CAPSTONE PROJECT

NETWORK INTRUSION DETECTION USING MACHINE LEARNING

Presented By:
1. Pratham.r.pasi - SSJCET- EXTC

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

Example: Modern digital infrastructure faces relentless threats from cyber-attacks that put sensitive data and organizational integrity at risk. As communication networks expand and traffic intensifies, the timely detection of malicious activity becomes crucial. Current systems often falter in recognizing sophisticated or novel intrusion patterns, leaving networks vulnerable. The challenge is to develop an intelligent, automated, and adaptive system that not only detects a spectrum of cyber-attacks—such as Denial-of-Service (DoS), Probing, Remote-to-Local (R2L), and User-to-Root (U2R)—but does so faster and more accurately than traditional approaches.

PROPOSED SOLUTION

- The proposed system leverages cutting-edge machine learning algorithms to build a robust Network Intrusion Detection System (NIDS). By continuously monitoring and analyzing network traffic, the model learns to recognize a broad spectrum of attack patterns as well as normal behavior. Training is conducted using the benchmark Kaggle dataset for network intrusion detection, ensuring model relevance and efficacy. Deployment on IBM Cloud Lite provides a scalable, easily accessible, and highly available environment, enabling real-time detection and rapid, automated responses to emerging network threats.

Key solution components include:

- Comprehensive data ingestion
- Rigorous data preprocessing and feature engineering
- Advanced machine learning model training and optimization
- Seamless deployment as a real-time cloud-based API

SYSTEM APPROACH

- **Data Source:** Network Intrusion Detection dataset from Kaggle
- **Platform:** IBM Cloud Lite (mandatory per project requirements)
- **Programming Language & Libraries:** Python, Pandas, Scikit-learn, XGBoost, IBM Watson Studio
- **Development Process**: Data collection, cleaning, feature extraction, model training, validation, and deployment as a secure API on IBM Cloud Lite

ALGORITHM & DEPLOYMENT

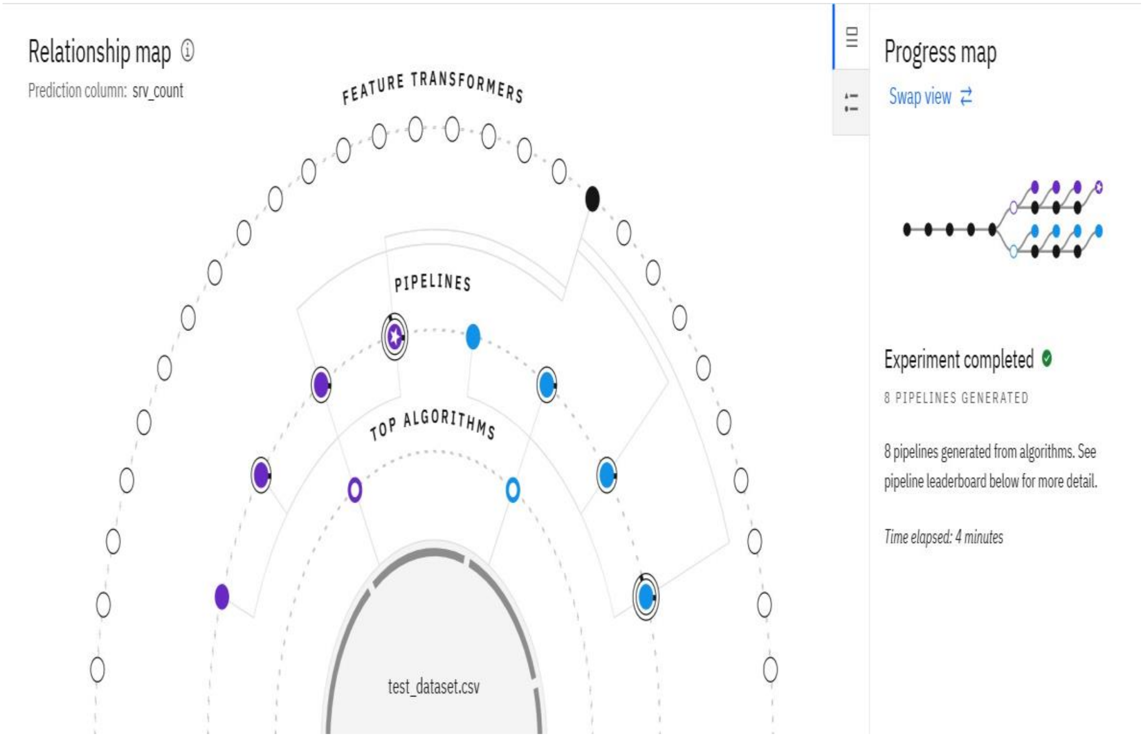
- **Algorithm Selection:** Ensemble learning methods such as Random Forest or XGBoost are selected for their accuracy in multi-class classification of network intrusions.

- **Input Features:** Diverse feature set encompassing protocol types, connection time, data throughput, flag status, and specific attack indicators.

- **Training & Validation:** Systematic train-test split, stratified sampling, and hyperparameter optimization ensure model robustness and generalizability.

- **Deployment:** The finalized model is containerized and exposed as a REST API on IBM Cloud Lite, allowing real-time querying and seamless integration with existing monitoring infrastructure.

RESULT

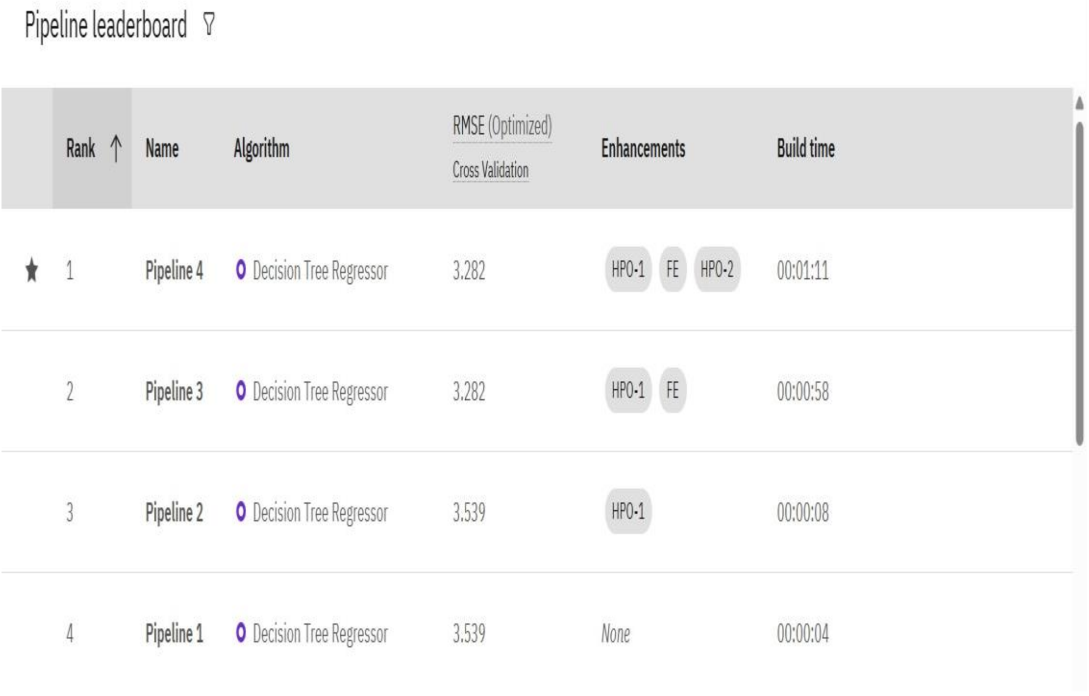


Experiment completed

8 PIPELINES GENERATED

8 pipelines generated from algorithms. See pipeline leaderboard below for more detail.

Time elapsed: 4 minutes



Pipeline leaderboard

	Rank	Name	Algorithm	RMSE (Optimized) Cross Validation	Enhancements	Build time
★	1	Pipeline 4	Decision Tree Regressor	3.282	HPO-1 FE HPO-2	00:01:11
	2	Pipeline 3	Decision Tree Regressor	3.282	HPO-1 FE	00:00:58
	3	Pipeline 2	Decision Tree Regressor	3.539	HPO-1	00:00:08
	4	Pipeline 1	Decision Tree Regressor	3.539	*None*	00:00:04

CONCLUSION

- This project demonstrates an effective and scalable artificial intelligence-driven solution for proactive network security. By combining state-of-the-art machine learning with IBM Cloud deployment, the system significantly improves threat detection capabilities and response times, substantially enhancing the cybersecurity posture of modern organizations.

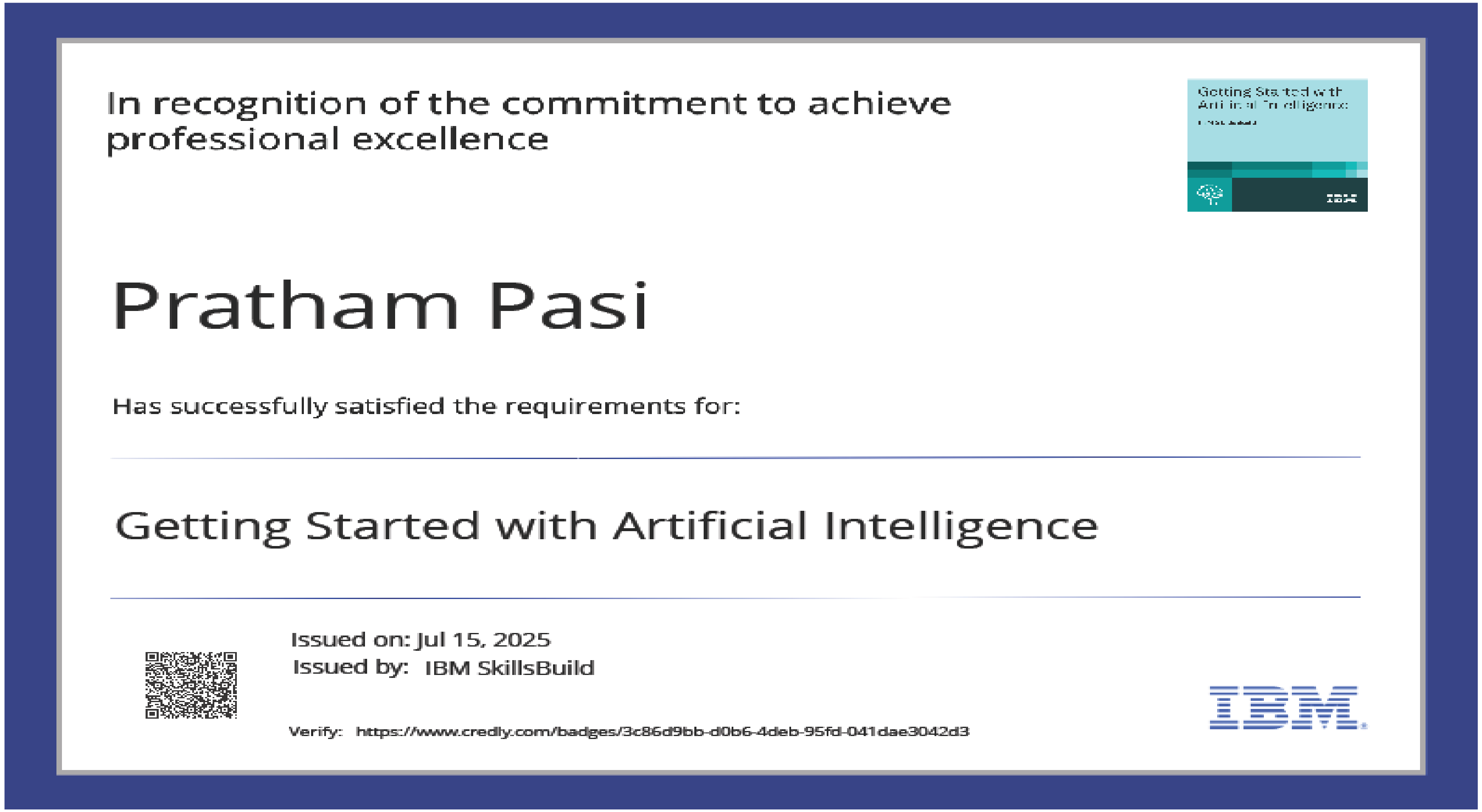
FUTURE SCOPE

- Expansion to larger, real-time datasets for even greater model accuracy
- Integration of deep learning architectures for anomaly and zero-day attack detection
- Deployment across multi-cloud and hybrid cloud environments
- Automated incident response and feedback mechanisms for continuous system improvement

REFERENCES

- List and cite all relevant research papers, datasets (such as the Kaggle NIDS dataset), and IBM Cloud documentation leveraged throughout the project.

IBM CERTIFICATIONS



In recognition of the commitment to achieve professional excellence

Pratham Pasi

Has successfully satisfied the requirements for:

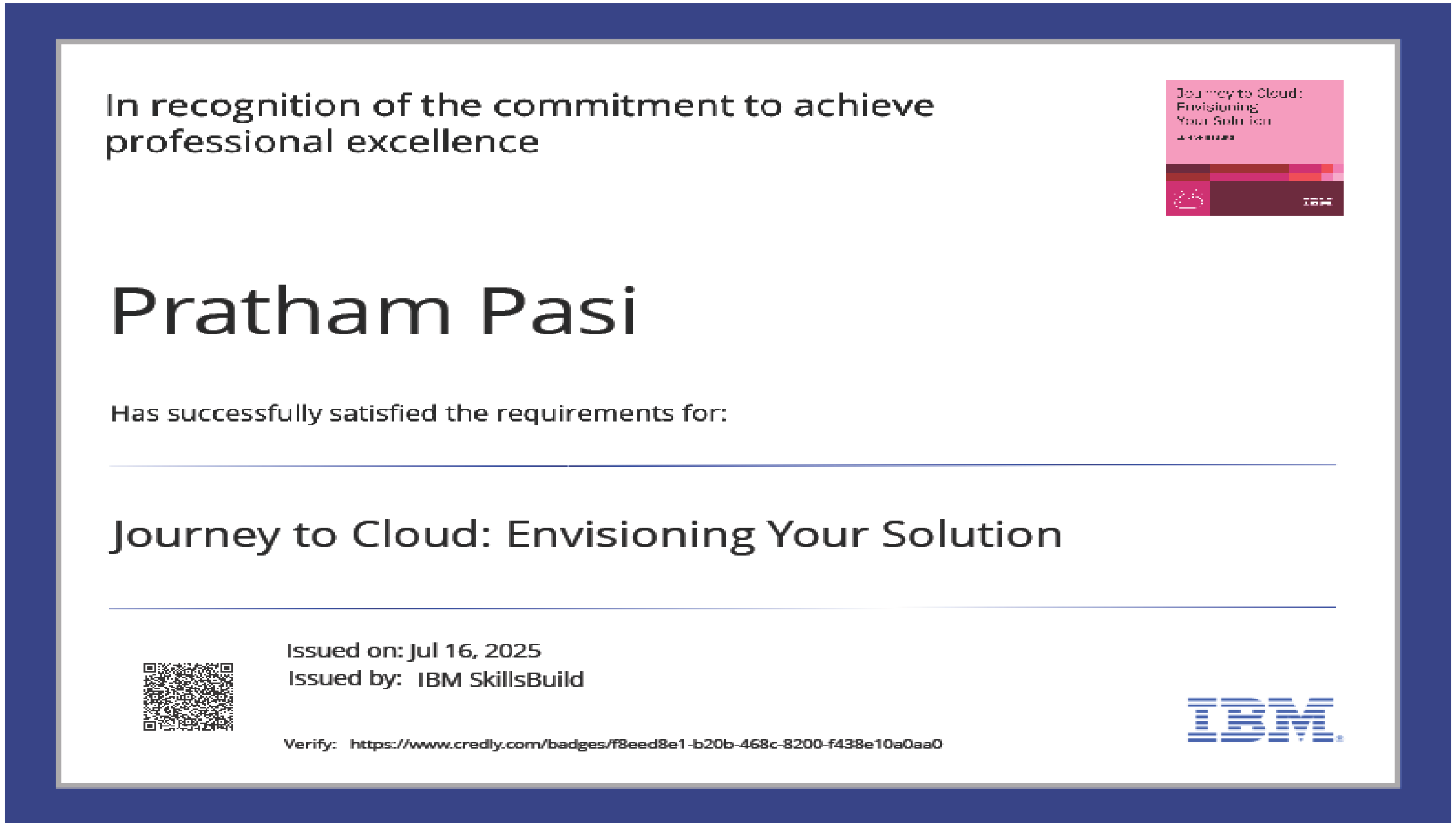
Getting Started with Artificial Intelligence

Issued on: Jul 15, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/3c86d9bb-d0b6-4deb-95fd-041dae3042d3

Getting Started with Artificial Intelligence
IBM
IBM

IBM CERTIFICATIONS



In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution
IBM

Pratham Pasi

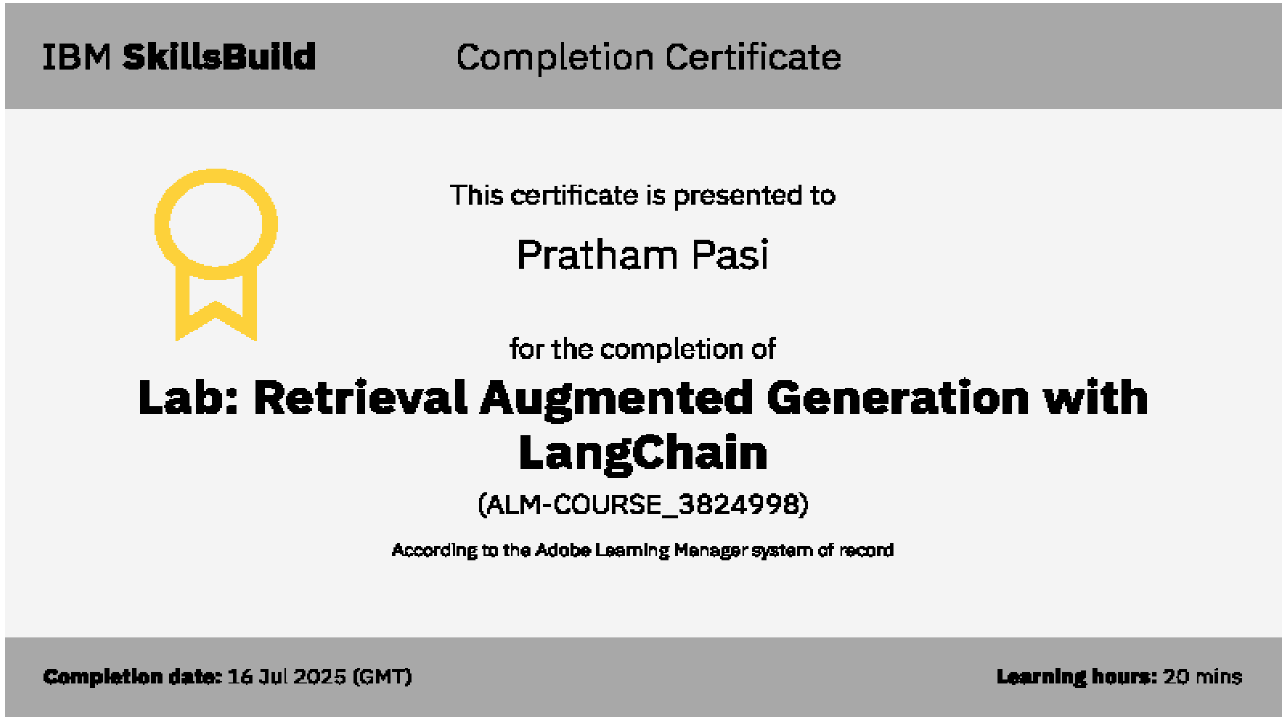
Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 16, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/f8eed8e1-b20b-468c-8200-f438e10a0aa0

IBM CERTIFICATIONS



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Pratham Pasi

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 16 Jul 2025 (GMT)

Learning hours: 20 mins

GIT-HUB LINK

- https://github.com/pratham133/network-intrusion-detection-ml.git

THANK YOU

edunet
foundation