# CAPSTONE PROJECT

# NETWORK INTRUSION DETECTION USING MACHINE LEARNING

Presented By:
1. Rudraksh Dattaram Chorge - VPM's BN Bandodkar College Of Science – BSC CS

edunet foundation

# OUTLINE

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

# PROBLEM STATEMENT

Modern network infrastructures are increasingly exposed to a wide range of cyber-attacks such as Denial of Service (DoS), Probing, Remote-to-Local (R2L), and User-to-Root (U2R). These attacks can compromise data integrity, service availability, and system confidentiality. The key challenge is to accurately distinguish between normal and malicious network traffic using large volumes of connection records and behavioral patterns, without relying on manual monitoring. Failure to do so can result in undetected intrusions and potential breaches across critical systems.

# PROPOSED SOLUTION

- A machine learning-based Network Intrusion Detection System (NIDS)
- Uses the **NSL-KDD** dataset for training of the model
- Classifies network traffic into multiple intrusion types
- Steps include:
  - Data cleaning and preprocessing
  - Feature encoding and scaling
  - Model training (e.g., Random Forest or AutoAI pipeline)
  - Evaluation and deployment on IBM Cloud

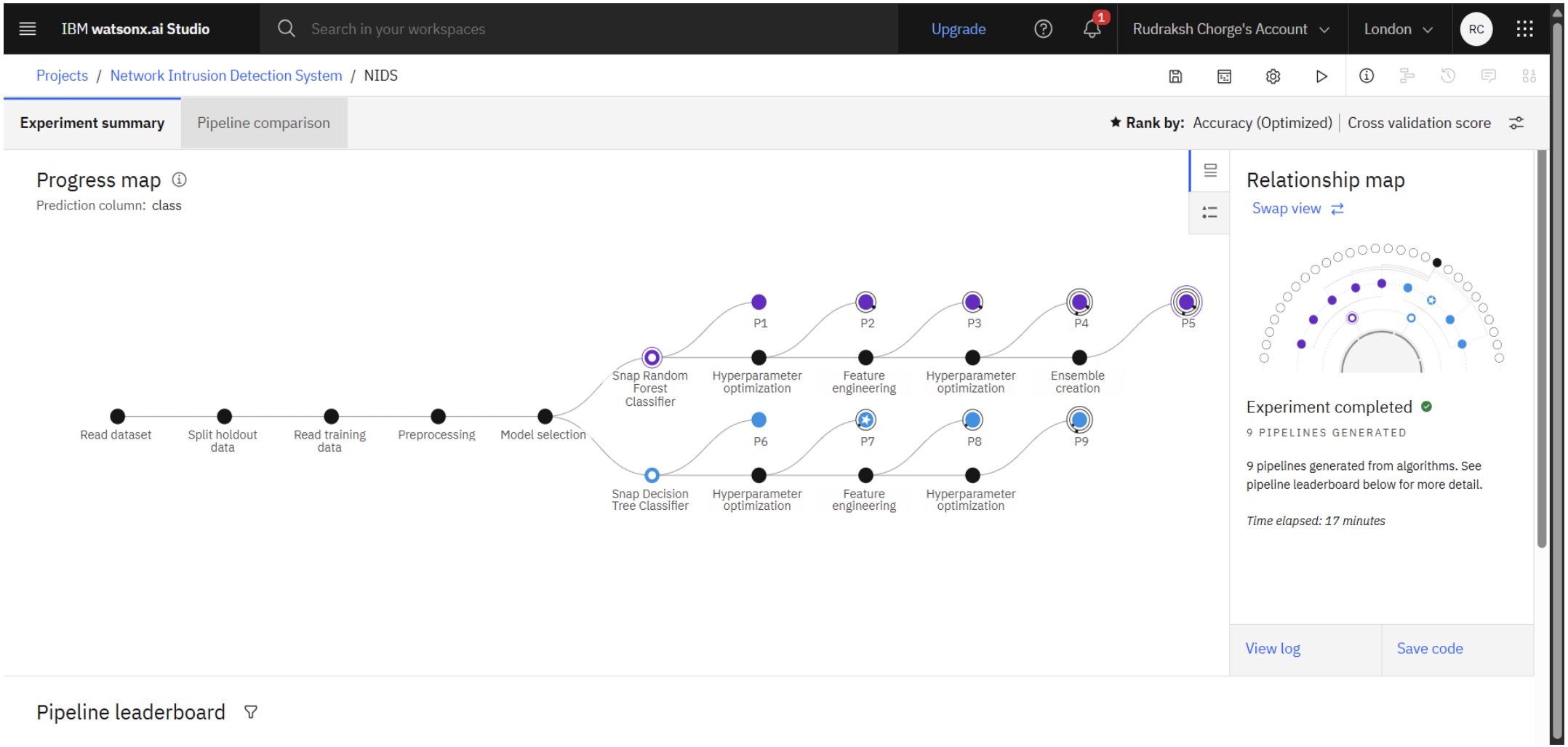
# SYSTEM APPROACH

- **Tools & Platforms:**
- IBM Cloud ( Mandatory )
- IBM Watson Studio for model  development and deployment.
- IBM Cloud Object Storage for dataset handling.
- **Dataset Used:**
- NSL-KDD Dataset (KDDTrain+) from Kaggle Dataset https://www.kaggle.com/datasets/hassan06/nslkdd?select=KDDTrain%2B.txt

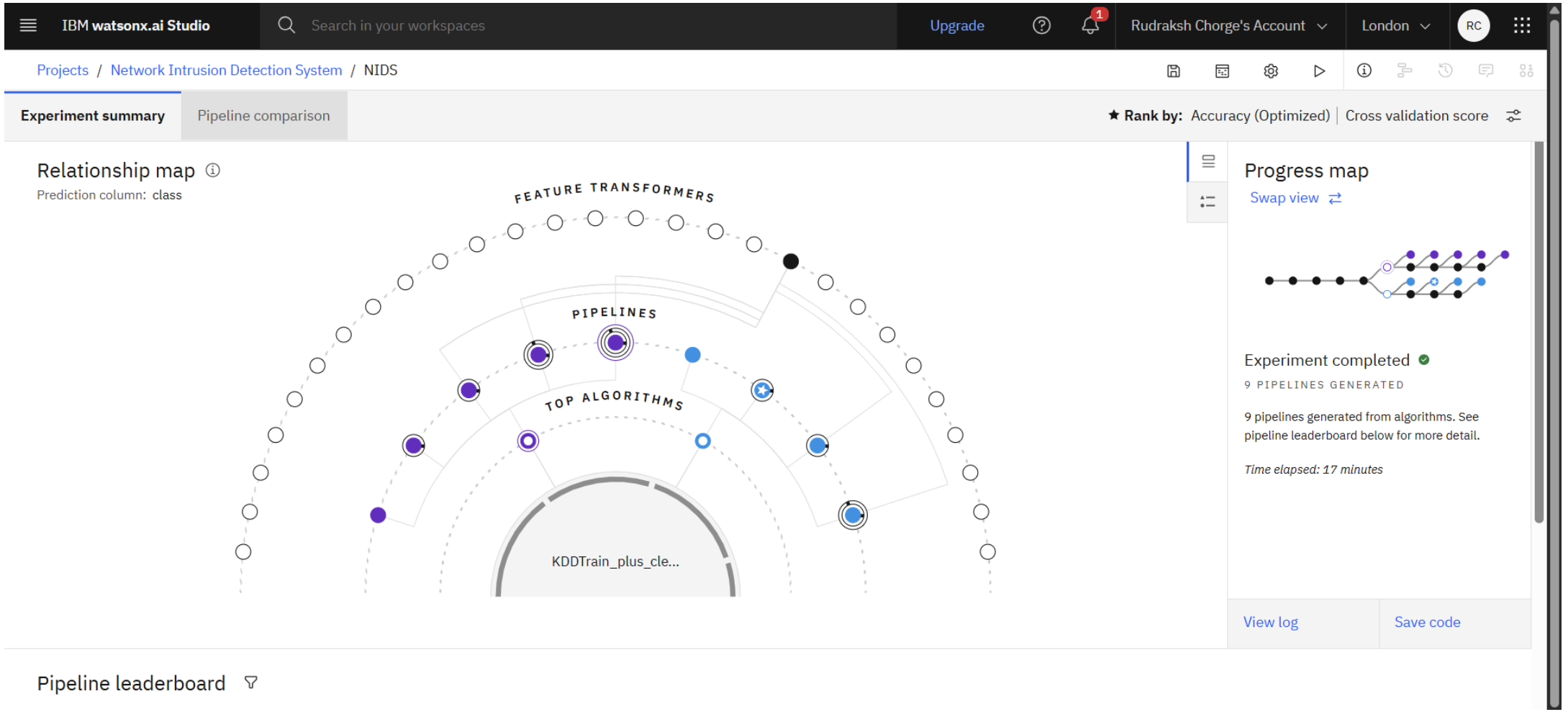
# ALGORITHM & DEPLOYMENT

- **Algorithm Used:** Random Forest Classifier (multiclass classification)
- **Input Features:** Protocol type, service, duration, bytes sent/received, error rates, etc.
- **Output:** Label representing intrusion type or normal
- **Training Process:**
- Categorical encoding + feature scaling
- Train-test split (80-20)
- **Deployment:**
- Trained model deployed on IBM Watson Studio with API endpoint for real time predictions.

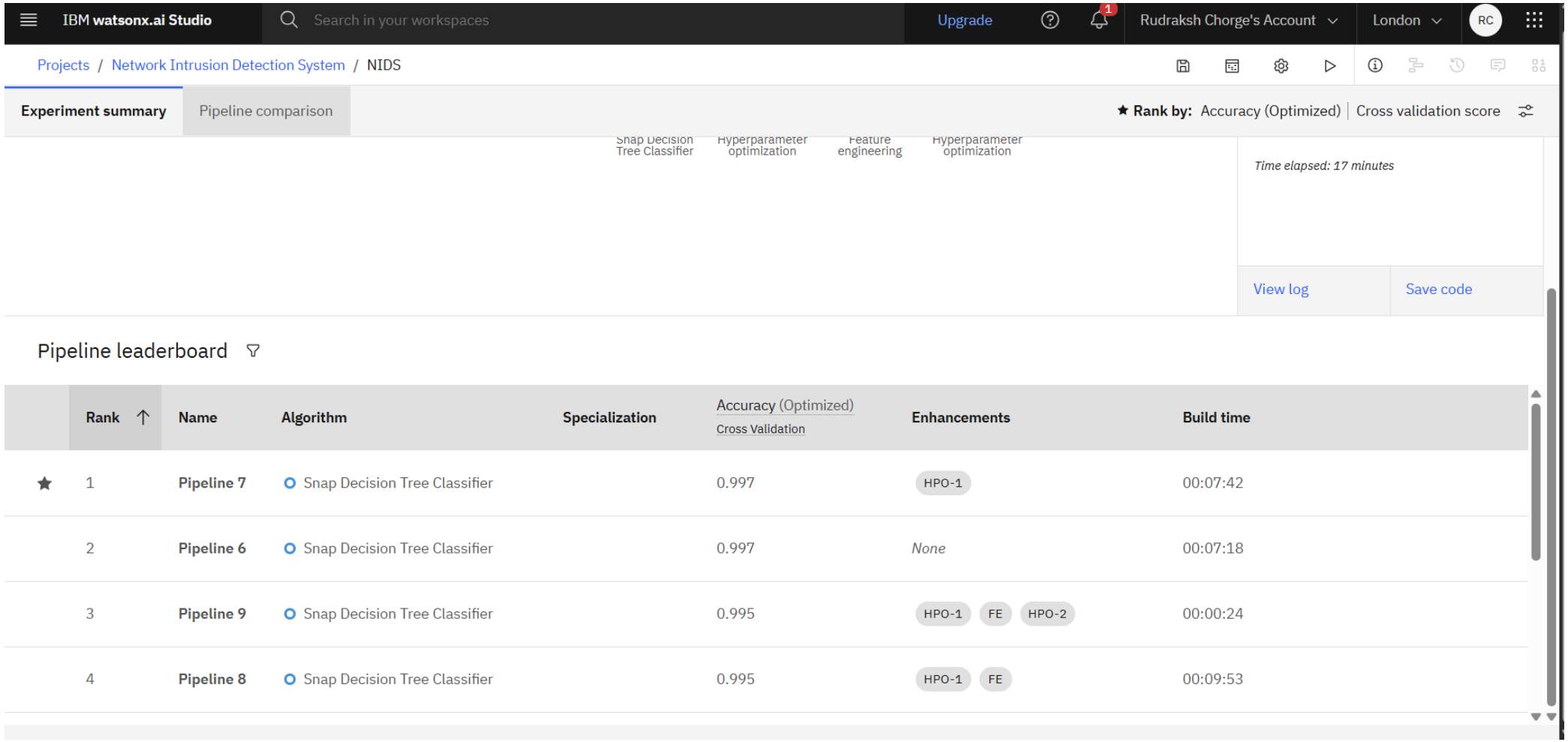
# RESULT



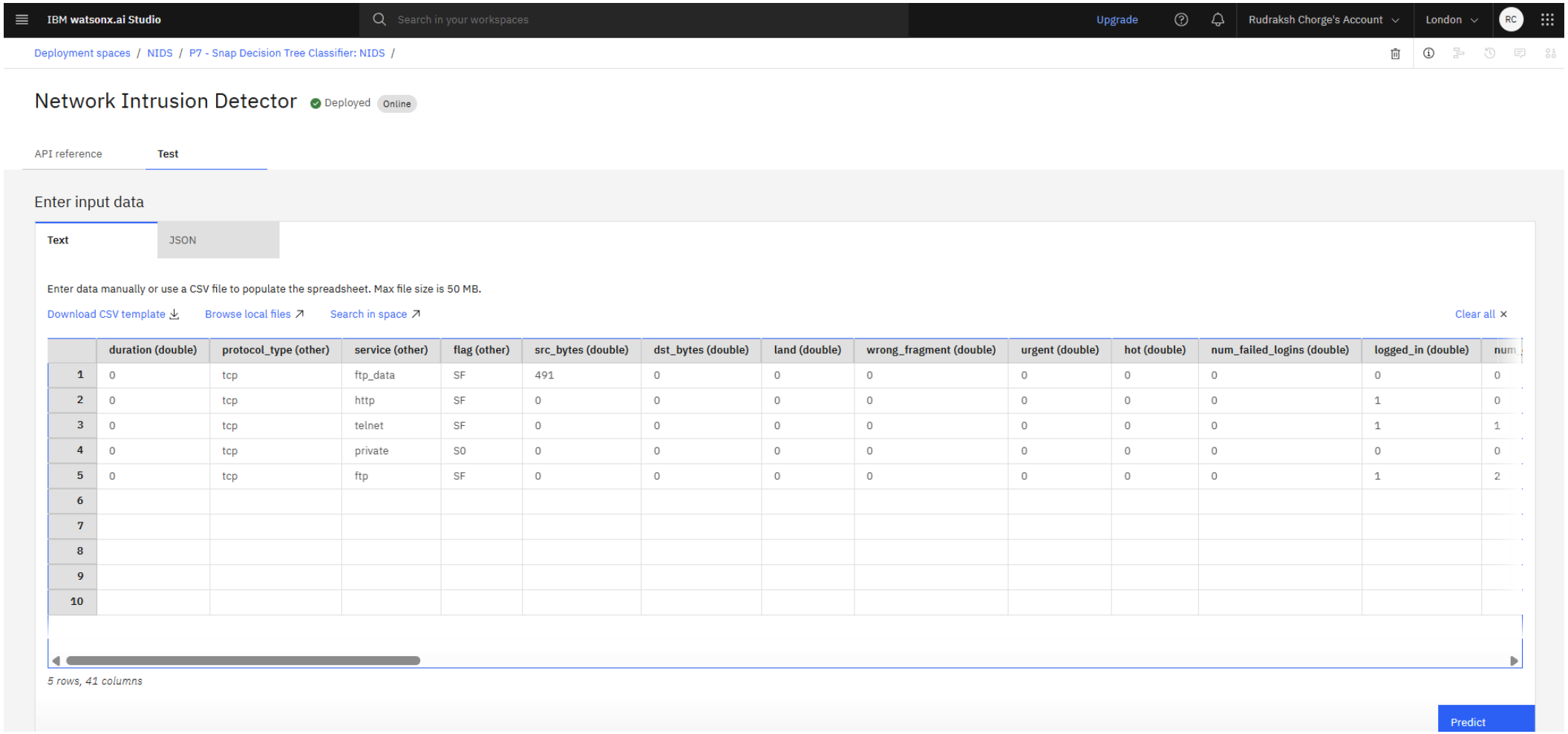
# RESULT



# RESULT



# RESULT

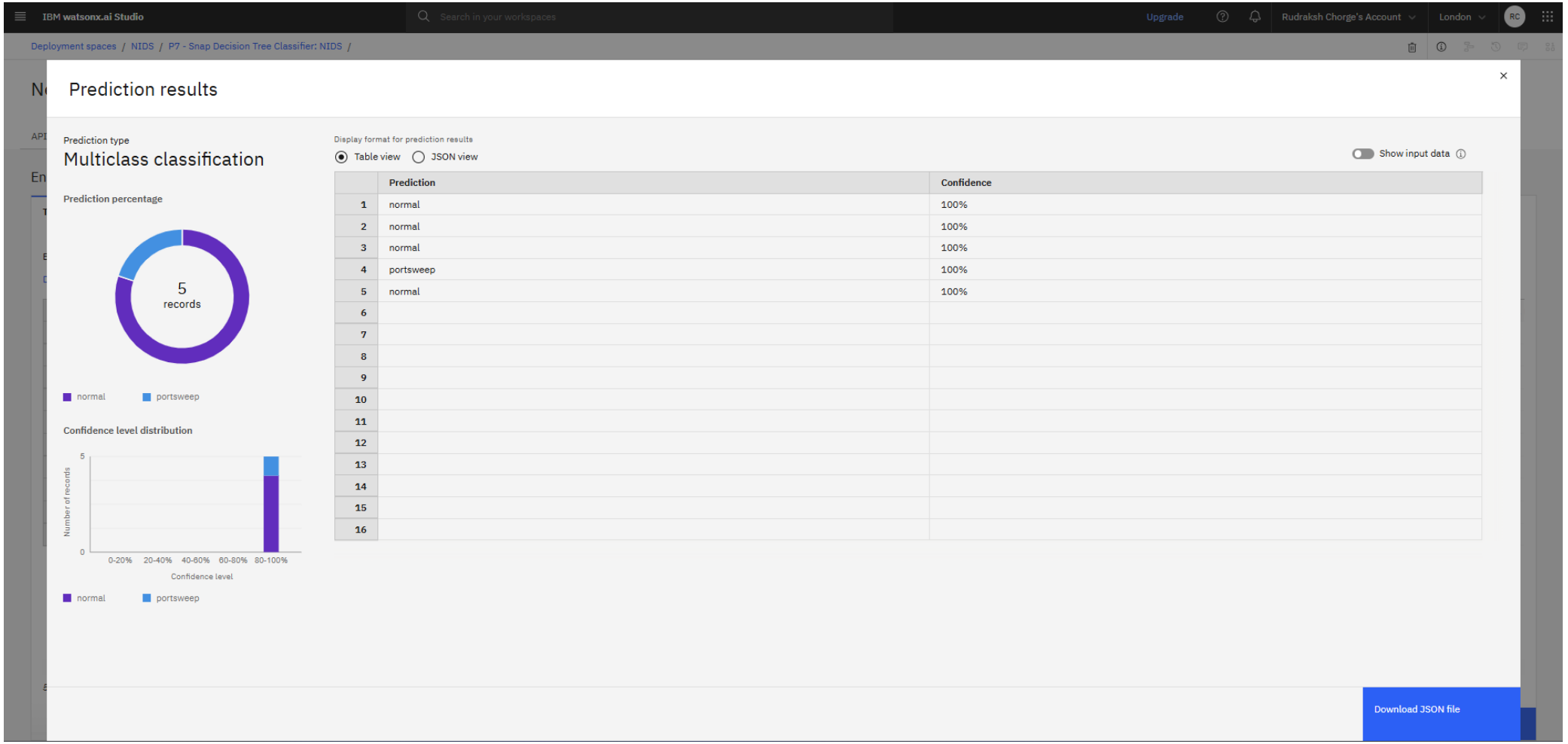



| | duration (double) | protocol_type (other) | service (other) | flag (other) | src_bytes (double) | dst_bytes (double) | land (double) | wrong_fragment (double) | urgent (double) | hot (double) | num_failed_logins (double) | logged_in (double) | num |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | tcp | ftp_data | SF | 491 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | tcp | http | SF | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 |
| 3 | 0 | tcp | telnet | SF | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| 4 | 0 | tcp | private | S0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | tcp | ftp | SF | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 2 |
| 6 | | | | | | | | | | | | | |
| 7 | | | | | | | | | | | | | |
| 8 | | | | | | | | | | | | | |
| 9 | | | | | | | | | | | | | |
| 10 | | | | | | | | | | | | | |

*Note: Only partial input shown here. Full input includes 42 features as per NSL-KDD dataset.*

edunet foundation

# RESULT




edunet foundation

# CONCLUSION

- The ML model effectively distinguishes between normal and malicious network traffic.
- IBM AutoAI streamlined model creation and deployment.
- NSL-KDD dataset helped train a robust, multiclass model.
- The system can help automate detection in real-time monitoring tools.

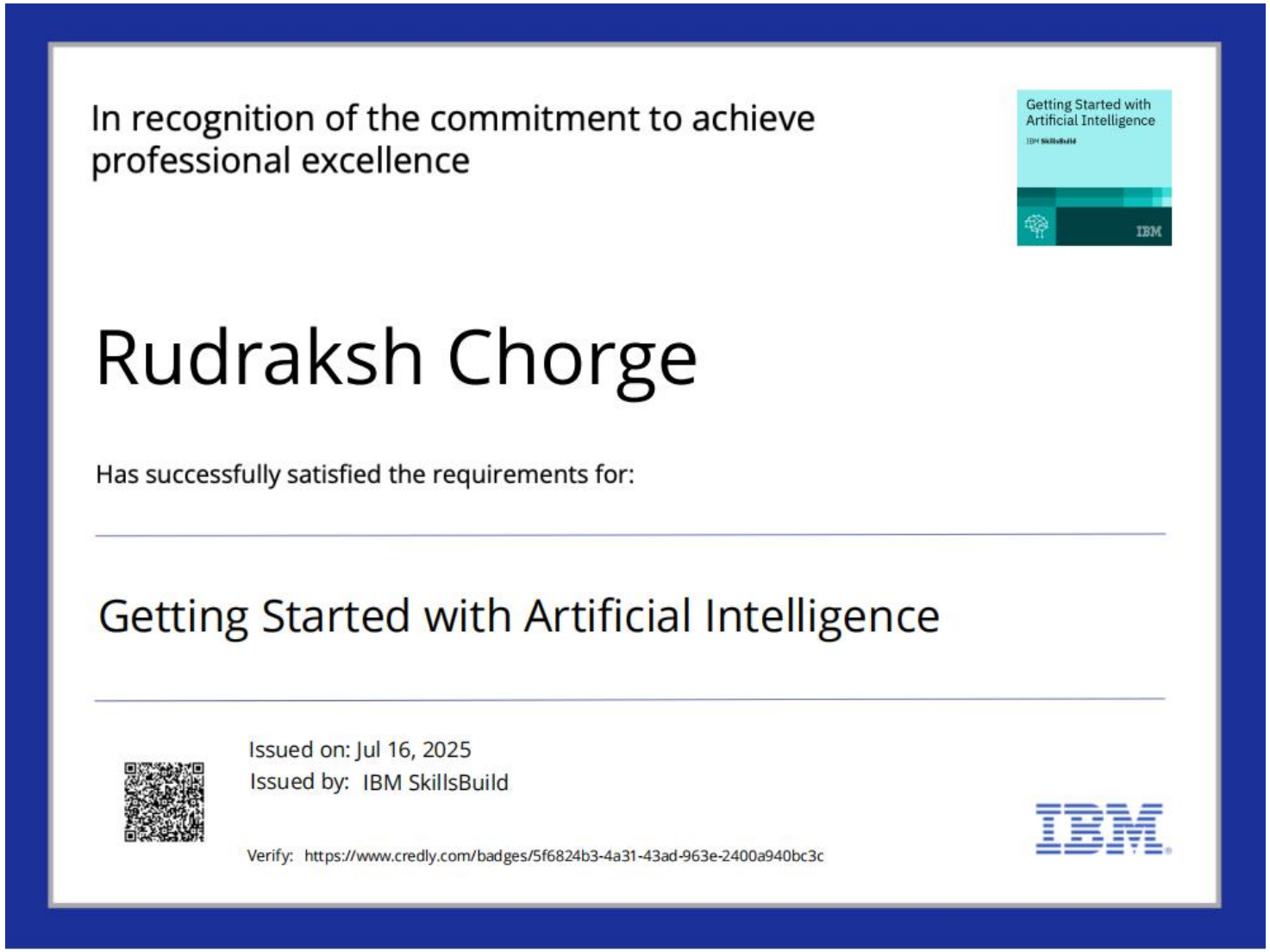
# FUTURE SCOPE

- Real-time intrusion detection with streaming data
- Integration with SIEM tools (e.g., Splunk, QRadar)
- Use of deep learning models (e.g., LSTM, CNN) for sequential analysis
- Handle encrypted packet features using advanced methods
- Deployment in **edge environments** (e.g., routers, IoT gateways) for low-latency detection
- Combining IDS with **threat intelligence platforms** for proactive defense
- Expanding the system to detect insider threats and anomalies in user behavior

# REFERENCES


- NSL-KDD Dataset: https://www.kaggle.com/datasets/hassan06/nslkdd?select=KDDTrain%2B.txt
- IBM Cloud and Watson Studio

# IBM CERTIFICATIONS



# IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM SkillsBuild

IBM

Rudraksh Chorge

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

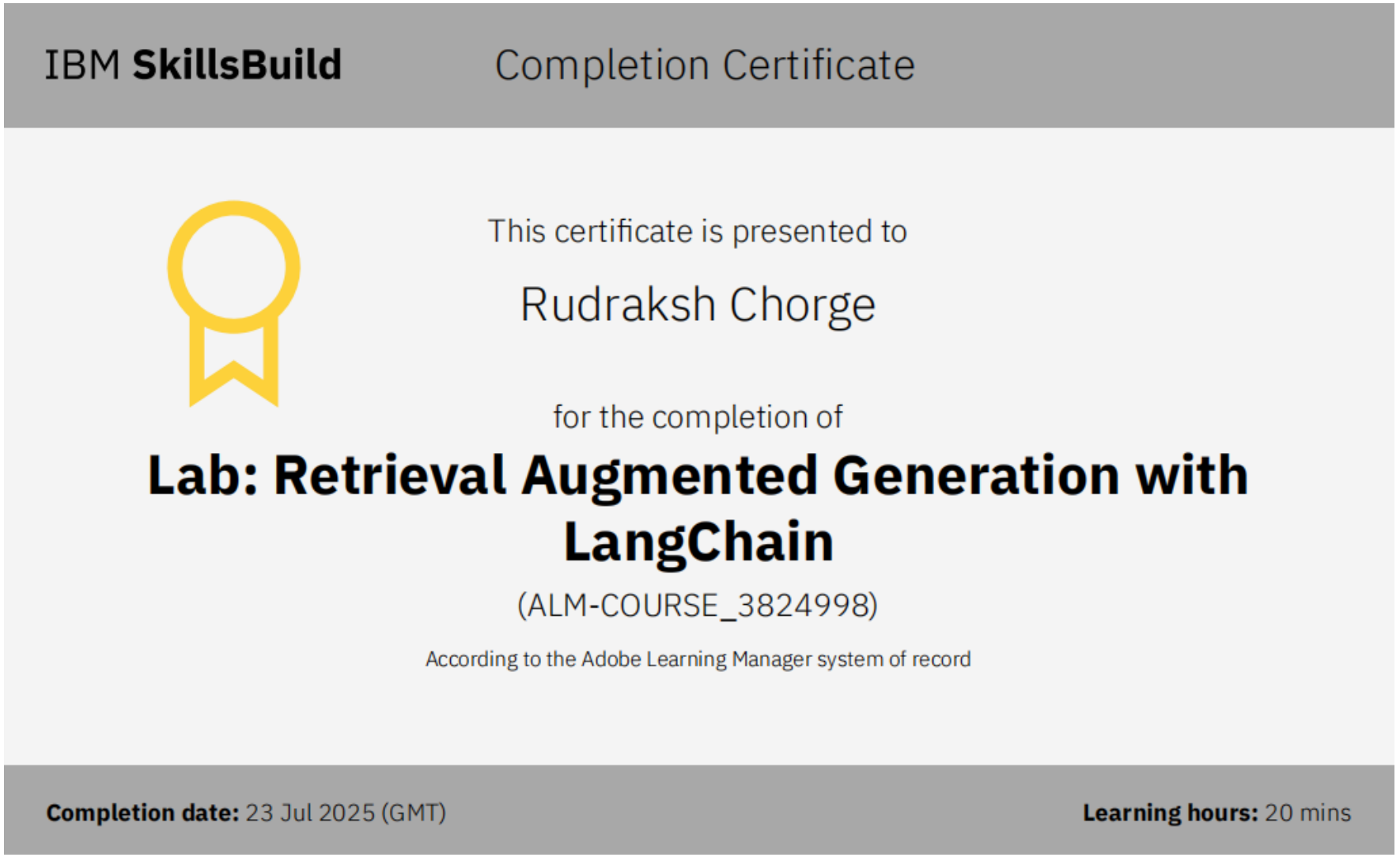
Issued on: Jul 19, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/ed198219-649e-4460-a8ec-b1d8f68b4518

IBM

edunet foundation

# IBM CERTIFICATIONS



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Rudraksh Chorge

for the completion of

**Lab: Retrieval Augmented Generation with LangChain**

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

**Completion date:** 23 Jul 2025 (GMT) **Learning hours:** 20 mins

edunet foundation

# THANK YOU

edunet foundation