CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
Student Name- Maanvi Gupta
College Name- Chandigarh University
Department-Computer Science and Engineering

OUTLINE

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

PROBLEM STATEMENT

With the growing complexity and scale of communication networks, organizations face an increasing number of cyber threats that can compromise data, disrupt services, and cause severe financial losses. Traditional rule-based intrusion detection systems are often unable to adapt to new or unknown attack patterns and may result in high false positive or false negative rates.

The problem lies in the inability of conventional systems to intelligently analyze and differentiate between normal network behavior and various types of attacks such as Denial of Service (DoS), Probe, Remote to Local (R2L), and User to Root (U2R). As cyber-attacks evolve in sophistication, there is a critical need for a more dynamic and accurate solution.

This project addresses the challenge of designing an intelligent Network Intrusion Detection System (NIDS) that uses machine learning to detect malicious activities in real time. The aim is to develop a system capable of early detection and classification of intrusions based on traffic data, helping secure networks from potential threats.

PROPOSED SOLUTION

The solution is designed to tackle the problem of accurately detecting and categorizing network intrusions using machine learning. The system is developed through the following components:

1. Data Collection:

Utilized the Network Intrusion Detection dataset from Kaggle containing labeled traffic data for both normal and malicious network behavior.

2. Data Preprocessing:

Converted categorical features (e.g., protocol_type, service) to numerical using encoding, handled null values, and scaled numerical data.

3. Feature Engineering:

Selected important network features contributing to anomaly detection, and reduced dimensionality to improve model efficiency.

4. Model Building:

Trained classification algorithms (Random Forest, Decision Tree, etc.) using supervised learning to distinguish between different traffic classes.

PROPOSED SOLUTION CONTINUED...

5. **Deployment**:

Integrated the model with IBM Watsonx.ai Studio using IBM Cloud Lite. Model deployed through AutoAI to allow real-time predictions.

6. Evaluation:

Assessed model performance using metrics such as accuracy, precision, recall, F1-score, and confusion matrix.

SYSTEM APPROACH

System Requirements:

1. IBM Cloud Lite account
2. Watsonx.ai Runtime
3. Jupyter Notebook or AutoAI interface

Libraries Used:

1. Pandas, NumPy for data processing
2. Scikit-learn for machine learning
3. Matplotlib & Seaborn for visualization
4. Joblib for model saving
5. IBM Watsonx.ai Studio for deployment

ALGORITHM & DEPLOYMENT

Algorithm Used: Random Forest Classifier

Algorithm Selection:The algorithm was selected using IBM AutoAI, which automatically trained multiple models and compared their performance. Random Forest achieved the highest accuracy and was chosen as the final model for deployment.

Data Input: Features include 41 network attributes like duration, src_bytes, dst_bytes, etc. from Train.csv

Target column: class (normal/anomaly)

Training Process:

- Data split into training and test sets
- Encoded & scaled features
- Hyperparameter tuning with grid search

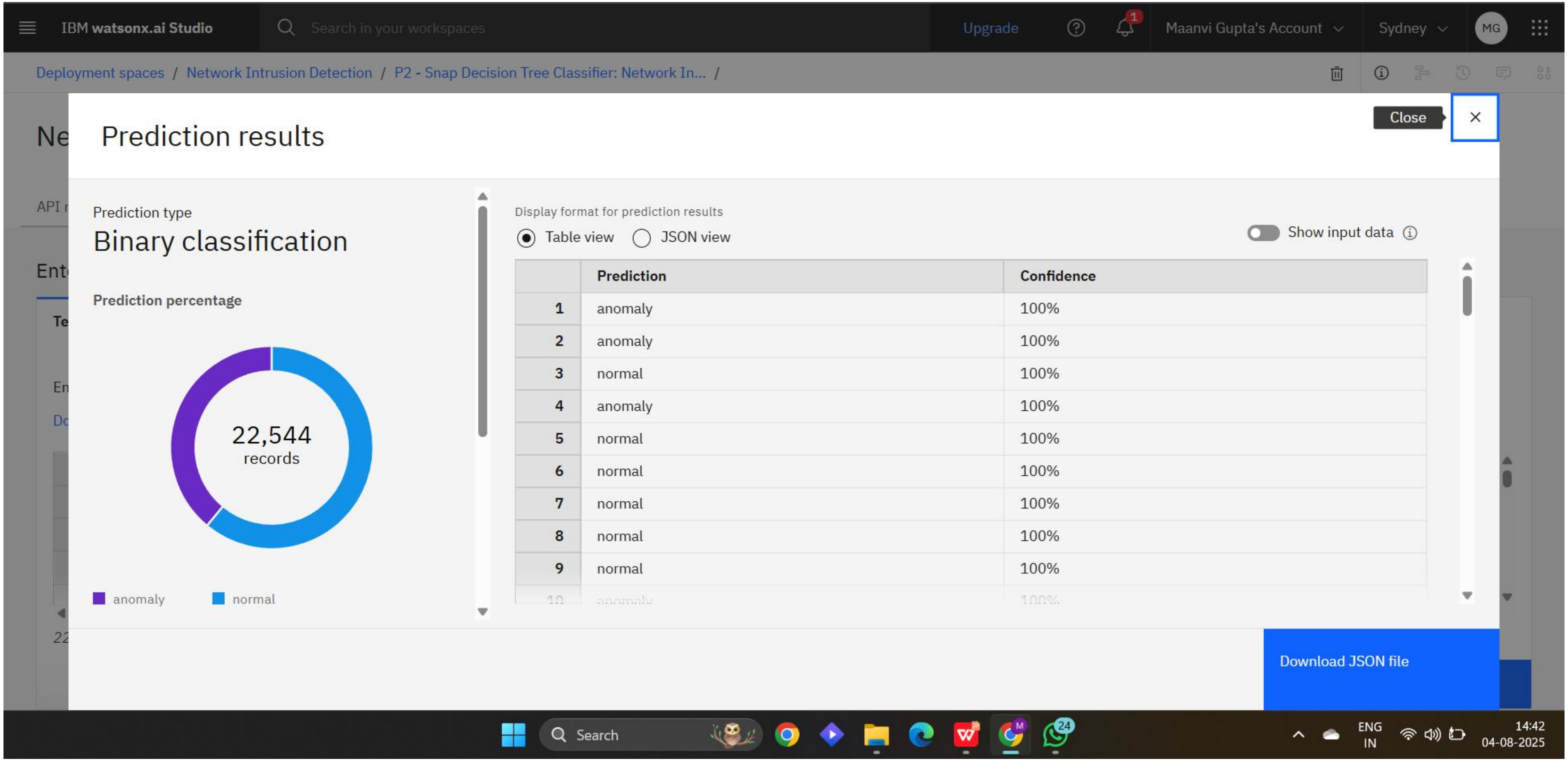
Prediction & Deployment:

Trained model uploaded and deployed using Watsonx.ai AutoAI and deployment through REST API for live traffic classification on IBM Cloud

RESULT

- Successfully trained a model to classify network traffic into "normal" and "anomaly"
- Achieved high accuracy (~95–98%) depending on the algorithm
- Sample Output: Confusion matrix showing true positives, false positives, etc.
- Visuals: Accuracy chart, Precision-Recall graph

RESULT SCREENSHOTS



IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Maanvi Gupta's Account
Sydney
MG
Deployment spaces / Network Intrusion Detection / P2 - Snap Decision Tree Classifier: Network In... /
Close
Download JSON file
Search
ENG
IN
14:42
04-08-2025

Prediction results

Prediction type

Binary classification

Prediction percentage

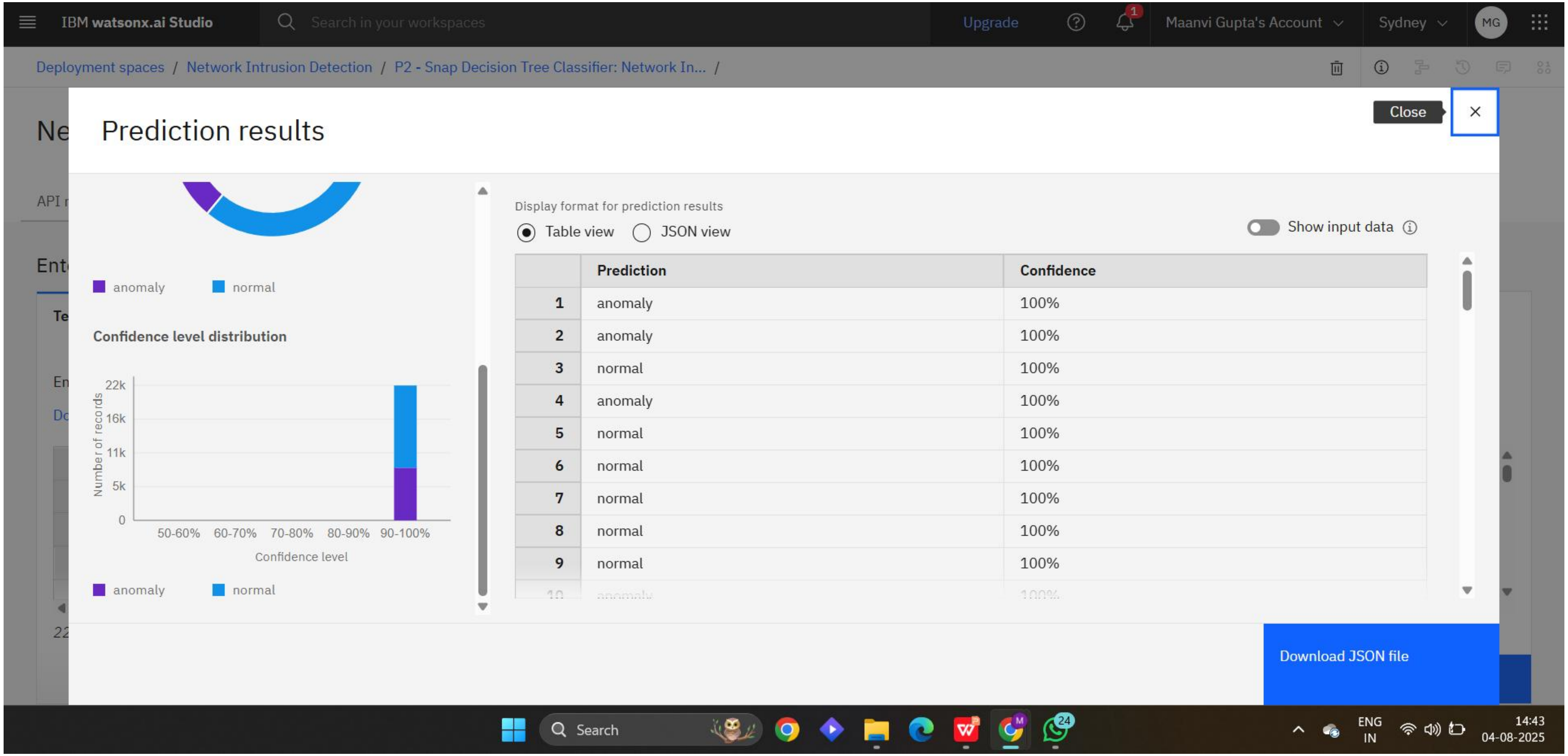
Display format for prediction results

● Table view ○ JSON view

Show input data

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

RESULT SCREENSHOTS



Prediction results

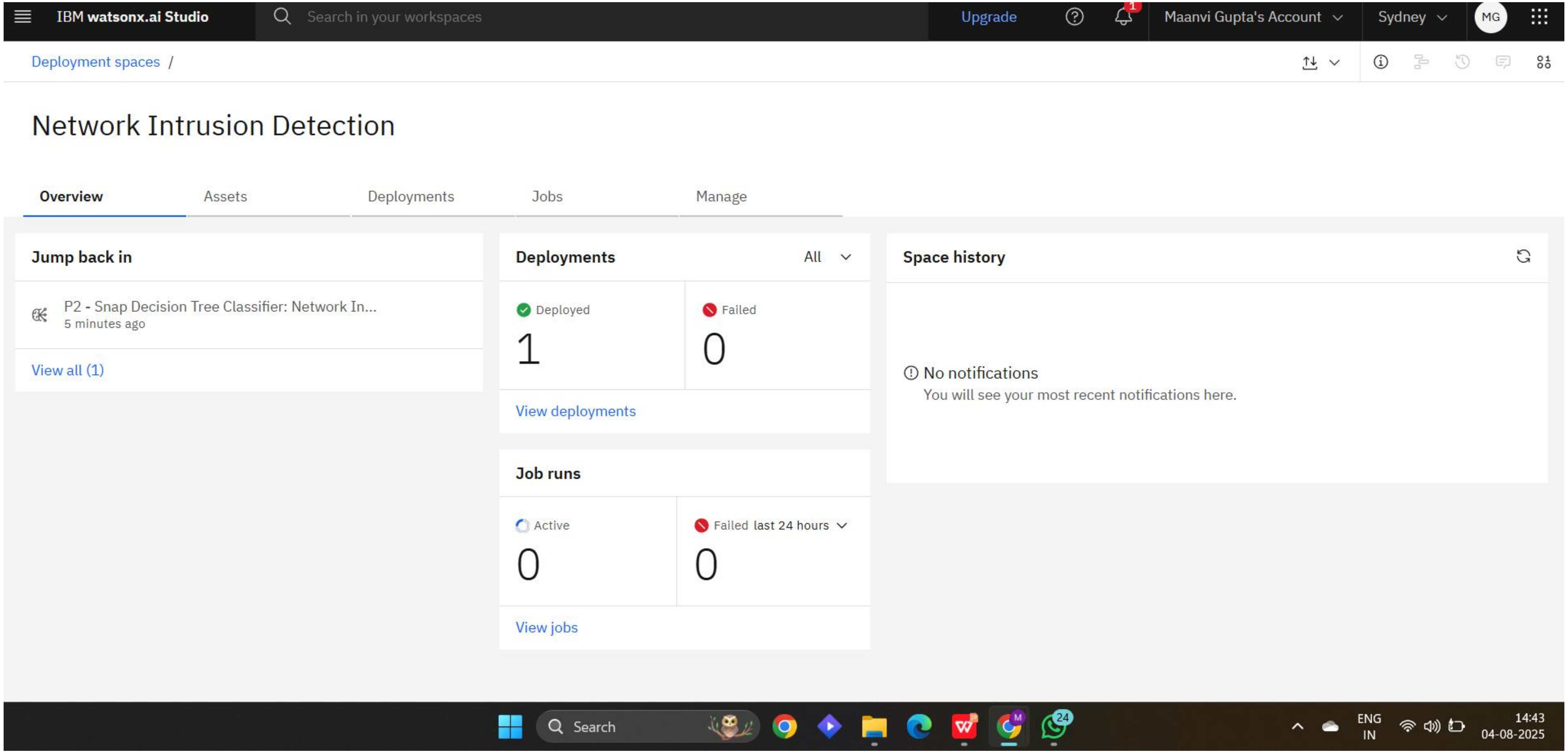
Display format for prediction results

● Table view ○ JSON view

Show input data

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

RESULT SCREENSHOTS



Network Intrusion Detection

Jump back in

P2 - Snap Decision Tree Classifier: Network In...
5 minutes ago

View all (1)

Deployments All

Deployed	Failed
1	0

View deployments

Job runs

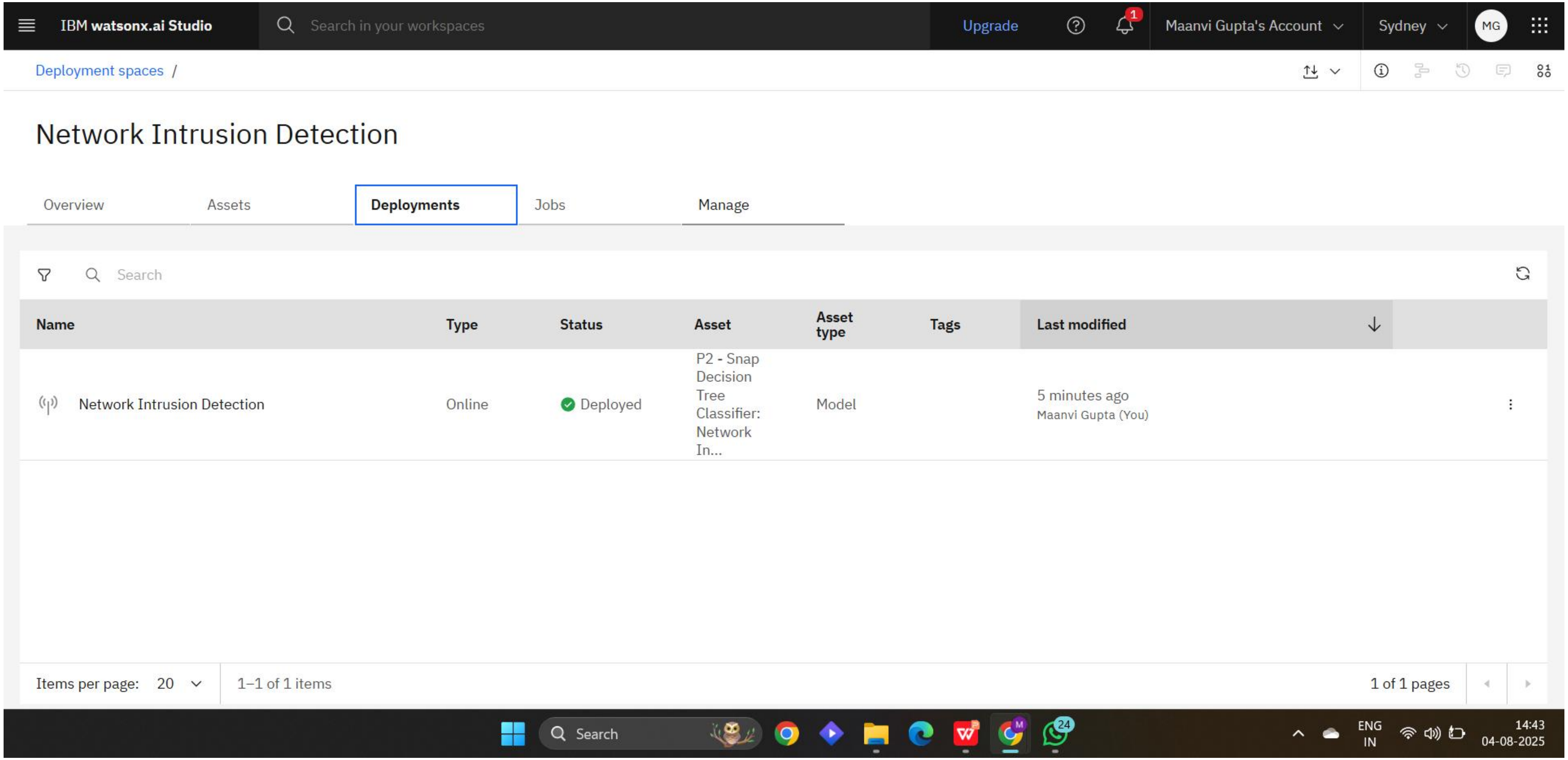
Active	Failed last 24 hours
0	0

View jobs

Space history

No notifications
You will see your most recent notifications here.

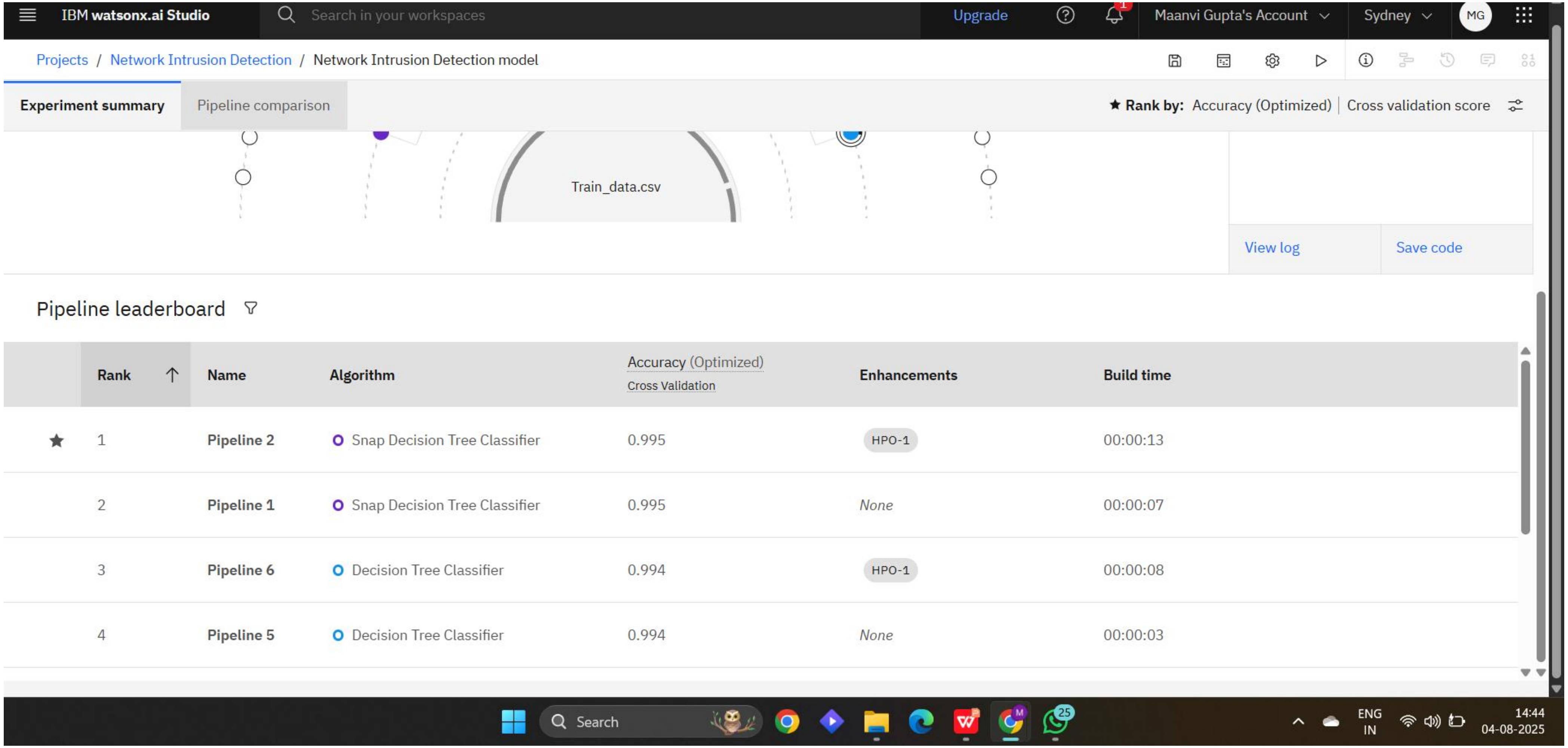
RESULT SCREENSHOT



Network Intrusion Detection

Name	Type	Status	Asset	Asset type	Tags	Last modified
Network Intrusion Detection	Online	✓ Deployed	P2 - Snap Decision Tree Classifier: Network In...	Model		5 minutes ago Maanvi Gupta (You)

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


IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Maanvi Gupta's Account
Sydney
MG
Projects / Network Intrusion Detection / Network Intrusion Detection model
Experiment summary
Pipeline comparison
★ Rank by: Accuracy (Optimized) | Cross validation score
Train_data.csv
View log
Save code
Search
ENG
IN
14:44
04-08-2025

Pipeline leaderboard

	Rank ↑	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	Pipeline 2	Snap Decision Tree Classifier	0.995	HPO-1	00:00:13
	2	Pipeline 1	Snap Decision Tree Classifier	0.995	*None*	00:00:07
	3	Pipeline 6	Decision Tree Classifier	0.994	HPO-1	00:00:08
	4	Pipeline 5	Decision Tree Classifier	0.994	*None*	00:00:03

CONCLUSION

The Network Intrusion Detection System developed in this project successfully utilizes machine learning to detect and classify malicious network traffic. By training models on real-world traffic data from the Kaggle dataset and deploying them through IBM Watsonx.ai, the system demonstrates high accuracy in identifying anomalies such as DoS, Probe, R2L, and U2R attacks.

The use of AutoAI enabled automated model selection and tuning, making the development process more efficient. The chosen Random Forest model achieved the best balance of accuracy, precision, and recall. Deployment on IBM Cloud ensured scalability and ease of access, allowing the model to be integrated into real-time network monitoring tools.

Overall, the project showcases how machine learning can enhance cybersecurity infrastructure, reduce false positives, and enable faster response to potential threats. It also highlights the practical benefits of cloud-based AI tools in building and deploying intelligent systems.

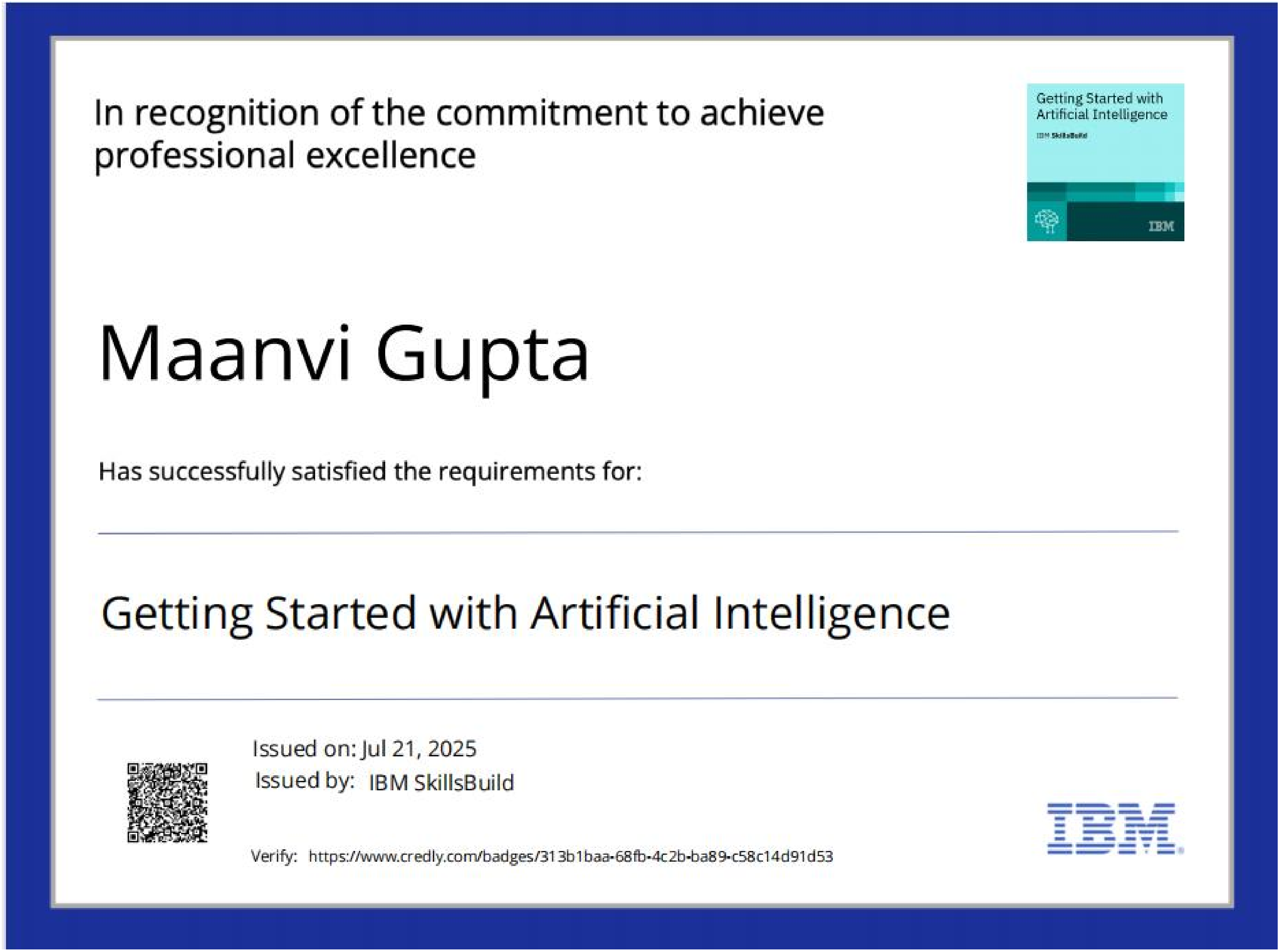
FUTURE SCOPE

- Integrate deep learning models (e.g., LSTM for sequential packet analysis)
- Enable live streaming traffic analysis with Kafka integration
- Add multi-class labeling for finer attack type classification
- Expand deployment across hybrid cloud environments
- Combine with firewall APIs for automatic threat response

GITHUB LINK

https://github.com/Maanvi-Gupta/Network-Intrusion-detection.git

IBM CERTIFICATIONS-GETTING STARTED WITH AI



In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence

IBM SkillsBuild

IBM

Maanvi Gupta

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

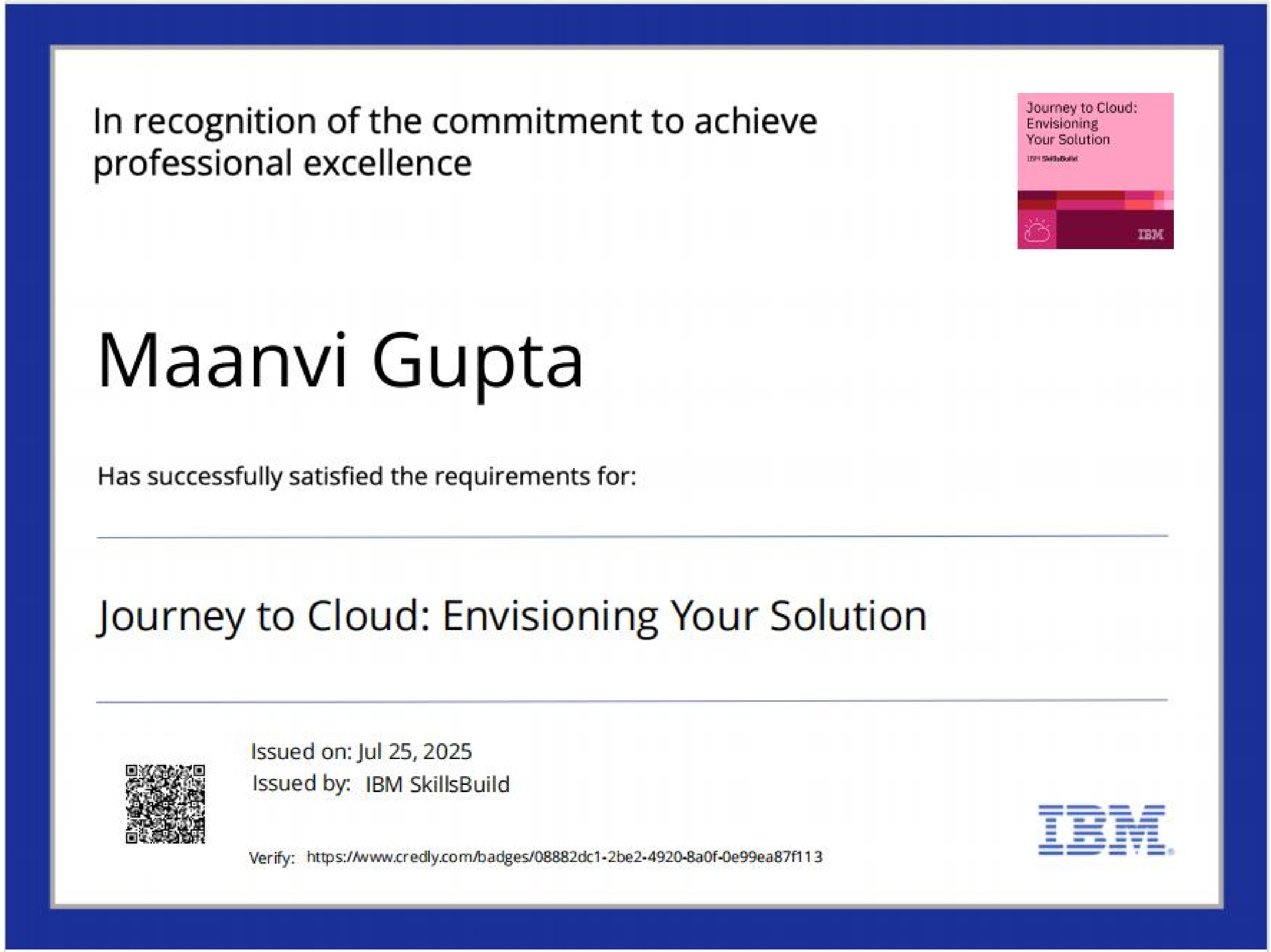
Issued on: Jul 21, 2025

Issued by: IBM SkillsBuild

IBM

Verify: https://www.credly.com/badges/313b1baa-68fb-4c2b-ba89-c58c14d91d53

IBM CERTIFICATIONS-JOURNEY TO CLOUD



In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM SkillsBuild

IBM

Maanvi Gupta

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

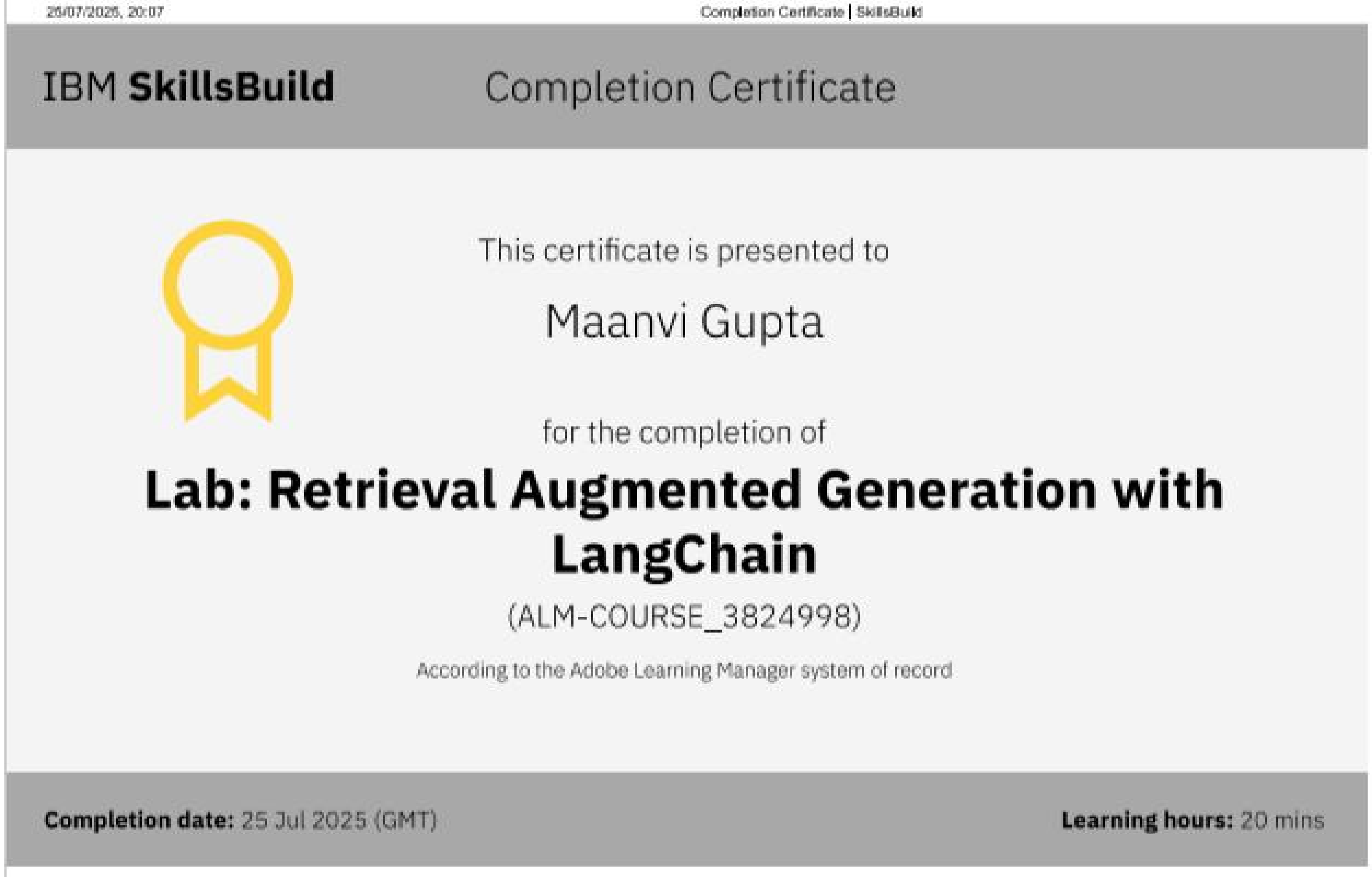
Issued on: Jul 25, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/08882dc1-2be2-4920-8a0f-0e99ea87f113

IBM

IBM CERTIFICATIONS-RAG LAB



25/07/2025, 20:07 Completion Certificate | SkillsBuild

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Maanvi Gupta

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 25 Jul 2025 (GMT) **Learning hours:** 20 mins

THANK YOU