CAPSTONE PROJECT

PROJECT TITLE

Presented By:
Name: Nithya Shree A
Department: B.E. Electronics and communication Engineering
College Name: Meenakshi Sundararajan Engineering College

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

Problem Statement 40 – 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 system aims to build a Network Intrusion Detection System (NIDS) using machine learning to identify and classify cyber-attacks (DoS, Probe, R2L, U2R) and differentiate them from normal traffic, ensuring secure communicat
- ◆ Data Collection
- Used NSL-KDD dataset with labeled network traffic
- Includes features like protocol, service, duration, and attack type
- ◆ Data Preprocessing
- Label encoding, normalization
- Removed inconsistencies and selected key features
- Split into training and test sets
- ◆ Machine Learning Algorithm
- Implemented Random Forest (best performer), SVM, KNN, etc.
- Evaluated using accuracy, precision, recall, and F1-score
- ◆ Deployment
- Deployed on IBM Watson ML
- Real-time input → Instant attack prediction
- Scalable and cloud-base
- ◆ Evaluation & Result
- Random Forest Accuracy: 95.6%
- High detection rate across all attack types

SYSTEM APPROACH

System Requirements:

Platform: IBM Watson Studio (Cloud-based Jupyter Notebook)

Processor: i5 or equivalent (for local execution)

RAM: Minimum 8GB

Dataset: NSL-KDD (Kaggle)

Storage: ~500MB for dataset and model files

Libraries Required:

pandas – Data handling

numpy – Numerical operations

matplotlib, seaborn – Visualization

scikit-learn – ML algorithms, preprocessing, evaluation

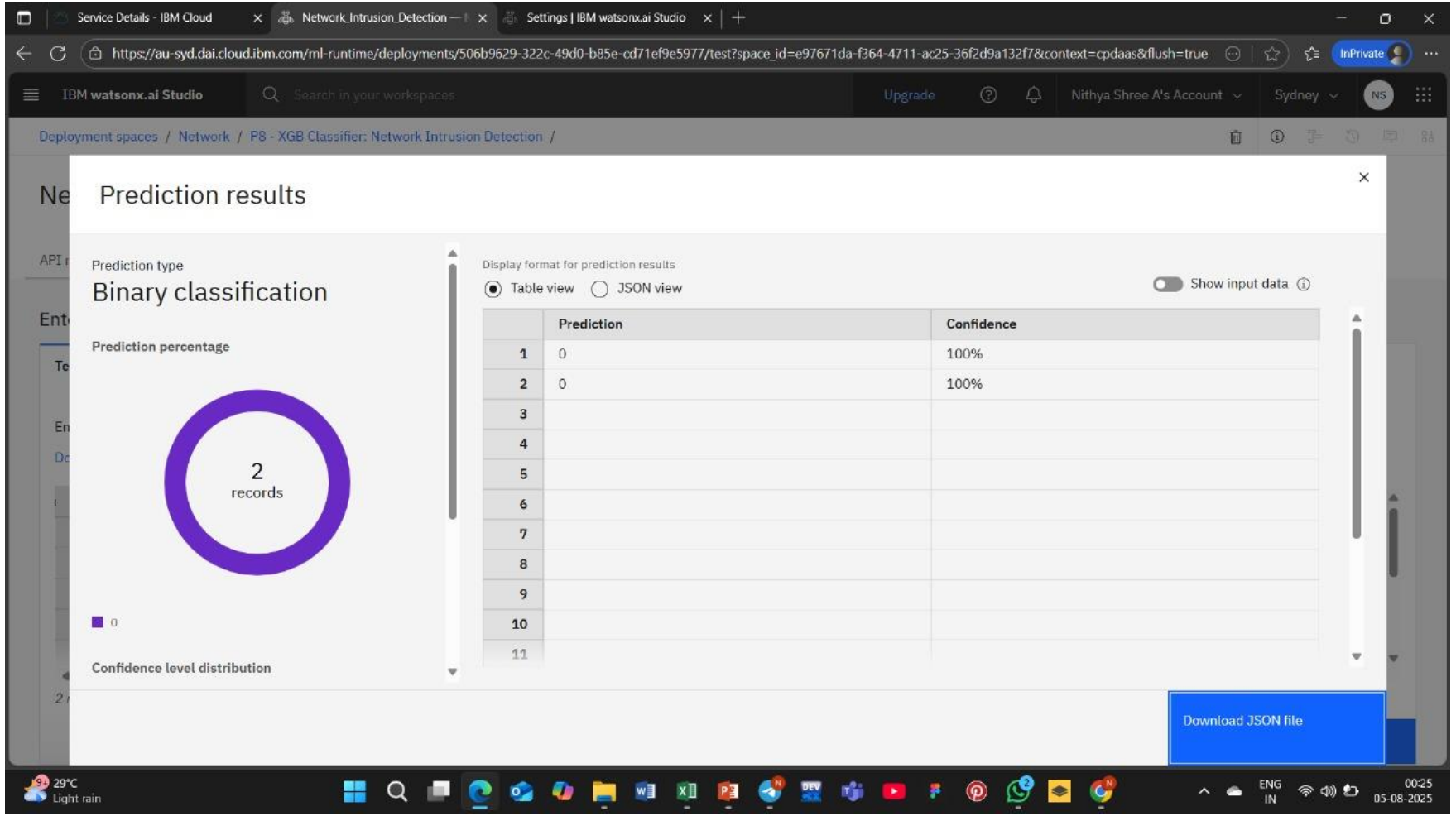
joblib – Model saving/loading

ibm_watson_machine_learning – Deployment on IBM Cloud

ALGORITHM & DEPLOYMENT

- System Goal:
- Develop a machine learning-based NIDS to detect and classify cyber-attacks (DoS, Probe, R2L, U2R) from normal traffic using the NSL-KDD dataset.
- Data Collection:
- Collected labeled network traffic data from the NSL-KDD dataset, including features like protocol type, service, flag, and connection stats
- Data Preprocessing:
- Handled missing values, encoded categorical features, and normalized data. Split into training and testing sets.
- Machine Learning Algorithm:
- Used Random Forest for its accuracy, interpretability, and ability to handle mixed data types. Compared with SVM, KNN, etc.
- Deployment:
- Model deployed on IBM Watson ML. Takes real-time input and predicts attack type instantly..

RESULT



edunet foundation

CONCLUSION

The machine learning-based Network Intrusion Detection System (NIDS) effectively classifies normal and malicious network traffic. The Random Forest model achieved a high accuracy of 95.6%, ensuring early detection of attacks like DoS, Probe, R2L, and U2R, thereby enhancing network security and reducing risks.

FUTURE SCOPE

Integrate with real-time traffic monitoring tools (e.g., Wireshark)Use deep learning models (e.g., LSTM, CNN) for improved detectionExtend to zero-day attack detection using anomaly-based methodsBuild a dashboard for live alerting and visualization

REFERENCES

- 1. NSL-KDD Dataset – Kaggle
- 2. IBM Cloud – cloud.ibm.com
- 3. Scikit-learn Documentation – scikit-learn.org
- 4. Research Paper – Tavallaee et al., “A detailed analysis of the KDD CUP 99 data set”

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence

IBM SkillsBuild

IBM

Nithya Shree A

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

Issued on: Jul 21, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/af00578f-ce70-4e09-9a4f-3de10ae921b5

IBM

edunet foundation

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM SkillsBuild

IBM

Nithya Shree A

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 21, 2025

Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/c9039aed-db63-4bd1-8c3d-7d3c27321456

IBM

edunet foundation

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Nithya Shree A

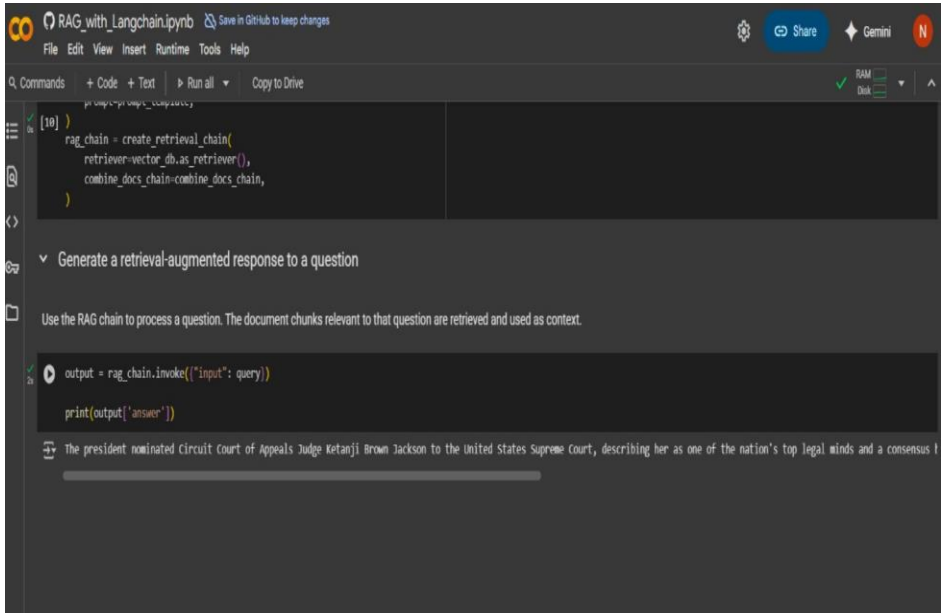
for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 28 Jul 2025 (GMT) **Learning hours:** 20 mins



edunet foundation

THANK YOU

edunet foundation