CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
Shreya Dubey
United college of engineering and research Allahabad-CSE

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

- **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.

PROPOSED SOLUTION

- **The proposed system aims to address the challenge of creating a robust network intrusion detection system using machine learning.**
- **The solution will analyze network traffic data to identify and classify various types of cyber-attacks.**
- **The system will distinguish malicious activities from normal network traffic to provide an early warning of potential threats.**
- - Data Collection from Kaggle Dataset (link provided)
- - Preprocessing of network traffic logs
- - Feature selection and extraction
- - ML model training for classification of attacks
- - Real-time detection and alert system
- The goal is accurate, early classification of attacks.

SYSTEM APPROACH

- System Requirements:
- - IBM Cloud Lite Services
- - Python with Scikit-learn, Pandas, NumPy
- - Kaggle dataset integration

- Libraries:
- - IBM Watson Studio for deployment

ALGORITHM & DEPLOYMENT

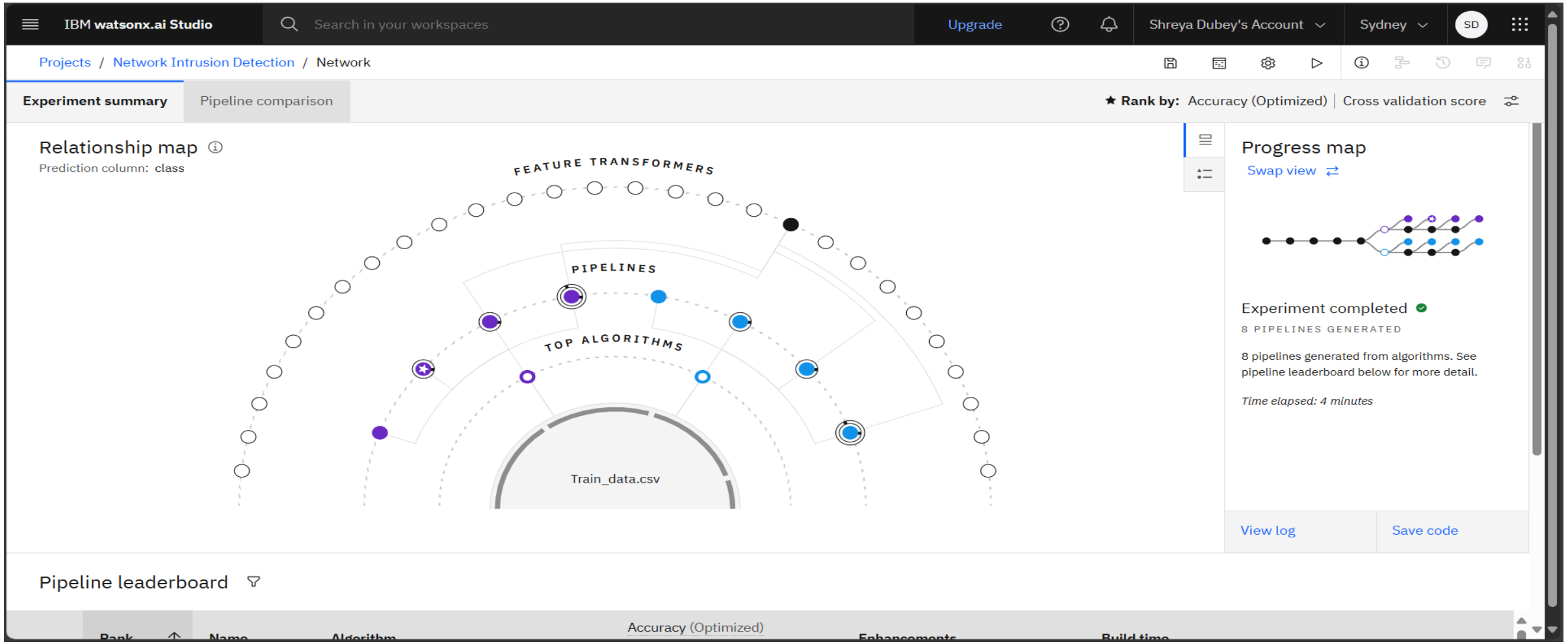
Algorithm:

Data Input:
- Network traffic features from the dataset
- Attack labels (normal, DoS, Probe, etc.)

Training:
- Train-test split (e.g., 80/20)
- Hyperparameter tuning using GridSearchCV

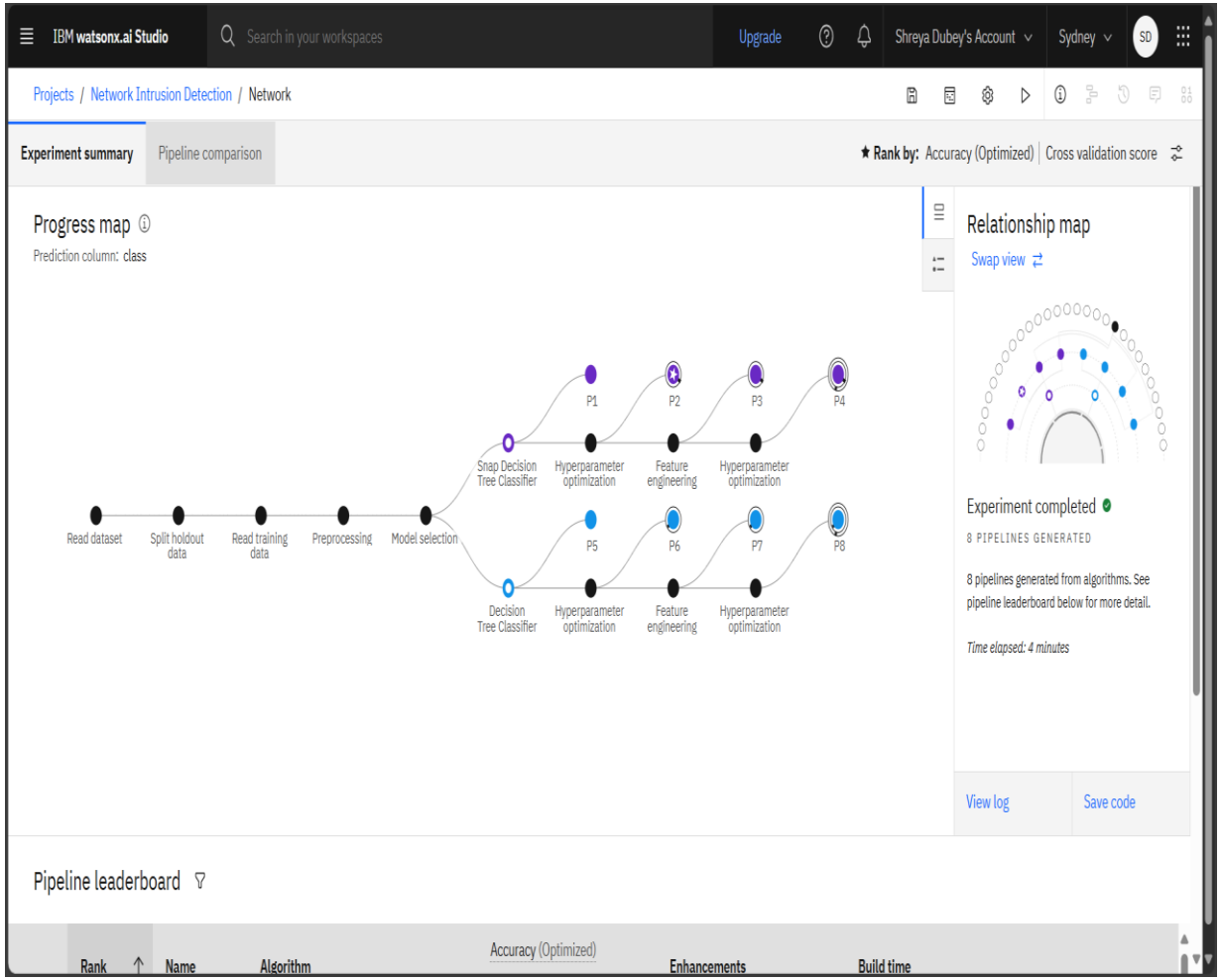
Deployment:
- Model hosted on IBM Watson Studio
- Real-time inference for network traffic inputs

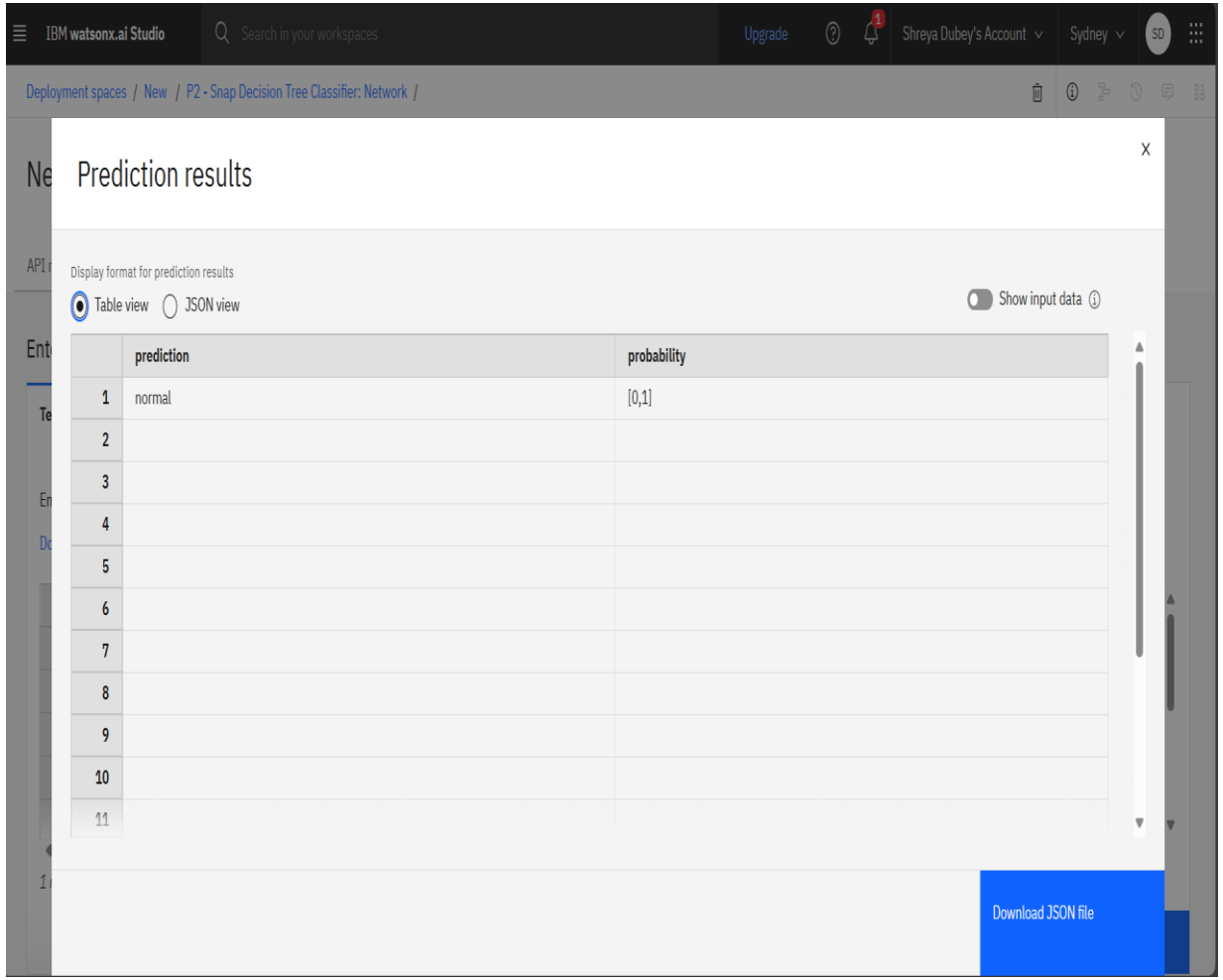
RESULT



edunet foundation

RESULT





edunet foundation

CONCLUSION

- The model accurately detects different intrusion types.
- Effective in classifying and warning about malicious network activities.
- Can be integrated with enterprise-grade firewalls or routers

FUTURE SCOPE

- Include real-time traffic capture from network devices.
- Use deep learning for improved accuracy.
- Expand system to detect zero-day attacks using anomaly detection

REFERENCES

- Dataset:- https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection
- IBM Watson Studio documentation
- Scikit-learn official guide
- Research papers on NIDS and ML-based classification

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Shreya Dubey

Has successfully satisfied the requirements for:

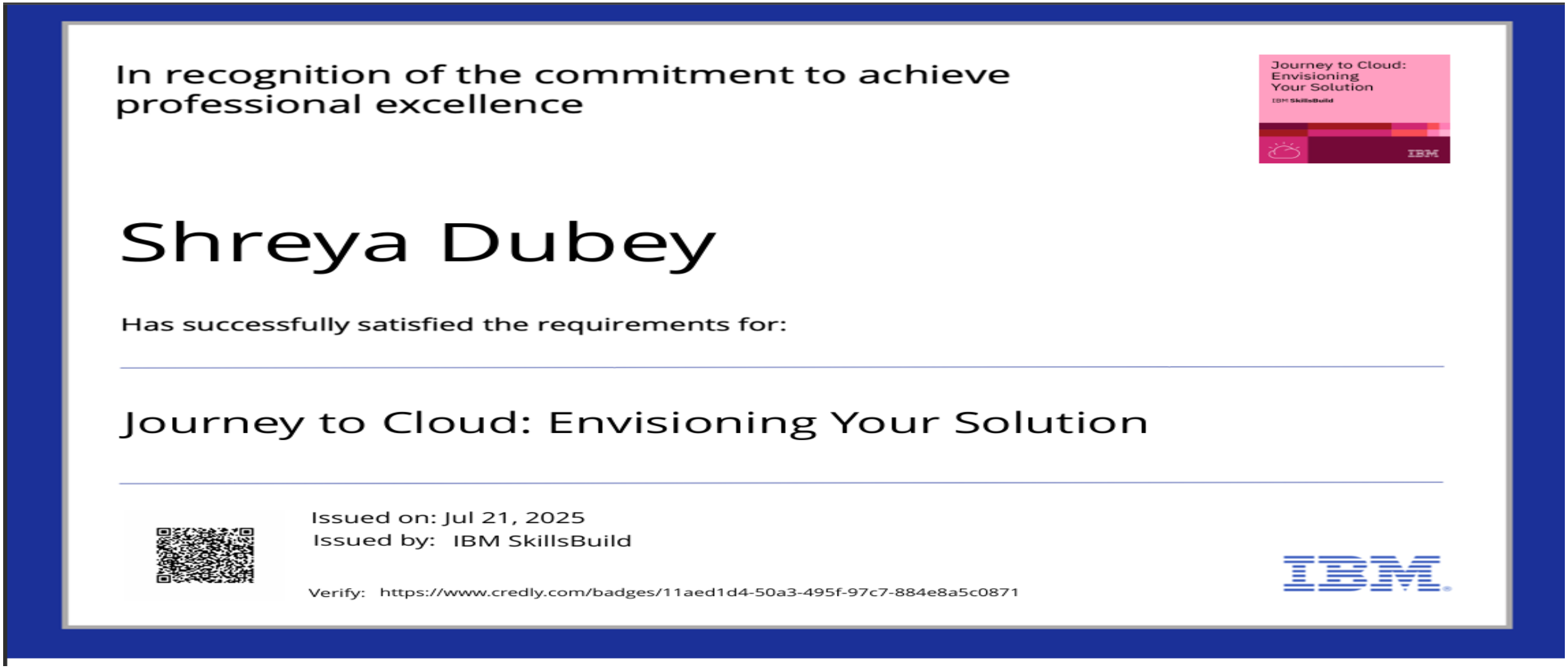
Getting Started with Artificial Intelligence

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

Verify: https://www.credly.com/badges/0e842df2-f912-4346-80c5-8093d052c2a8

IBM

IBM CERTIFICATIONS



IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Shreya Dubey

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