CAPSTONE PROJECT

NETWORK INTRUSION DETECTION

Presented By:
1. Deyon Tomy Joseph – Fr. C. Rodrigues Institute of Technology – B. Tech in Computer Engineering

edunet foundation

OUTLINE

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

PROBLEM STATEMENT

Nowadays, with the exponential growth of internet-based services, network systems can largely be attacked by malicious attacks and abnormal traffic. To ensure the security of these networks, suspicious activity needs to be detected timely and accurately. The most essential part is to identify various types of cyber-attacks, namely Denial of Service (DoS), Probe, R2L, and U2R, at an early stage to prevent further damage. Therefore, it is necessarily required to develop a system capable of predicting and classifying network intrusions based on real-time traffic patterns for a secure and stable communication network.

PROPOSED SOLUTION

- The proposed system aims to address the challenge of detecting and classifying network intrusions in real-time to ensure secure and uninterrupted network services. This involves leveraging machine learning techniques to analyze network traffic patterns and accurately identify potential cyber-attacks. The solution will consist of the following components:
- Data Collection:
  - Kaggle dataset link – https://www.kaggle.com/datasets/sampadab17/network intrusion-detection
  - We downloaded 2 data sets: Test_data.csv , Train_data.csv
- Data Preprocessing:
  - We uploaded the Train_data.csv file into watsonx.ai studio to create a Machine Learning model.
- Machine Learning Algorithm:
  - The studio analyzed the content of the csv file and created multiple ML model and showing their accuracy as well.
- Deployment:
  - We deployed the ML model online.
  - Store the trained model in IBM Cloud Object Storage for loading during inference.
- Evaluation:
  - Assess the model's performance using appropriate metrics.
  - Fine-tune the model based on feedback and continuous monitoring of prediction accuracy.
  - Result:Perform real-time testing using simulated traffic inputs to validate live performance.

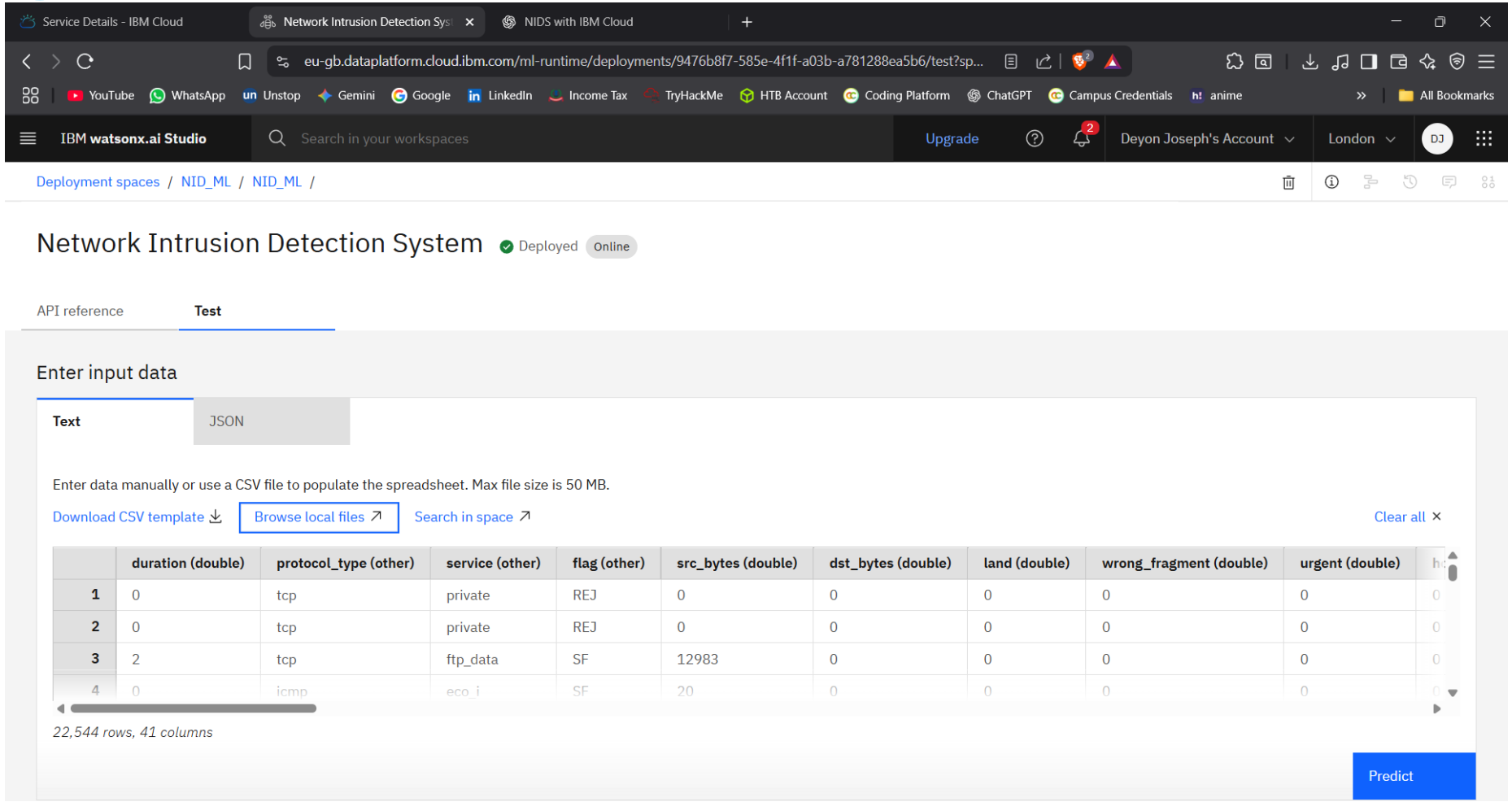
SYSTEM APPROACH

- System requirements
  - IBM Cloud Lite Account
  - IBM Cloud Object Storage
  - Minimum 4 GB RAM
  - 2.0 GHz dual-core processor or higher
- Library required to build the model
  - watsonx.ai studio
  - API
  - watsonx.ai studio runtime

ALGORITHM & DEPLOYMENT

- **Algorithm Selection:**
  - We used watsonx.ai studio to make things easy and created an ML model with its help.
- **Data Input:**
  - We downloaded csv data sets from Kaggle dataset – https://www.kaggle.com/datasets/sampadab17/network intrusion-detection.
  - 2 files – Train_data.csv , Test_data.csv
- **Training Process:**
  - We uploaded the Train_data.csv file into watsonx.ai studio and it created multiple ML models with their accuracy rate.
- **Prediction Process:**
  - We used Test_data.csv file for testing how the most efficient ML model made prediction by uploading the file directly into the studio.

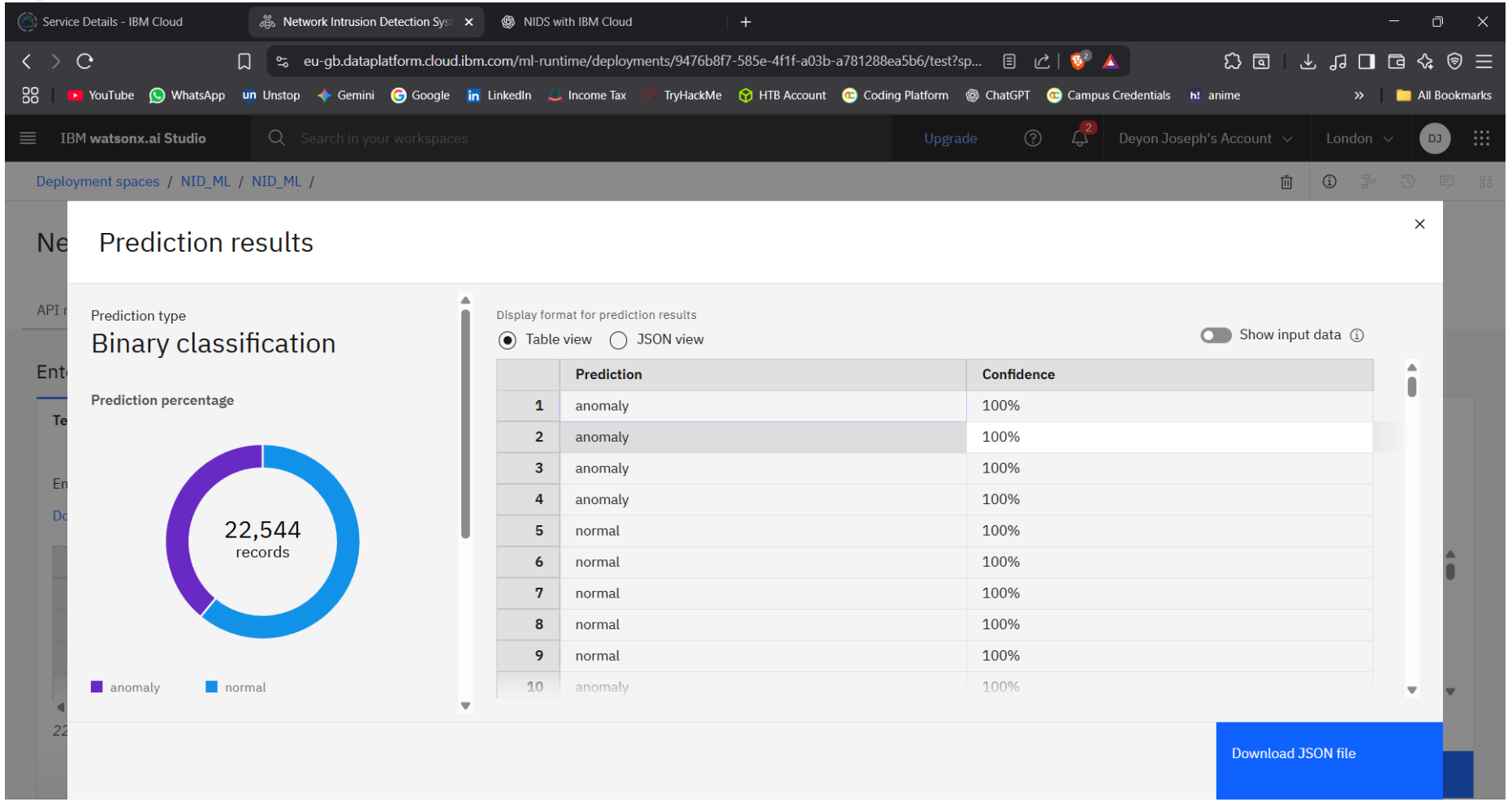
RESULT



Data Inserted

edunet foundation

RESULT



Prediction by ML Model

edunet foundation

CONCLUSION

- The proposed Network Intrusion Detection System effectively detects and classifies network intrusions using machine learning. It analyzes traffic patterns to identify attacks like DoS, Probe, R2L, and U2R. Integrated with IBM Cloud, the system offers scalable and real-time threat detection, enhancing network security and providing early warnings against cyber threats.

FUTURE SCOPE

- **Real-time Detection**: Integrate live network traffic streams for real-time intrusion detection.
- **Deep Learning Models**: Use LSTM or autoencoders for better detection of complex attack patterns.
- **Adaptive Learning**: Enable the model to continuously learn from new types of attacks.
- **Visualization Dashboard**: Build an interface to monitor alerts and intrusion trends.
- **Multi-cloud Support**: Extend deployment beyond IBM Cloud for cross-platform scalability.
- **Hybrid NIDS**: Combine anomaly-based and signature-based detection for higher accuracy.

REFERENCES

- **Kaggle Dataset: Network Intrusion Detection**
  Dataset used for model training and testing.
  https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

- **IBM Cloud Documentation**
  Used for deployment guidance and services like Cloud Functions, Object Storage, and Watson Studio.
  https://cloud.ibm.com/docs

IBM CERTIFICATIONS

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Deyon Joseph

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

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

Verify: https://www.credly.com/badges/4eb4b0c6-f239-4d3a-827b-5b2bdf4516fe

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Deyon Tomy Joseph

for the completion of

Lab: Retrieval Augmented Generation with LangChain

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

Completion date: 23 Jul 2025 (GMT) **Learning hours:** 20 mins

edunet foundation

THANK YOU

edunet foundation