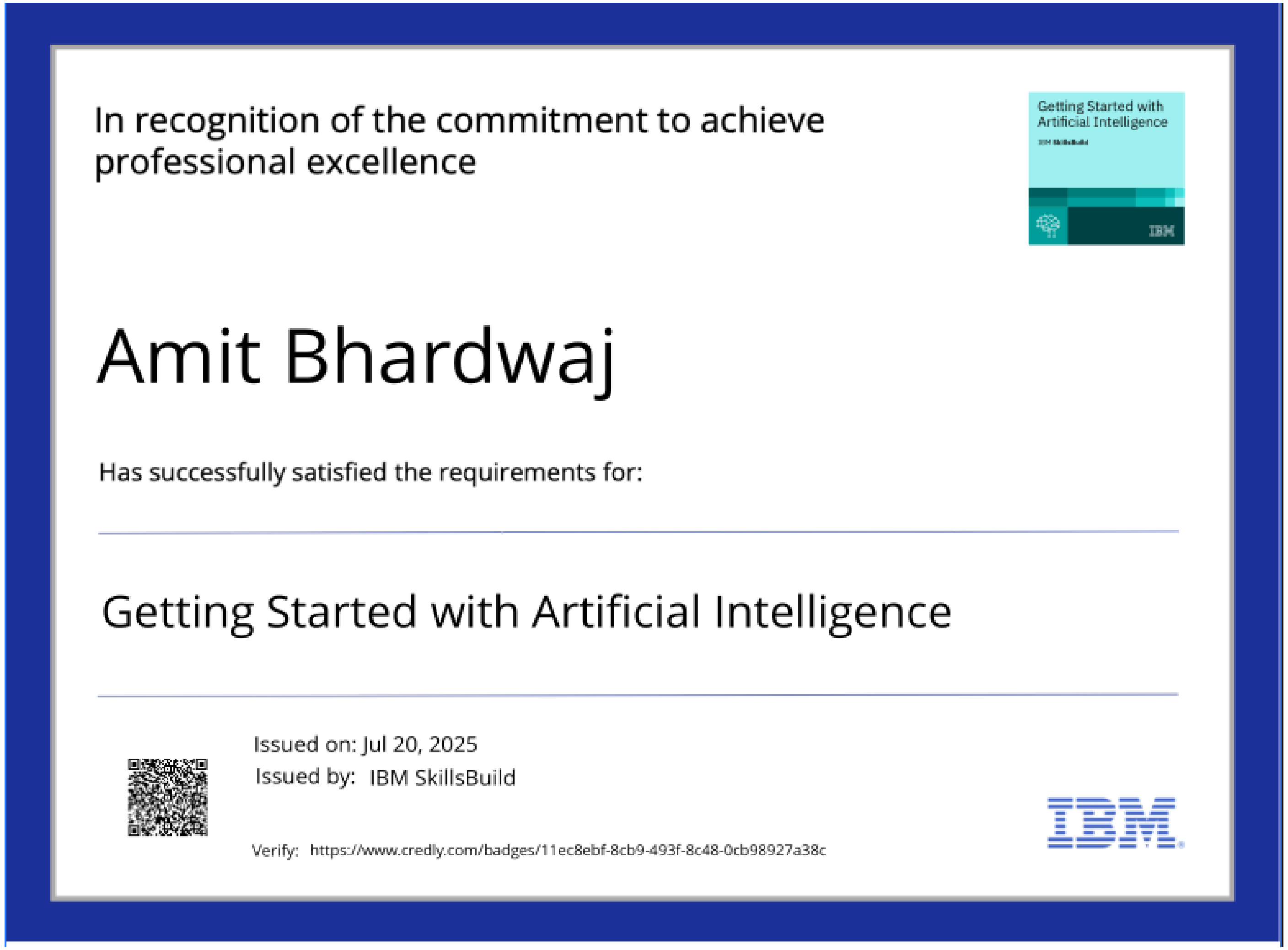
FUTURE SCOPE

- **Integration with Real-Time Network Traffic:**
  Extend the current system to monitor live traffic using tools like Wireshark, Zeek, or custom packet sniffers.
- **Enhanced Data Sources:**
  Incorporate real-world enterprise network traffic or cloud security logs to improve model generalization and robustness.
- **Threat Intelligence Integration:**
  Combine the model with external threat intelligence feeds to improve detection of zero-day or evolving threats.
- **Model Retraining Pipeline:**
  Develop an automated retraining system that updates the model periodically using recent labeled data to stay current with new attack vectors.
- **Scalable Production Deployment:**
  Host the model on IBM Kubernetes Service or Code Engine for handling high-throughput, real-time monitoring in large networks.
- **Visualization and Alerting System:**
  Build a dashboard interface to visualize network anomalies, prediction trends, and generate security alerts for SOC teams.
- **Multi-Cloud or Edge Integration:**
  Extend the system for multi-cloud environments or deploy lightweight models on edge devices for low-latency intrusion detection in IoT networks.

REFERENCES

- IBM Watsonx.ai Documentation – AutoAI
  https://dataplatform.cloud.ibm.com/docs/content/wsj/autoai/
- Kaggle – Network Intrusion Detection Dataset (NSL-KDD)
  https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

IBM CERTIFICATIONS



Getting Started with Artificial Intelligence
IBM SkillsBuild
IBM

In recognition of the commitment to achieve professional excellence

Amit Bhardwaj

Has successfully satisfied the requirements for:

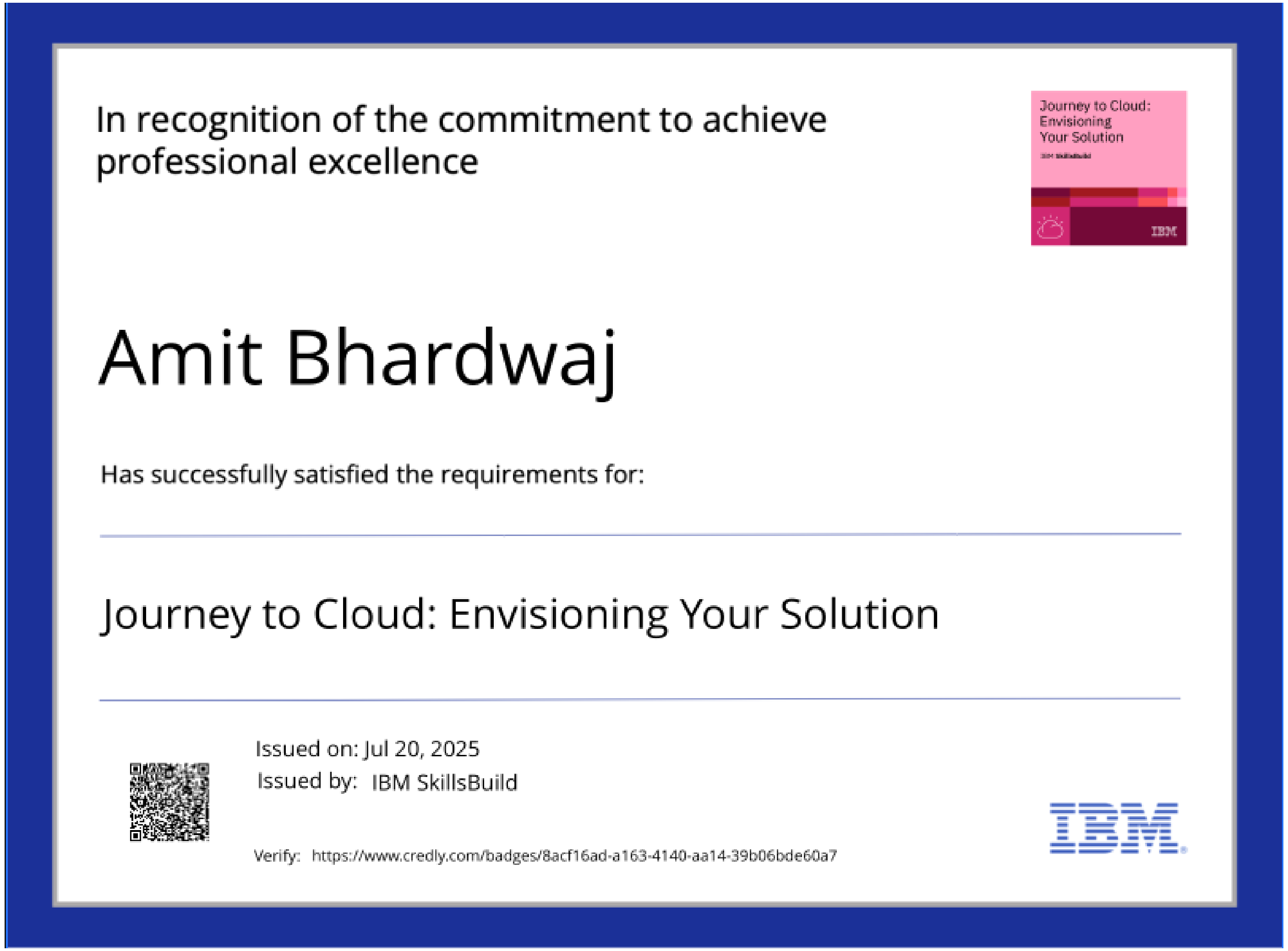
Getting Started with Artificial Intelligence

Issued on: Jul 20, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/11ec8ebf-8cb9-493f-8c48-0cb98927a38c

IBM

IBM CERTIFICATIONS



Journey to Cloud: Envisioning Your Solution

IBM SkillsBuild

IBM

In recognition of the commitment to achieve professional excellence

Amit Bhardwaj

Has successfully satisfied the requirements for:

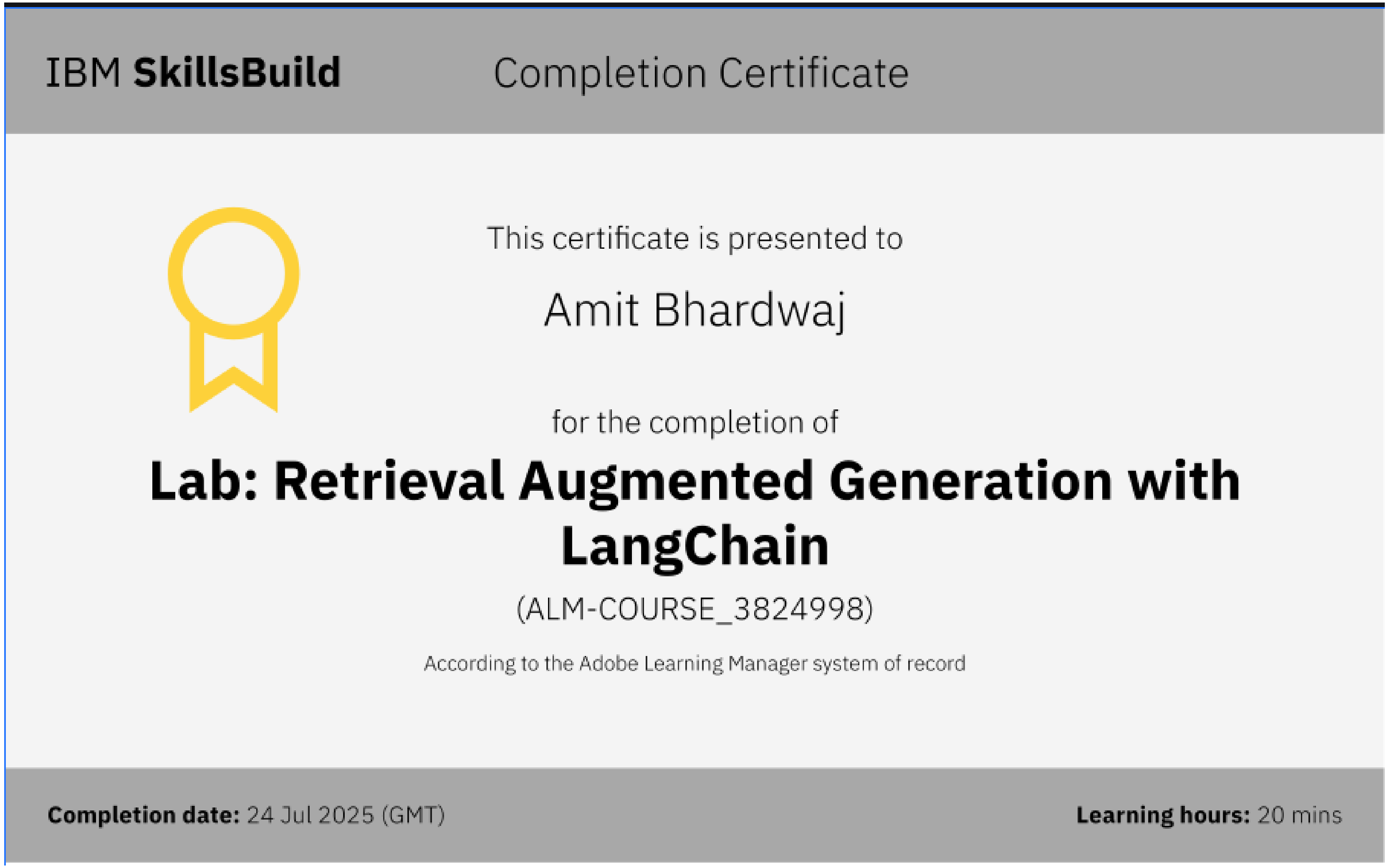
Journey to Cloud: Envisioning Your Solution

Issued on: Jul 20, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/8acf16ad-a163-4140-aa14-39b06bde60a7

IBM

IBM CERTIFICATIONS



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Amit Bhardwaj

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