CAPSTONE PROJECT

NETWORK INTRUSION DETECTION SYSTEM

Presented By:

Ayush Anand
CSE Department
Galgotias University

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

Network Intrusion Detection

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 addresses the growing challenge of identifying cyber-attacks by analyzing network traffic using machine learning.
- A supervised learning model is built using the KDD-based intrusion detection dataset, which contains both normal and malicious traffic records.
- A Decision Tree Classifier is chosen due to its interpretability and efficiency in handling both numerical and categorical data.
- IBM Watson Studio's AutoAI is used to automate model building, hyperparameter tuning, and pipeline selection without requiring manual coding.
- The system converts raw network traffic attributes (like protocol, bytes sent, connection flags, etc.) into structured features suitable for training.
- The final trained model is deployed using IBM Watson Machine Learning as a REST API for real-time classification.
- The model can predict whether a given network connection is:
  - Normal
  - Or part of a known attack class (e.g., DoS, Probe, etc. if using multi-class).
- IBM Cloud services ensure scalability, reliability, and ease of integration into existing security frameworks.
- This solution enables proactive monitoring of network traffic and early detection of suspicious patterns to prevent system compromise.

SYSTEM APPROACH

Technologies & Services:

- IBM Cloud (Lite Plan)

- IBM Watson Studio

- IBM AutoAI for automated model selection

- Dataset from Kaggle

- No manual coding required (no-code ML pipeline)

Libraries/Tools:

- AutoAI (built-in to Watson Studio)

- Web UI for testing deployed models

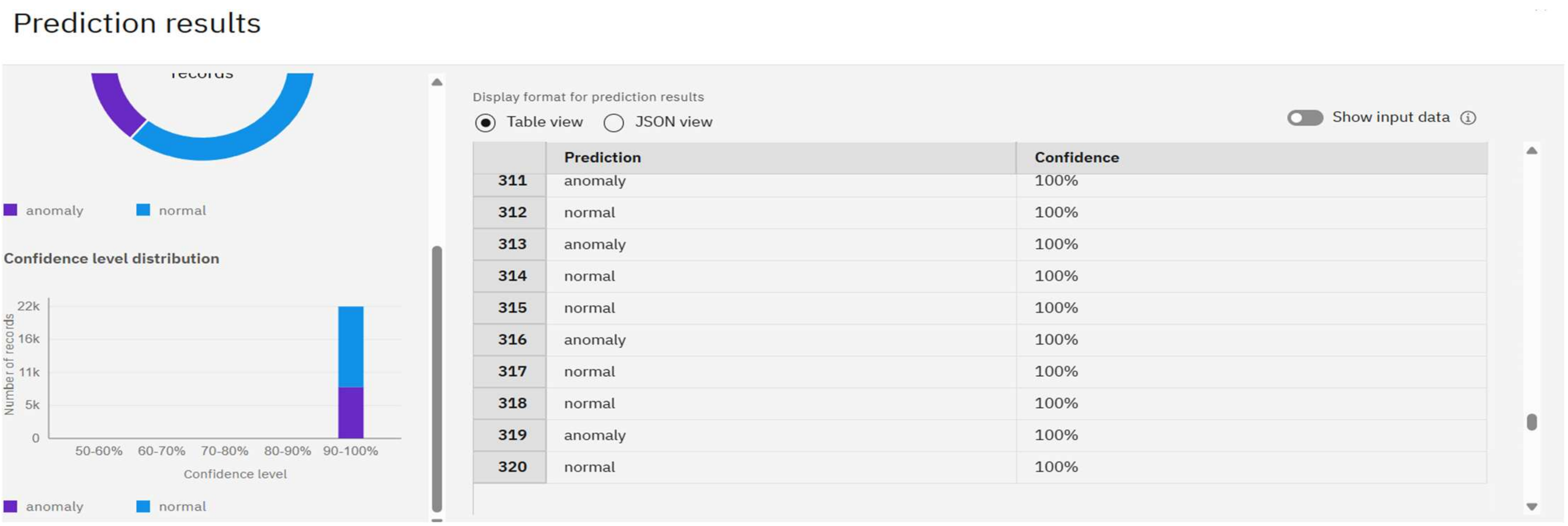
ALGORITHM & DEPLOYMENT

- Algorithm Used:
- - Decision Tree Classifier (selected by AutoAI)
- Input Features:
  - Network traffic attributes: protocol type, service, byte counts, flag, host behavior, etc.
- Training Process:
  - - AutoAI explored multiple pipelines
  - - Best pipeline selected based on accuracy/F1-score
  - - No manual tuning required
- Deployment:
  - Model deployed as an online REST API using IBM Watson Machine Learning
- Tested via UI and ready for integration with other systems

RESULT

Model successfully trained and deployed using IBM Watson Studio.

Prediction interface available for real-time classification of network activity.



Display format for prediction results

● Table view ○ JSON view

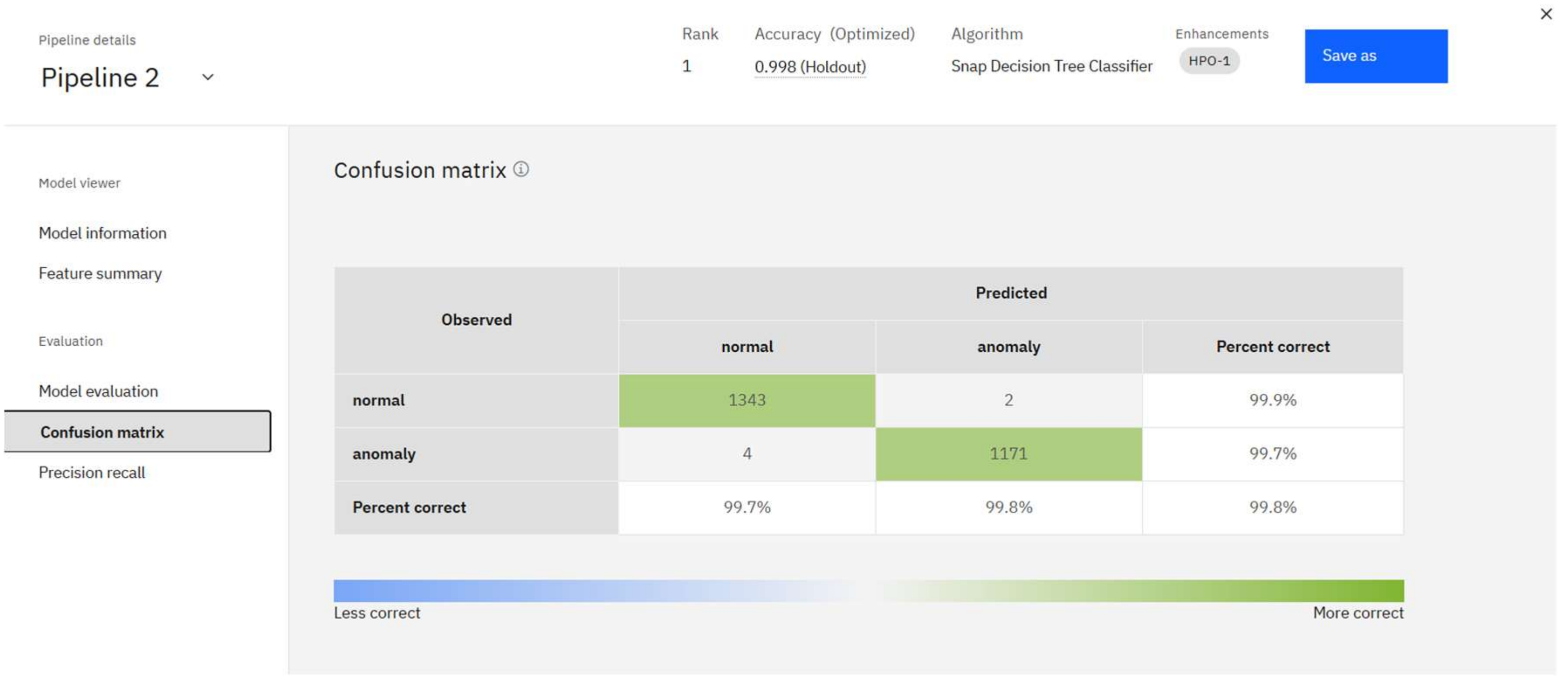
Show input data ⓘ

	Prediction	Confidence
311	anomaly	100%
312	normal	100%
313	anomaly	100%
314	normal	100%
315	normal	100%
316	anomaly	100%
317	normal	100%
318	normal	100%
319	anomaly	100%
320	normal	100%

RESULT

Model successfully trained and deployed using IBM Watson Studio.

Prediction interface available for real-time classification of network activity.



Rank	Accuracy (Optimized)	Algorithm	Enhancements
1	0.998 (Holdout)	Snap Decision Tree Classifier	HPO-1

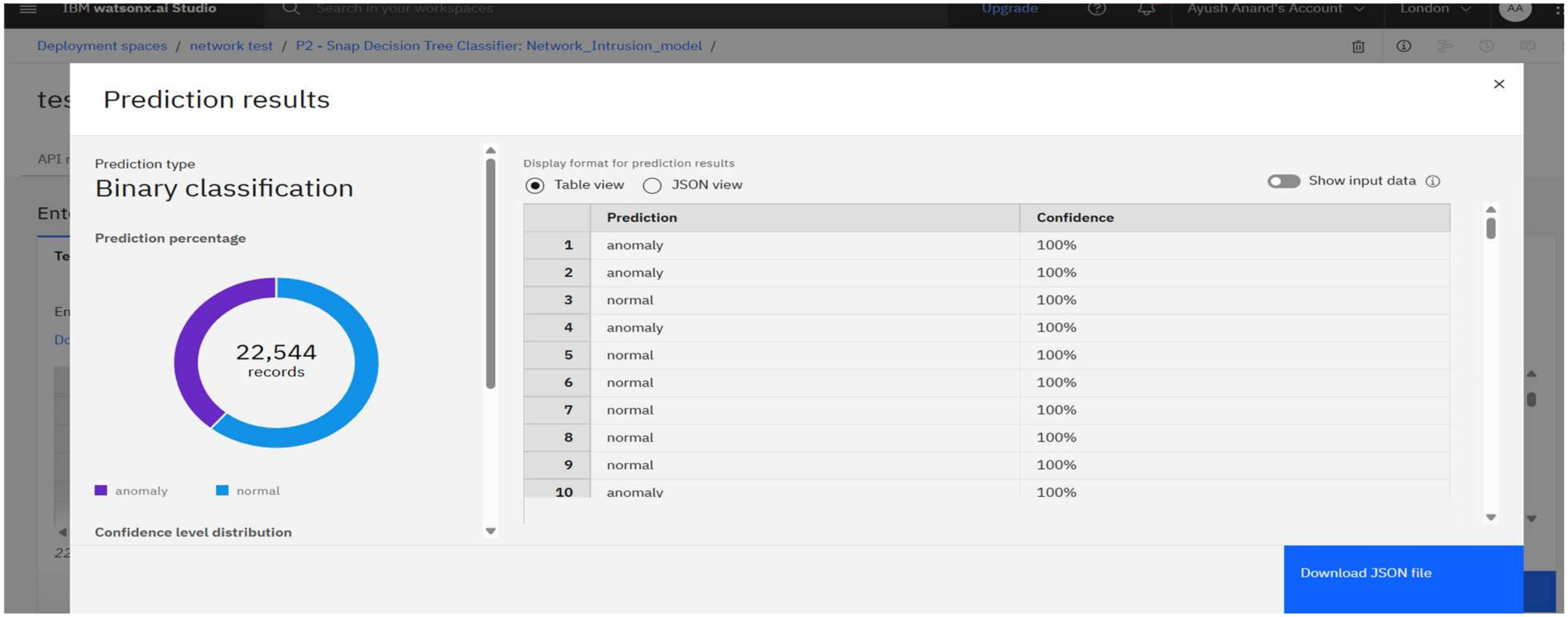
Confusion matrix ⓘ

Observed	Predicted		
	normal	anomaly	Percent correct
normal	1343	2	99.9%
anomaly	4	1171	99.7%
Percent correct	99.7%	99.8%	99.8%

RESULT

Model successfully trained and deployed using IBM Watson Studio.

Prediction interface available for real-time classification of network activity.


IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Ayush Anand's Account
London
AA
Deployment spaces / network test / P2 - Snap Decision Tree Classifier: Network_Intrusion_model /
22,544
records
anomaly
normal
Download JSON file

Prediction results

Prediction type

Binary classification

Prediction percentage

Confidence level distribution

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%

CONCLUSION

- The Decision Tree model deployed on IBM Cloud successfully detects network intrusions.
- AutoAI simplified the entire ML lifecycle, from training to deployment.
- This solution provides a foundational step toward intelligent and scalable intrusion detection systems.

FUTURE SCOPE

- Upgrade to ensemble models like Random Forest or XGBoost

- Real-time data streaming and alert generation

- Integration with dashboards or SIEM tools

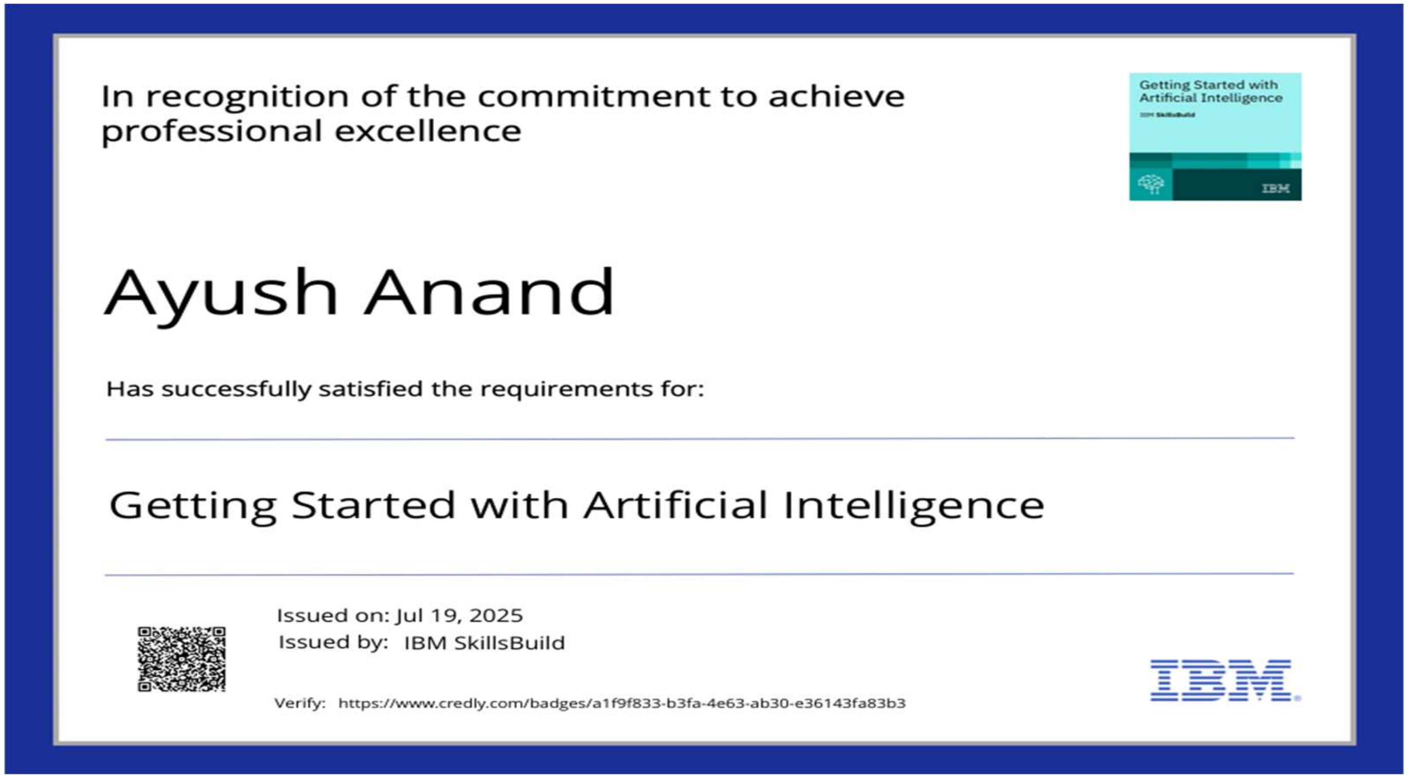
- Fine-grained classification of individual attack types (DoS, R2L, etc.)

REFERENCES

- - https://www.kaggle.com/datasets/sampadab17/networkintrusion-detection
- - IBM Watson Studio documentation
- - IBM Cloud Machine Learning Services
- - Scikit-learn documentation (for Decision Tree concepts)

IBM CERTIFICATIONS

Getting Started with Artifical Intelligence



In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence
IBM SkillsBuild
IBM

Ayush Anand

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

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

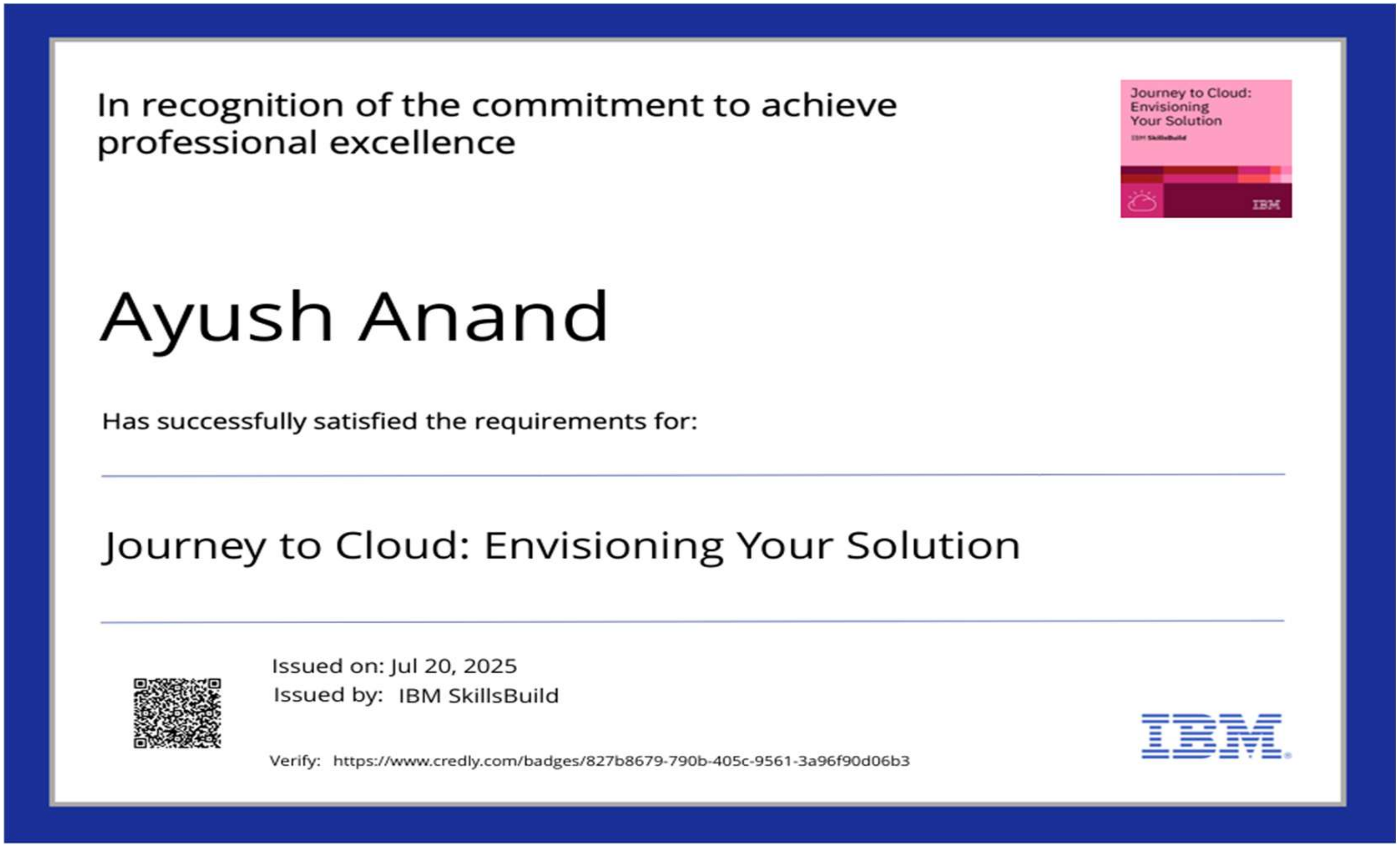
Verify: https://www.credly.com/badges/a1f9f833-b3fa-4e63-ab30-e36143fa83b3

IBM

edunet
foundation

IBM CERTIFICATIONS

Journey to Cloud


Journey to Cloud:
Envisioning
Your Solution
IBM SkillsBuild
IBM

In recognition of the commitment to achieve professional excellence

Ayush Anand

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

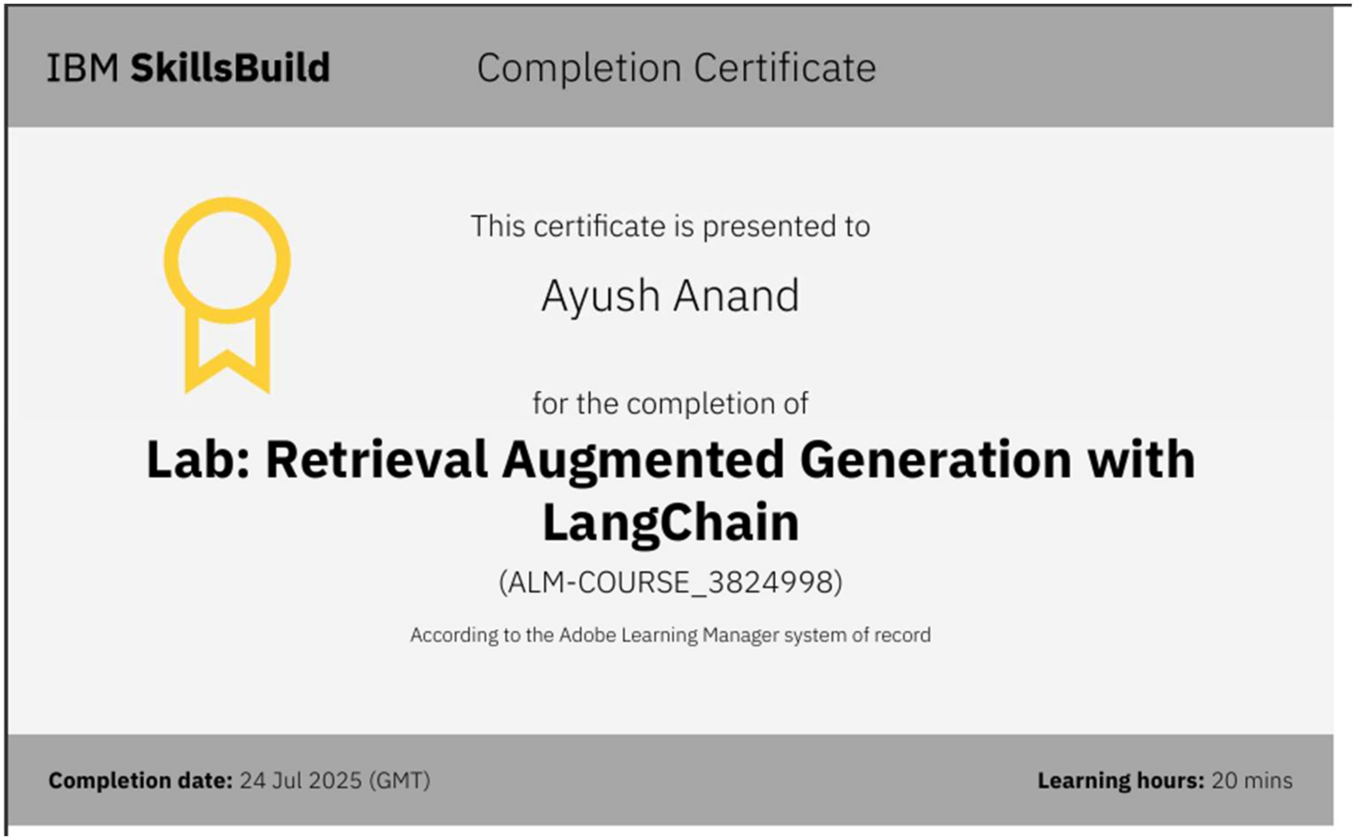
Issued on: Jul 20, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/827b8679-790b-405c-9561-3a96f90d06b3

IBM

IBM CERTIFICATIONS

RAG lab



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Ayush Anand

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

THANK YOU