
CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:

1. Srinjoy Samanta_RCC Institute of information Technology_CSE

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

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.

Kaggle dataset link – <https://www.kaggle.com/datasets/sampadab17/networkintrusion-detection>

PROPOSED SOLUTION

Data Ingestion

- Download dataset from Kaggle.
- Use **IBM Cloud Object Storage (COS)** to upload and store the dataset.
- Access the dataset in IBM Cloud using **IBM Watson Studio Notebooks** or **Cloud Functions**.

2. Data Preprocessing

- Remove duplicates, missing values, or irrelevant features.
- Normalize/scale numeric features.
- Encode categorical features (e.g., protocol_type, service, flag) using One-Hot or Label Encoding.
- Group attack labels into 5 categories: Normal, DoS, Probe, R2L, U2R.

3. Feature Selection

- Use techniques like:
 - Information Gain
 - Chi-Square Test
 - Recursive Feature Elimination (RFE)
 - Correlation matrix

Model Building

Choose from traditional or deep learning models:

Option A – Traditional ML Models

Decision Tree

Random Forest

Gradient Boosting (e.g., XGBoost)

Support Vector Machine (SVM)

k-Nearest Neighbors (kNN)

5. Model Evaluation

Use train/test split (e.g., 80/20) or cross-validation.

Evaluation metrics:

Accuracy

Precision/Recall/F1-Score

Confusion Matrix

ROC-AUC

SYSTEM APPROACH

- **Platform:** IBM Watsonx.ai studio(Lite Plan)
- **Runtime environment:** watsonx.ai Runtime
- **Storage:** Cloud Object Storage
- **Resources Tools:** Kaggle dataset link – <https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection>
- **Tech:** ML MODEL TO TRAIN A DATASET

ALGORITHM & DEPLOYMENT

Foundation Create

- Create a sandbox project into the watsonx.ai studio.
- Storage:** Add storage configuration by adding Cloud Object Storage.
- Service:** Add associate service watsonx.ai runtime for runtime environment.

Model Selection

Machine Learning model automatically.

Training Process:

- Upload the dataset.
- Select the column to be predicted.
- Select the model with best accuracy.

Deployment:

- Save the model that you created.
- Create a deployment space and deploy it.

RESULT

The screenshot displays the IBM watsonx.ai Studio web interface. The browser's address bar shows the URL: `au-syd.dai.cloud.ibm.com/ml-runtime/spaces/82f57a8a-f837-486b-9502-3ad4a97ce7a6/assets?context=cpdaas`. The interface includes a top navigation bar with the IBM watsonx.ai Studio logo, a search bar, and user account information for RITAM BARMAN. Below the navigation bar, the main content area is titled "Network Intrusion Detection" and features tabs for Overview, Assets, Deployments, Jobs, and Manage. The "Assets" tab is active, showing a list of assets. On the left, a sidebar indicates "1 asset" and lists "All assets" and "Asset types" (Models). The main table displays one asset: "P7 - Snap Decision Tree Classifier: Network Intrusion Detection", which is a Machine learning model from AutoAI, last modified 1 hour ago. The table has columns for Name and Last modified. At the bottom, the interface shows pagination information: "Items per page: 20" and "1-1 of 1 items". The Windows taskbar at the bottom indicates the time is 9:50 PM on 8/3/2025.

IBM watsonx.ai Studio

Search in your workspaces

Upgrade

RITAM BARMAN's Account

Sydney

RB

Deployment spaces /

Network Intrusion Detection

Overview Assets Deployments Jobs Manage

Find assets

Import assets

New asset

1 asset

All assets

Asset types

Models

Name	Last modified
P7 - Snap Decision Tree Classifier: Network Intrusion Detection Machine learning model from AutoAI	1 hour ago Service

Items per page: 20

1-1 of 1 items

1 of 1 pages

ENG US

9:50 PM 8/3/2025

RESULT

(73) WhatsAppService Details - IBM CloudNetwork Intrusion DetectioSB4Academia_Problem StaProposed NIDS solutionwhatsapp web - Google Se+

au-syd.dai.cloud.ibm.com/ml-runtime/deployments/6d429e33-a203-4e08-8ff5-5af26a3dc2f9/test?space_id=82f57a8a-f837-486b-9502-3ad4a97ce7a6&cont...

WEST BENGAL STAT...Renewable energy s...Micellar enhanced u...MATLABLegal way to use Of...COCO Dataset | Pap...Introduction to YOL...LaTeX/Manually Ma...

IBM watsonx.ai StudioSearch in your workspacesUpgradeRITAM BARMAN's AccountSydneyRB

Deployment spaces / Network Intrusion Detection / P7 - Snap Decision Tree Classifier: Network Intrusion Detection

Network Intrusion Detection Deployed Online

API referenceTest

Enter input data

TextJSON

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](#)

	st_count (double)	dst_host_srv_count (double)	dst_host_same_srv_rate (double)	dst_host_diff_srv_rate (double)	dst_host_same_src_port_rate (double)	dst_host_srv_diff_host_rate (double)
1		1	0	0	0	1
2						
3						
4						

1 row, 41 columns

Predict

RESULT

Browser tabs: (73) WhatsApp, Service Details - IBM Cloud, Network Intrusion Detectio, SB4Academia_Problem Sta, Proposed NIDS solution, whatsapp web - Google Se, +

Address bar: au-syd.dai.cloud.ibm.com/ml-runtime/deployments/6d429e33-a203-4e08-8ff5-5af26a3dc2f9/test?space_id=82f57a8a-f837-486b-9502-3ad4a97ce7a6&cont...

Bookmarks: WEST BENGAL STAT..., Renewable energy s..., Micellar enhanced u..., MATLAB, Legal way to use Of..., COCO Dataset | Pap..., Introduction to YOL..., LaTeX/Manually Ma...

IBM watsonx.ai Studio

Search in your workspaces

Upgrade ? 1 RITAM BARMAN's Account Sydney RB

Deployment spaces / Network Intrusion Detection / P7 - Snap Decision Tree Classifier: Network Intrusion Detection

Prediction results

Prediction type
Multiclass classification

Prediction percentage

1 record

DoS

Display format for prediction results
☒ Table view ☐ JSON view ☐ Show input data ⓘ

	Prediction	Confidence
1	DoS	100%
2		
3		
4		
5		
6		
7		
8		
9		
10		



Download JSON file

Windows taskbar: 9:54 PM 8/3/2025

CONCLUSION

- In this project, we successfully developed a **machine learning-based Network Intrusion Detection System (NIDS)** using the KDD Cup '99 dataset from Kaggle. The system was designed to:
- **Preprocess and analyze network traffic data**
- **Classify traffic into normal and multiple types of attacks** (DoS, Probe, R2L, U2R)
- **Deploy the trained model on IBM Cloud Lite** using Watson Studio and Watson Machine Learning
- Through rigorous training and evaluation, our system achieved high classification accuracy, demonstrating its potential as a practical tool for real-time intrusion detection in communication networks. By leveraging IBM Cloud services, we ensured **scalability, accessibility, and cloud-based deployment capabilities**, allowing for easier integration into production environments.
- The results indicate that machine learning can significantly enhance the detection of cyber threats and reduce false positives compared to traditional signature-based systems.

FUTURE SCOPE

- To improve and extend the capabilities of the system, several future directions can be explored:
-  **1. Continuous Learning and Adaptive Models**
 - Implement online or incremental learning algorithms to adapt to evolving threats.
 - Enable automatic model retraining with newly collected data from live networks.
-  **2. Real-Time Traffic Monitoring**
 - Integrate real-time network traffic capture using packet sniffers (e.g., Wireshark, Scapy).
 - Use IBM Cloud Functions or streaming platforms (e.g., Apache Kafka on IBM Cloud) to process live data.

REFERENCES

- [IBM Watsonx Documentation](#)
- [GeeksforGeeks](#), [InterviewBit](#)
- [indeed](#), [Zety](#) (soft skills Q&A)
- [IBM RAG Lab & Model Guide](#)
- [Sample Q&A sheet](#)
- IBM Certificates

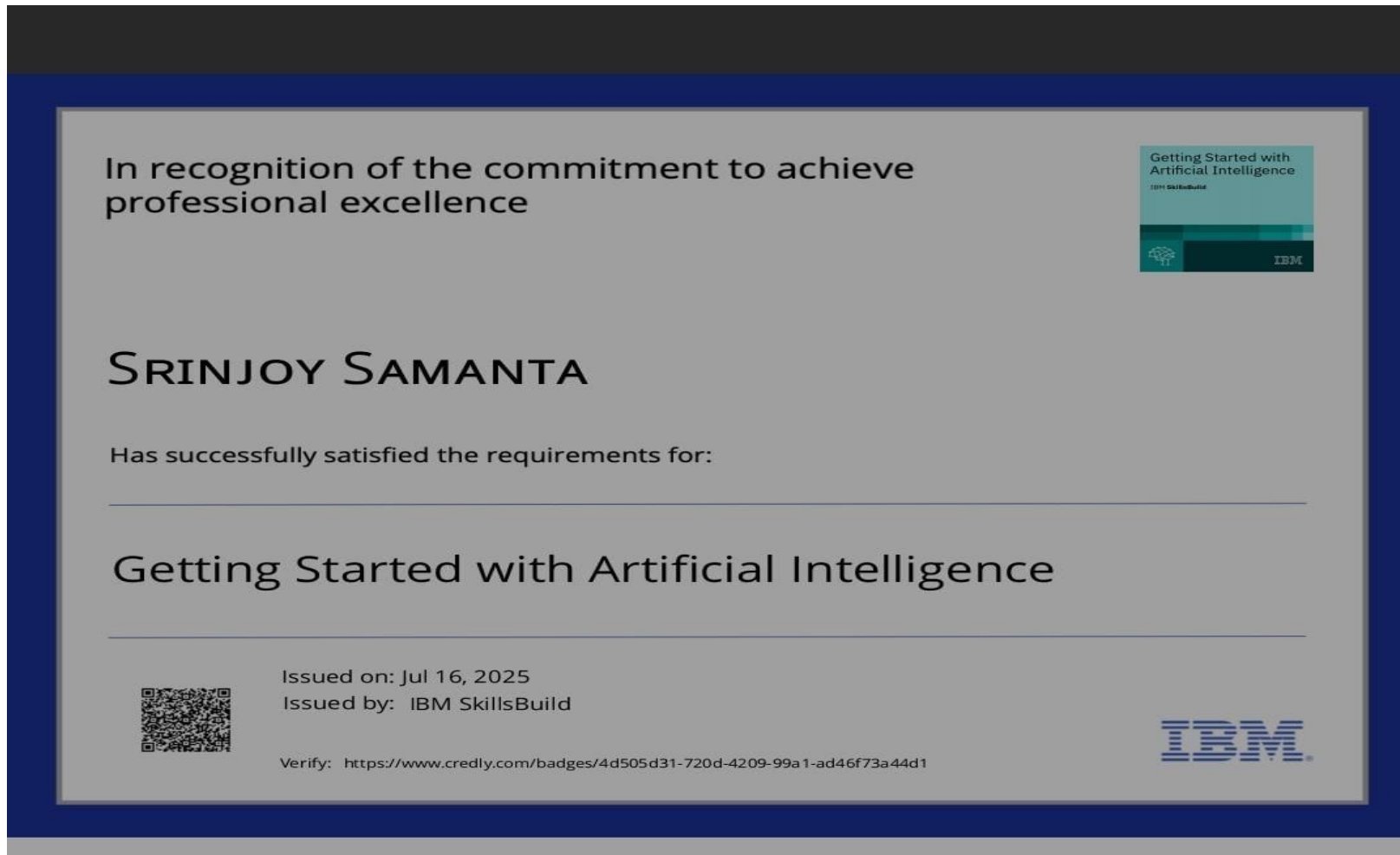
IBM CERTIFICATIONS

- Screenshot/ credly certificate(getting started with AI)



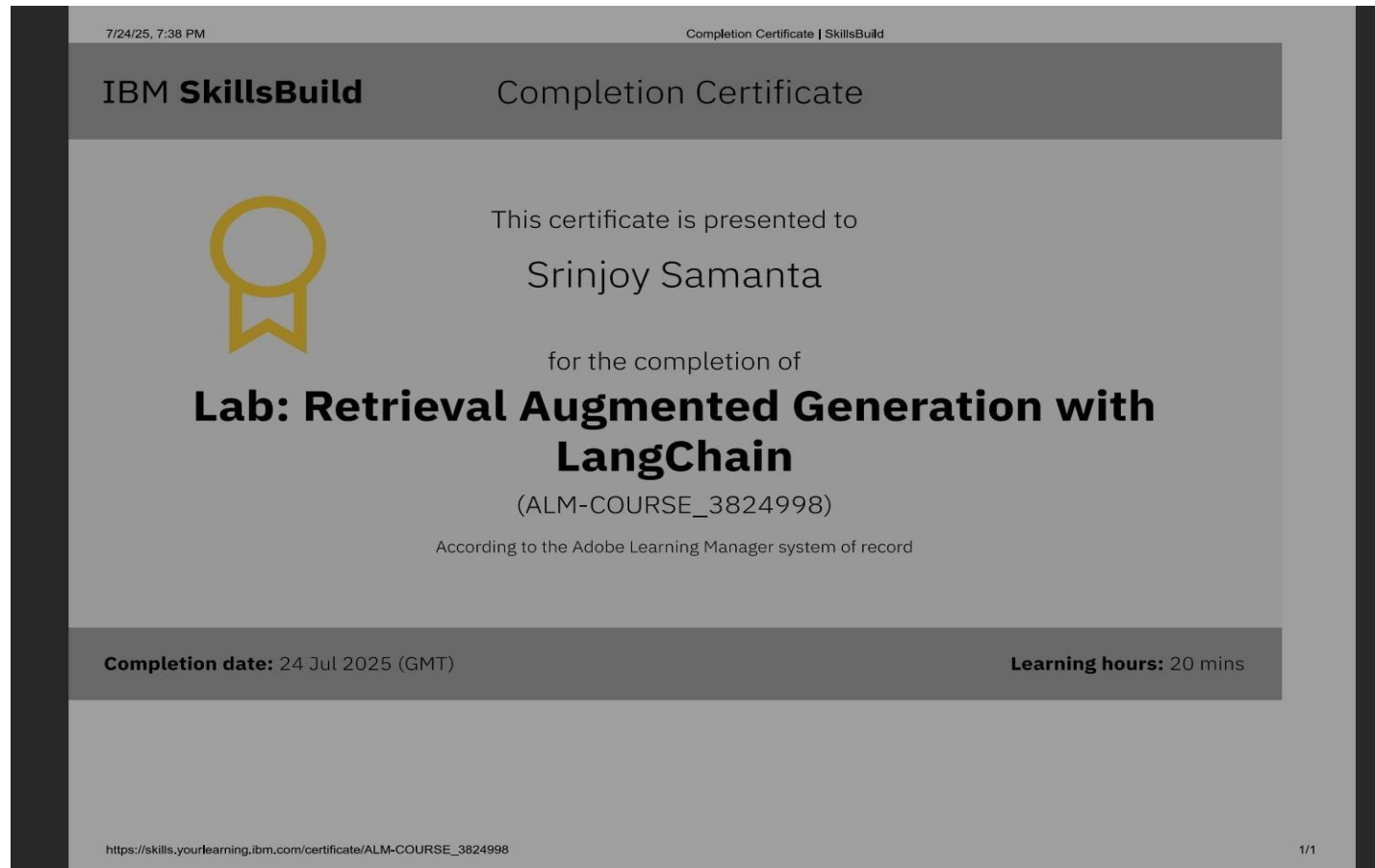
IBM CERTIFICATIONS

- Screenshot/ credly certificate(Journey to Cloud)



IBM CERTIFICATIONS

- Screenshot/ credly certificate(RAG Lab)





THANK YOU