# 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)

edunet foundation

# 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

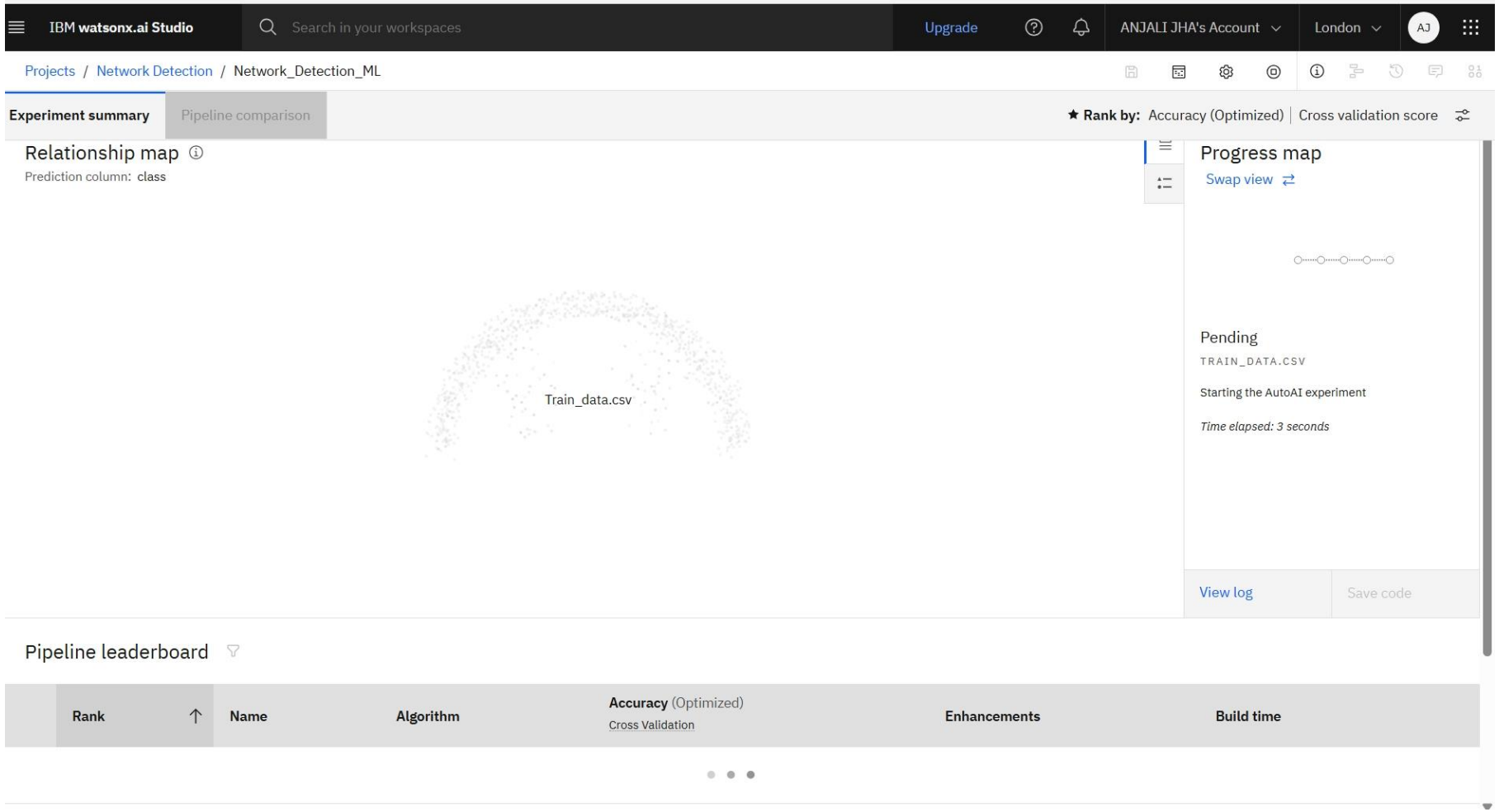
The "System Approach" section outlines the overall strategy and methodology for developing and implementing the Network Intrusion Detection prediction system. Here's a suggested structure for this section:

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

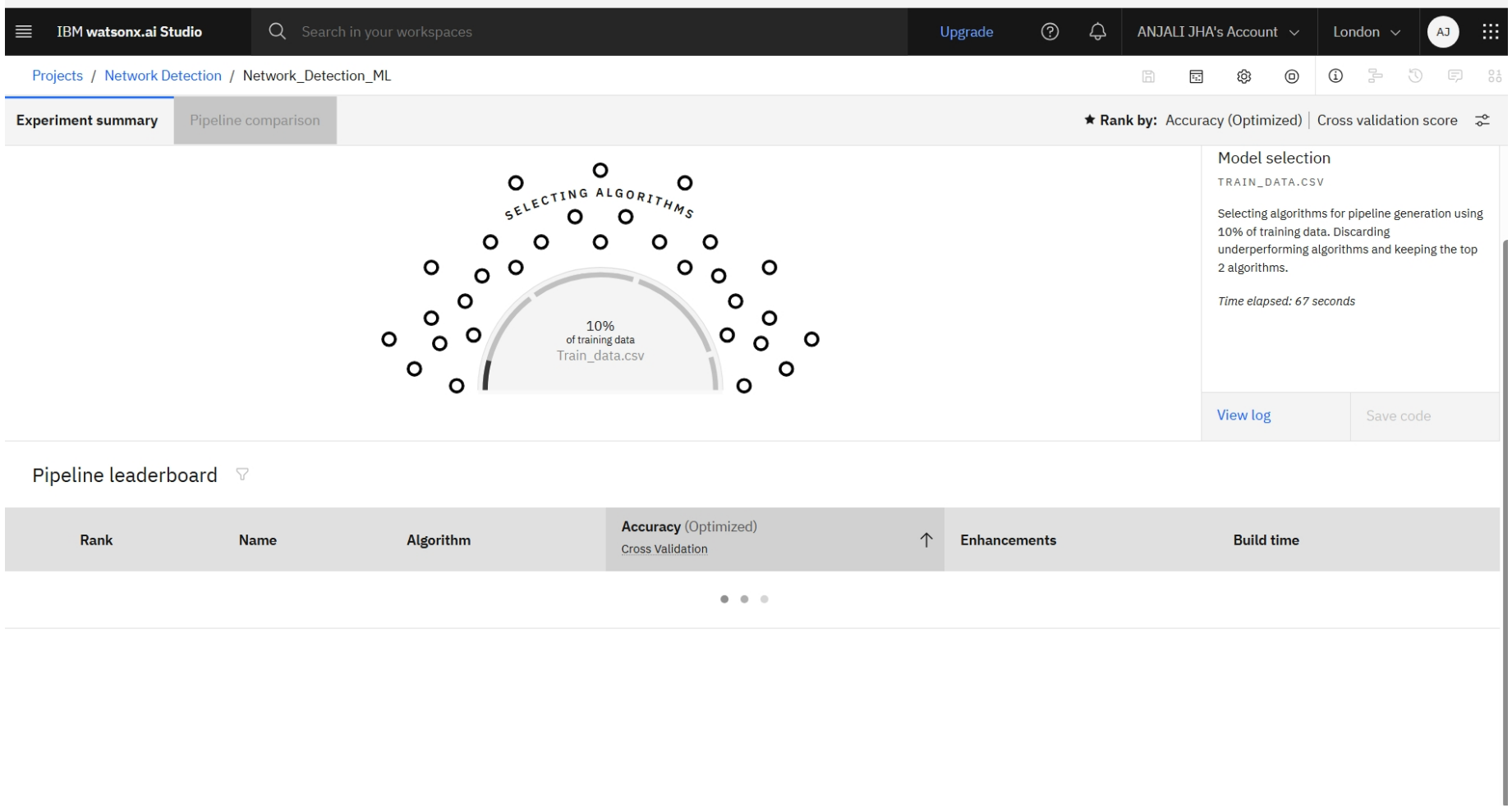
# ALGORITHM & DEPLOYMENT

- 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

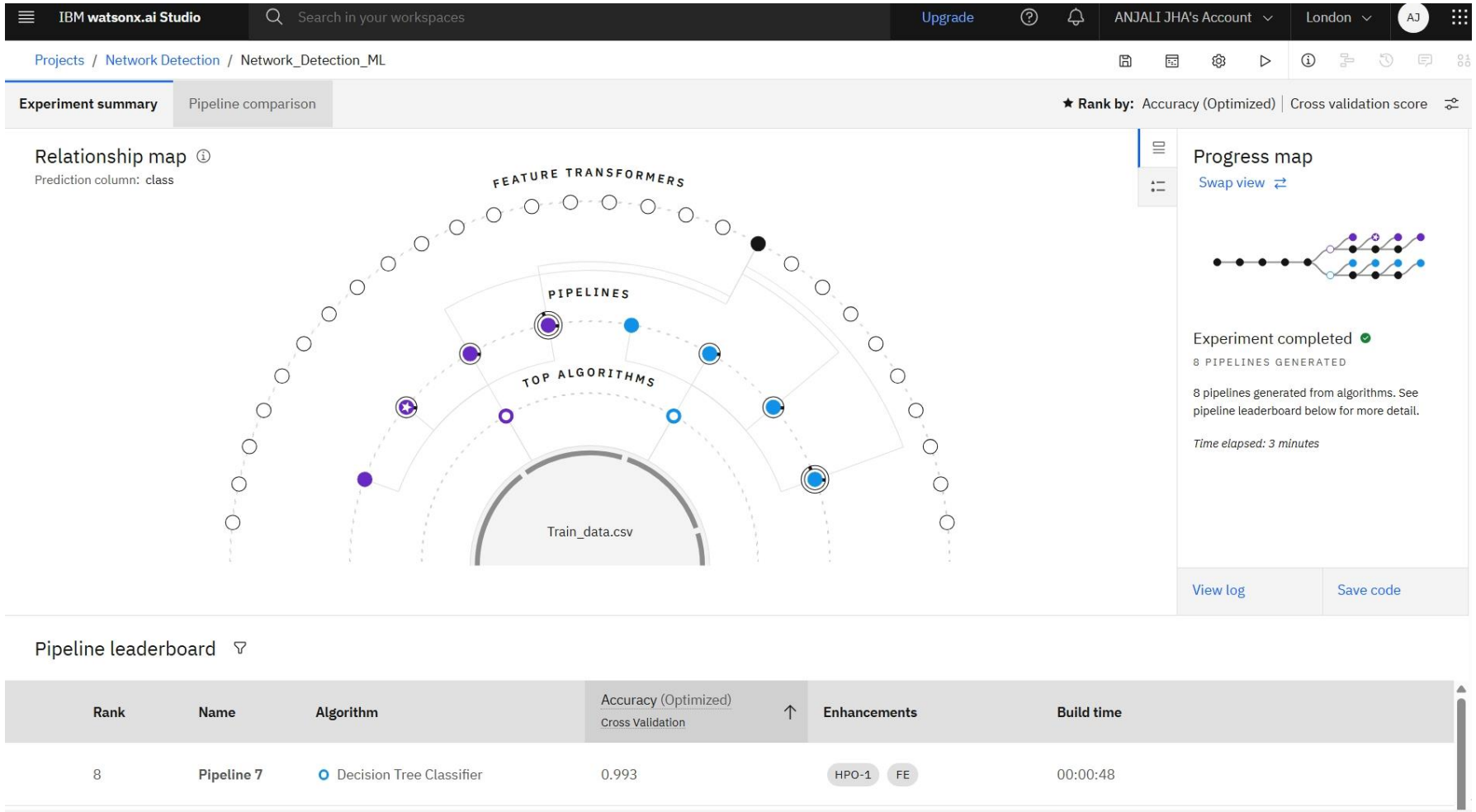


# RESULT

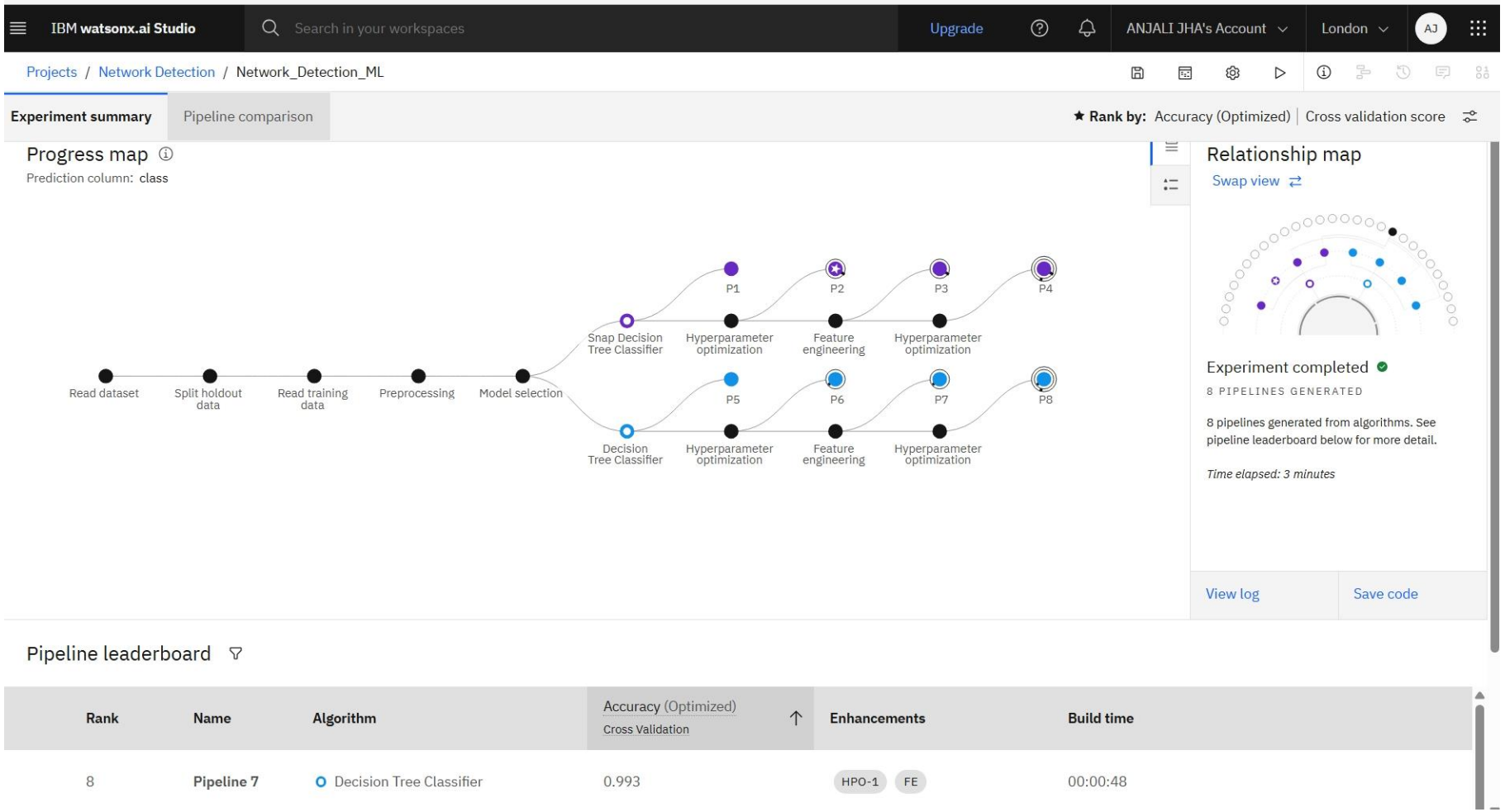



edunet foundation

# RESULT

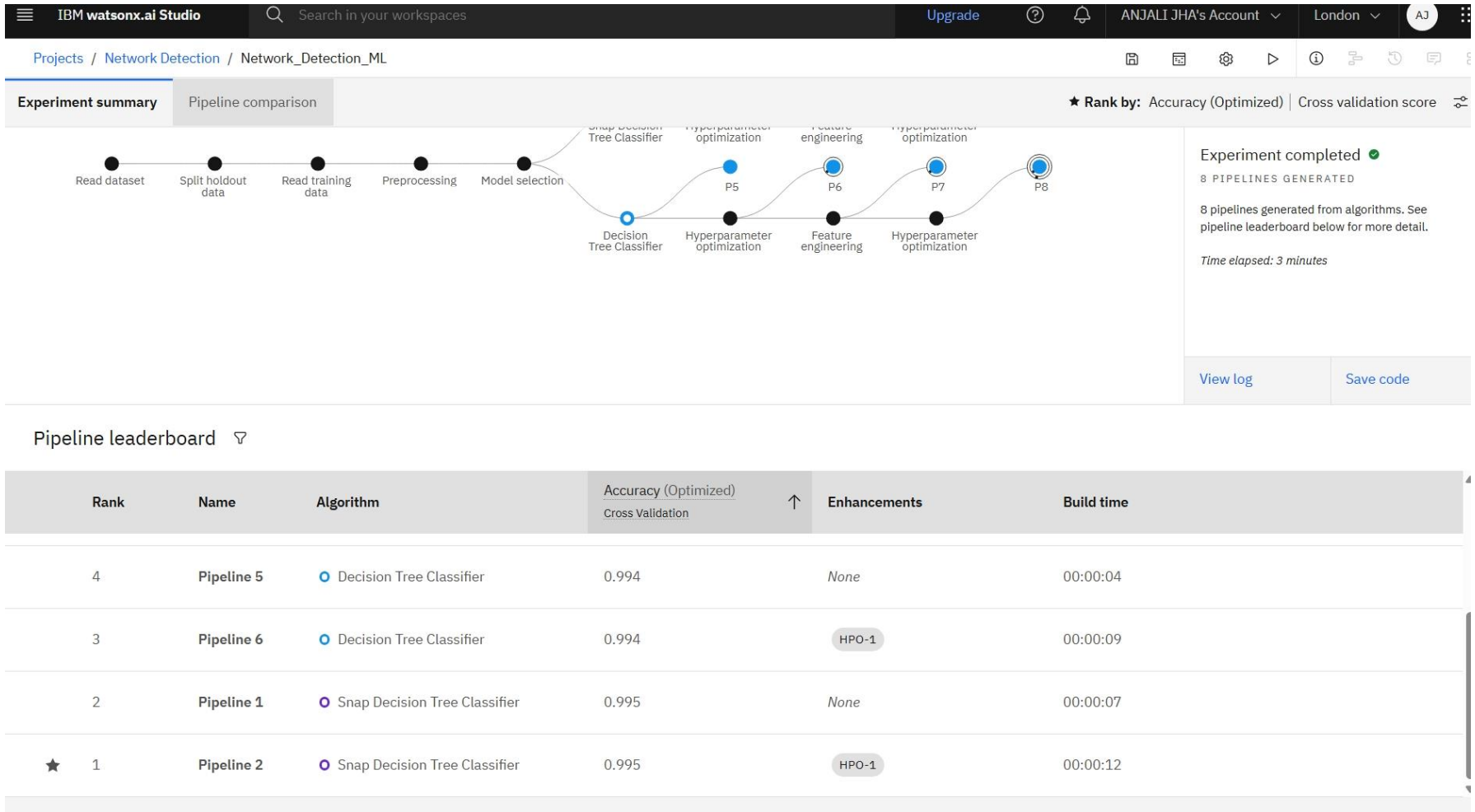


# RESULT



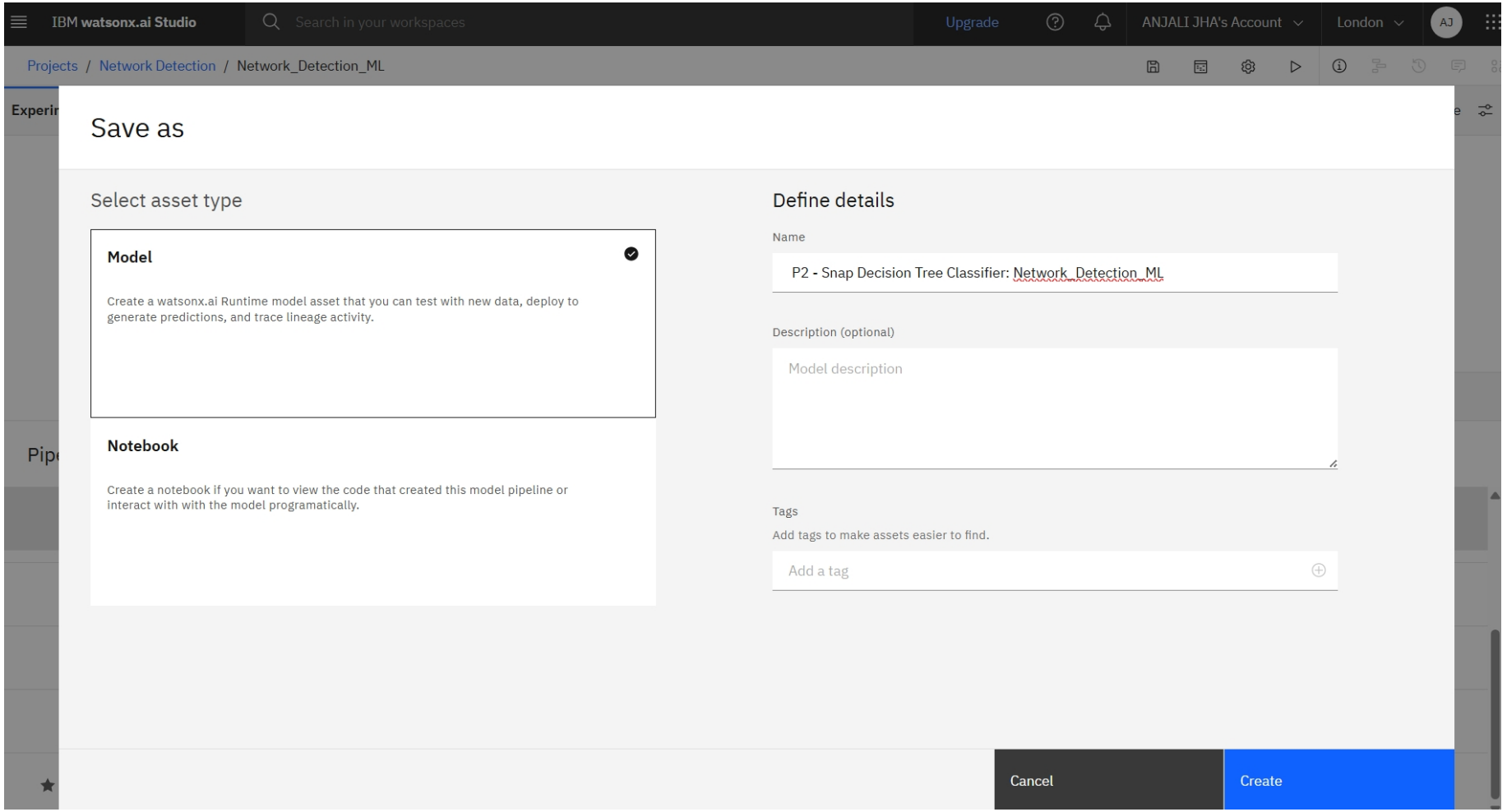

edunet foundation

# RESULT



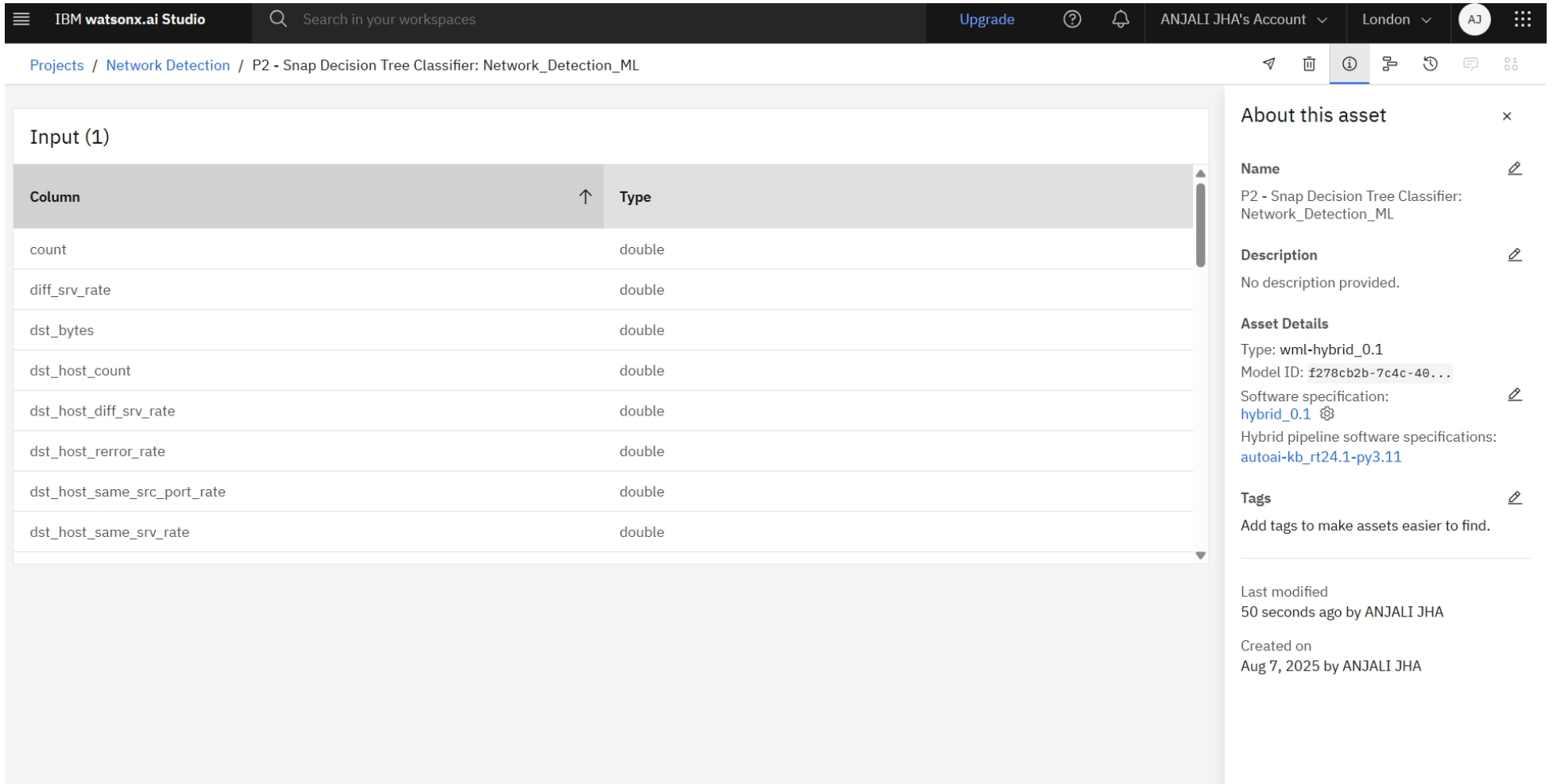

edunet foundation

# RESULT

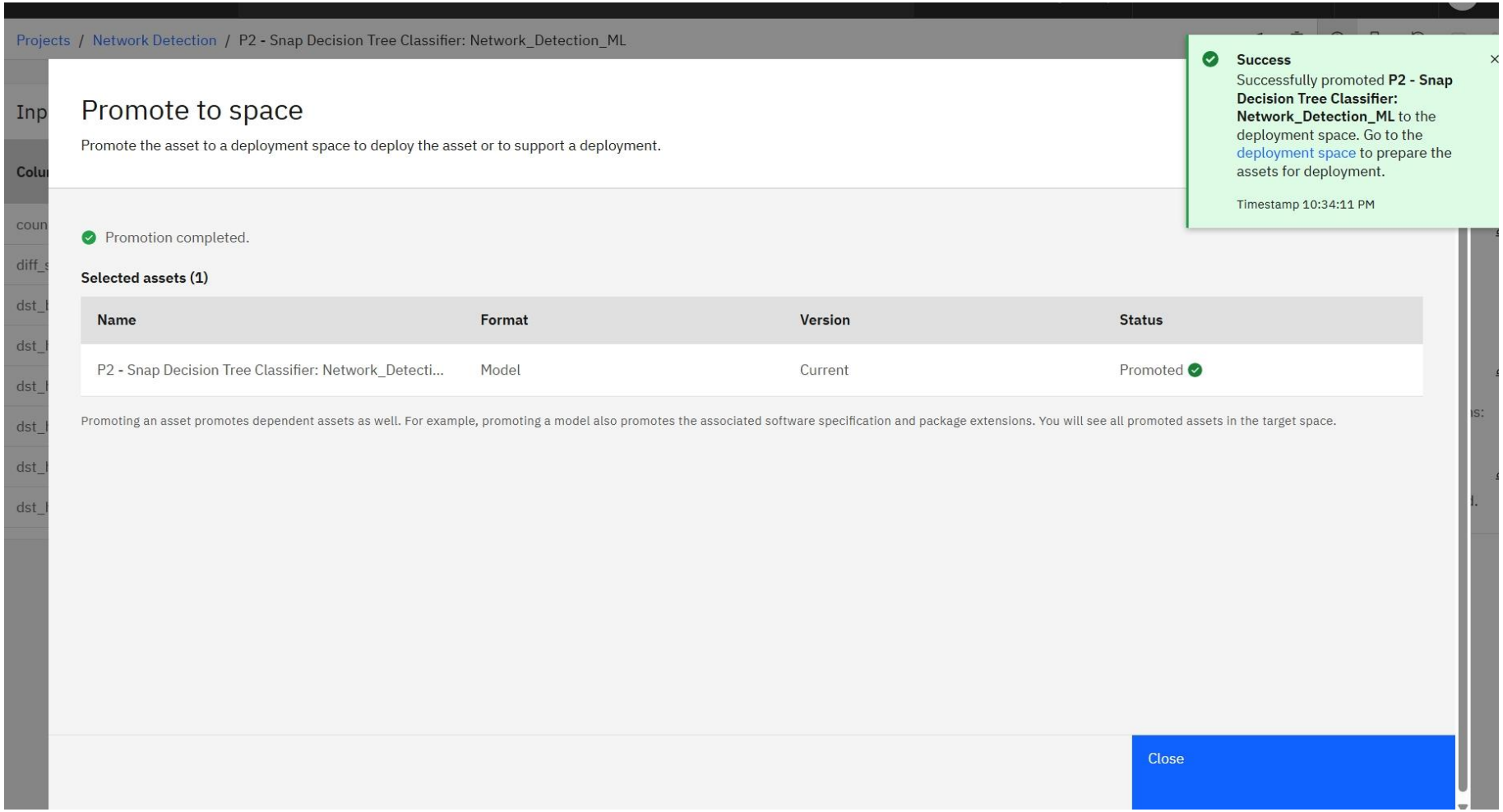



edunet foundation

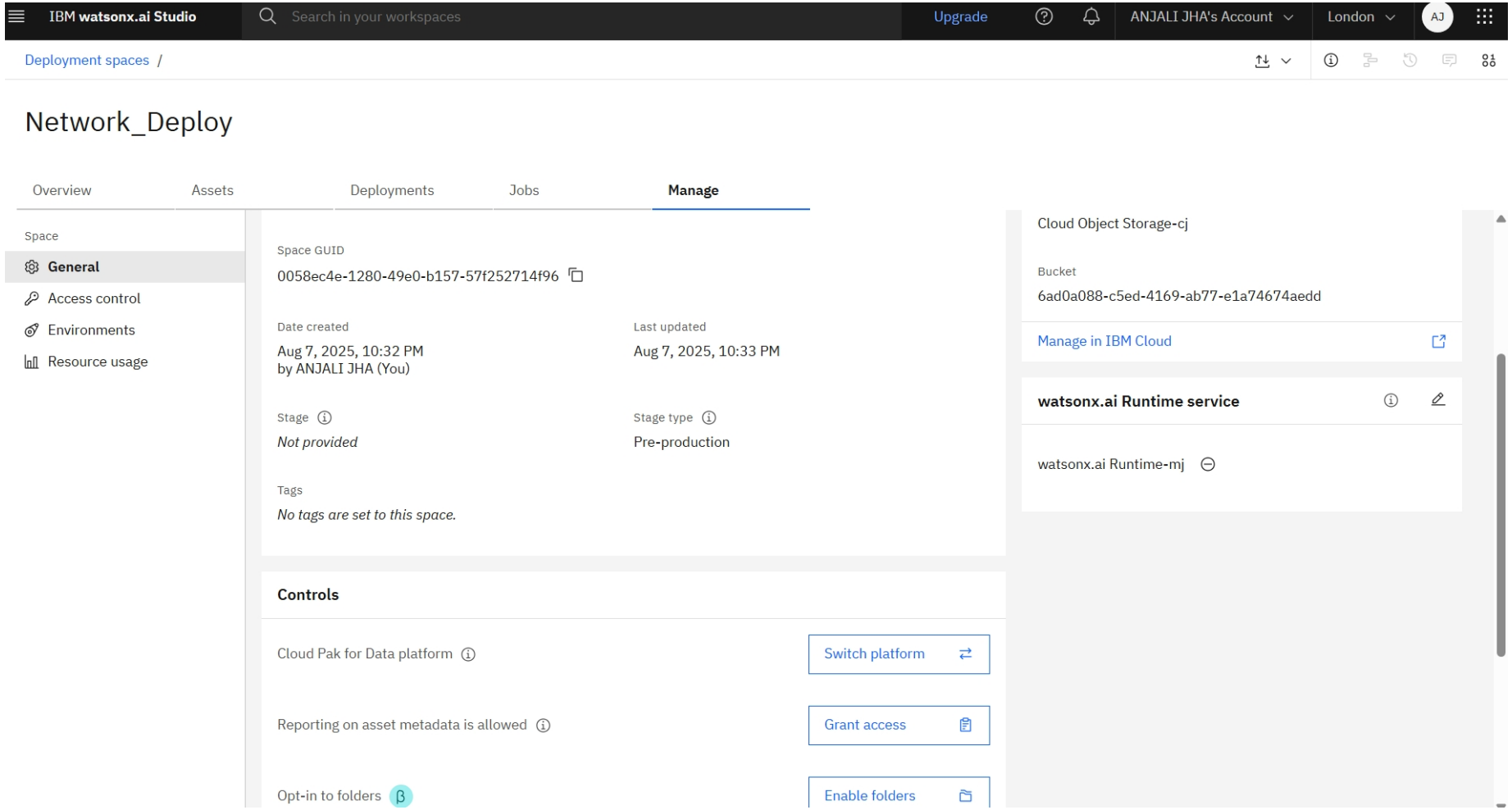
# RESULT



# RESULT

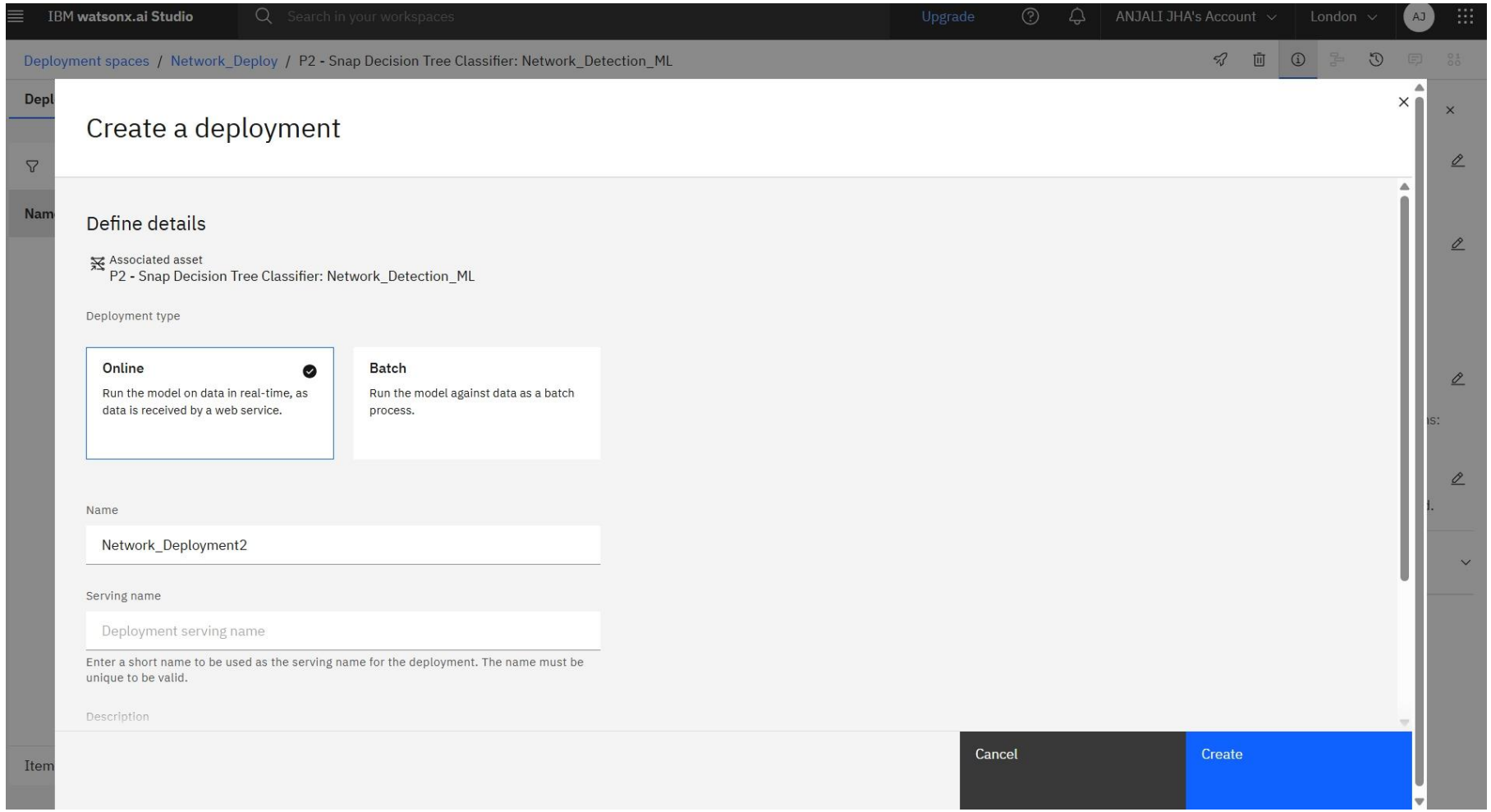


# RESULT

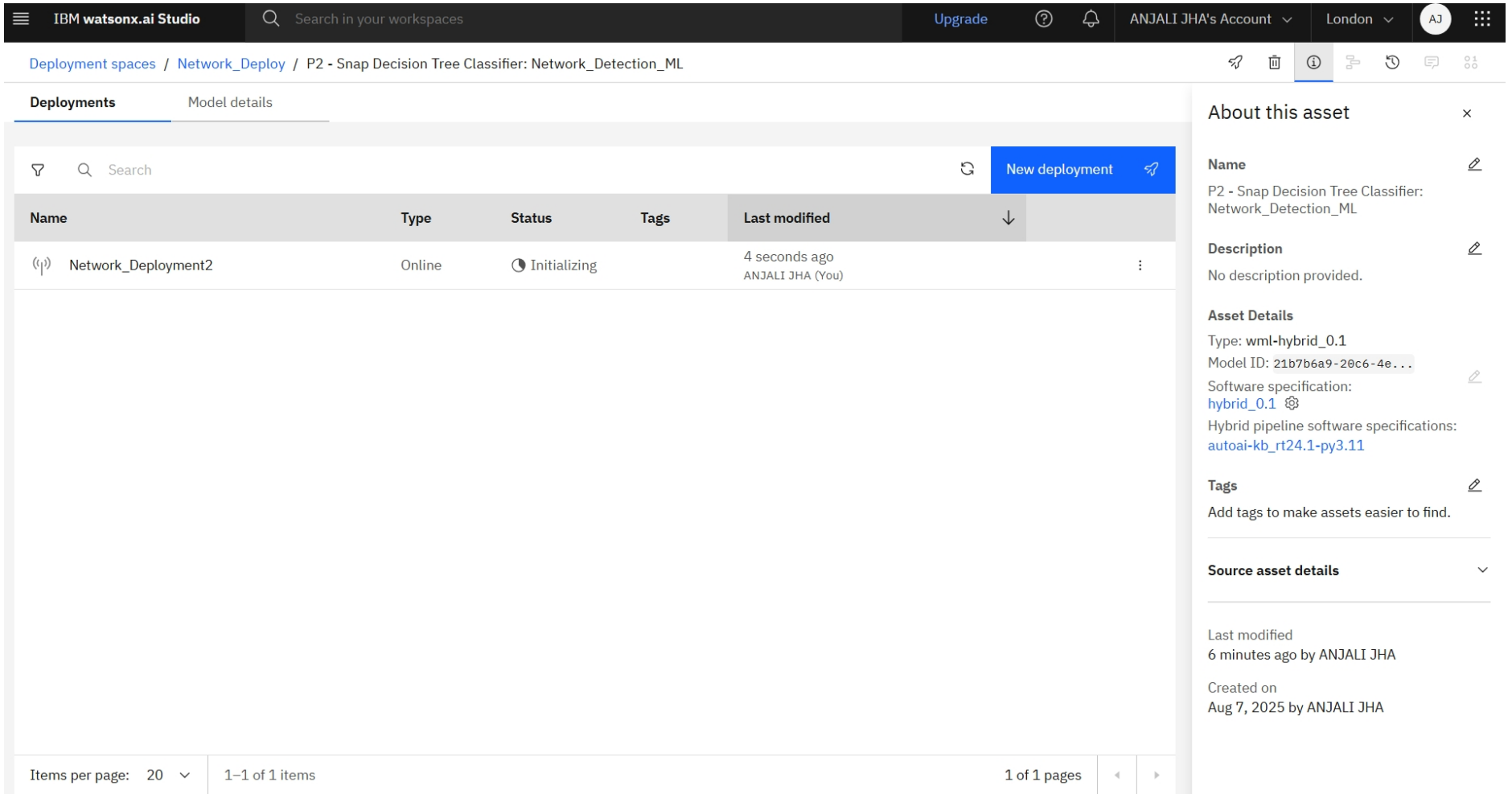



edunet foundation

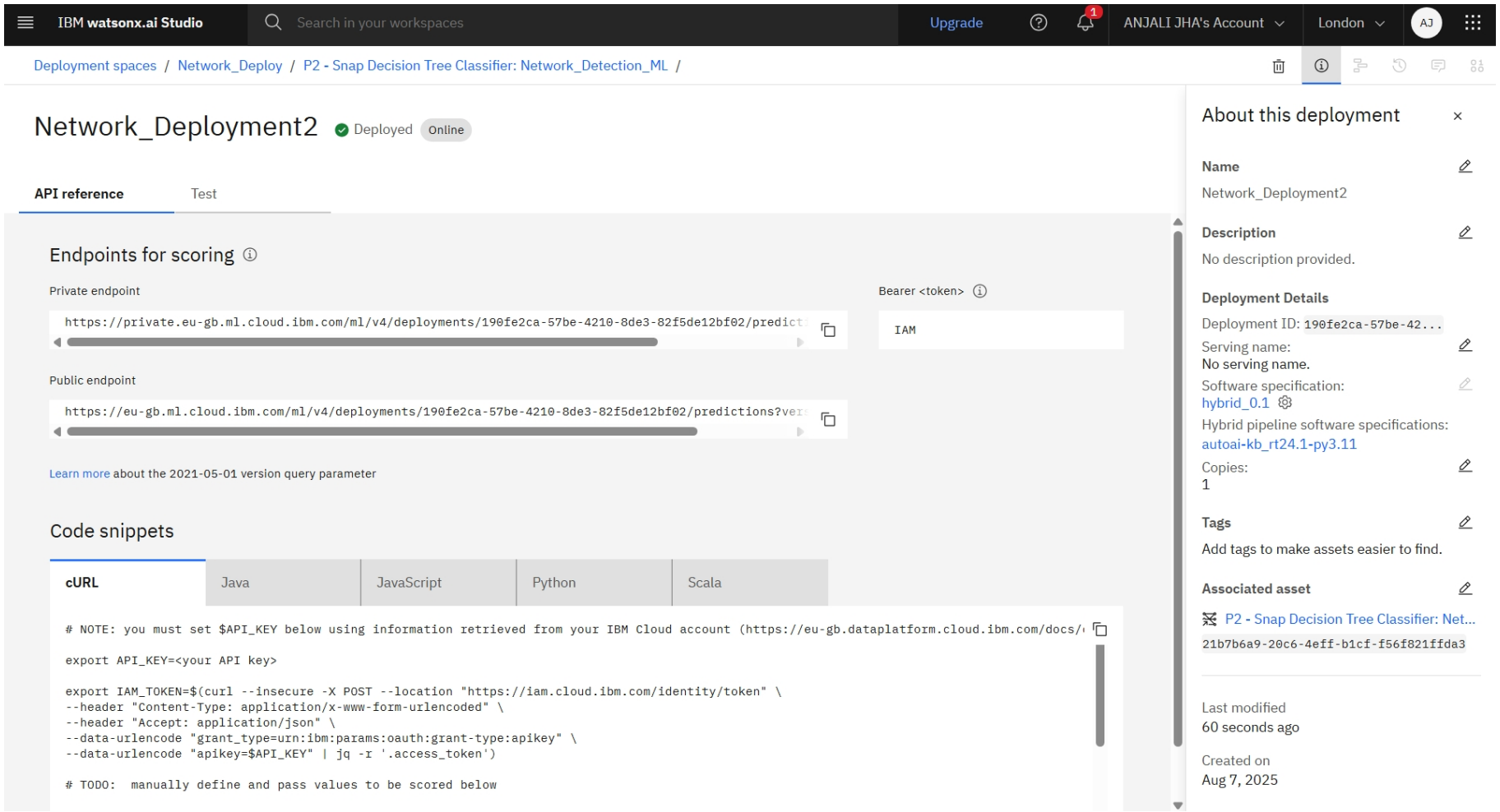
# RESULT


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
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

# RESULT

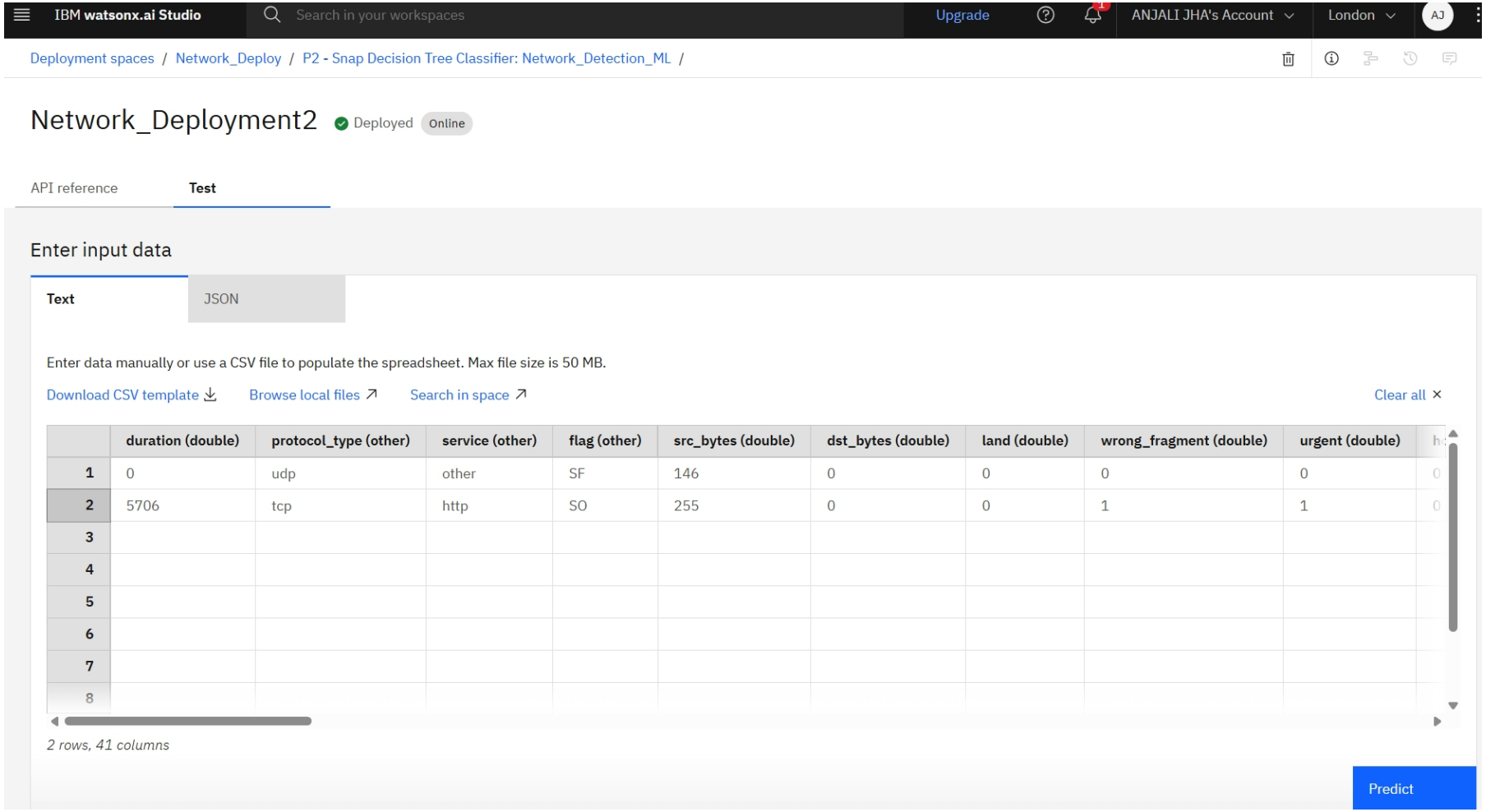


# RESULT



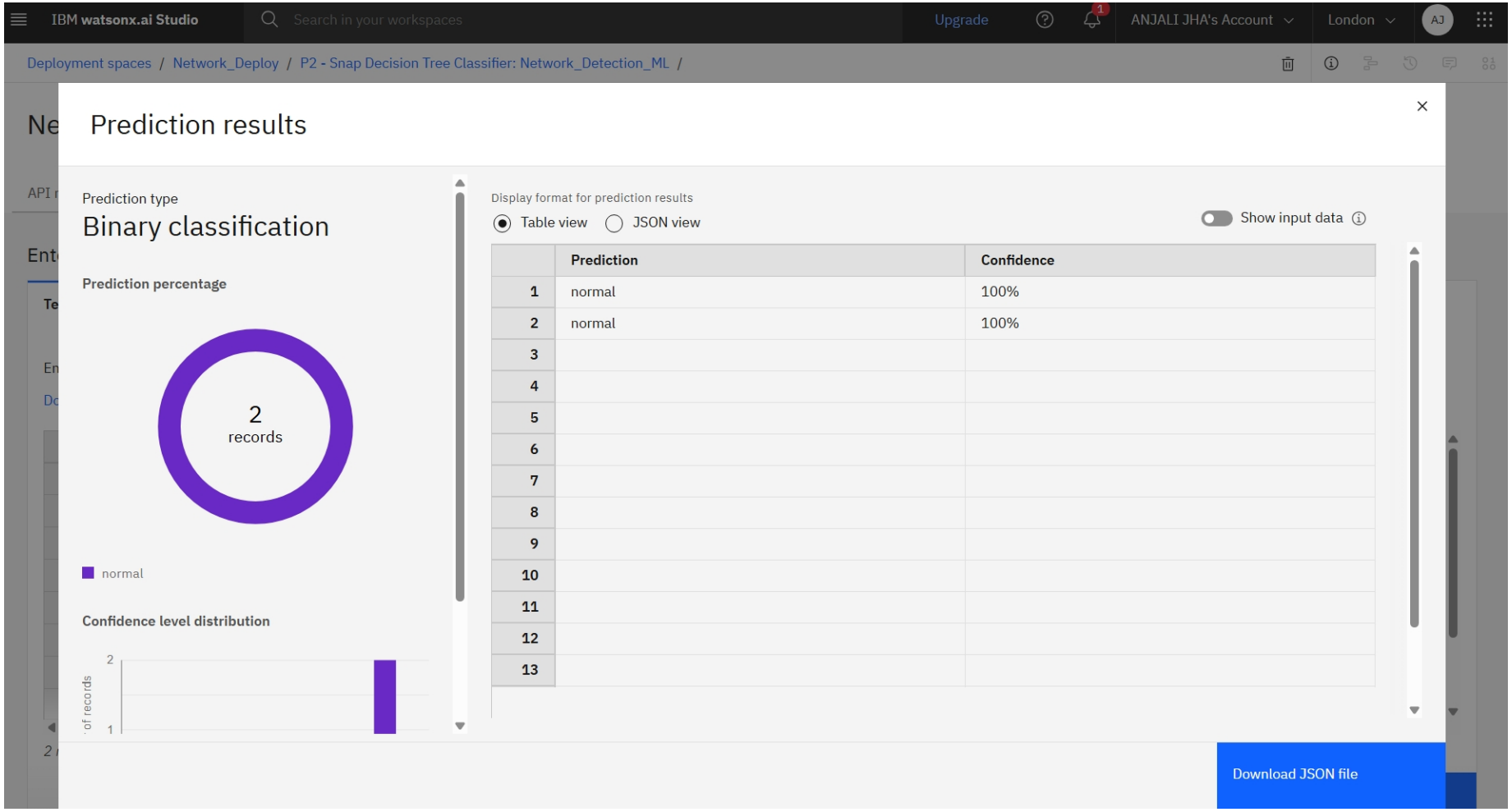

edunet foundation

# RESULT




edunet foundation

# RESULT




edunet foundation

# 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.

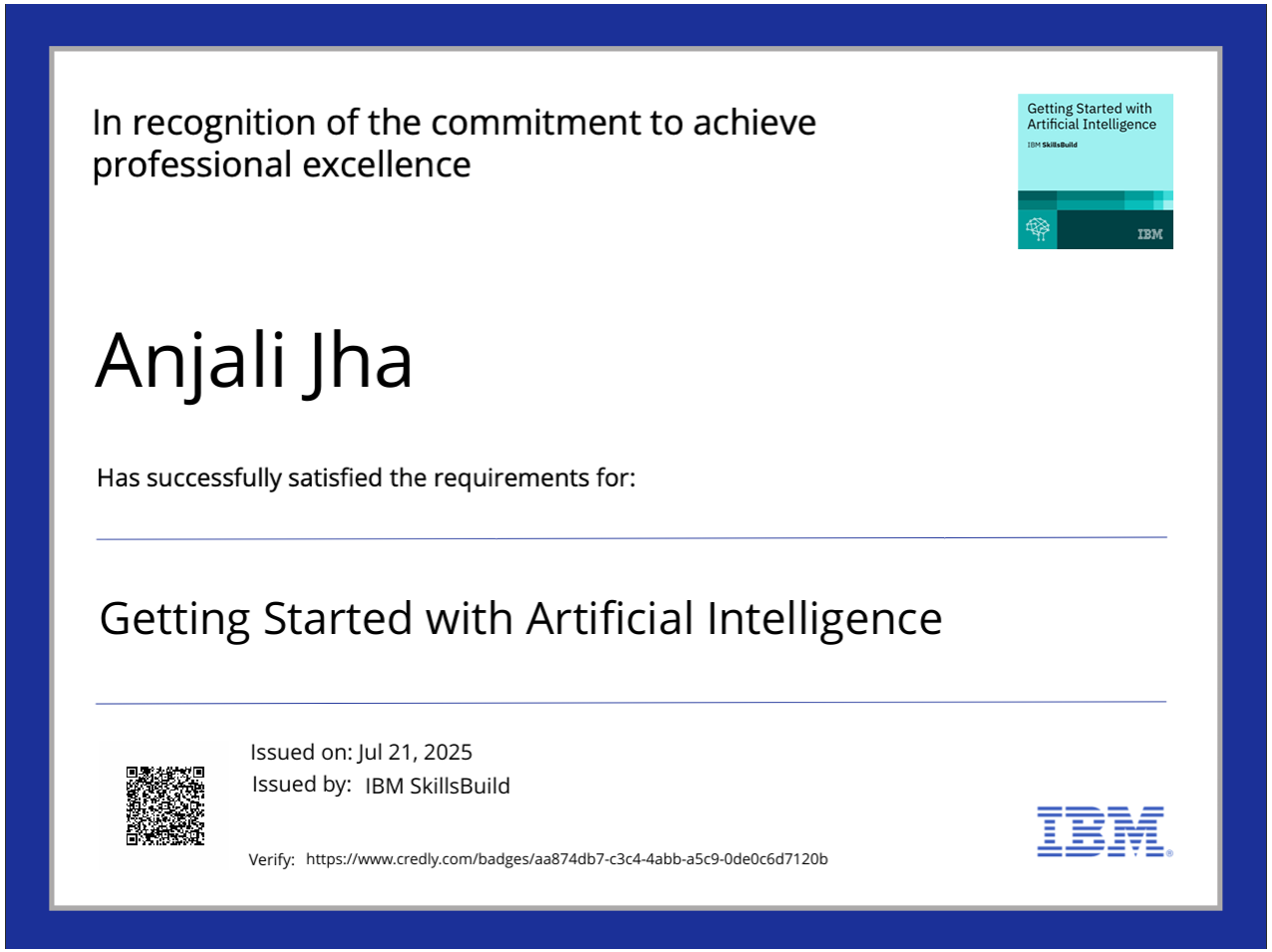
# FUTURE SCOPE

- 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



In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence
IBM SkillsBuild

IBM

Anjali Jha

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

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

Verify: https://www.credly.com/badges/aa874db7-c3c4-4abb-a5c9-0de0c6d7120b

IBM

# IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution
IBM SkillsBuild

IBM

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

# IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Anjali Jha

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

edunet foundation

# THANK YOU

edunet foundation