CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:

Student Name :- Ritika Singh
College Name :- SANDIP UNIVERSITY
Department :- BTech(CSE)
AICTE Student ID: STU6857ab2c1b8881750575916
Internship ID: INTERNSHIP_1748937226683eaa0a58abc
Technology: IBM Watsonx.ai Studio

OUTLINE

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

PROBLEM STATEMENT

Network Intrusion Detection The Challenge:

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.

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

PROPOSED SOLUTION

The proposed solution is an intelligent system built on the IBM Cloud platform that leverages machine learning to automate threat detection.

- **Data Source:** Utilizes the well-known NSL-KDD dataset from Kaggle, which contains a wide variety of network intrusions.
- **Automated Model Building:** Employs the **AutoAI** feature within **IBM Watsonx.ai** to automatically preprocess the data, select the best classification algorithm, and optimize its performance.
- **Prediction Goal:** The model will be trained to predict the **'class'** of network activity (e.g., 'normal', 'dos', 'probe', etc.).
- **Deployment:** The final, most accurate model will be deployed as a live web service (API), capable of making real-time predictions on new network data.

SYSTEM APPROACH

This project was developed using a suite of powerful cloud-based AI tools:

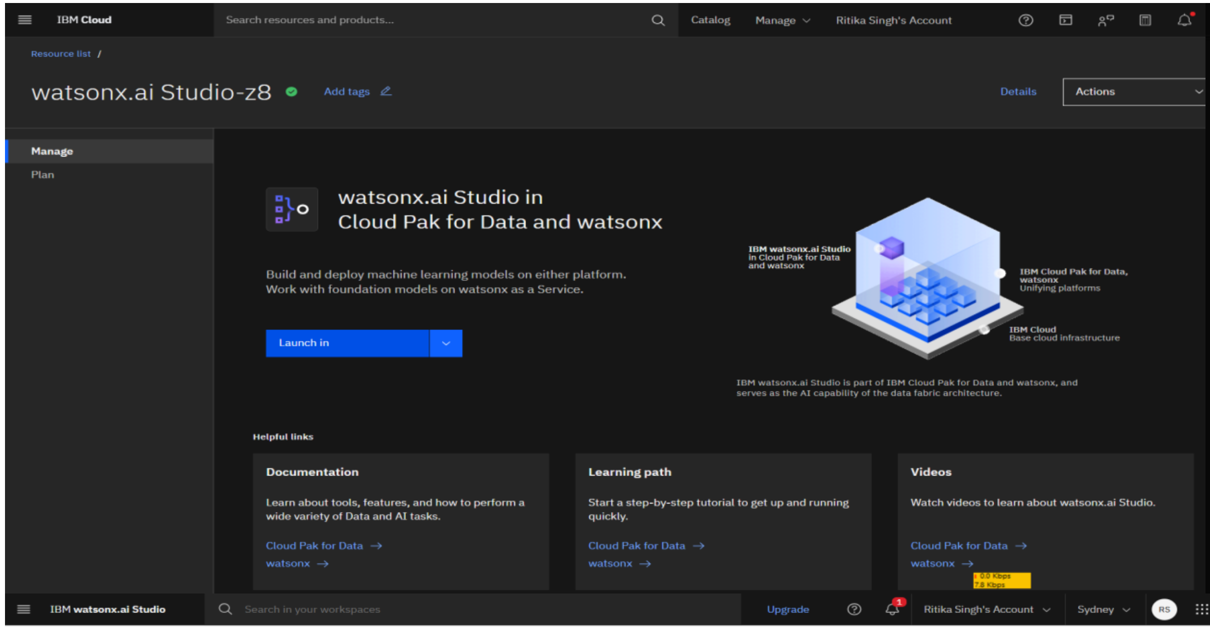
- **Cloud Platform:** IBM Cloud
- **AI/ML Studio:** IBM Watsonx.ai
- **Core Engine:** AutoAI Experiment
- **Model Deployment:** Watson Machine Learning Service
- **Dataset:** NSL-KDD Network Intrusion Dataset (from Kaggle)
  - Kaggle dataset link – https://www.kaggle.com/datasets/sampadab17/network intrusion-detection

ALGORITHM & DEPLOYMENT

The project was executed following a precise, step-by-step workflow within the IBM Cloud environment:

1. Logged into the **IBM Cloud** platform.
2. Cleared the resource list to ensure a clean workspace.
3. Created a **New Project** in Watsonx.ai, configuring the necessary runtime and storage services.
4. Navigated to the "Build machine learning model automatically" section.
5. Configured the **AutoAI Experiment** with a name and description.
6. Uploaded the **Train_data.csv** as the data source.
7. **Ran the experiment**, which automatically trained and evaluated multiple models.
8. Selected and **saved the pipeline** with the highest accuracy from the results.
9. **Promoted the model** to a deployment space and deployed it as a live service.
10. **Tested** the deployed model to ensure it was making predictions correctly.

SCREENSHOTS OF WORKFLOW



IBM Cloud
Search resources and products...
Catalog
Manage
Ritika Singh's Account
Resource list /

watsonx.ai Studio-z8

Add tags
Details
Actions
Manage
Plan

watsonx.ai Studio in Cloud Pak for Data and watsonx

Build and deploy machine learning models on either platform. Work with foundation models on watsonx as a Service.

Launch in
IBM watsonx.ai Studio in Cloud Pak for Data and watsonx
IBM Cloud Pak for Data, watsonx Unifying platforms
IBM Cloud Base cloud infrastructure

IBM watsonx.ai Studio is part of IBM Cloud Pak for Data and watsonx, and serves as the AI capability of the data fabric architecture.

Helpful links

Documentation

Learn about tools, features, and how to perform a wide variety of Data and AI tasks.

Cloud Pak for Data →
watsonx →

Learning path

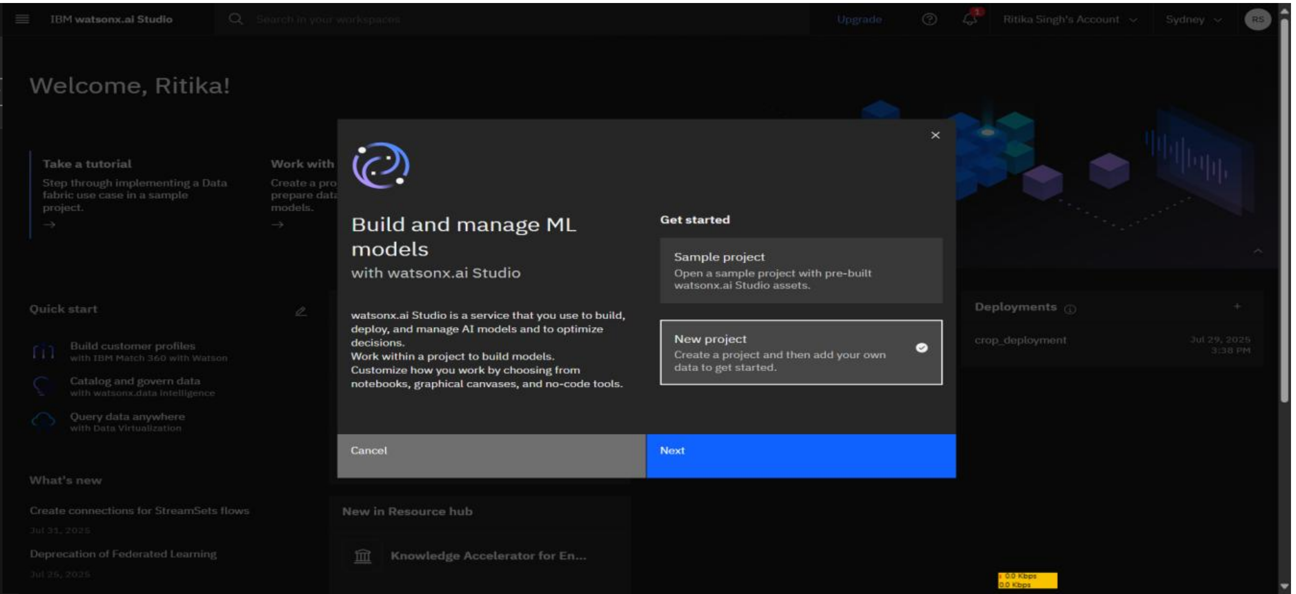
Start a step-by-step tutorial to get up and running quickly.

Cloud Pak for Data →
watsonx →

Videos

Watch videos to learn about watsonx.ai Studio.

Cloud Pak for Data →
watsonx →



IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Ritika Singh's Account
Sydney
RS

Welcome, Ritika!

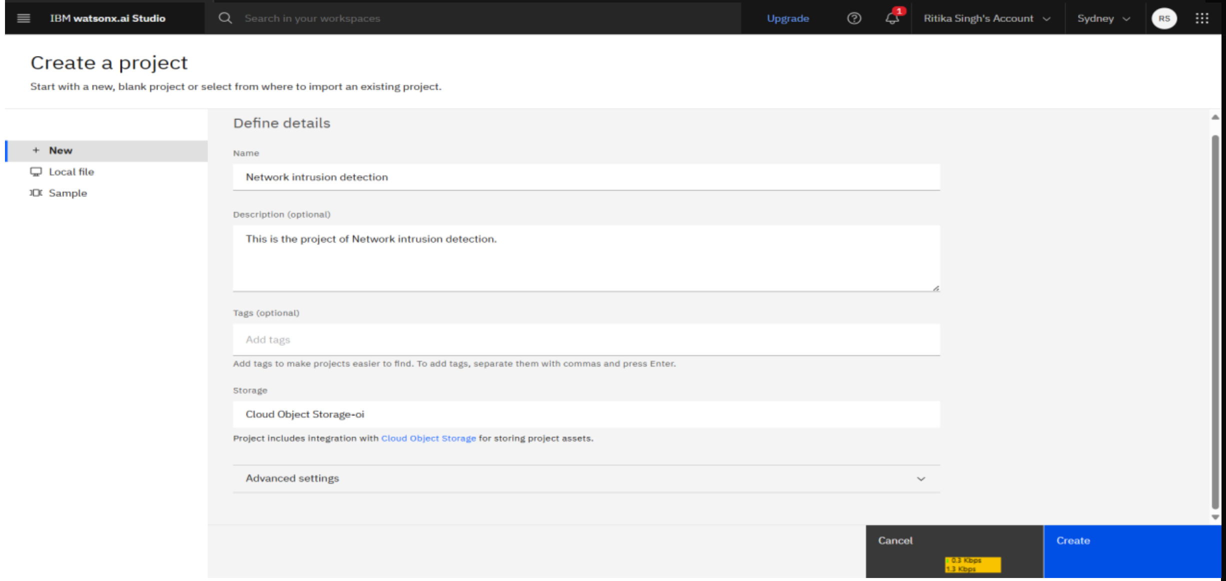
Take a tutorial
Step through implementing a Data fabric use case in a sample project.
Work with
Quick start
Build customer profiles with IBM Match 360 with Watson
Catalog and govern data with watsonx.data intelligence
Query data anywhere with Data Virtualization
What's new
Create connections for StreamSets flows
Deprecation of Federated Learning
New in Resource hub
Knowledge Accelerator for En...
Deployments
crop_deployment

Build and manage ML models with watsonx.ai Studio

watsonx.ai Studio is a service that you use to build, deploy, and manage AI models and to optimize decisions.
Work within a project to build models.
Customize how you work by choosing from notebooks, graphical canvases, and no-code tools.

Get started

- Sample project
  Open a sample project with pre-built watsonx.ai Studio assets.
- New project ●
  Create a project and then add your own data to get started.



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): This is the project of Network intrusion detection.

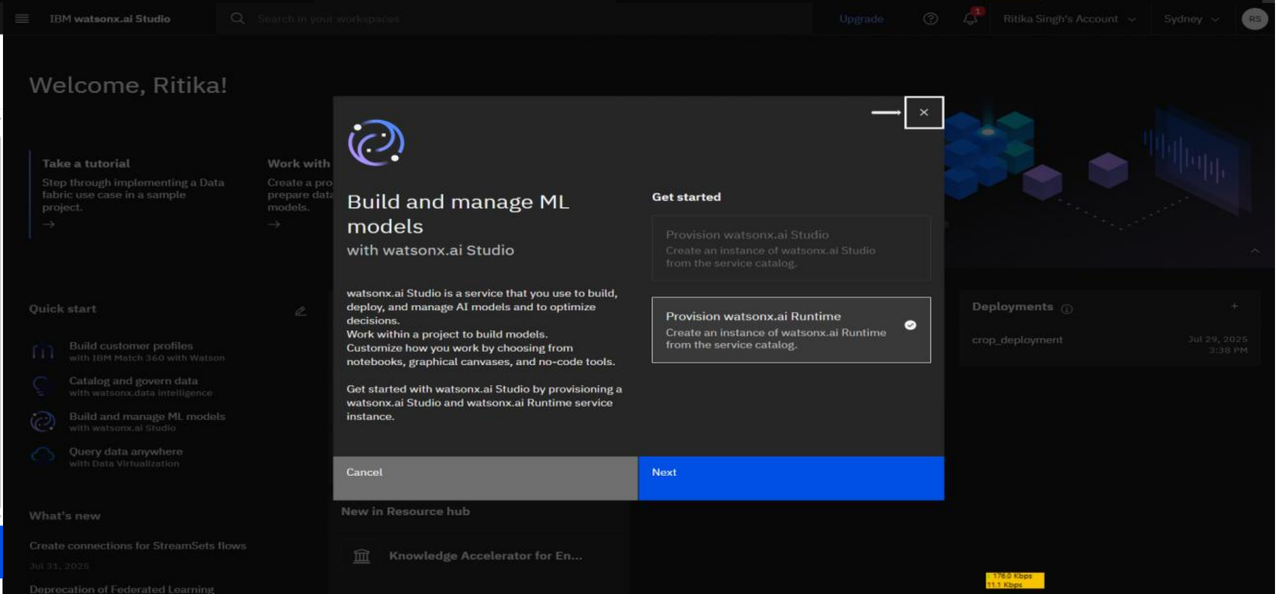
Tags (optional): Add tags

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

Storage: Cloud Object Storage-oi

Project includes integration with Cloud Object Storage for storing project assets.

Advanced settings
Cancel
Create



IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Ritika Singh's Account
Sydney
RS

Welcome, Ritika!

Take a tutorial
Step through implementing a Data fabric use case in a sample project.
Work with
Quick start
Build customer profiles with IBM Match 360 with Watson
Catalog and govern data with watsonx.data intelligence
Build and manage ML models with watsonx.ai Studio
Query data anywhere with Data Virtualization
What's new
Create connections for StreamSets flows
Deprecation of Federated Learning
New in Resource hub
Knowledge Accelerator for En...
Deployments
crop_deployment

Build and manage ML models with watsonx.ai Studio

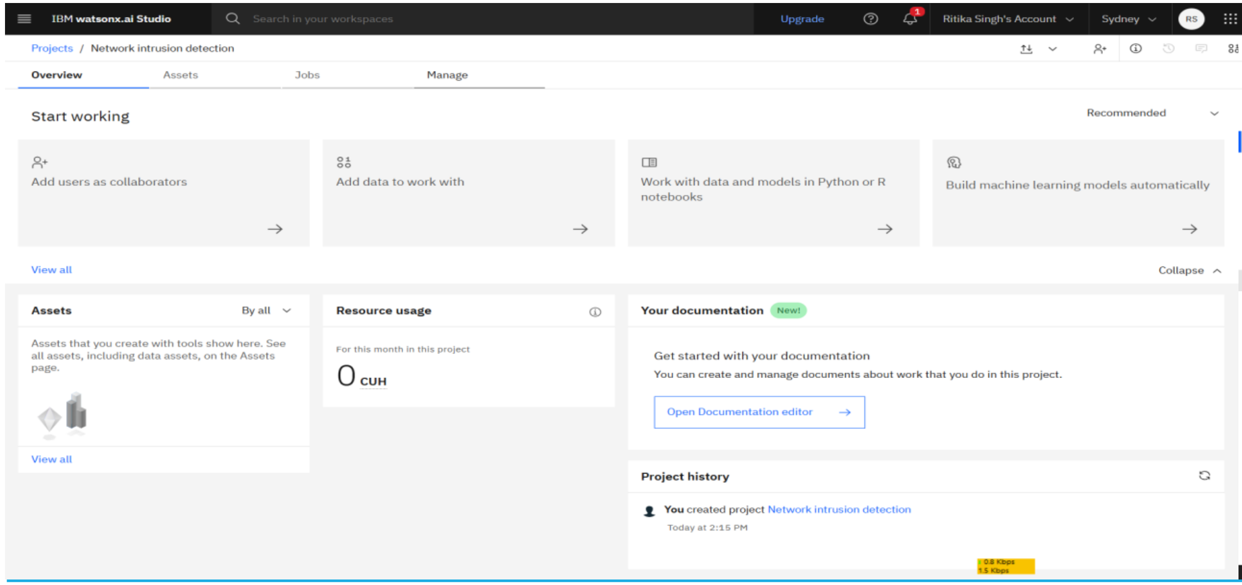
watsonx.ai Studio is a service that you use to build, deploy, and manage AI models and to optimize decisions.
Work within a project to build models.
Customize how you work by choosing from notebooks, graphical canvases, and no-code tools.

Get started with watsonx.ai Studio by provisioning a watsonx.ai Studio and watsonx.ai Runtime service instance.

Get started

- Provision watsonx.ai Studio
  Create an instance of watsonx.ai Studio from the service catalog.
- Provision watsonx.ai Runtime ●
  Create an instance of watsonx.ai Runtime from the service catalog.

SCREENSHOTS OF WORKFLOW



IBM watsonx.ai Studio | Search in your workspaces | Upgrade | Ritika Singh's Account | Sydney | RS

Projects / Network intrusion detection

Overview | Assets | Jobs | Manage

Start working — Recommended

- Add users as collaborators
- Add data to work with
- Work with data and models in Python or R notebooks
- Build machine learning models automatically

View all — Collapse

Assets — By all

Assets that you create with tools show here. See all assets, including data assets, on the Assets page.

View all

Resource usage

For this month in this project

0 CUH

Your documentation New!

Get started with your documentation

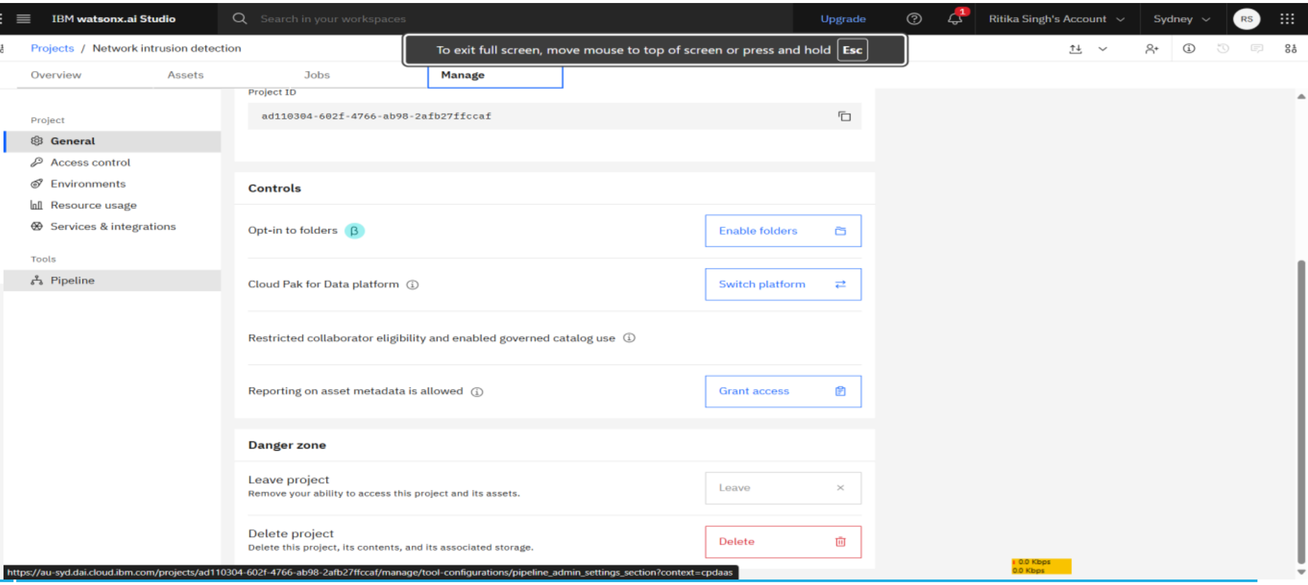
You can create and manage documents about work that you do in this project.

Open Documentation editor

Project history

You created project Network intrusion detection

Today at 2:15 PM



IBM watsonx.ai Studio | Search in your workspaces | Upgrade | Ritika Singh's Account | Sydney | RS

Projects / Network intrusion detection

To exit full screen, move mouse to top of screen or press and hold Esc

Overview | Assets | Jobs | Manage

Project: General, Access control, Environments, Resource usage, Services & integrations

Tools: Pipeline

Project ID

ad110304-602f-4766-ab98-2afb27ffccaf

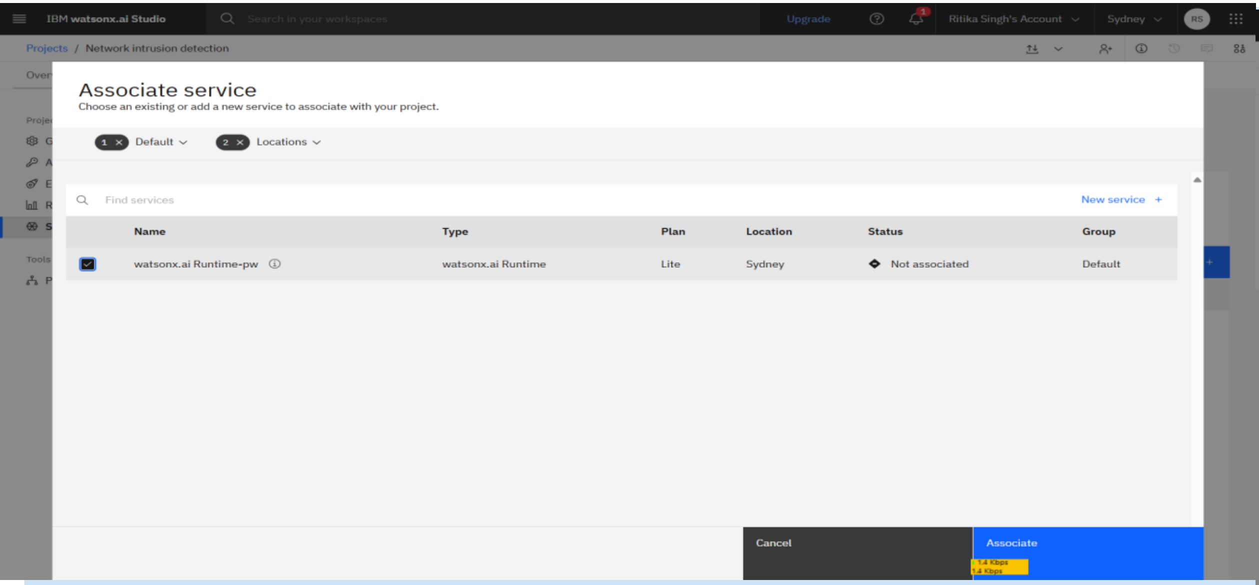
Controls

- Opt-in to folders β — Enable folders
- Cloud Pak for Data platform — Switch platform
- Restricted collaborator eligibility and enabled governed catalog use
- Reporting on asset metadata is allowed — Grant access

Danger zone

- Leave project — Remove your ability to access this project and its assets. — Leave
- Delete project — Delete this project, its contents, and its associated storage. — Delete

https://au-syd.dai.cloud.ibm.com/projects/ad110304-602f-4766-ab98-2afb27ffccaf/manage/tool-configurations/pipeline_admin_settings_section?context=cpdaas



IBM watsonx.ai Studio | Search in your workspaces | Upgrade | Ritika Singh's Account | Sydney | RS

Projects / Network intrusion detection

Associate service

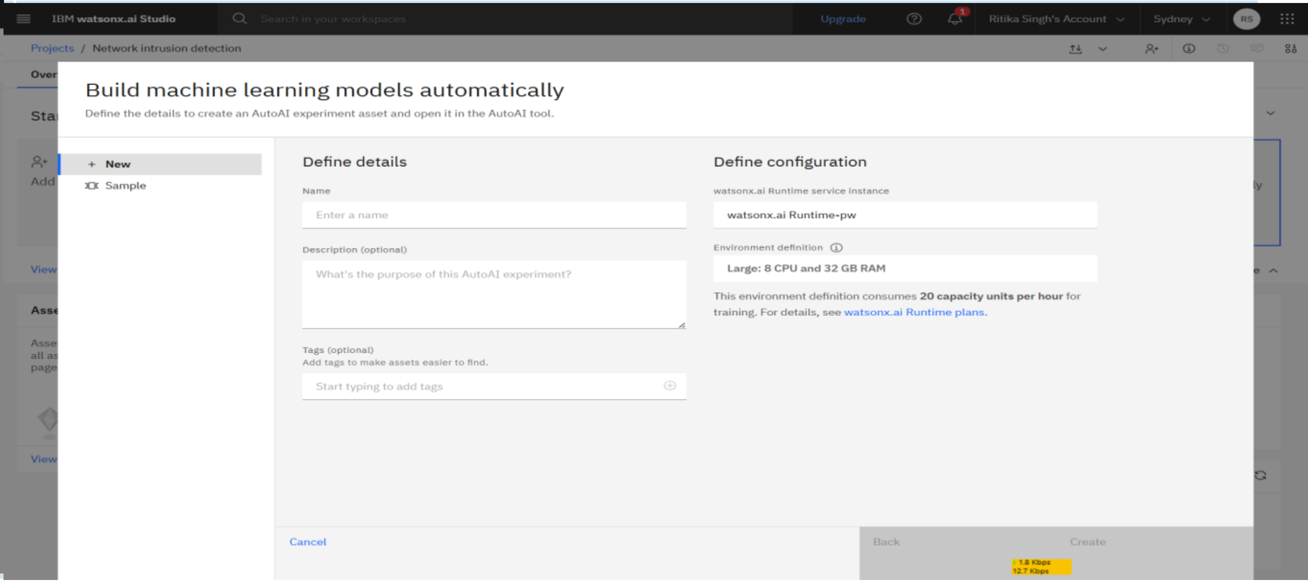
Choose an existing or add a new service to associate with your project.

1 × Default | 2 × Locations

Find services — New service +

	Name	Type	Plan	Location	Status	Group
☑	watsonx.ai Runtime-pw	watsonx.ai Runtime	Lite	Sydney	Not associated	Default

Cancel | Associate



IBM watsonx.ai Studio | Search in your workspaces | Upgrade | Ritika Singh's Account | Sydney | RS

Projects / Network intrusion detection

Build machine learning models automatically

Define the details to create an AutoAI experiment asset and open it in the AutoAI tool.

+ New | Sample

Define details

Name: Enter a name

Description (optional): What's the purpose of this AutoAI experiment?

Tags (optional): Add tags to make assets easier to find. — Start typing to add tags

Define configuration

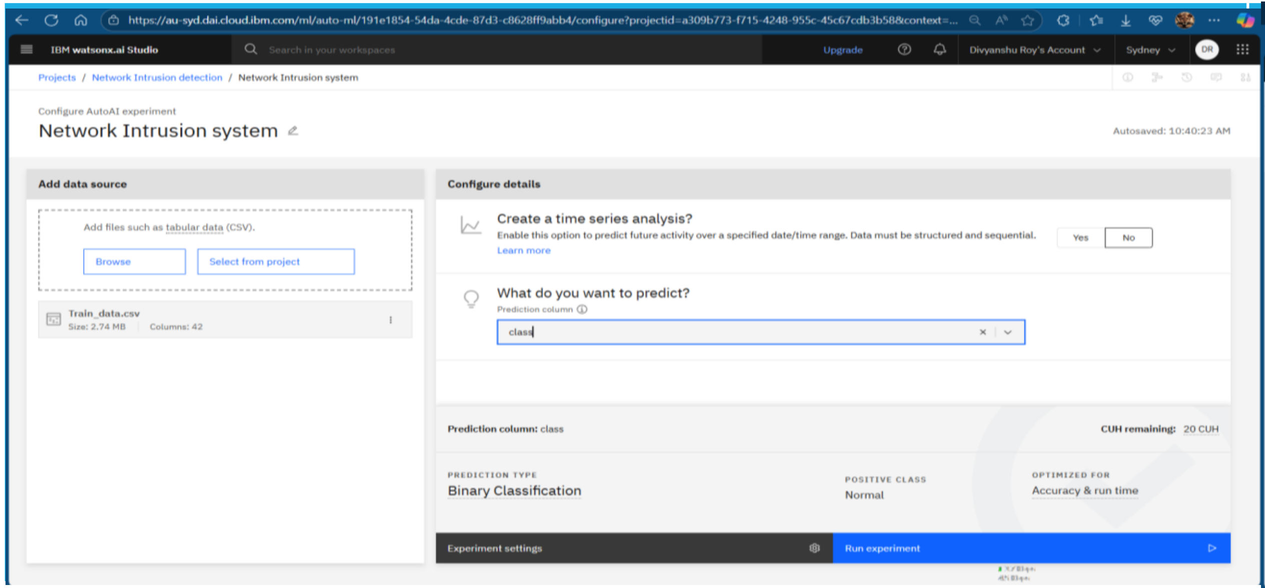
watsonx.ai Runtime service instance: watsonx.ai Runtime-pw

Environment definition: Large: 8 CPU and 32 GB RAM

This environment definition consumes 20 capacity units per hour for training. For details, see watsonx.ai Runtime plans.

Cancel | Back | Create

SCREENSHOTS OF WORKFLOW



https://au-syd.dai.cloud.ibm.com/ml/auto-ml/191e1854-54da-4cde-87d3-c8628ff9abb4/configure?projectid=a309b773-f715-4248-955c-45c67cdb3b58&context=...

Projects / Network Intrusion detection / Network Intrusion system

Configure AutoAI experiment

Network Intrusion system

Autosaved: 10:40:23 AM

Add data source

Add files such as tabular data (CSV).

Train_data.csv
Size: 2.74 MB | Columns: 42

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

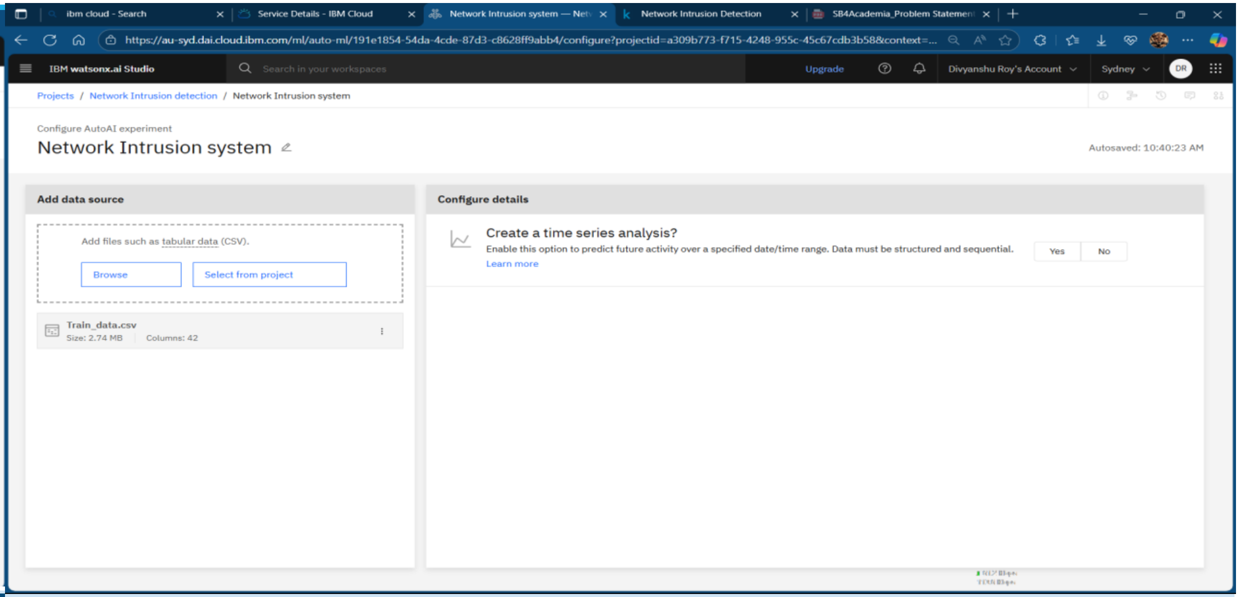
Yes [✓ No]

What do you want to predict?
Prediction column: class

Prediction column: class | CUH remaining: 20 CUH

PREDICTION TYPE: Binary Classification
POSITIVE CLASS: Normal
OPTIMIZED FOR: Accuracy & run time

Experiment settings
Run experiment



ibm cloud - Search
Service Details - IBM Cloud
Network Intrusion system — Net
Network Intrusion Detection
SB4Academia_Problem Statement

https://au-syd.dai.cloud.ibm.com/ml/auto-ml/191e1854-54da-4cde-87d3-c8628ff9abb4/configure?projectid=a309b773-f715-4248-955c-45c67cdb3b58&context=...

IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Divyanshu Roy's Account
Sydney
DR

Projects / Network Intrusion detection / Network Intrusion system

Configure AutoAI experiment

Network Intrusion system

Autosaved: 10:40:23 AM

Add data source

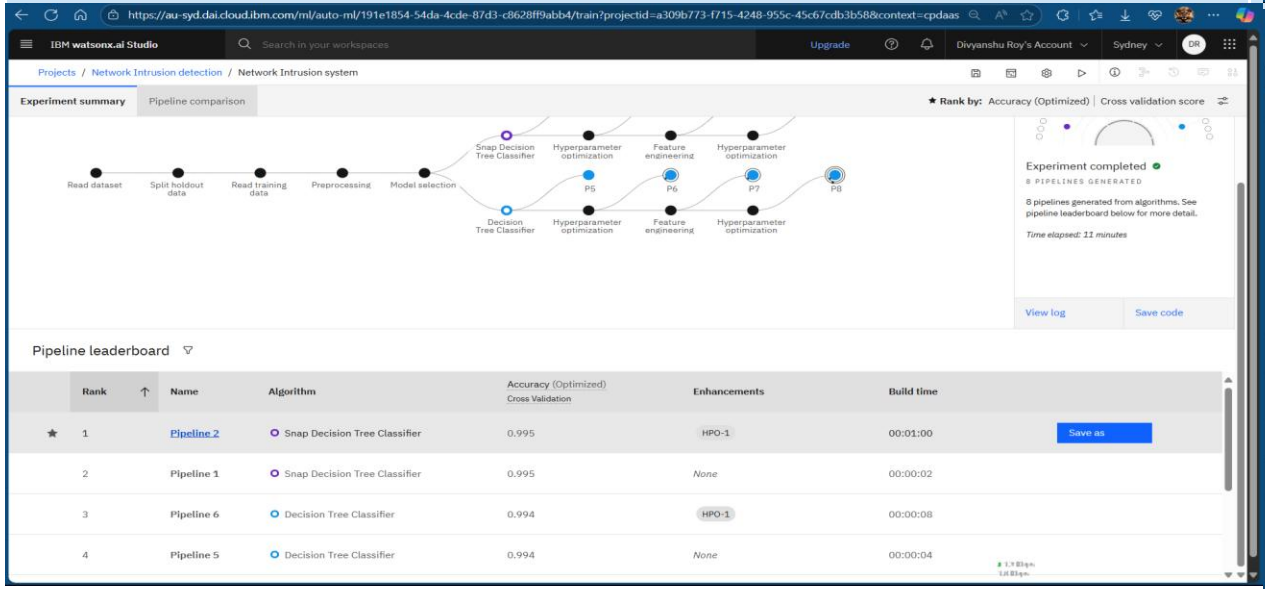
Add files such as tabular data (CSV).

Browse
Select from project

Train_data.csv
Size: 2.74 MB | Columns: 42

Configure details

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



https://au-syd.dai.cloud.ibm.com/ml/auto-ml/191e1854-54da-4cde-87d3-c8628ff9abb4/train?projectid=a309b773-f715-4248-955c-45c67cdb3b58&context=cpdaas

Projects / Network Intrusion detection / Network Intrusion system

Rank by: Accuracy (Optimized) | Cross validation score

Experiment completed

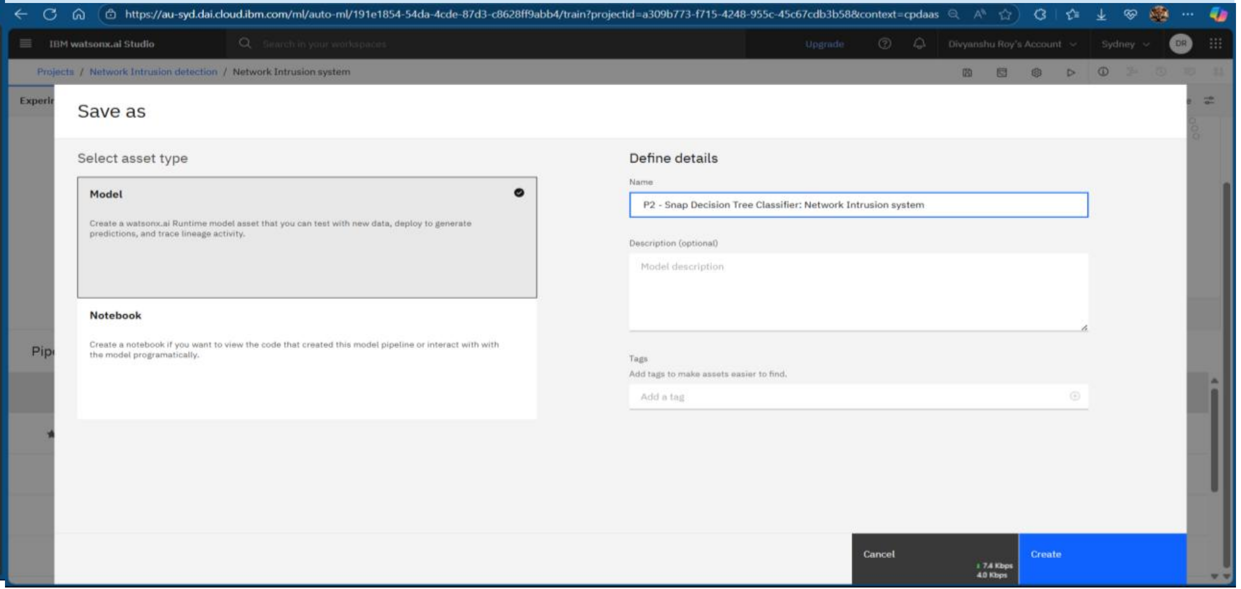
8 PIPELINES GENERATED

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

Time elapsed: 11 minutes

Pipeline leaderboard

	Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time	
★	1	Pipeline 2	Snap Decision Tree Classifier	0.995	HPO-1	00:01:00	Save as
	2	Pipeline 1	Snap Decision Tree Classifier	0.995	*None*	00:00:02	
	3	Pipeline 6	Decision Tree Classifier	0.994	HPO-1	00:00:08	
	4	Pipeline 5	Decision Tree Classifier	0.994	*None*	00:00:04	



https://au-syd.dai.cloud.ibm.com/ml/auto-ml/191e1854-54da-4cde-87d3-c8628ff9abb4/train?projectid=a309b773-f715-4248-955c-45c67cdb3b58&context=cpdaas

Projects / Network Intrusion detection / Network Intrusion system

Save as

Select asset type

Model ✓
Create a watsonx.ai Runtime model asset that you can test with new data, deploy to generate predictions, and trace lineage activity.

Notebook
Create a notebook if you want to view the code that created this model pipeline or interact with with the model programatically.

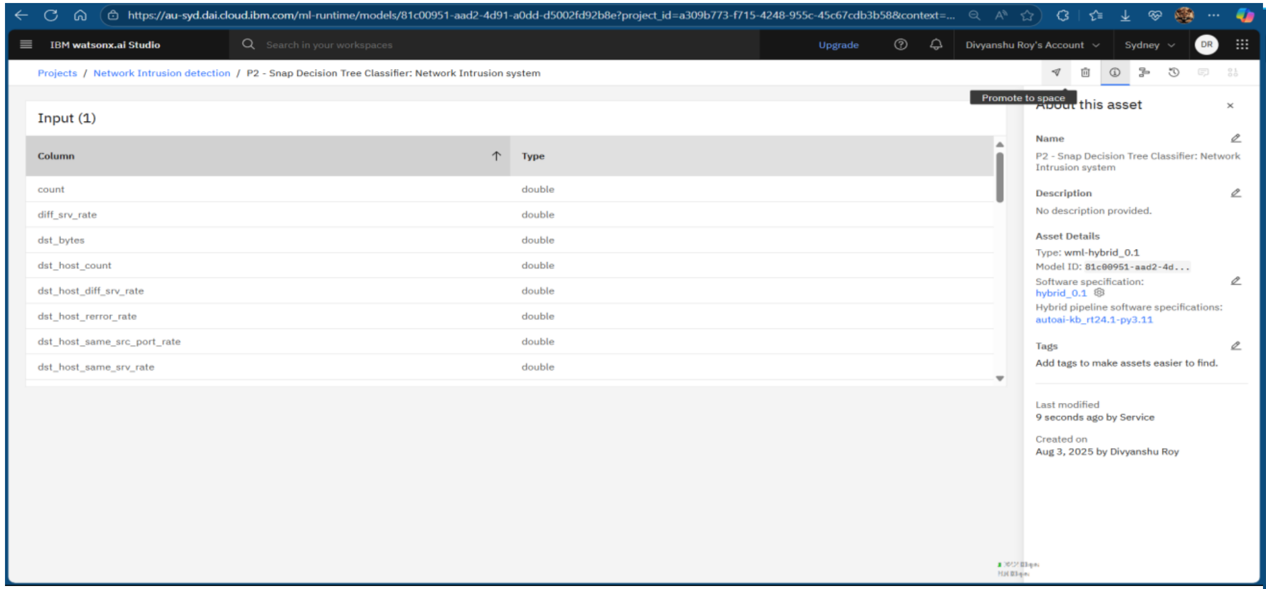
Define details

Name: P2 - Snap Decision Tree Classifier: Network Intrusion system

Description (optional): Model description

Tags
Add tags to make assets easier to find.
Add a tag

SCREENSHOTS OF WORKFLOW



https://au-syd.dai.cloud.ibm.com/ml-runtime/models/81c00951-aad2-4d91-a0dd-d5002fd92b8e?project_id=a309b773-f715-4248-955c-45c67cdb3b58&context=...

Projects / Network Intrusion detection / P2 - Snap Decision Tree Classifier: Network Intrusion system

Input (1)

Column	Type
count	double
diff_srv_rate	double
dst_bytes	double
dst_host_count	double
dst_host_diff_srv_rate	double
dst_host_rerror_rate	double
dst_host_same_src_port_rate	double
dst_host_same_srv_rate	double

About this asset

Name: P2 - Snap Decision Tree Classifier: Network Intrusion system

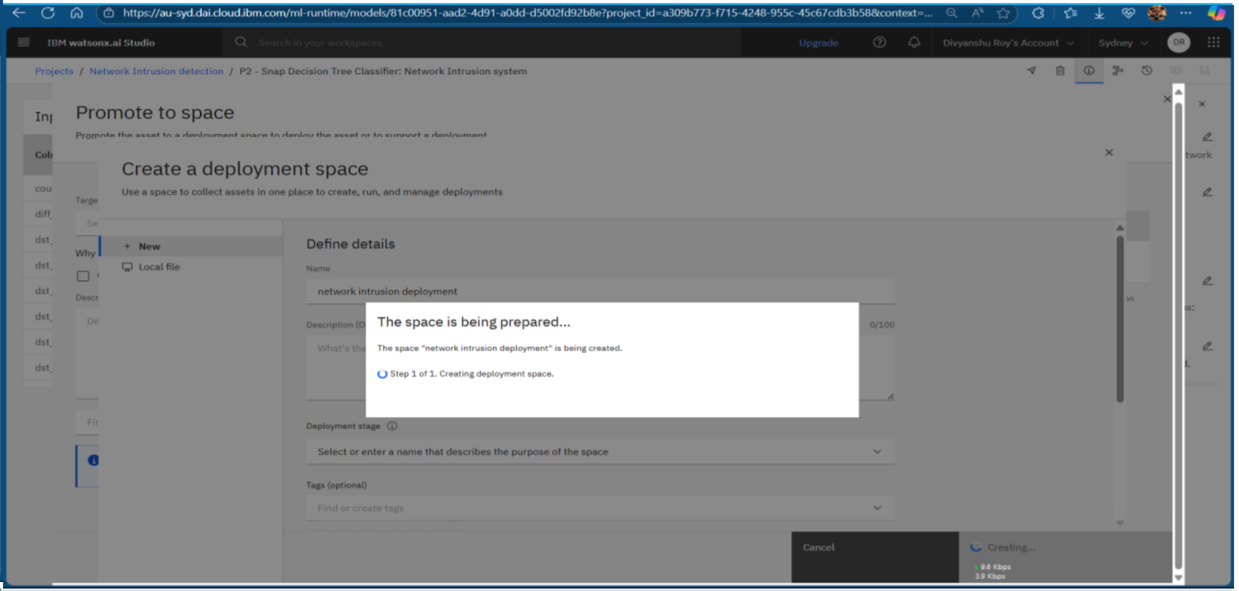
Description: No description provided.

Asset Details
Type: wml-hybrid_0.1
Model ID: 81c00951-aad2-4d...
Software specification: hybrid_0.1
Hybrid pipeline software specifications: autoai-kb_rt24.1-py3.11

Tags: Add tags to make assets easier to find.

Last modified: 9 seconds ago by Service

Created on: Aug 3, 2025 by Divyanshu Roy



https://au-syd.dai.cloud.ibm.com/ml-runtime/models/81c00951-aad2-4d91-a0dd-d5002fd92b8e?project_id=a309b773-f715-4248-955c-45c67cdb3b58&context=...

Projects / Network Intrusion detection / P2 - Snap Decision Tree Classifier: Network Intrusion system

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 deployment

Description (O... 0/100

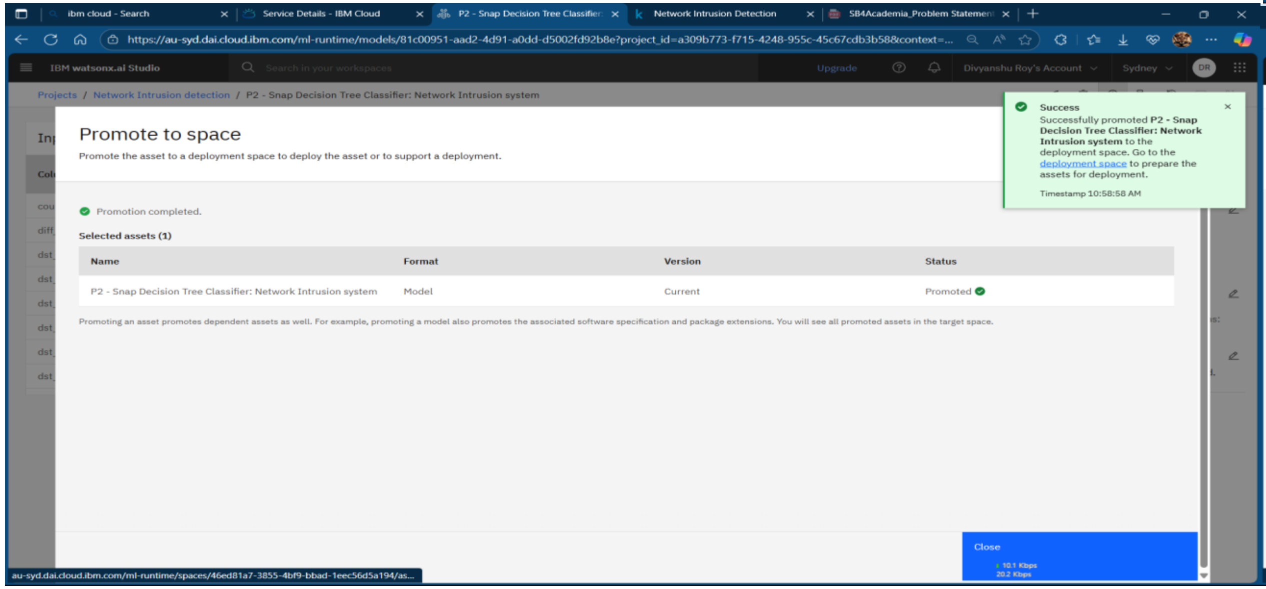
The space is being prepared...

The space "network intrusion deployment" is being created.

Step 1 of 1. Creating deployment space.

Deployment stage: Select or enter a name that describes the purpose of the space

Tags (optional): Find or create tags


ibm cloud - Search
Service Details - IBM Cloud
P2 - Snap Decision Tree Classifier
Network Intrusion Detection
SB4Academia_Problem Statement
IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Divyanshu Roy's Account
Sydney
Close

https://au-syd.dai.cloud.ibm.com/ml-runtime/models/81c00951-aad2-4d91-a0dd-d5002fd92b8e?project_id=a309b773-f715-4248-955c-45c67cdb3b58&context=...

Projects / Network Intrusion detection / P2 - Snap Decision Tree Classifier: Network Intrusion system

Promote to space

Promote the asset to a deployment space to deploy the asset or to support a deployment.

Promotion completed.

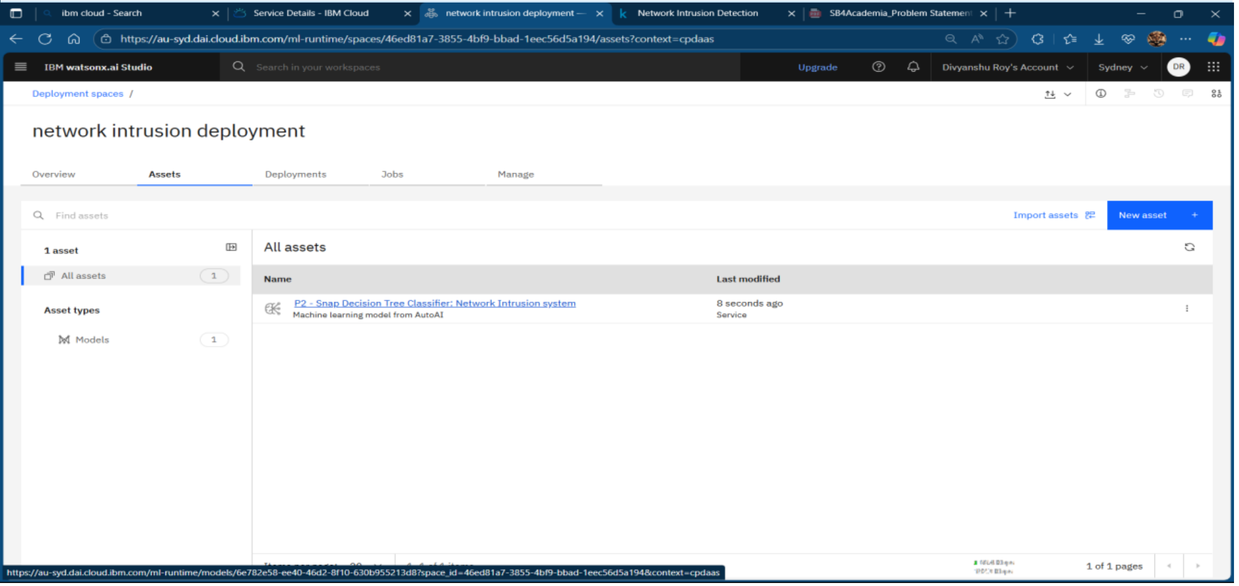
Selected assets (1)

Name	Format	Version	Status
P2 - Snap Decision Tree Classifier: Network Intrusion system	Model	Current	Promoted ✓

Promoting an asset promotes dependent assets as well. For example, promoting a model also promotes the associated software specification and package extensions. You will see all promoted assets in the target space.

Success
Successfully promoted **P2 - Snap Decision Tree Classifier: Network Intrusion system** to the deployment space. Go to the deployment space to prepare the assets for deployment.
Timestamp 10:58:58 AM

au-syd.dai.cloud.ibm.com/ml-runtime/spaces/46ed81a7-3855-4bf9-bbad-1eec56d5a194/as...



https://au-syd.dai.cloud.ibm.com/ml-runtime/spaces/46ed81a7-3855-4bf9-bbad-1eec56d5a194/assets?context=cpdaas

Deployment spaces /

network intrusion deployment

1 asset

All assets 1

Models 1

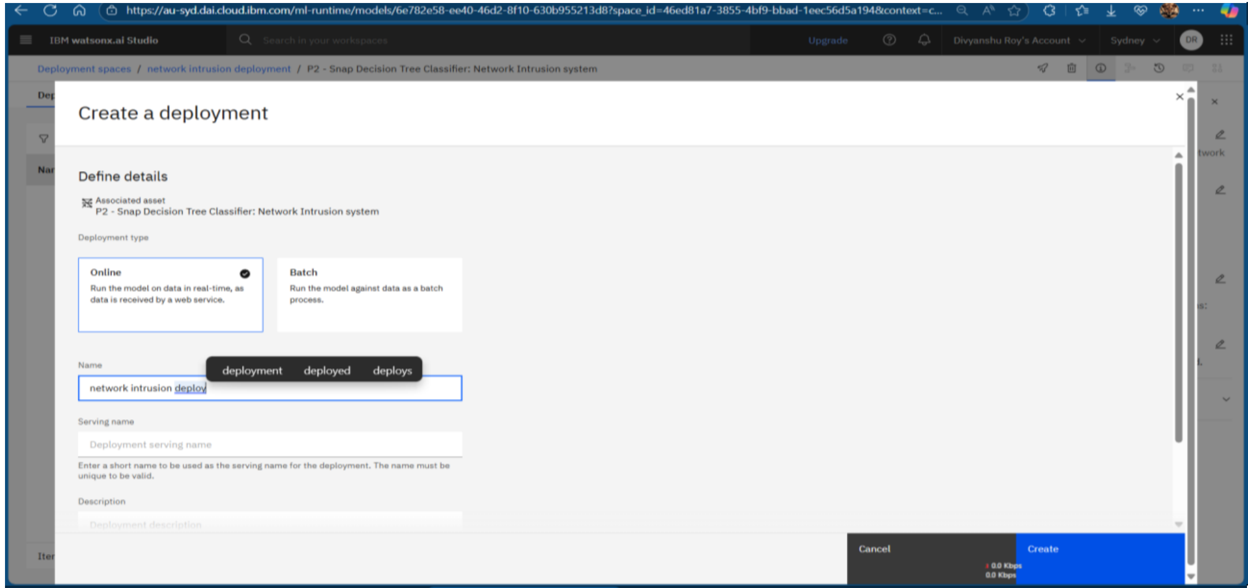
All assets

Name	Last modified
P2 - Snap Decision Tree Classifier: Network Intrusion system Machine learning model from AutoAI	8 seconds ago Service

1 of 1 pages

https://au-syd.dai.cloud.ibm.com/ml-runtime/models/6e782e58-ee40-46d2-8f10-630b955213d8?space_id=46ed81a7-3855-4bf9-bbad-1eec56d5a194&context=cpdaas

SCREENSHOTS OF WORKFLOW



Deployment spaces / network intrusion deployment / P2 - Snap Decision Tree Classifier: Network Intrusion system

Create a deployment

Define details

Associated asset
P2 - Snap Decision Tree Classifier: Network Intrusion system

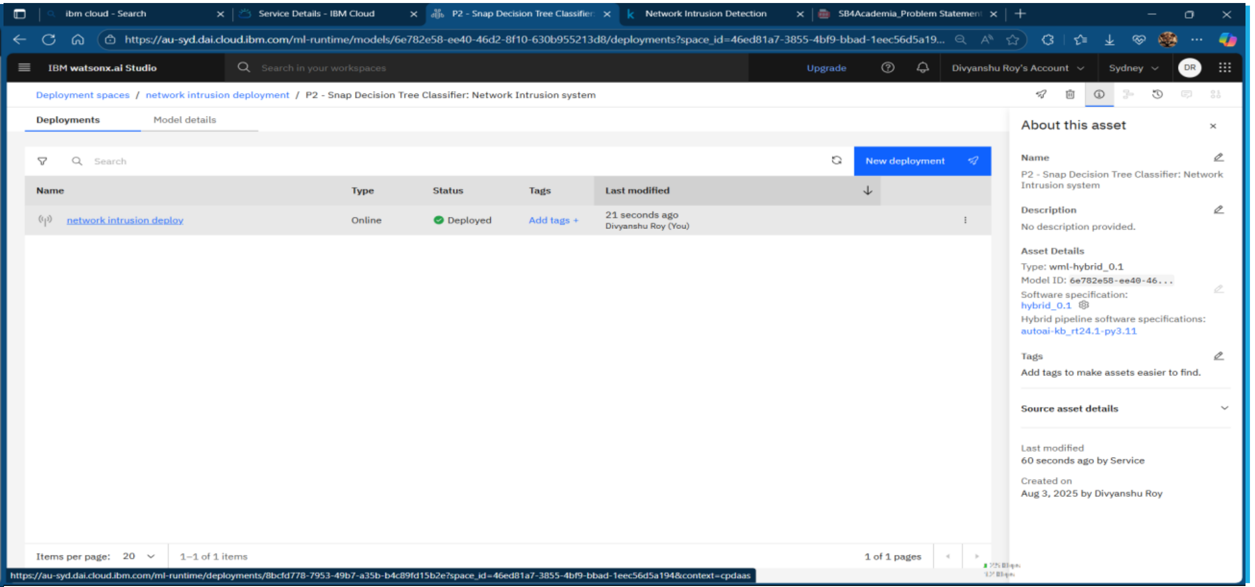
Deployment type

- ● Online: Run the model on data in real-time, as data is received by a web service.
- Batch: Run the model against data as a batch process.

Name: network intrusion deploy

Serving name: Deployment serving name
Enter a short name to be used as the serving name for the deployment. The name must be unique to be valid.

Description: Deployment description



Deployment spaces / network intrusion deployment / P2 - Snap Decision Tree Classifier: Network Intrusion system

Name	Type	Status	Tags	Last modified
network intrusion deploy	Online	Deployed	Add tags +	21 seconds ago Divyanshu Roy (You)

Items per page: 20 · 1–1 of 1 items · 1 of 1 pages

About this asset

Name: P2 - Snap Decision Tree Classifier: Network Intrusion system

Description: No description provided.

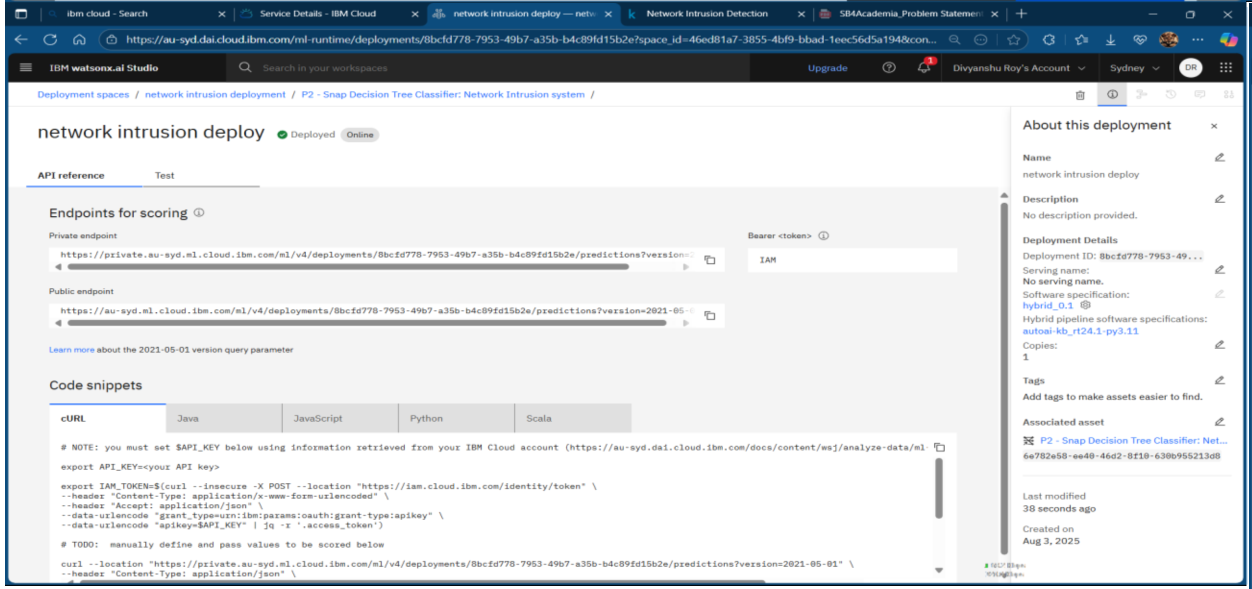
Asset Details
Type: wml-hybrid_0.1
Model ID: 6e782e58-ee40-46...
Software specification: hybrid_0.1
Hybrid pipeline software specifications: autoai-kb_rt24.1-py3.11

Tags: Add tags to make assets easier to find.

Source asset details

Last modified: 60 seconds ago by Service

Created on: Aug 3, 2025 by Divyanshu Roy



Deployment spaces / network intrusion deployment / P2 - Snap Decision Tree Classifier: Network Intrusion system /

network intrusion deploy · Deployed · Online

Endpoints for scoring

Private endpoint

```
https://private.au-syd.ml.cloud.ibm.com/ml/v4/deployments/8bcfd778-7953-49b7-a35b-b4c89fd15b2e/predictions?version=2
```

Public endpoint

```
https://au-syd.ml.cloud.ibm.com/ml/v4/deployments/8bcfd778-7953-49b7-a35b-b4c89fd15b2e/predictions?version=2021-05-
```

Bearer <token>: IAM

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://au-syd.dai.cloud.ibm.com/docs/content/wsj/analyze-data/ml-

export API_KEY=<your API key>

export IAM_TOKEN=$(curl --insecure -X POST --location "https://iam.cloud.ibm.com/identity/token" \
--header "Content-Type: application/x-www-form-urlencoded" \
--header "Accept: application/json" \
--data-urlencode "grant_type=urn:ibm:params:oauth:grant-type:apikey" \
--data-urlencode "apikey=$API_KEY" | jq -r '.access_token')

# TODO:  manually define and pass values to be scored below

curl --location "https://private.au-syd.ml.cloud.ibm.com/ml/v4/deployments/8bcfd778-7953-49b7-a35b-b4c89fd15b2e/predictions?version=2021-05-01" \
--header "Content-Type: application/json" \
```

About this deployment

Name: network intrusion deploy

Description: No description provided.

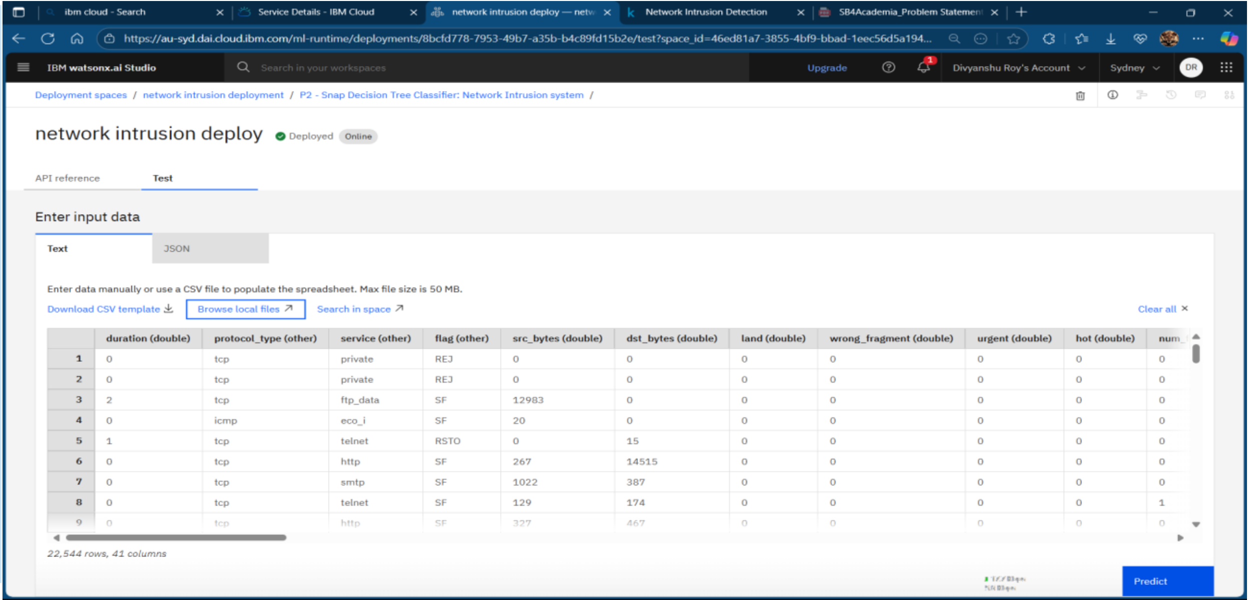
Deployment Details
Deployment ID: 8bcfd778-7953-49...
Serving name: No serving name.
Software specification: hybrid_0.1
Hybrid pipeline software specifications: autoai-kb_rt24.1-py3.11
Copies: 1

Tags: Add tags to make assets easier to find.

Associated asset: P2 - Snap Decision Tree Classifier: Net...
6e782e58-ee40-46d2-8f10-630b955213d8

Last modified: 38 seconds ago

Created on: Aug 3, 2025



Deployment spaces / network intrusion deployment / P2 - Snap Decision Tree Classifier: Network Intrusion system /

network intrusion deploy · Deployed · Online

Enter input data

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

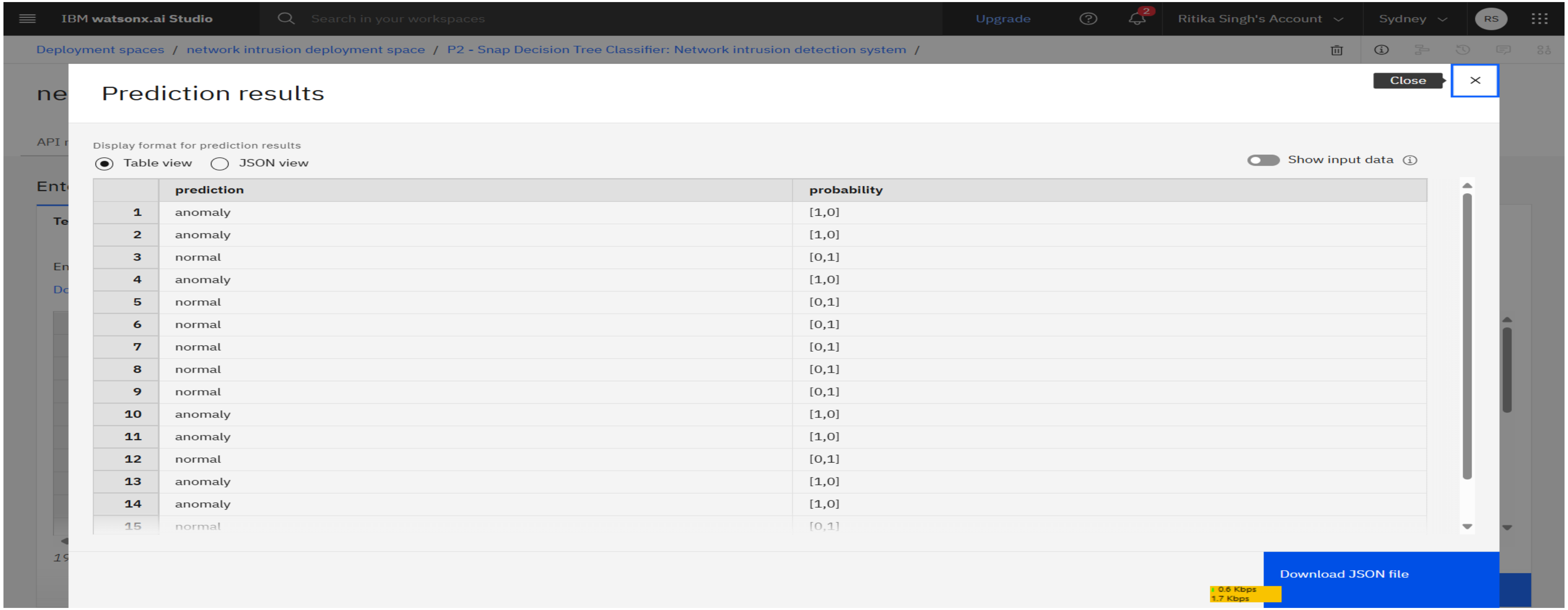
Download CSV template · Browse local files · Search in space · Clear all

	duration (double)	protocol_type (other)	service (other)	flag (other)	src_bytes (double)	dst_bytes (double)	land (double)	wrong_fragment (double)	urgent (double)	hot (double)	num_
1	0	tcp	private	REJ	0	0	0	0	0	0	0
2	0	tcp	private	REJ	0	0	0	0	0	0	0
3	2	tcp	ftp_data	SF	12983	0	0	0	0	0	0
4	0	icmp	eco_i	SF	20	0	0	0	0	0	0
5	1	tcp	telnet	RSTO	0	15	0	0	0	0	0
6	0	tcp	http	SF	267	14515	0	0	0	0	0
7	0	tcp	smtp	SF	1022	387	0	0	0	0	0
8	0	tcp	telnet	SF	129	174	0	0	0	0	1
9	0	tcp	http	SF	327	467	0	0	0	0	0

22,544 rows, 41 columns

RESULT

The AutoAI experiment successfully generated multiple pipelines, with the top-performing model (**Pipeline 2**) achieving an accuracy of **99.5%**. The model was then deployed and tested, correctly identifying network traffic as 'normal' or 'anomaly'.


IBM watsonx.ai Studio
Search in your workspaces
Upgrade
2
Ritika Singh's Account
Sydney
RS
Deployment spaces / network intrusion deployment space / P2 - Snap Decision Tree Classifier: Network intrusion detection system /
Close
Download JSON file
0.6 Kbps
1.7 Kbps

Prediction results

Display format for prediction results

● Table view ○ JSON view

Show input data

	prediction	probability
1	anomaly	[1,0]
2	anomaly	[1,0]
3	normal	[0,1]
4	anomaly	[1,0]
5	normal	[0,1]
6	normal	[0,1]
7	normal	[0,1]
8	normal	[0,1]
9	normal	[0,1]
10	anomaly	[1,0]
11	anomaly	[1,0]
12	normal	[0,1]
13	anomaly	[1,0]
14	anomaly	[1,0]
15	normal	[0,1]

CONCLUSION

❑ This project successfully demonstrated the creation and deployment of a highly accurate Network Intrusion Detection System.

❑ Using IBM Watsonx.ai and its AutoAI capabilities significantly accelerated the development process, automating tasks that would typically require extensive manual coding and expertise.

❑ The final deployed model serves as a powerful and scalable solution for enhancing network security through real-time threat detection.

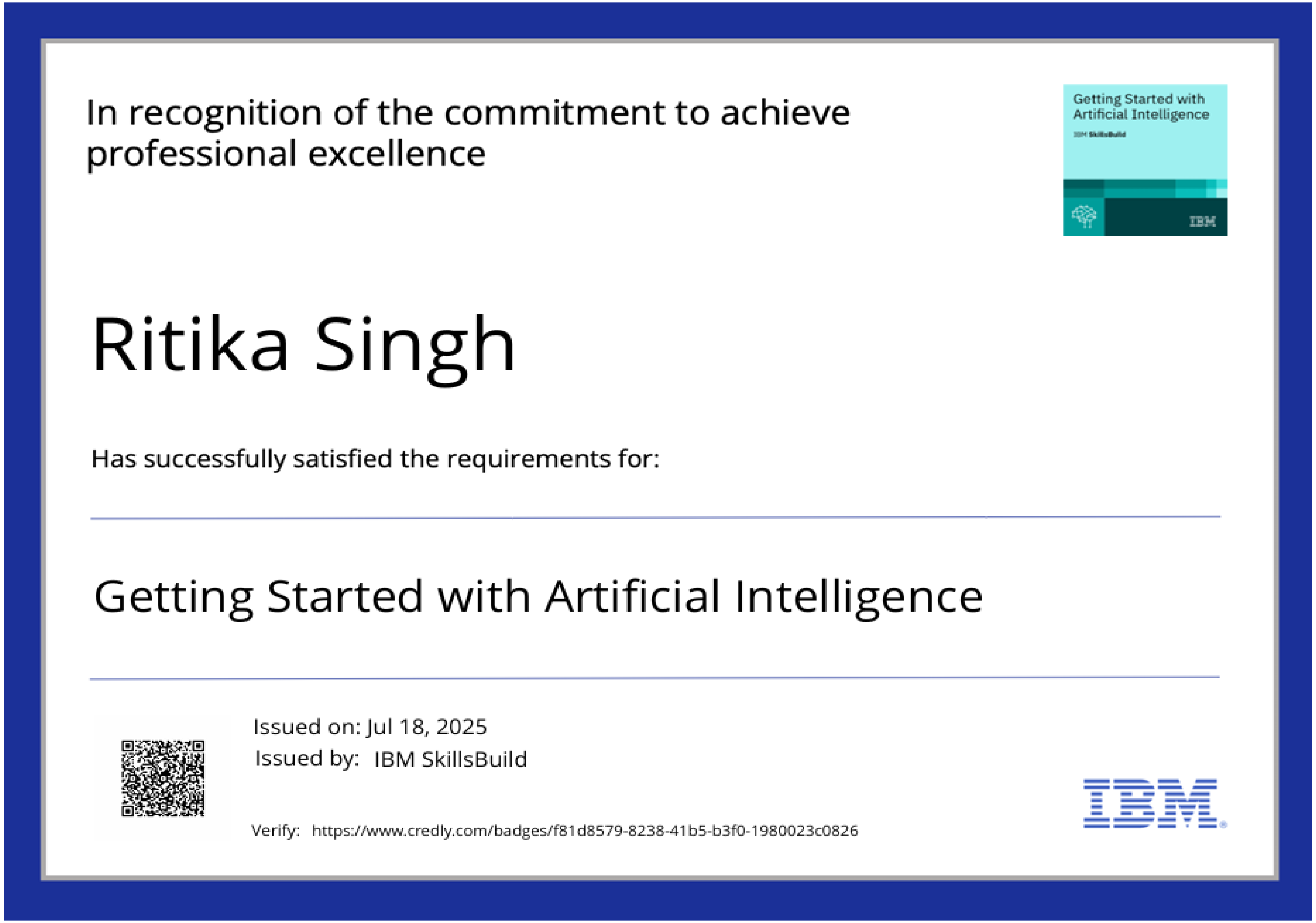
FUTURE SCOPE

- ❑ **Real-time Integration:** Integrate the deployed API with a live network monitoring tool (like Wireshark or a custom dashboard) to analyze traffic in real-time.
- ❑ **Automated Retraining:** Implement a CI/CD pipeline to automatically retrain and redeploy the model as new attack data becomes available.
- ❑ **Advanced Explainability:** Use AI explainability tools to better understand *why* the model flags certain activities as malicious, providing deeper insights for security analysts.

REFERENCES

- ❑ **Dataset:** "NSL-KDD Dataset" from Kaggle.
- ❑ *Link: https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection*
- ❑ **Platform:** IBM Cloud & Watsonx.ai Documentation.

IBM CERTIFICATIONS



Getting Started with Artificial Intelligence

IBM SkillsBuild

IBM

In recognition of the commitment to achieve professional excellence

Ritika Singh

Has successfully satisfied the requirements for:

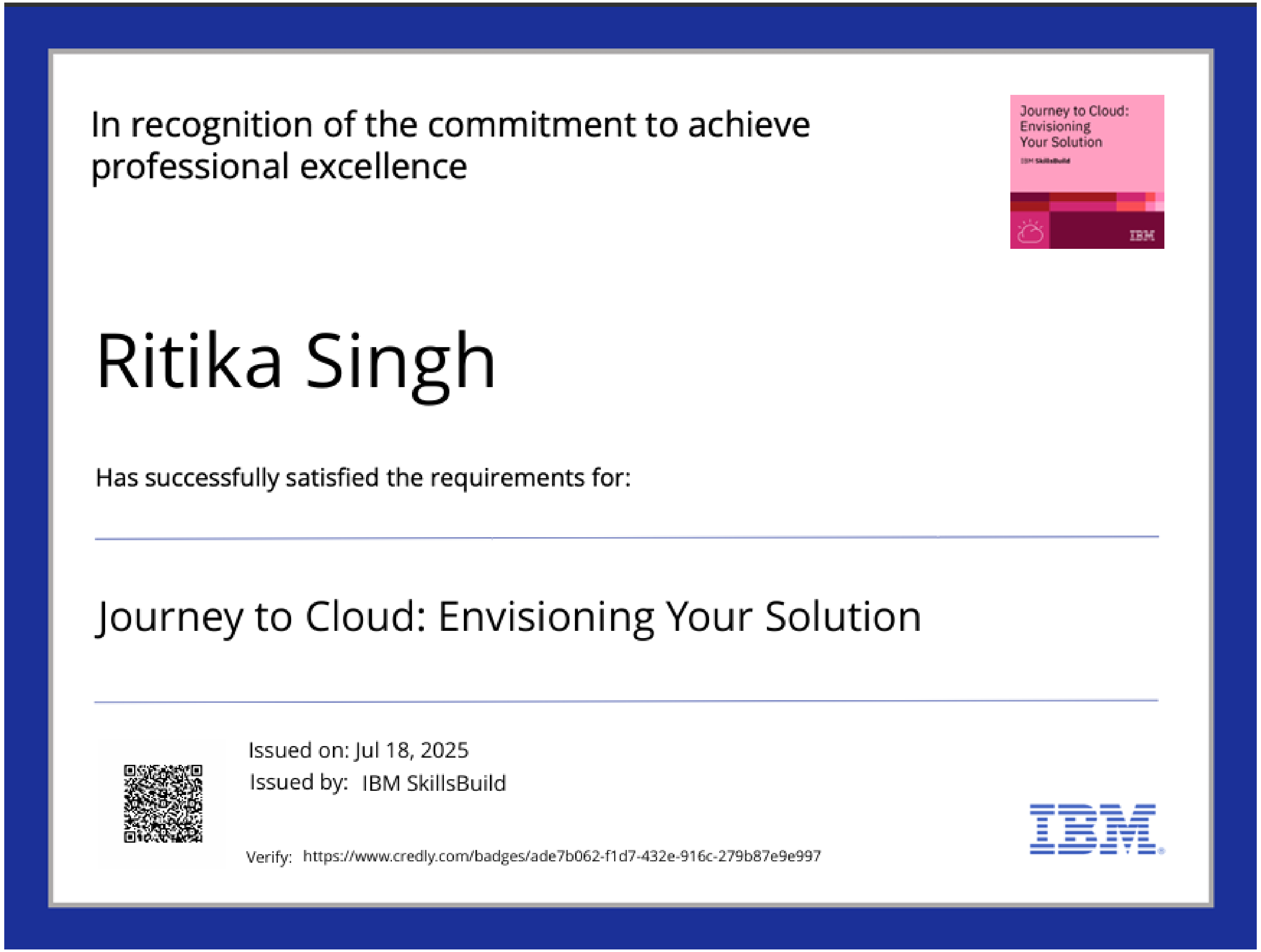
Getting Started with Artificial Intelligence

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

Verify: https://www.credly.com/badges/f81d8579-8238-41b5-b3f0-1980023c0826

IBM

IBM CERTIFICATIONS



Journey to Cloud:
Envisioning
Your Solution
IBM SkillsBuild
IBM

In recognition of the commitment to achieve professional excellence

Ritika Singh

Has successfully satisfied the requirements for:

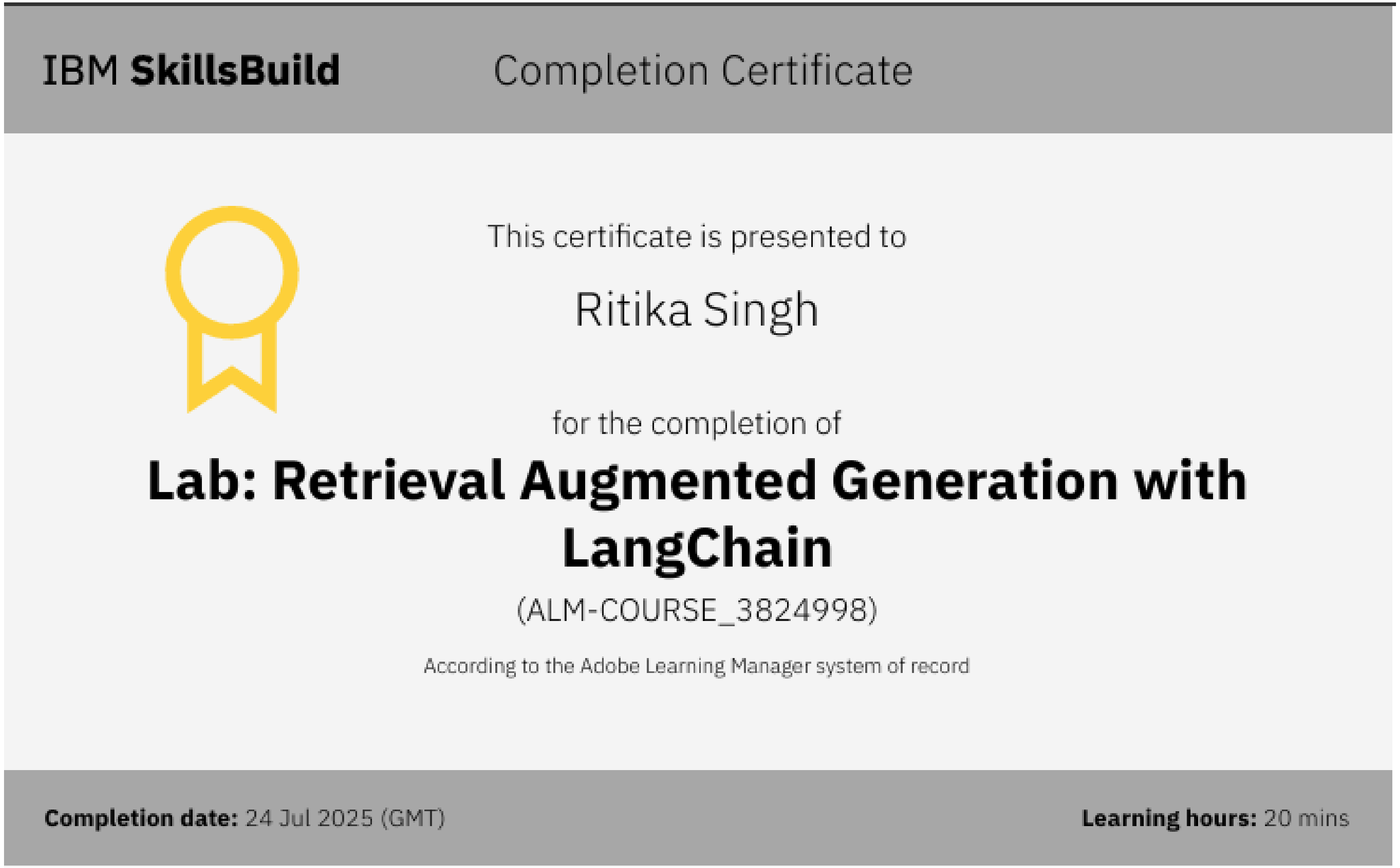
Journey to Cloud: Envisioning Your Solution

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

Verify: https://www.credly.com/badges/ade7b062-f1d7-432e-916c-279b87e9e997

IBM

IBM CERTIFICATIONS



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Ritika Singh

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