CAPSTONE PROJECT

NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING

Presented By:
1. B K Rama Krishna Vamshi- St. Peter's Engineering College-
Computer Science and Engineering

OUTLINE

- **Problem Statement** (Should not include solution)
- **Proposed System/Solution**
- **System Development Approach** (Technology Used)
- **Algorithm & Deployment**
- **Result (Output Image)**
- **Conclusion**
- **Future Scope**
- **References**

PROBLEM STATEMENT

Design a machine learning-based Network Intrusion Detection System (NIDS) capable of analyzing network traffic to accurately detect and classify cyber-attacks—such as DoS, Probe, R2L, and U2R—while distinguishing them from normal activity. The system should leverage structured datasets and provide reliable early warnings to enhance network security.

PROPOSED SOLUTION

- Develop a machine learning model for the dataset provided. Preprocess the data, train classifiers like Random Forest or XGBoost, and evaluate performance using standard metrics. The model will classify network traffic and detect intrusions in real-time or batch mode, enhancing network security.
- Data Collection:
  - Use Kaggle Dataset for Training and Testing the Model
- Data Preprocessing:
  - Clean and preprocess the collected data to handle missing values, outliers, and inconsistencies.
- Machine Learning Model:
  - Designing a machine learning Model, (like Random Forest, Snap Logistic Regression)to predict Network Intrusion based on given data.
- Evaluation:
  - Assessing the model's performance using appropriate metrics such as Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), or other relevant metrics.
  - Fine-tune the model based on feedback and continuous monitoring of prediction accuracy.

SYSTEM APPROACH

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

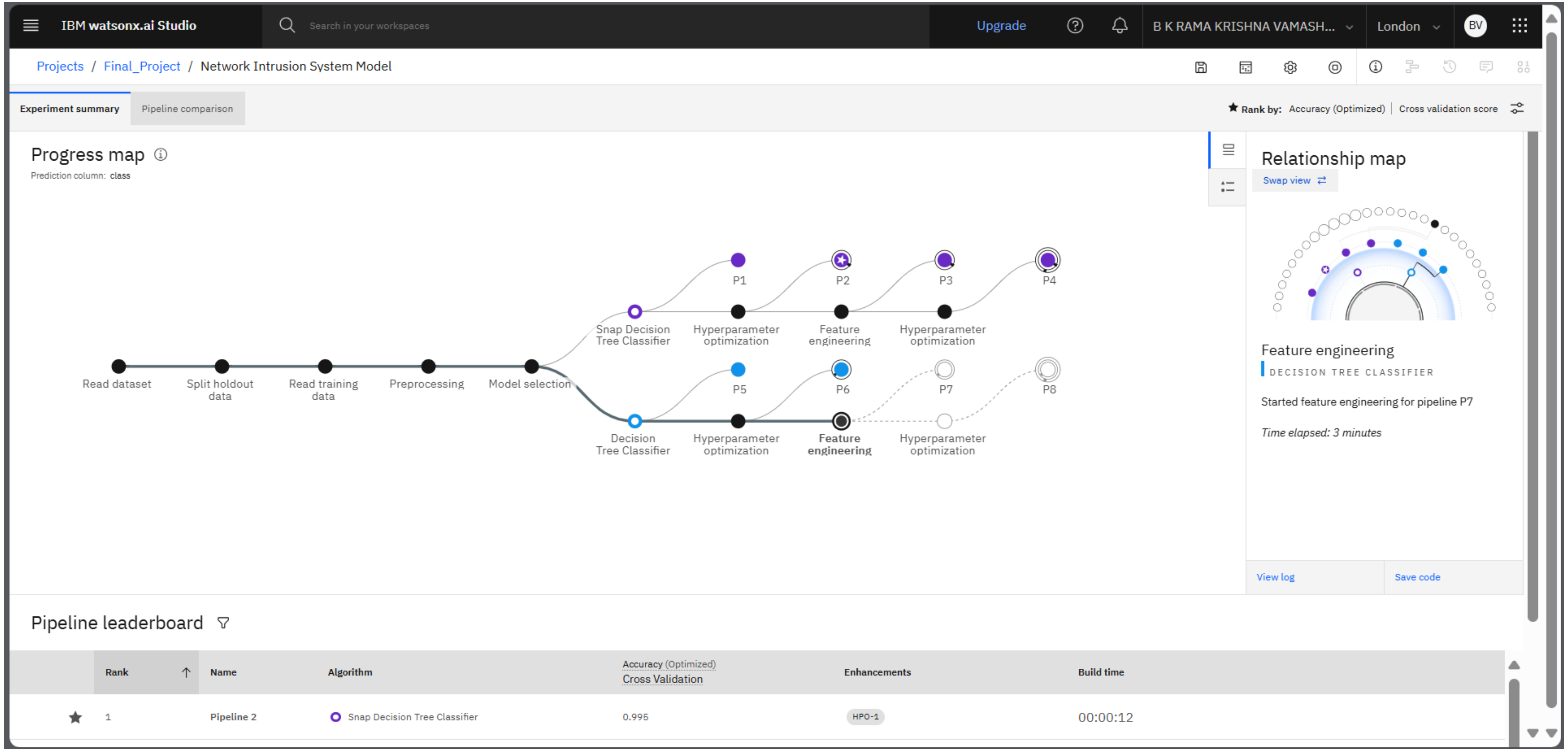
- System requirements
  - IBM Cloud Platform
  - IBM WatsonX.AI Studio
  - IBM Cloud Storage

ALGORITHM & DEPLOYMENT

- **Algorithm Selection:**
  - Decision Tree Classifier and Snap Decision Tree Classifier.
- **Data Input:**
  - Network Service Protocol, Network Service, Service Flag.
- **Training Process:**
  - Supervised Learning Model using Network Intrusion Dataset.
- **Prediction Process:**
  - The Supervised Learning model deployed on WatsonX.AI Studio with API endpoint for real-time predictions

RESULT

Classification Model-1



Feature engineering

DECISION TREE CLASSIFIER

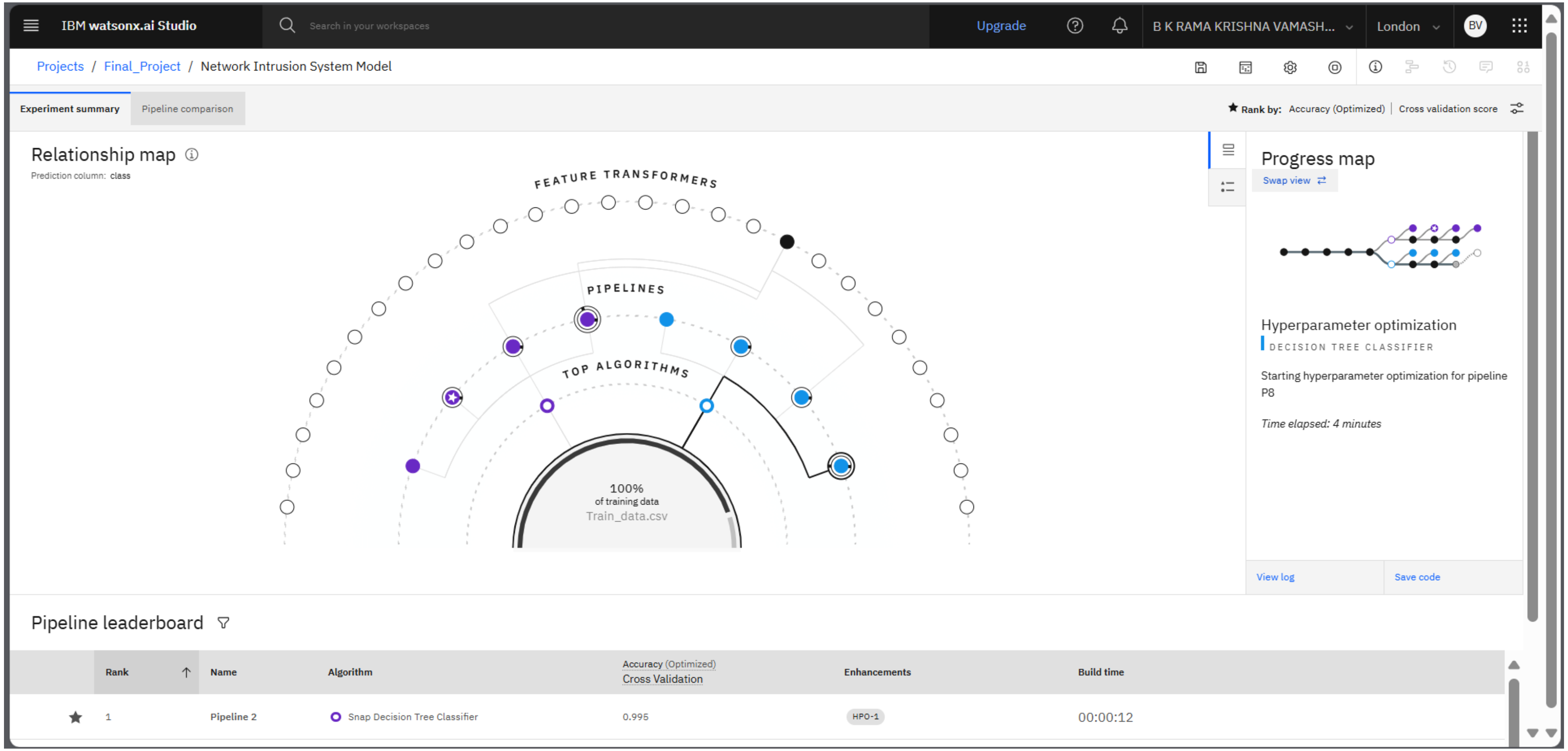
Started feature engineering for pipeline P7

Time elapsed: 3 minutes

	Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	Pipeline 2	Snap Decision Tree Classifier	0.995	HPO-1	00:00:12

RESULT

Classification Model-2



Hyperparameter optimization

DECISION TREE CLASSIFIER

Starting hyperparameter optimization for pipeline P8

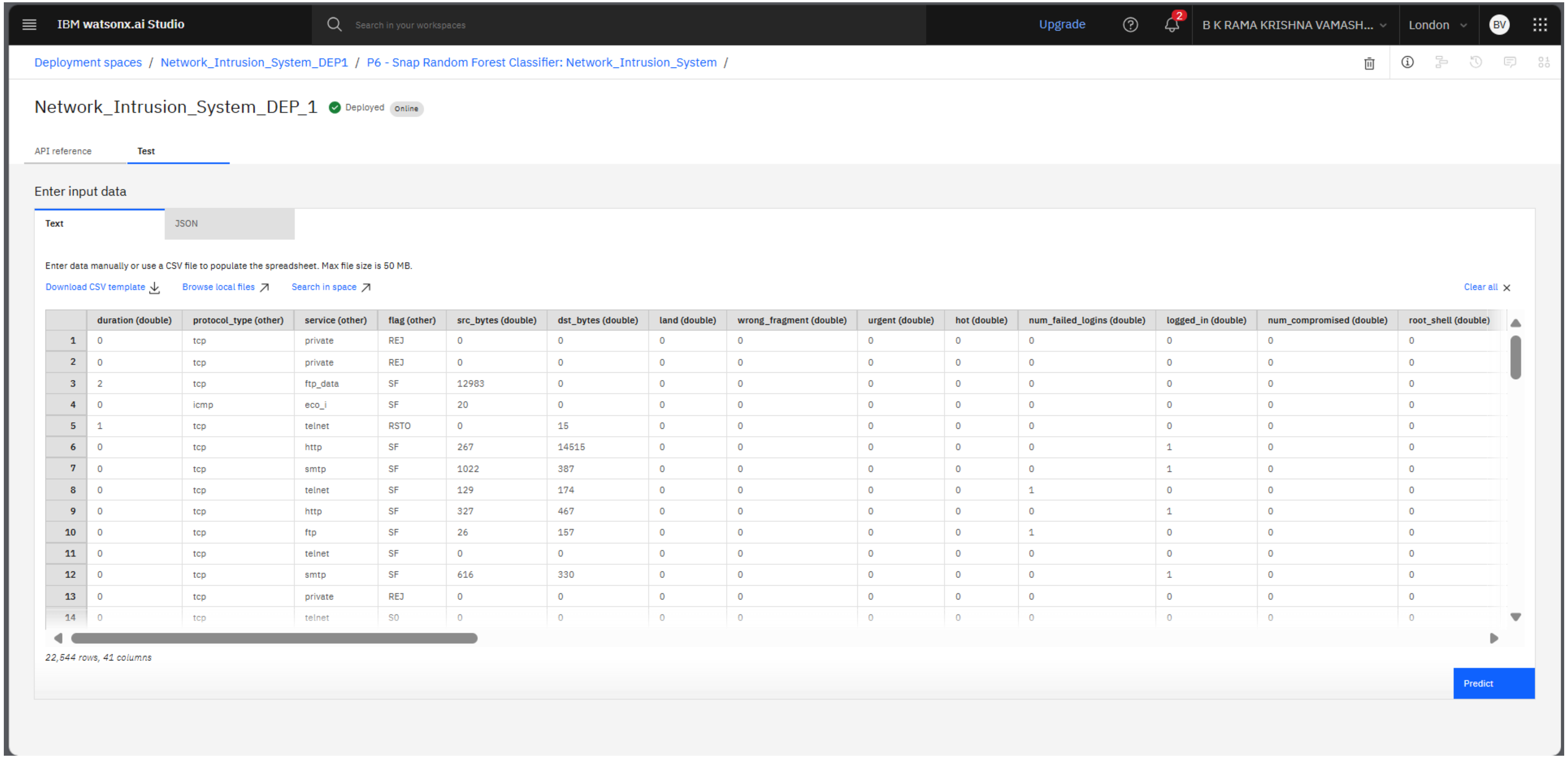
Time elapsed: 4 minutes

Pipeline leaderboard

	Rank	Name	Algorithm	Accuracy (Optimized) Cross Validation	Enhancements	Build time
★	1	Pipeline 2	○ Snap Decision Tree Classifier	0.995	HPO-1	00:00:12

RESULT

Input Data



Deployment spaces / Network_Intrusion_System_DEP1 / P6 - Snap Random Forest Classifier: Network_Intrusion_System /

Network_Intrusion_System_DEP_1 Deployed Online

Enter input data

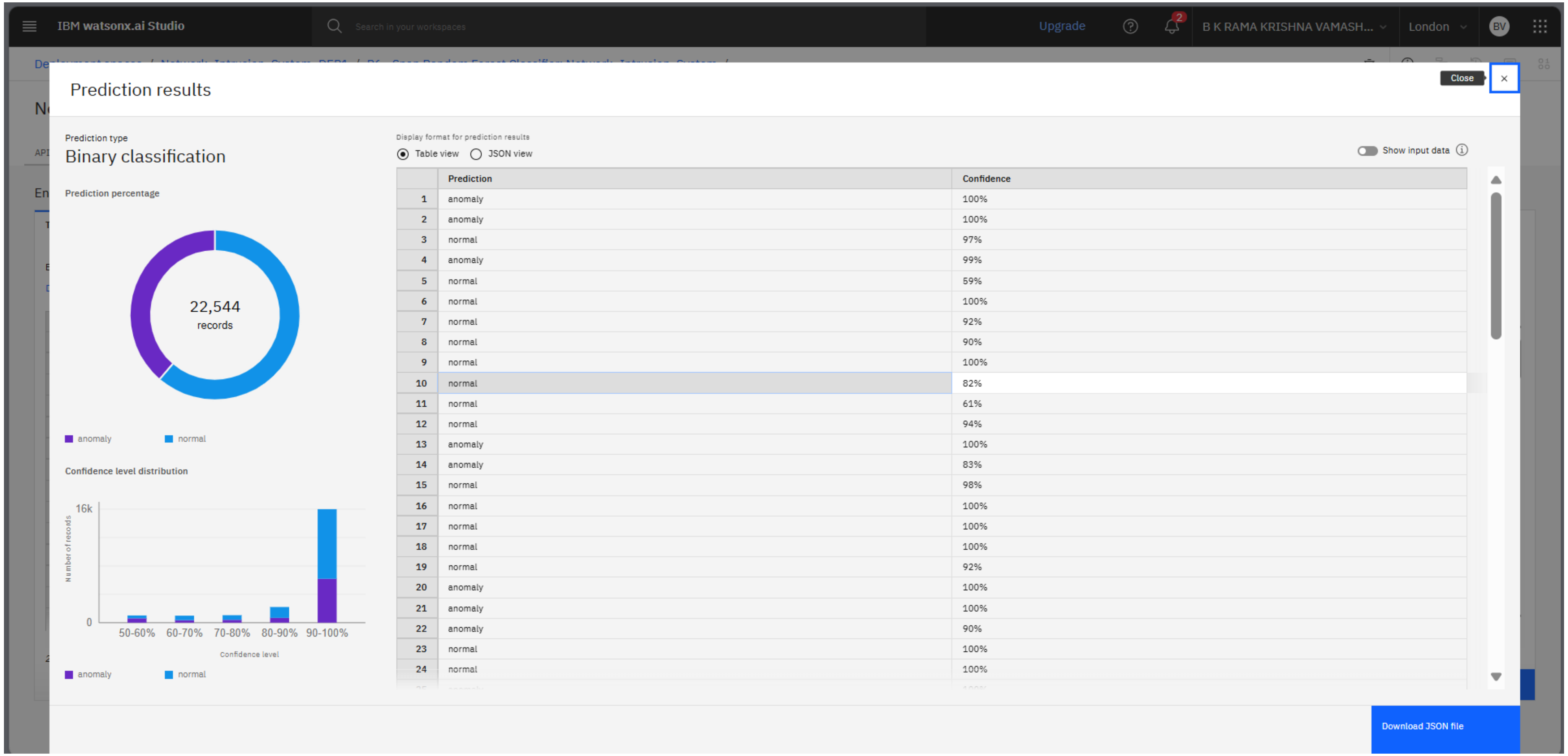
Enter data manually or use a CSV file to populate the spreadsheet. Max file size is 50 MB.

	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_compromised (double)	root_shell (double)
1	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0
2	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0
3	2	tcp	ftp_data	SF	12983	0	0	0	0	0	0	0	0	0
4	0	icmp	eco_i	SF	20	0	0	0	0	0	0	0	0	0
5	1	tcp	telnet	RSTO	0	15	0	0	0	0	0	0	0	0
6	0	tcp	http	SF	267	14515	0	0	0	0	0	1	0	0
7	0	tcp	smtp	SF	1022	387	0	0	0	0	0	1	0	0
8	0	tcp	telnet	SF	129	174	0	0	0	0	1	0	0	0
9	0	tcp	http	SF	327	467	0	0	0	0	0	1	0	0
10	0	tcp	ftp	SF	26	157	0	0	0	0	1	0	0	0
11	0	tcp	telnet	SF	0	0	0	0	0	0	0	0	0	0
12	0	tcp	smtp	SF	616	330	0	0	0	0	0	1	0	0
13	0	tcp	private	REJ	0	0	0	0	0	0	0	0	0	0
14	0	tcp	telnet	S0	0	0	0	0	0	0	0	0	0	0

22,544 rows, 41 columns

RESULT

Output Data



Prediction results

Prediction type
Binary classification

Display format for prediction results
● Table view ○ JSON view

Show input data

	Prediction	Confidence
1	anomaly	100%
2	anomaly	100%
3	normal	97%
4	anomaly	99%
5	normal	59%
6	normal	100%
7	normal	92%
8	normal	90%
9	normal	100%
10	normal	82%
11	normal	61%
12	normal	94%
13	anomaly	100%
14	anomaly	83%
15	normal	98%
16	normal	100%
17	normal	100%
18	normal	100%
19	normal	92%
20	anomaly	100%
21	anomaly	100%
22	anomaly	90%
23	normal	100%
24	normal	100%
25	anomaly	100%

CONCLUSION

- A machine learning-based Network Intrusion Detection System was developed using the simulated military network dataset to detect and classify Network Intrusions. By extracting 41 features from TCP/IP connections, models like Decision Tree and Snap Decision Tree Classifier effectively distinguished between normal and various attack types (DoS, Probe, R2L, U2R). This solution enhances early detection and strengthens network security.

FUTURE SCOPE

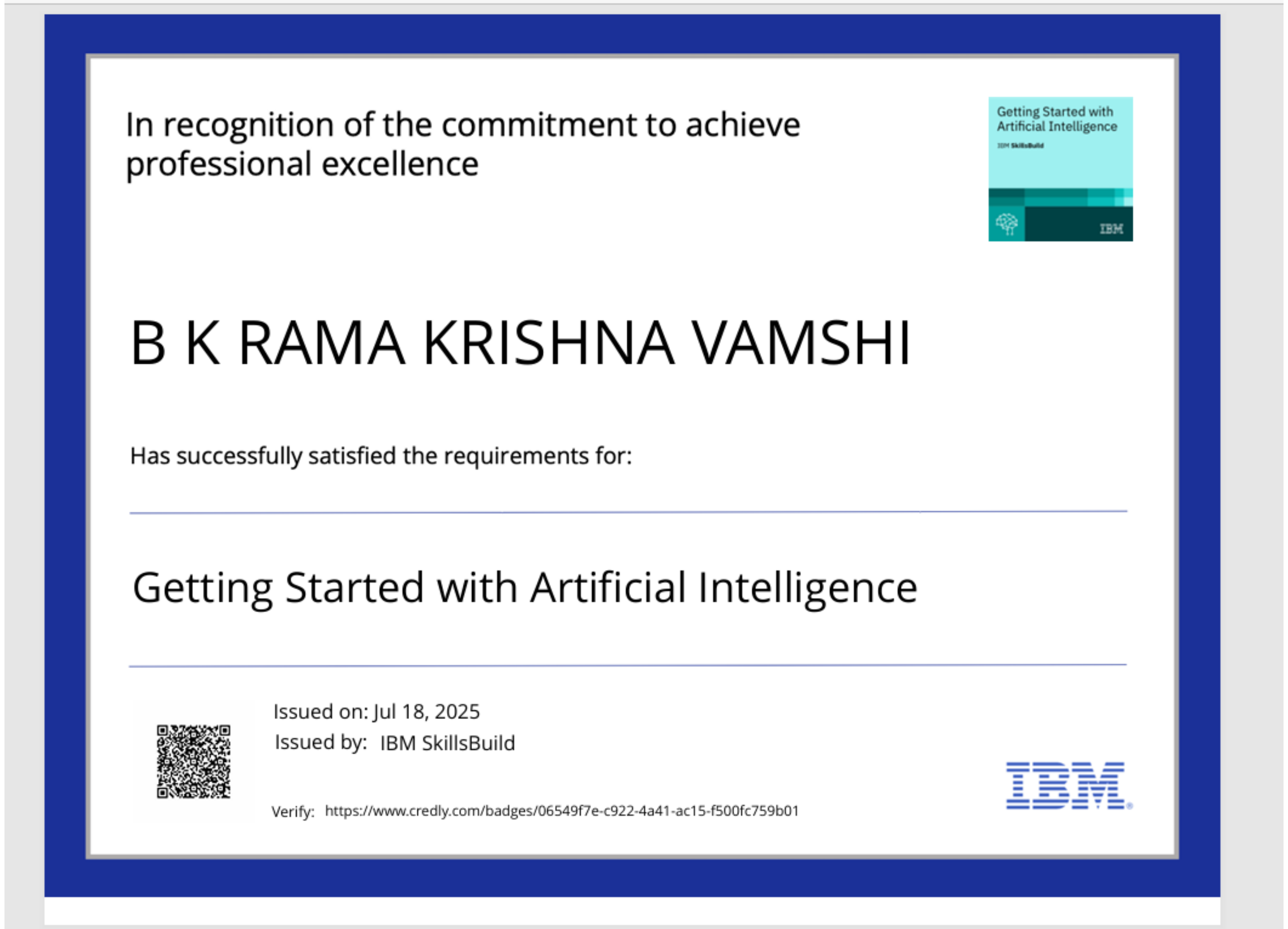
- Future enhancements include deploying the NIDS in real-time network environments using streaming data, integrating deep learning models like LSTM for sequential analysis, and adapting the system for encrypted traffic.

REFERENCES

- Kaggle Dataset: https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection
- Train.csv
- Test.csv

IBM CERTIFICATIONS

Getting Started With AI Certification


Getting Started with
Artificial Intelligence
IBM SkillsBuild
IBM

In recognition of the commitment to achieve professional excellence

B K RAMA KRISHNA VAMSHI

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

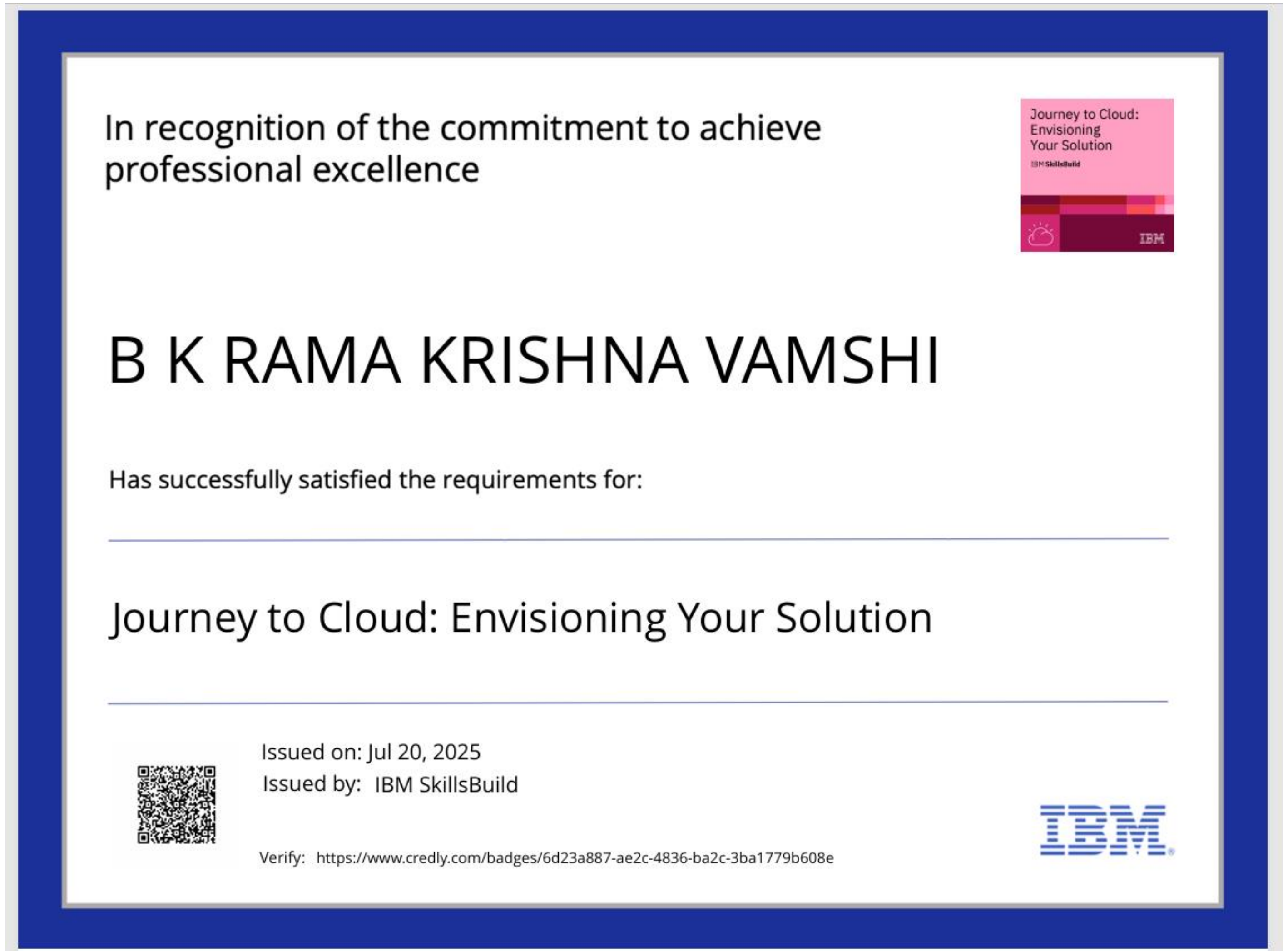
Issued on: Jul 18, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/06549f7e-c922-4a41-ac15-f500fc759b01

IBM

IBM CERTIFICATIONS

Journey to Cloud Certification



Journey to Cloud: Envisioning Your Solution
IBM SkillsBuild
IBM

In recognition of the commitment to achieve professional excellence

B K RAMA KRISHNA VAMSHI

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

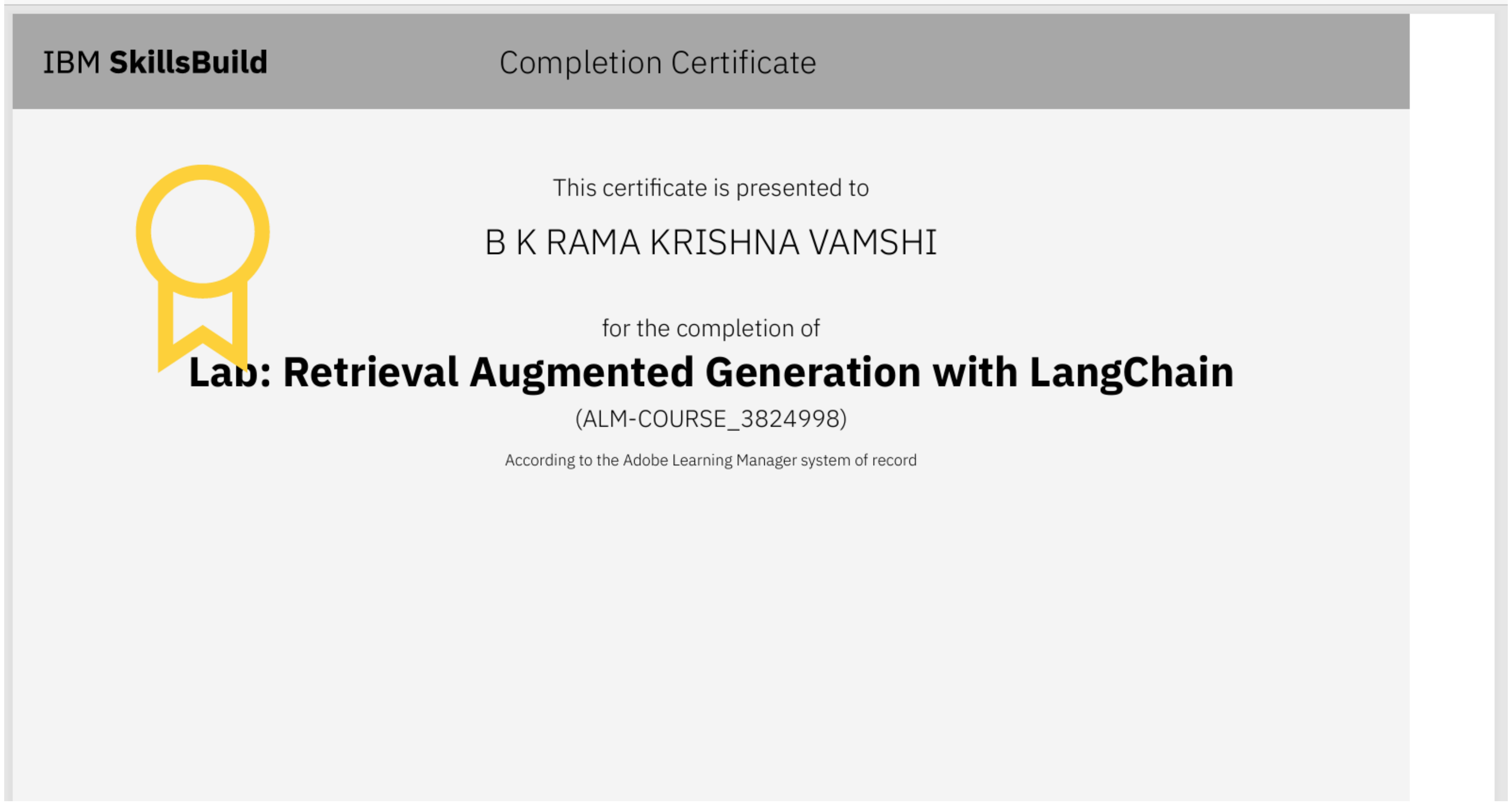
Issued on: Jul 20, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/6d23a887-ae2c-4836-ba2c-3ba1779b608e

IBM

IBM CERTIFICATIONS

Credly RAG LAB Certification



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

B K RAMA KRISHNA VAMSHI

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

THANK YOU