CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. Student Name-Abhinav Tripathi
2.College-Name-University of Lucknow
3.Branch- Electronics and Communication Engineering(ECE)
4.Student ID - STU68335878106bb1748195448

edunet foundation

OUTLINE

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

edunet foundation

PROBLEM STATEMENT

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

1. *Data Collection*: Gather network traffic data, including packet captures, logs, and threat intelligence feeds.

2. *Data Preprocessing*: Clean and preprocess data, handle missing values, and extract relevant features (e.g., packet headers, payload analysis).

3. *Machine Learning Algorithm*: Implement a machine learning model (e.g., Random Forest, SVM, or Deep Learning) to detect and classify network intrusions based on patterns and anomalies.

4. *Deployment*: Develop a real-time intrusion detection system with a user-friendly interface for security analysts.

5. *Evaluation*: Assess model performance using metrics (accuracy, precision, recall, F1-score) and fine-tune based on feedback and continuous monitoring.

SYSTEM APPROACH

1. *Network Monitoring*: Continuously monitor network traffic to identify potential security threats.
2. *Data Collection*: Gather network traffic data, including packet captures and logs.
3. *Data Analysis*: Analyze collected data using machine learning algorithms to detect anomalies and identify potential threats.
4. *Threat Detection*: Identify and classify potential security threats, including known and unknown attacks.
5. *Alert Generation*: Generate alerts for security analysts and administrators when potential threats are detected.
6. *Incident Response*: Provide incident response capabilities to quickly respond to security threats.

Key Features:

- Real-time network monitoring and threat detection
- Advanced machine learning-based analysis
- Comprehensive threat classification and alert generation
- Integration with incident response systems

ALGORITHM & DEPLOYMENT

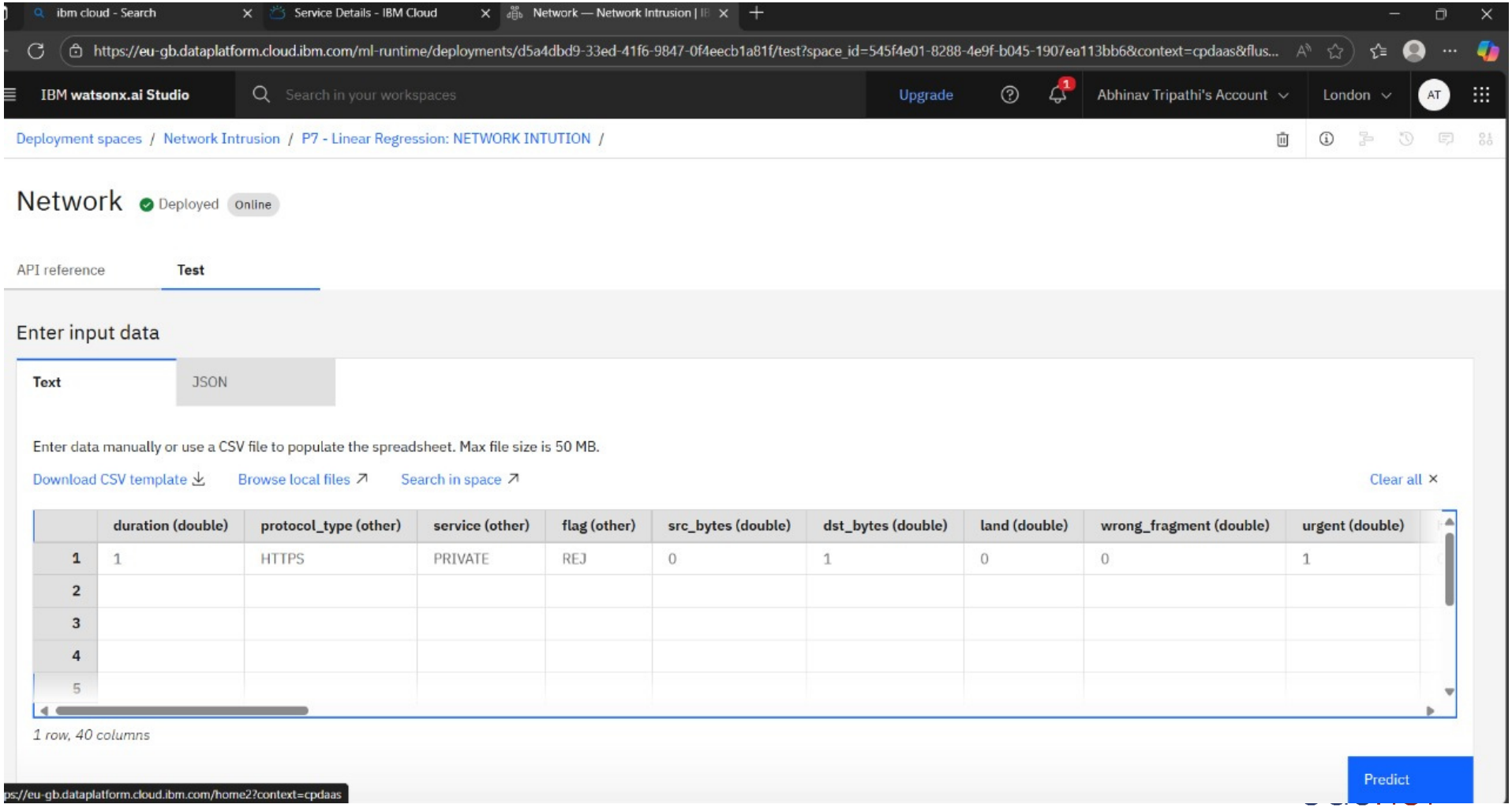
- *Algorithm:*
- 1. *Random Forest*: Utilize Random Forest algorithm for anomaly detection and classification.
- 2. *Support Vector Machine (SVM)*: Employ SVM for classification and regression tasks.
- 3. *Deep Learning*: Leverage deep learning techniques, such as Convolutional Neural Networks (CNNs) or Recurrent Neural Networks (RNNs), for advanced threat detection.
- *Deployment on IBM Cloud Lite:*
- 1. *Cloud Foundry*: Deploy the NIDS application on IBM Cloud Lite using Cloud Foundry.
- 2. *Containerization*: Utilize Docker containers to package the application and ensure seamless deployment.
- 3. *Serverless Computing*: Leverage IBM Cloud Functions (serverless computing) to scale the application and reduce costs.
- 4. *Monitoring and Logging*: Use IBM Cloud Monitoring and Logging services to track application performance and logs.

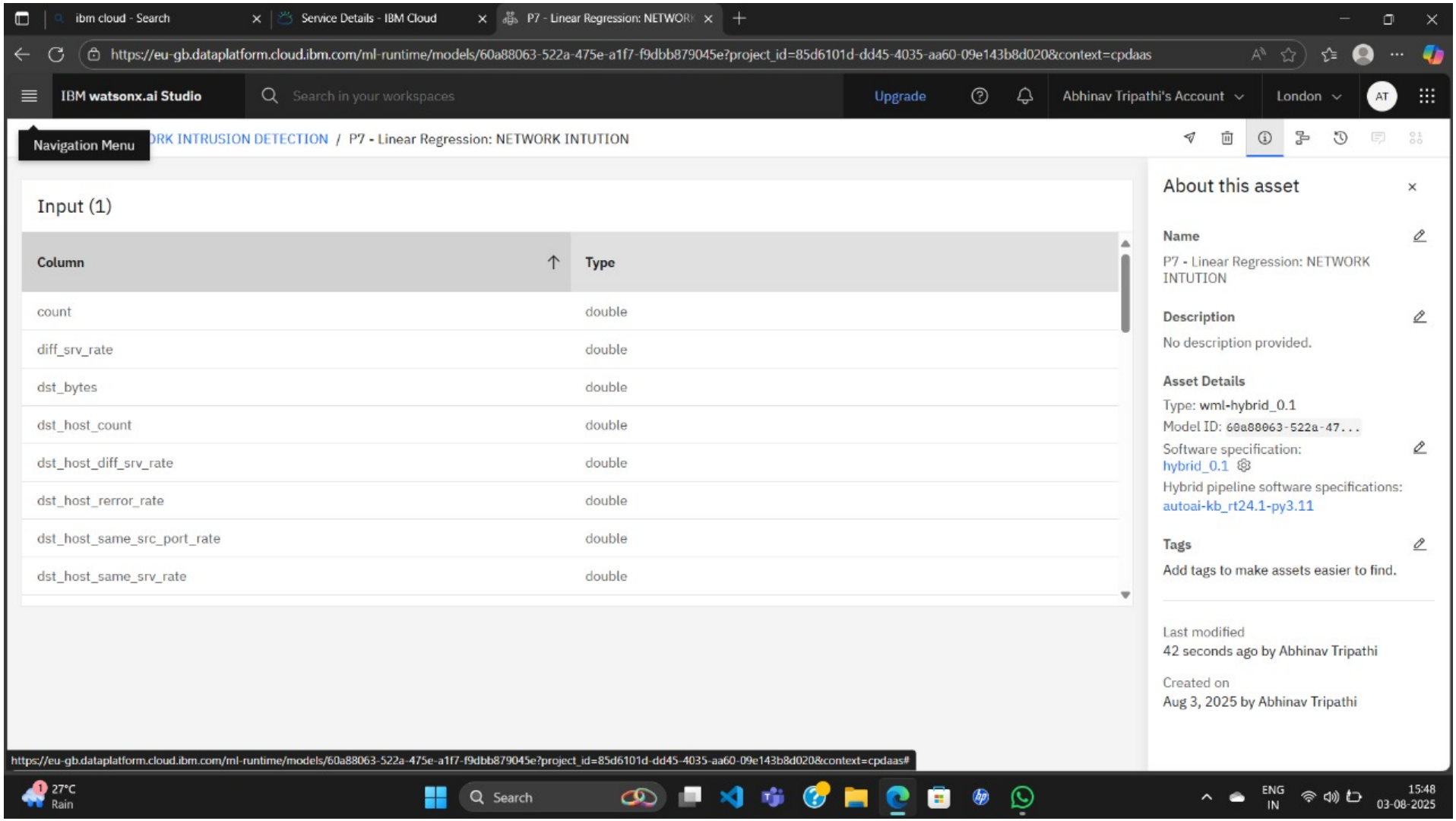
RESULT

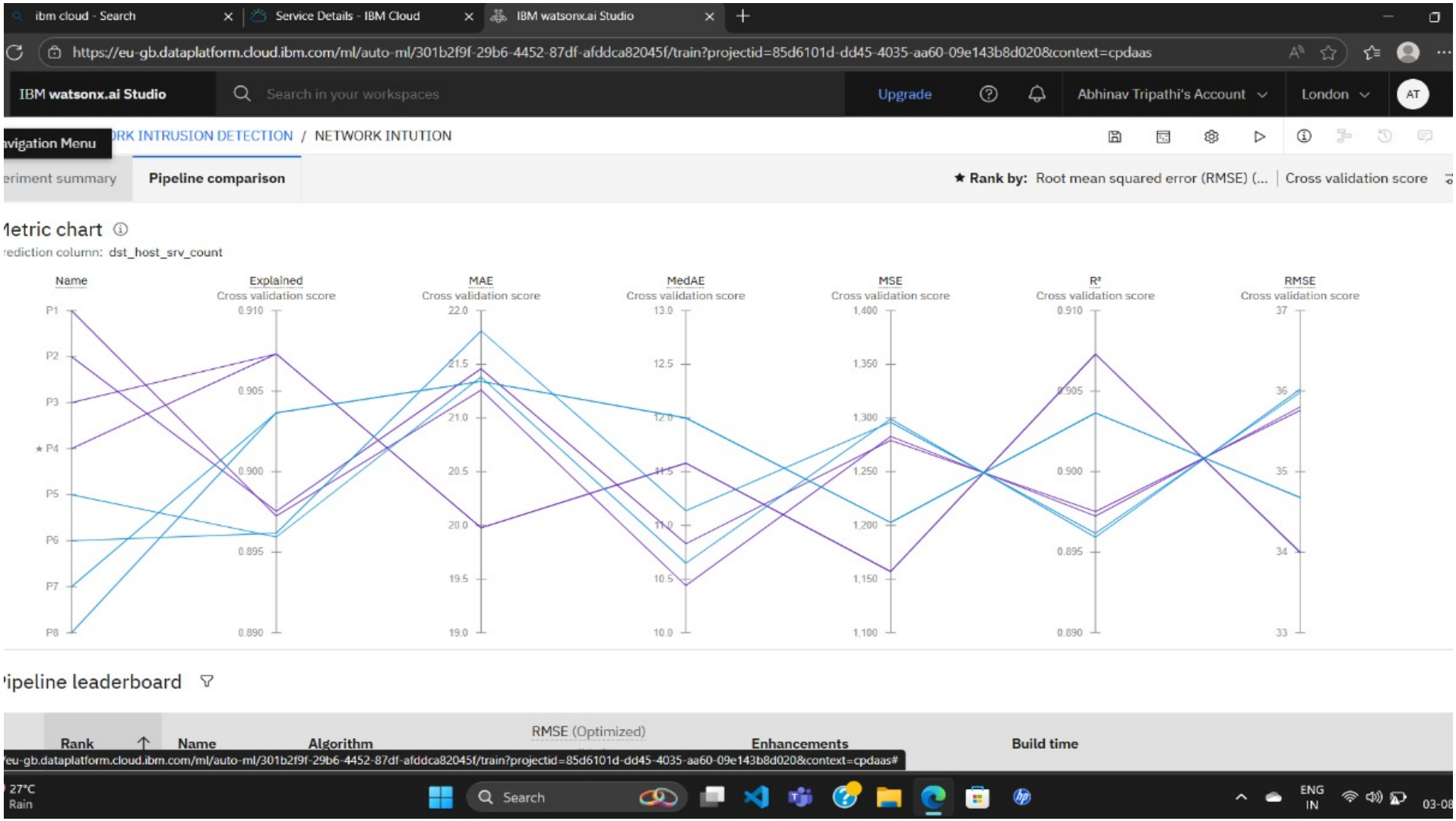
https://github.com/abhinavtripathi-cloud/Network-Intrusion-Detection.git

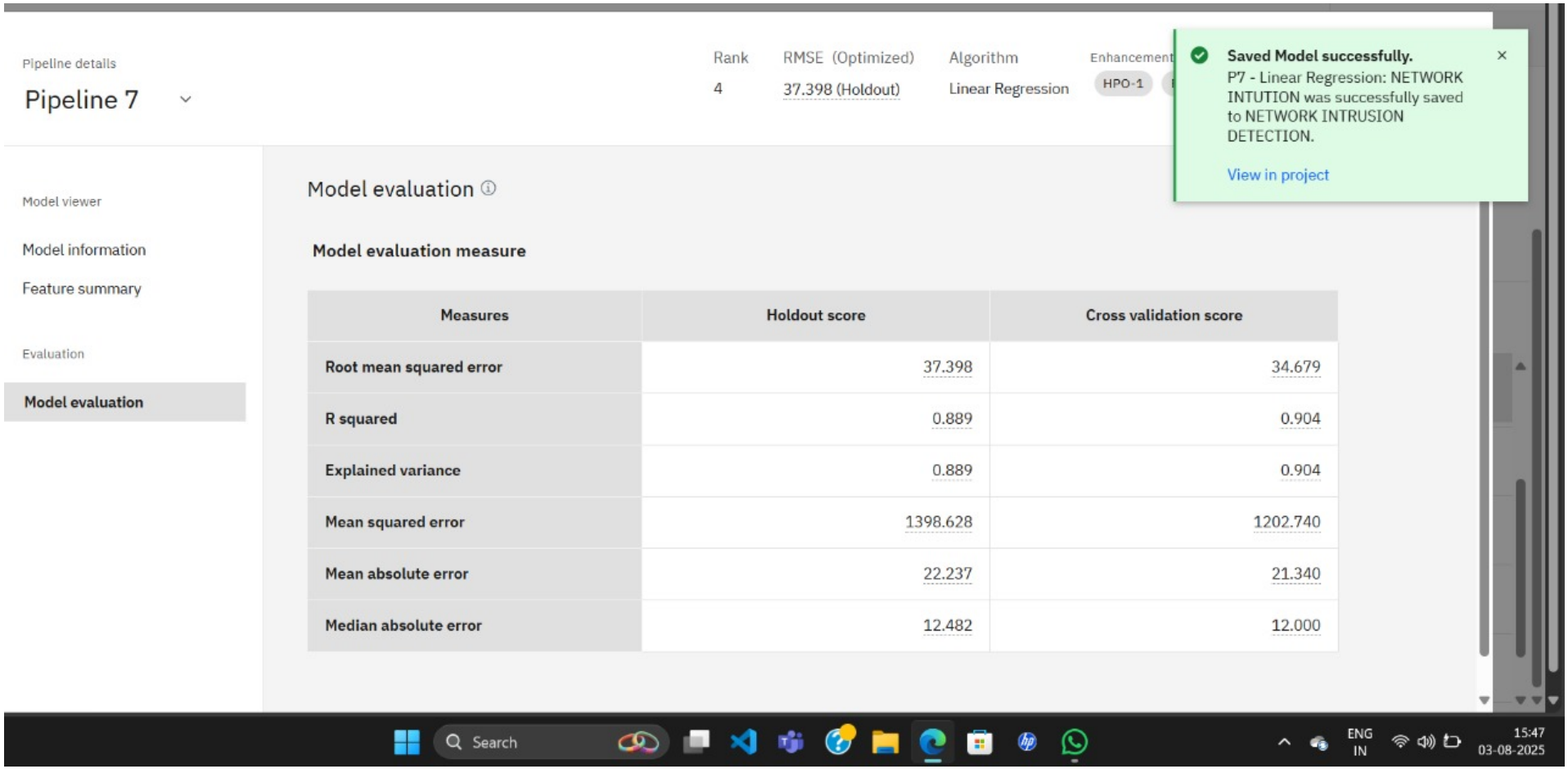
https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

edunet foundation

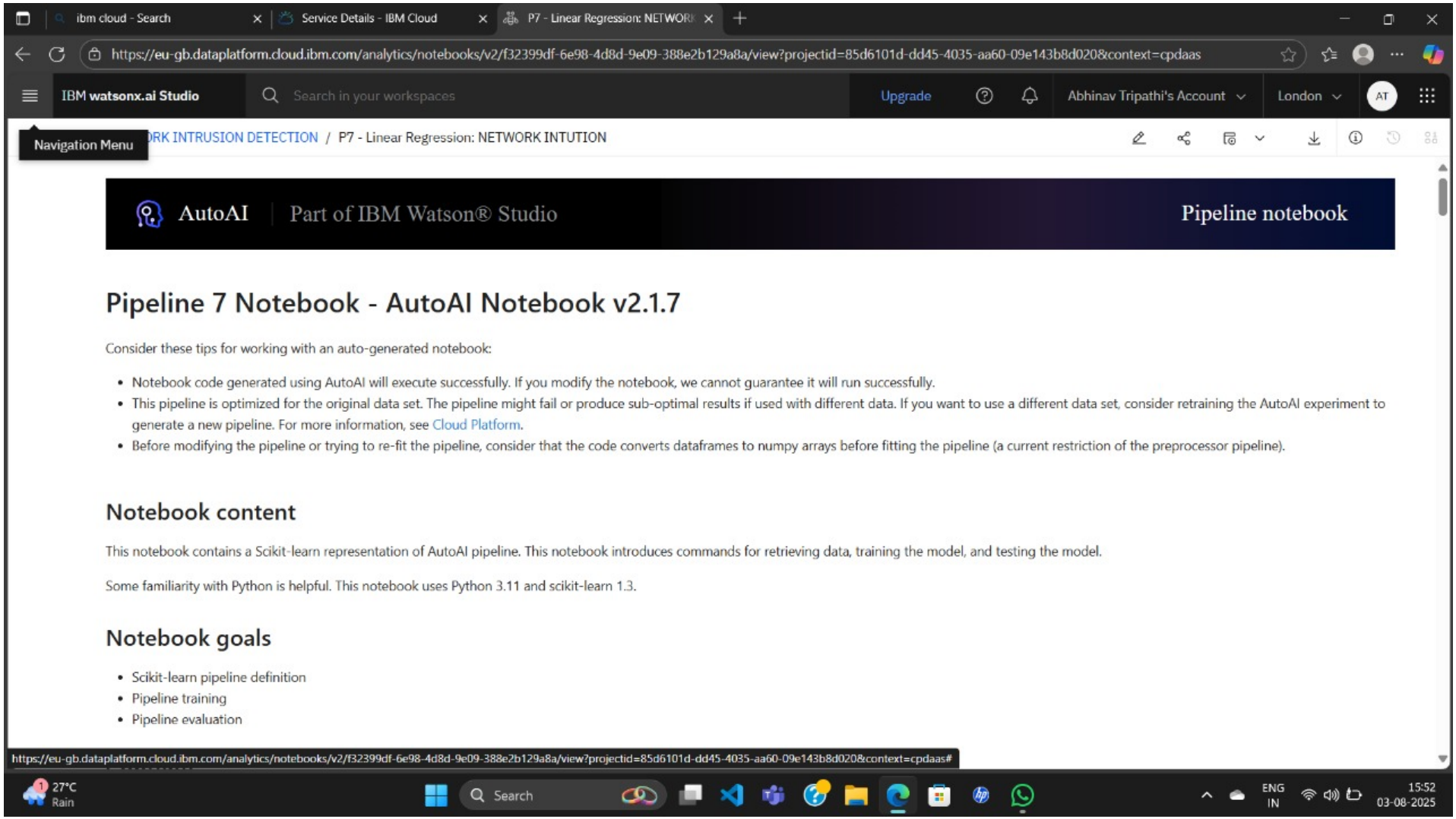

ibm cloud - Search
Service Details - IBM Cloud
Network — Network Intrusion | IB
https://eu-gb.dataplatform.cloud.ibm.com/ml-runtime/deployments/d5a4dbd9-33ed-41f6-9847-0f4eecb1a81f/test?space_id=545f4e01-8288-4e9f-b045-1907ea113bb6&context=cpdaas&flus...
IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Abhinav Tripathi's Account
London
AT
Deployment spaces / Network Intrusion / P7 - Linear Regression: NETWORK INTUTION /
Network
Deployed
Online
API reference
Test
Enter input data
Text
JSON
Enter data manually or use a CSV file to populate the spreadsheet. Max file size is 50 MB.
Download CSV template
Browse local files
Search in space
Clear all
duration (double)
protocol_type (other)
service (other)
flag (other)
src_bytes (double)
dst_bytes (double)
land (double)
wrong_fragment (double)
urgent (double)
1 HTTPS PRIVATE REJ 0 1 0 0 1
2
3
4
5
1 row, 40 columns
Predict
https://eu-gb.dataplatform.cloud.ibm.com/home2?context=cpdaas


ibm cloud - Search
Service Details - IBM Cloud
P7 - Linear Regression: NETWORK
https://eu-gb.dataplatform.cloud.ibm.com/ml-runtime/models/60a88063-522a-475e-a1f7-f9dbb879045e?project_id=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas
IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Abhinav Tripathi's Account
London
AT
Navigation Menu
ORK INTRUSION DETECTION / P7 - Linear Regression: NETWORK INTUTION
Input (1)
Column
Type
count
double
diff_srv_rate
double
dst_bytes
double
dst_host_count
double
dst_host_diff_srv_rate
double
dst_host_rerror_rate
double
dst_host_same_src_port_rate
double
dst_host_same_srv_rate
double
About this asset
Name
P7 - Linear Regression: NETWORK INTUTION
Description
No description provided.
Asset Details
Type: wml-hybrid_0.1
Model ID: 60a88063-522a-47...
Software specification:
hybrid_0.1
Hybrid pipeline software specifications:
autoai-kb_rt24.1-py3.11
Tags
Add tags to make assets easier to find.
Last modified
42 seconds ago by Abhinav Tripathi
Created on
Aug 3, 2025 by Abhinav Tripathi
https://eu-gb.dataplatform.cloud.ibm.com/ml-runtime/models/60a88063-522a-475e-a1f7-f9dbb879045e?project_id=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas#
27°C
Rain
Search
ENG
IN
15:48
03-08-2025


ibm cloud - Search
Service Details - IBM Cloud
IBM watsonx.ai Studio
https://eu-gb.dataplatform.cloud.ibm.com/ml/auto-ml/301b2f9f-29b6-4452-87df-afddca82045f/train?projectid=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas
IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Abhinav Tripathi's Account
London
AT
ORK INTRUSION DETECTION / NETWORK INTUTION
eriment summary
Pipeline comparison
★ Rank by: Root mean squared error (RMSE) (...
Cross validation score
Metric chart
rediction column: dst_host_srv_count
Name
Explained
Cross validation score
MAE
Cross validation score
MedAE
Cross validation score
MSE
Cross validation score
R²
Cross validation score
RMSE
Cross validation score
P1
P2
P3
★ P4
P5
P6
P7
P8
0.910
0.905
0.900
0.895
0.890
22.0
21.5
21.0
20.5
20.0
19.5
19.0
13.0
12.5
12.0
11.5
11.0
10.5
10.0
1,400
1,350
1,300
1,250
1,200
1,150
1,100
0.910
0.905
0.900
0.895
0.890
37
36
35
34
33
ipeline leaderboard
Rank
Name
Algorithm
RMSE (Optimized)
Enhancements
Build time
eu-gb.dataplatform.cloud.ibm.com/ml/auto-ml/301b2f9f-29b6-4452-87df-afddca82045f/train?projectid=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas#
27°C
Rain
Search
ENG
IN
03-08



edunet foundation


ibm cloud - Search
Service Details - IBM Cloud
P7 - Linear Regression: NETWORK
https://eu-gb.dataplatform.cloud.ibm.com/analytics/notebooks/v2/f32399df-6e98-4d8d-9e09-388e2b129a8a/view?projectid=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas
IBM watsonx.ai Studio
Search in your workspaces
Upgrade
Abhinav Tripathi's Account
London
AT
Navigation Menu
ORK INTRUSION DETECTION / P7 - Linear Regression: NETWORK INTUTION
AutoAI | Part of IBM Watson® Studio
Pipeline notebook
Pipeline 7 Notebook - AutoAI Notebook v2.1.7
Consider these tips for working with an auto-generated notebook:
Notebook code generated using AutoAI will execute successfully. If you modify the notebook, we cannot guarantee it will run successfully.
This pipeline is optimized for the original data set. The pipeline might fail or produce sub-optimal results if used with different data. If you want to use a different data set, consider retraining the AutoAI experiment to generate a new pipeline. For more information, see Cloud Platform.
Before modifying the pipeline or trying to re-fit the pipeline, consider that the code converts dataframes to numpy arrays before fitting the pipeline (a current restriction of the preprocessor pipeline).
Notebook content
This notebook contains a Scikit-learn representation of AutoAI pipeline. This notebook introduces commands for retrieving data, training the model, and testing the model.
Some familiarity with Python is helpful. This notebook uses Python 3.11 and scikit-learn 1.3.
Notebook goals
Scikit-learn pipeline definition
Pipeline training
Pipeline evaluation
https://eu-gb.dataplatform.cloud.ibm.com/analytics/notebooks/v2/f32399df-6e98-4d8d-9e09-388e2b129a8a/view?projectid=85d6101d-dd45-4035-aa60-09e143b8d020&context=cpdaas#
27°C
Rain
Search
ENG
IN
15:52
03-08-2025

CONCLUSION

- Effective network intrusion detection requires a combination of machine learning, advanced threat detection, and continuous monitoring to identify and prevent unauthorized access, ensuring the security and integrity of network systems. By leveraging AI-powered intrusion detection systems, organizations can improve detection accuracy, reduce false positives, and respond quickly to potential threats. Implementing a robust intrusion detection system is crucial for protecting sensitive data and maintaining the trust of customers and stakeholders

FUTURE SCOPE

.The future scope of network intrusion detection systems (NIDS) is vast and exciting, with several areas of research and development worth exploring:

Key Areas:

- *Quantum-Enhanced Machine Learning*: Integrating quantum computing with machine learning algorithms to improve the detection accuracy and efficiency of NIDS.

- *Federated Learning*: Implementing federated learning techniques to enable multiple organizations to collaborate on intrusion detection while maintaining data privacy.

- *Explainable AI (XAI)*: Developing XAI-powered NIDS to provide transparency and interpretability in AI-driven decision-making.

- *Advanced Methodologies*: Exploring advanced methodologies like deep learning, reinforcement learning, and ensemble methods to improve NIDS performance.

- *Metaverse Security*: Developing NIDS specifically designed for the Metaverse, focusing on real-time threat detection and response.[1][2][3][4]

Future Directions:

- *Improving Detection Accuracy*: Continuously improving detection accuracy and reducing false positives through advanced algorithms and techniques.

- *Enhancing Scalability*: Developing NIDS that can handle large volumes of network traffic and scale to meet growing demands.

- *Integrating with Incident Response*: Integrating NIDS with incident response plans to enable quick and effective response to detected threats.

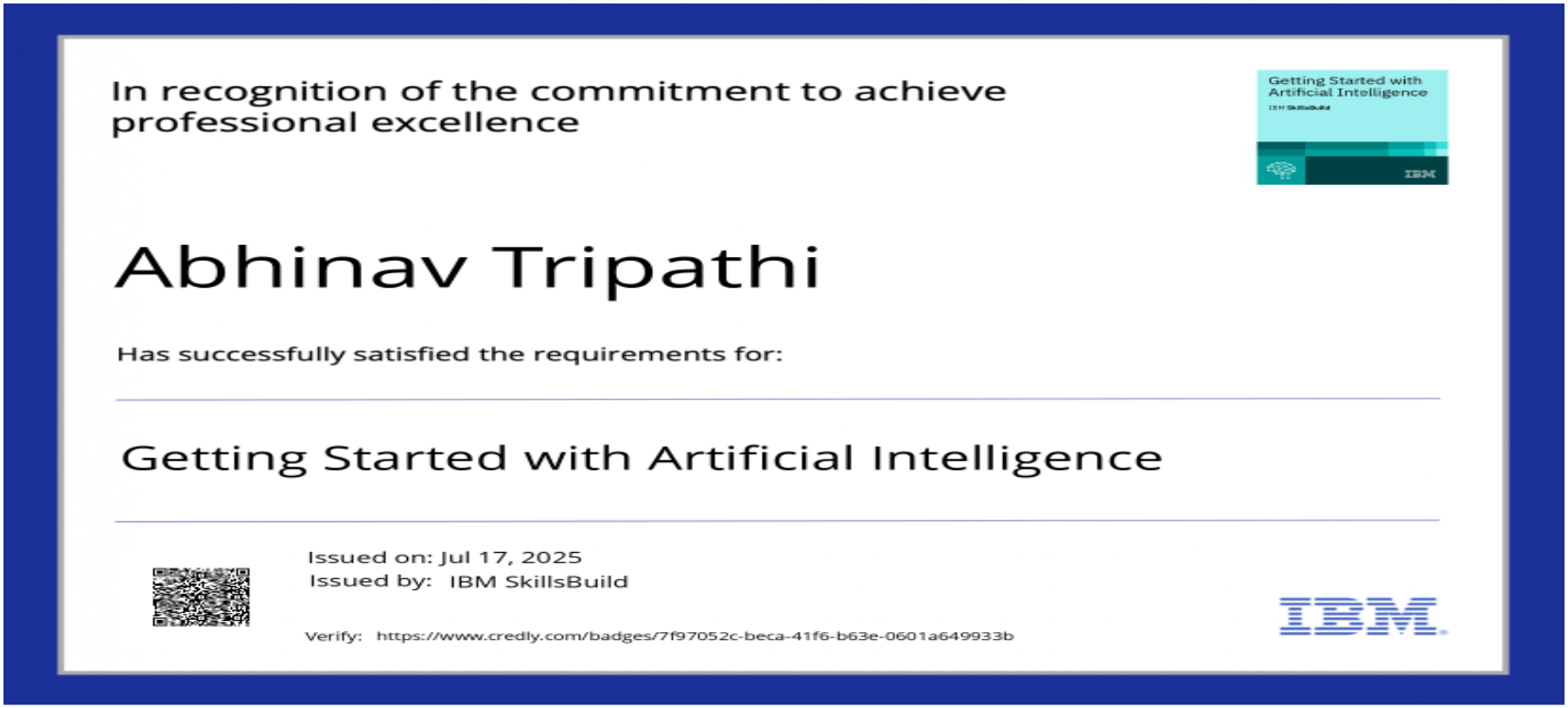
REFERENCES

- Liu, Y., Wang, L., & Wang, X. (2020). A survey on deep learning for network intrusion detection. Journal of Intelligent Information Systems, 57(2), 279-297.

- Zhao, Y., Li, M., & Lai, L. (2021). Federated learning for network intrusion detection. IEEE Transactions on Neural Networks and Learning Systems, 32(5), 2111-2122.

- Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., ... & Gao, X. (2018). Machine learning for network intrusion detection: A survey. IEEE Communications Surveys & Tutorials, 20(2), 1328-1356.

IBM CERTIFICATIONS



In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence

IBM

Abhinav Tripathi

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

Issued on: Jul 17, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/7f97052c-beca-41f6-b63e-0601a649933b

IBM

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Abhinav Tripathi

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

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

Verify: https://www.credly.com/badges/7f67365f-800d-4c71-a7bd-bdf02d03db31

IBM

edunet foundation

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Abhinav Tripathi

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

edunet
foundation