

---

# **CAPSTONE PROJECT**

## **NETWORK INTRUSION DETECTION**

**(PROBLEM STATEMENT-40)**

**Presented By:**

- 1. Student Name- Anjali Jha**
- 2. College Name- CSE (Galgotias College of Engineering and Technology)**

---

# OUTLINE

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

# PROBLEM STATEMENT

## Network Intrusion Detection:

- Network Intrusion Detection refers to the process of monitoring network traffic to identify unauthorized access, malicious activities, or policy violations in real time.
- **The Problem**
- Modern networks are constantly under threat from:
  - Hackers trying to steal data
  - Malware spreading through systems
  - Internal users misusing access

# PROPOSED SOLUTION

- The proposed system aims to Train models to classify network traffic as normal or malicious. The solution will consist of the following components:
- **Data Collection:**
  - Gather These datasets include network traffic logs with labeled records (normal vs. attack types)
  - IP addresses, protocols, packet sizes, flags, timestamps etc to enhance prediction accuracy.
- **Data Preprocessing**
  - Clean and preprocess the collected data to handle missing values, outliers, and inconsistencies.
  - Convert categorical data (like protocol type) into numerical format using one-hot encoding or label encoding.
  - Use techniques like PCA or correlation analysis to reduce dimensionality and improve performance.
  - **Machine Learning Algorithm:**
    - Implement a machine learning algorithm, such as High accuracy, handles large datasets well ,Good for binary classification, effective in high-dimensional space, Simple and intuitive, good baseline. (e.g. SVM, KNN).
- **Deployment:**
  - Develop a user-friendly interface or application that provides real-time predictions for suspicious network detection.
  - Deploy the solution on a scalable and reliable platform, considering factors like server infrastructure, response time, and user accessibility.
- **Evaluation:**
  - Assess the model's performance using appropriate metrics. Ensure the model is reliable, efficient, and minimizes false alarms.
  - Fine-tune the model based on real time input and continuous monitoring of prediction accuracy.
  - Result:

# SYSTEM APPROACH

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

- System requirements : IBM cloud
- Library required to build the model: Watsonx ai studio

# ALGORITHM & DEPLOYMENT

- In the Algorithm section, describe the machine learning algorithm chosen for predicting bike counts. Here's an example structure for this section:
- **Data Input:**
  - Specify the input features used by the algorithm, such as large network dataset, types of attacks (DoS, Probe, R2L, U2R, Normal)
- **Training Process:**
  - Explain how the algorithm is trained using train dataset (from Kaggle.com).
- **Prediction Process:**
  - We used 0.995% accurate machine learning model and trained this model with dataset. And given correct prediction, any real-time data inputs.

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

ANJALI JHA's Account

London

AJ

Projects / Network Detection / Network\_Detection\_ML


Experiment summary

Pipeline comparison

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


Relationship map

Prediction column: class



Progress map

Swap view



Pending

TRAIN\_DATA.CSV

Starting the AutoAI experiment

Time elapsed: 3 seconds

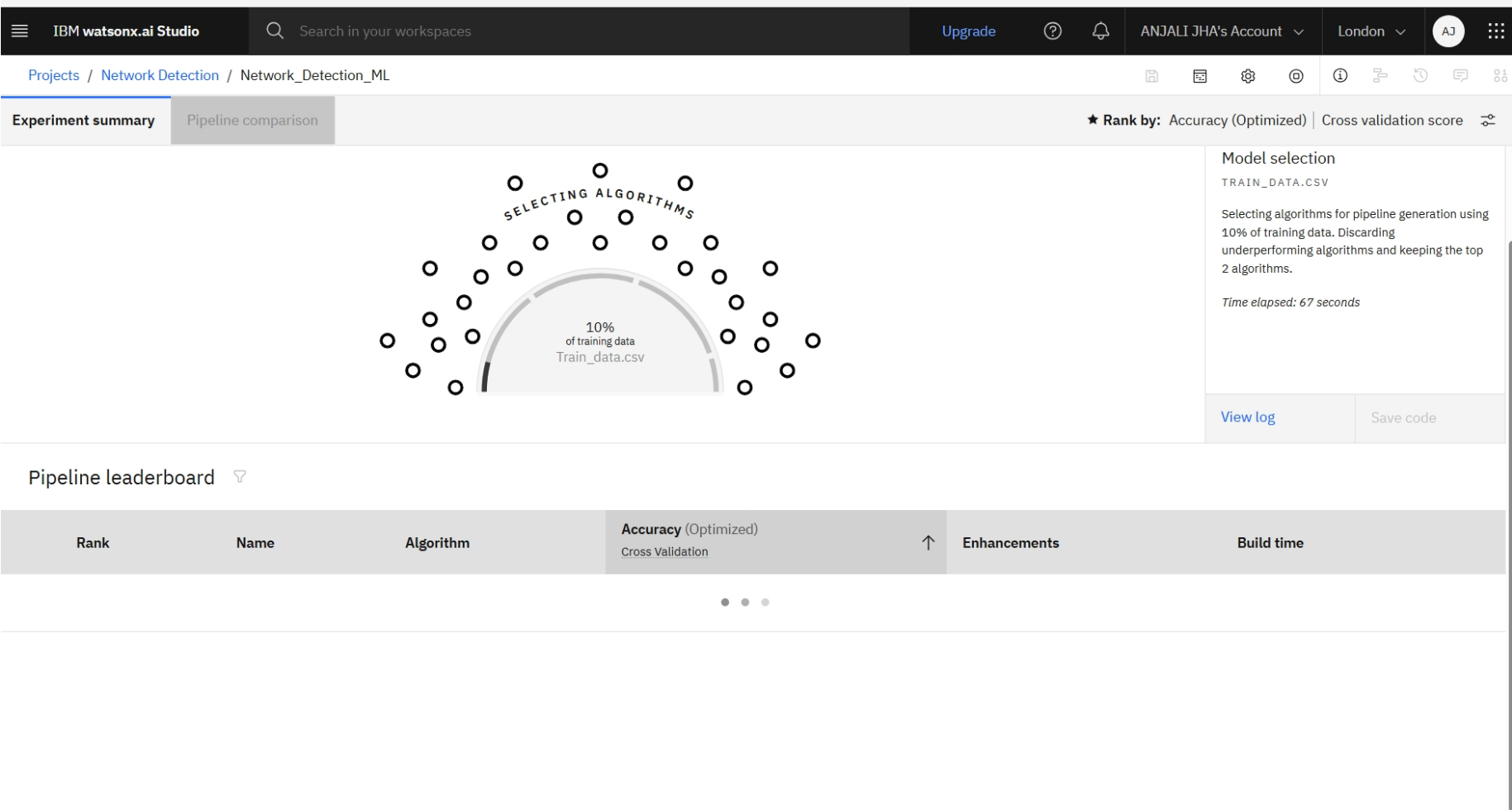
View log

Save code

Pipeline leaderboard

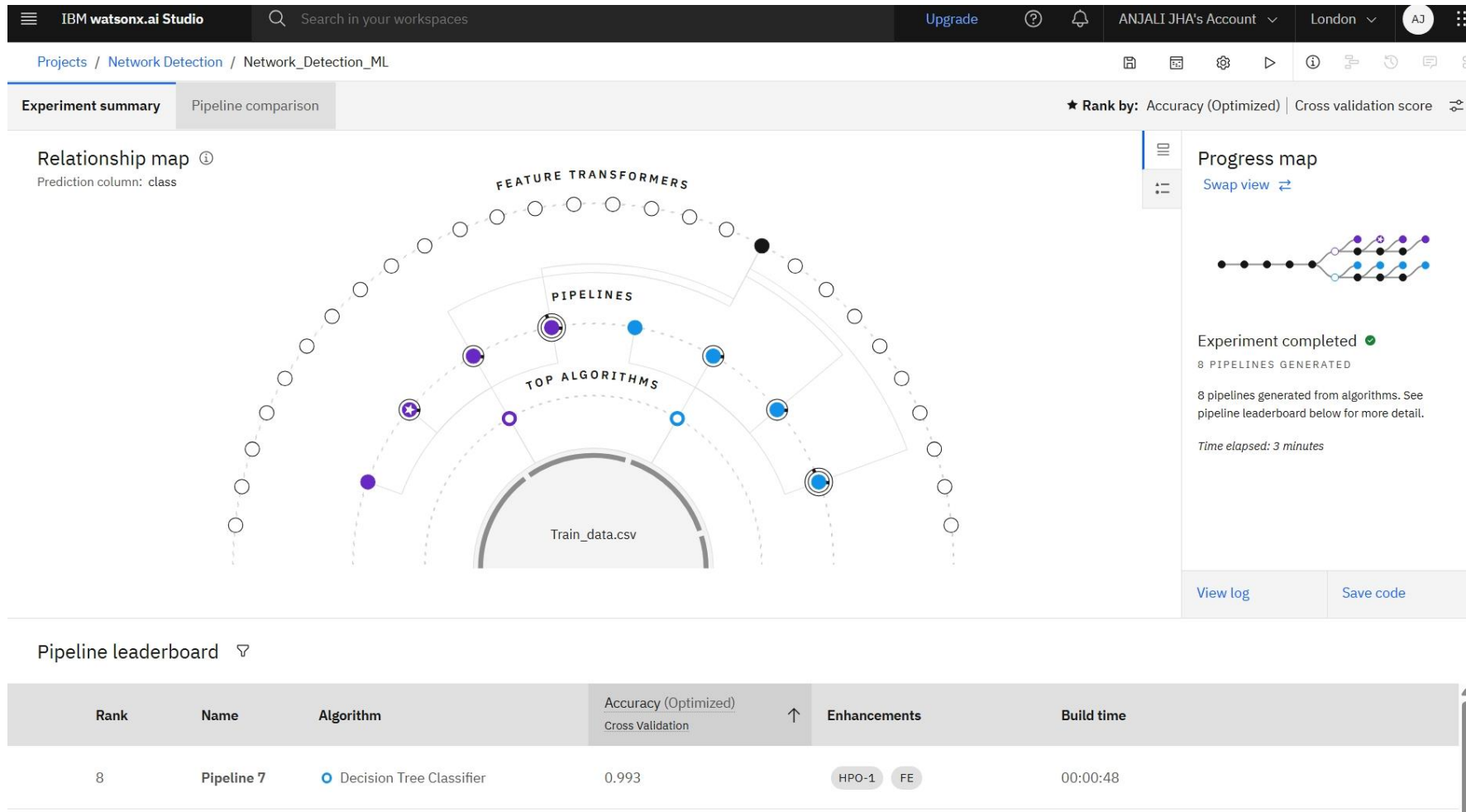
Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time

# RESULT

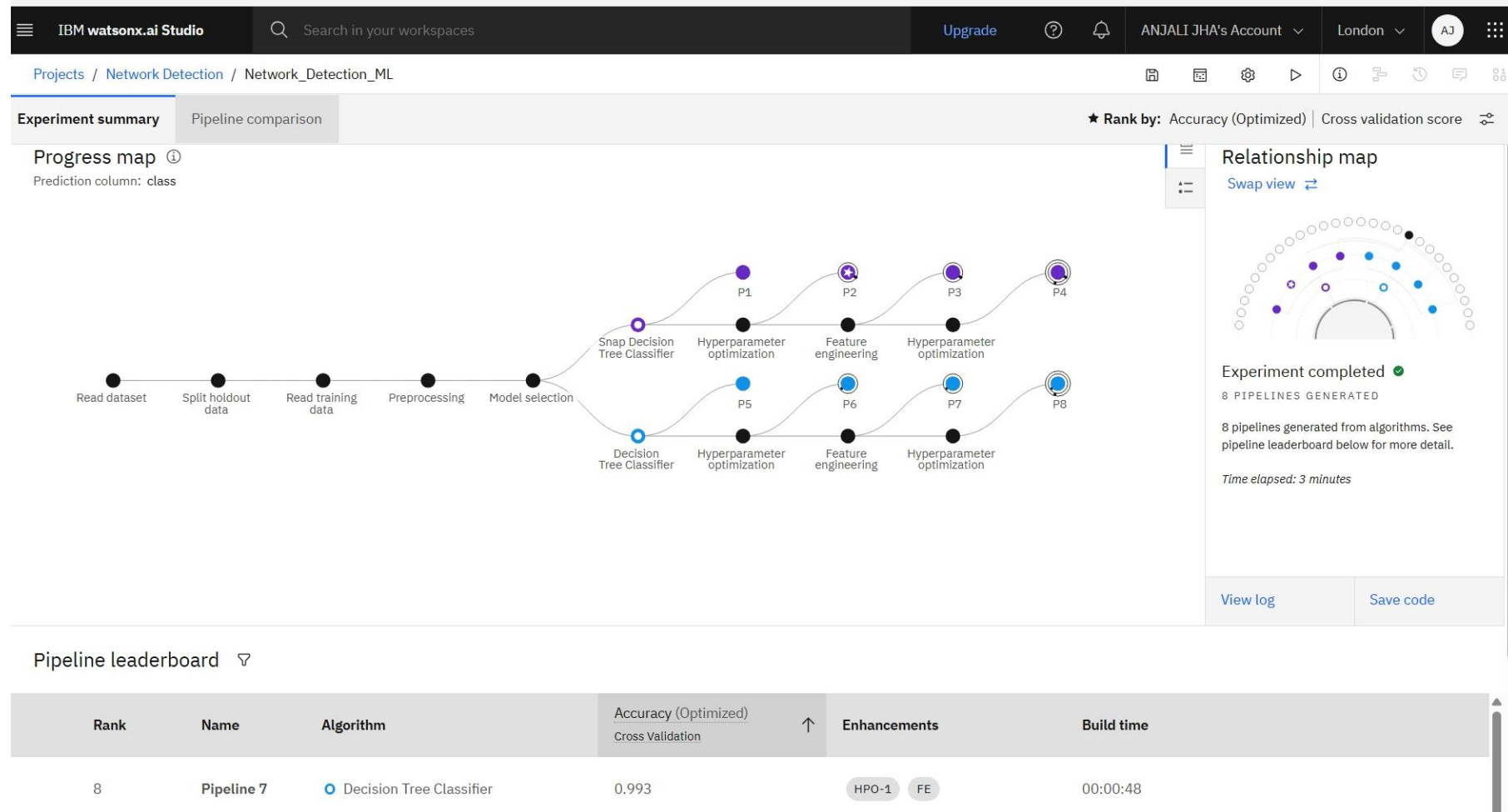




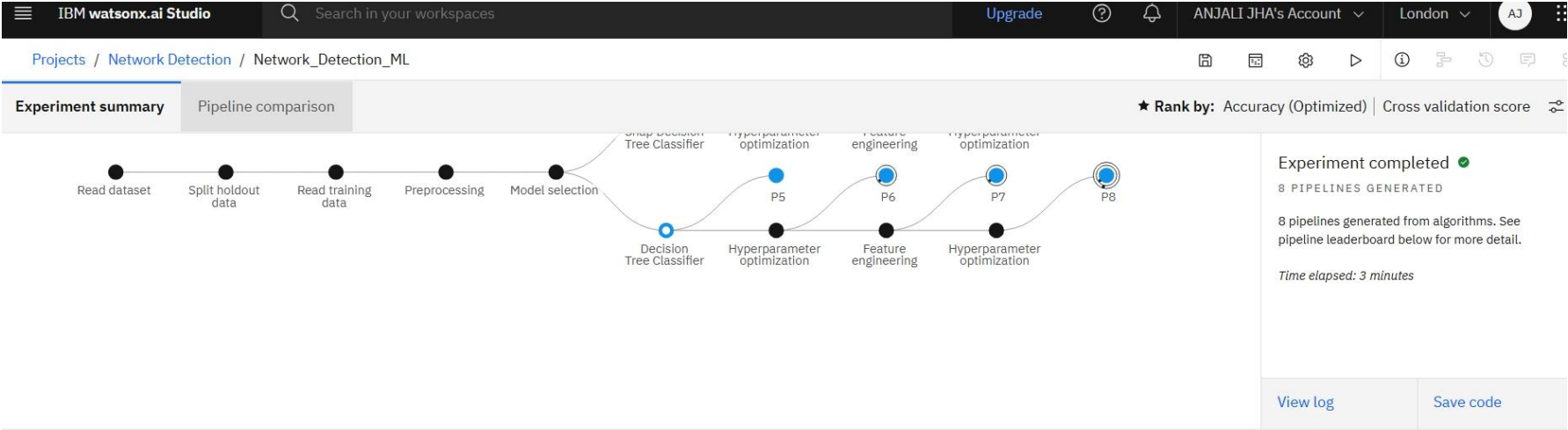
# RESULT



# RESULT



# RESULT



## Pipeline leaderboard

Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
4	Pipeline 5	Decision Tree Classifier	0.994	None	00:00:04
3	Pipeline 6	Decision Tree Classifier	0.994	HPO-1	00:00:09
2	Pipeline 1	Snap Decision Tree Classifier	0.995	None	00:00:07
★ 1	Pipeline 2	Snap Decision Tree Classifier	0.995	HPO-1	00:00:12

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

ANJALI JHA's Account

London

AJ

Projects / Network Detection / Network\_Detection\_ML

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\_Detection\_ML

Description (optional)

Model description

Tags

Add tags to make assets easier to find.

Add a tag

Cancel

Create

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

ANJALI JHA's Account

London

AJ

Projects / Network Detection / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML

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\_Detection\_ML

Description

No description provided.

Asset Details

Type: wml-hybrid\_0.1

Model ID: f278cb2b-7c4c-40...

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

50 seconds ago by ANJALI JHA

Created on

Aug 7, 2025 by ANJALI JHA

# RESULT

Projects / Network Detection / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML

## 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_Detecti...	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.

Close

✓ **Success**

Successfully promoted **P2 - Snap Decision Tree Classifier: Network\_Detection\_ML** to the deployment space. Go to the [deployment space](#) to prepare the assets for deployment.

Timestamp 10:34:11 PM

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

ANJALI JHA's Account

London

AJ

Deployment spaces /

Network\_Deploy

OverviewAssetsDeploymentsJobsManage

Space

General

Access control

Environments

Resource usage

Space GUID

0058ec4e-1280-49e0-b157-57f252714f96

Date created

Aug 7, 2025, 10:32 PM

by ANJALI JHA (You)

Last updated

Aug 7, 2025, 10:33 PM

Stage

Not provided

Stage type

Pre-production

Tags

No tags are set to this space.

Controls

Cloud Pak for Data platform

Switch platform

Reporting on asset metadata is allowed

Grant access

Opt-in to folders

Enable folders

Cloud Object Storage-cj

Bucket

6ad0a088-c5ed-4169-ab77-e1a74674aedd

Manage in IBM Cloud

watsonx.ai Runtime service

watsonx.ai Runtime-mj

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

?

ANJALI JHA's Account

London

AJ

Deployment spaces / Network\_Deploy / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML

Depl

Filter

Name

Item

Create a deployment

Define details

Associated asset

P2 - Snap Decision Tree Classifier: Network\_Detection\_ML

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\_Deployment2

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

Cancel

Create

edunet

foundation



# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

ANJALI JHA's Account

London

AJ

[Deployment spaces](#) / [Network\\_Deploy](#) / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML

Deployments

Model details

Search

New deployment

Name	Type	Status	Tags	Last modified	
<div><div></div><div>Network_Deployment2</div></div>	Online	<div></div> Initializing		4 seconds ago ANJALI JHA (You)	<div></div>

Items per page: 20

1-1 of 1 items

1 of 1 pages

About this asset

Name

P2 - Snap Decision Tree Classifier:  
Network\_Detection\_ML

Description

No description provided.

Asset Details

Type: wml-hybrid\_0.1

Model ID: 21b7b6a9-20c6-4e...

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  
6 minutes ago by ANJALI JHA

Created on  
Aug 7, 2025 by ANJALI JHA

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

ANJALI JHA's Account

London

AJ

Deployment spaces / Network\_Deploy / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML /

Network\_Deployment2

Deployed Online

API reference

Test

Endpoints for scoring

Private endpoint

https://private.eu-gb.ml.cloud.ibm.com/ml/v4/deployments/190fe2ca-57be-4210-8de3-82f5de12bf02/predictions?version=2021-05-01

Public endpoint

https://eu-gb.ml.cloud.ibm.com/ml/v4/deployments/190fe2ca-57be-4210-8de3-82f5de12bf02/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
```

About this deployment

Name

Network\_Deployment2

Description

No description provided.

Deployment Details

Deployment ID: 190fe2ca-57be-42...

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...

21b7b6a9-20c6-4eff-b1cf-f56f821ffda3

Last modified

60 seconds ago

Created on

Aug 7, 2025

# RESULT

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

ANJALI JHA's Account

London

AJ

Deployment spaces / Network\_Deploy / P2 - Snap Decision Tree Classifier: Network\_Detection\_ML /

Network\_Deployment2 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.

Download CSV template

Browse local files

Search in space

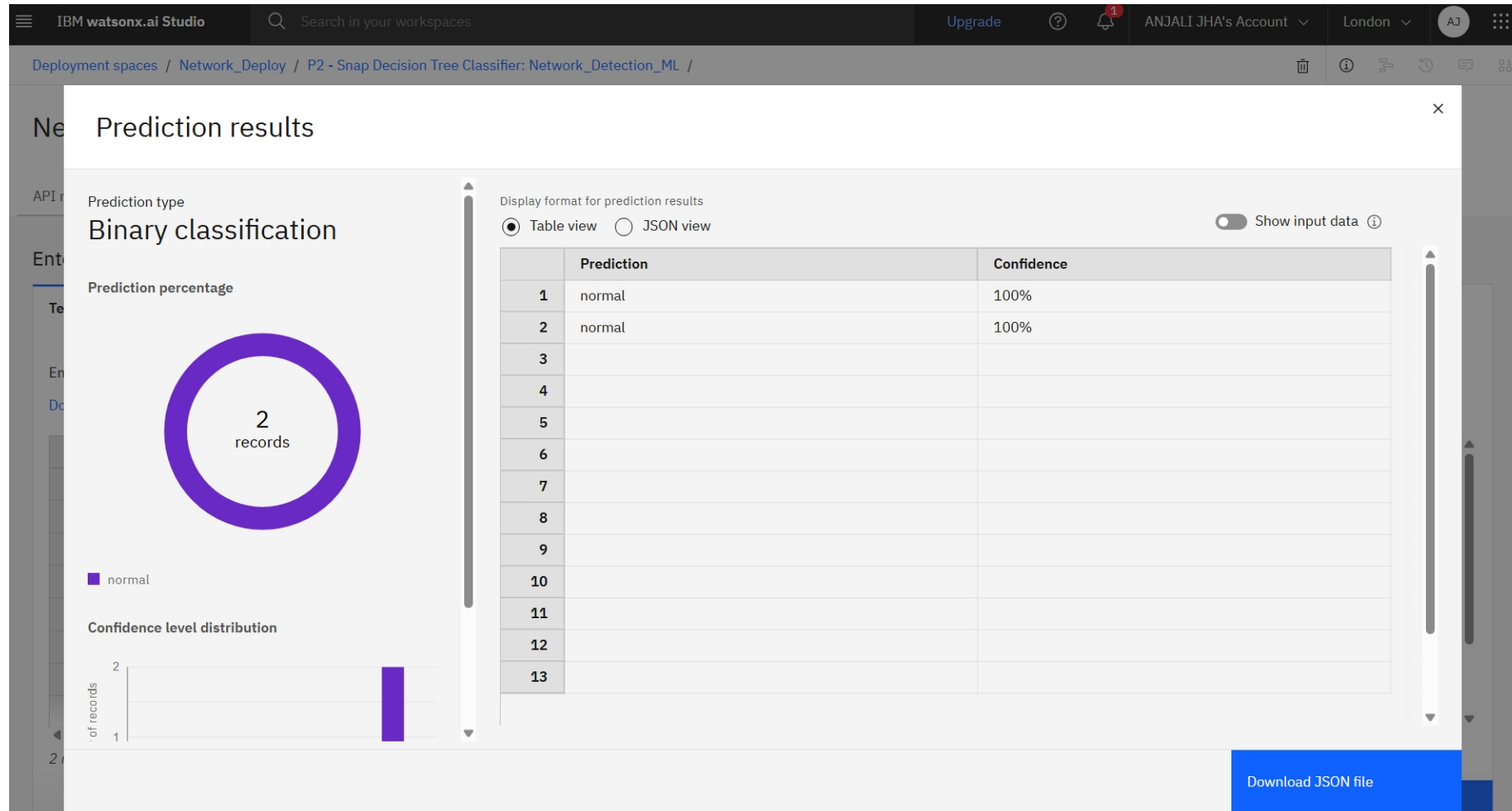
Clear all

	duration (double)	protocol_type (other)	service (other)	flag (other)	src_bytes (double)	dst_bytes (double)	land (double)	wrong_fragment (double)	urgent (double)	h...
1	0	udp	other	SF	146	0	0	0	0	0
2	5706	tcp	http	SO	255	0	0	1	1	0
3										
4										
5										
6										
7										
8										

2 rows, 41 columns

Predict

# RESULT



# CONCLUSION

- The proposed Network Intrusion Detection System successfully demonstrates the potential of machine learning in enhancing cybersecurity by accurately identifying various types of network intrusions such as DoS, Probe, R2L, and U2R attacks. By leveraging labeled datasets and integrating IBM Cloud Lite services with ML models, the solution achieves a high detection rate while minimizing false positives.

# FUTURE SCOPE

- Network Intrusion Detection Systems are evolving with AI and deep learning to detect complex and unknown threats more accurately. Cloud-native and edge-based IDS models are enabling real-time monitoring across hybrid environments and IoT devices. Privacy-focused approaches like federated learning are enhancing data security. Future IDS will also support compliance with global cybersecurity standards. With tools like IBM Watsonx . Ai studio, this field offers strong potential for innovation and career growth.

# REFERENCES

- Use of IBM cloud lite services
- course like : journey to Cloud: Envisioning Your Solution, Getting Started with Artificial Intelligence, Rag Lab
- Kaggle dataset

# IBM CERTIFICATIONS





# IBM CERTIFICATIONS

In recognition of the commitment to achieve  
professional excellence



Anjali Jha

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution



Issued on: Jul 21, 2025  
Issued by: IBM SkillsBuild

Verify: <https://www.credly.com/badges/d9141447-7963-4cee-81ae-870458b44663>



# IBM CERTIFICATIONS





**THANK YOU**