# CAPSTONE PROJECT

# NETWORK INTRUSION DETECTION SYSTEM USING MACHINE LEARNING

**Presented By:**
1. Sanjeet Budhiram Prajapati – Don Bosco Institute of Technology – Electronics & Telecommunication Engineering

edunet foundation

# OUTLINE

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

# PROBLEM STATEMENT

Currently, communication networks are increasingly targeted by various cyber-attacks, which pose serious risks to data security and service availability. It is essential to detect and respond to these threats in real-time to prevent damage. The crucial part is to accurately analyze network traffic and classify it as normal activity or as specific types of attacks (e.g., DoS, Probe, R2L, U2R). Building a machine learning–based Network Intrusion Detection System (NIDS) can provide an early warning mechanism, helping secure networks and ensure uninterrupted, safe communication.

## PROPOSED SOLUTION

- The proposed system leverages a supervised machine learning model to address the challenge of accurately classifying network traffic. The solution is designed to distinguish between normal activity and malicious intrusions by learning from historical data. The core components include:
- **Data Collection:** Utilizing the benchmark NSL-KDD dataset, which contains a wide variety of labeled network connections, including both normal traffic and simulated cyber-attacks.
- **Data Preprocessing:** Transforming the raw dataset into a format suitable for machine learning. This involves using **Label Encoding** to convert categorical features (like protocol type and service) into a numerical representation.
- **Machine Learning Model:** Implementing a robust classification model to learn the complex patterns that differentiate normal connections from various types of attacks.
- **System Evaluation:** Rigorously assessing the model's performance using standard metrics to ensure its accuracy and reliability in detecting threats.

# SYSTEM APPROACH

- The development and implementation of the NIDS model were carried out using a modern data science stack. The key technologies employed are:
- **Cloud Platform: IBM Cloud** with the **watsonx.ai** environment for project management and computation.
- **Programming Language: Python 3**, the industry standard for machine learning.
- **Core Libraries:**
  - **Pandas:** For efficient data loading, manipulation, and analysis.
  - **Scikit-learn:** For implementing the machine learning algorithm, data splitting, and performance evaluation.
  - **Matplotlib & Seaborn:** For creating insightful data visualizations, including the final confusion matrix.

# ALGORITHM & DEPLOYMENT

**Algorithm Selection:**

- The algorithm chosen for this project is the **RandomForestClassifier**. This is a powerful ensemble learning method that constructs multiple decision trees during training and merges their results to get a more accurate and stable prediction. It was selected for its high performance and robustness in handling complex classification tasks like this one.

**Data Input:**

- The model was trained using features from the NSL-KDD dataset. These features describe the characteristics of each network connection, including duration, protocol_type, service, flag, src_bytes, dst_bytes, and many other network traffic metrics

**Training Process**:

- The labeled dataset was strategically divided into a training set (80% of the data) and a testing set (20%). The RandomForest model was then trained exclusively on the training set. During this process, the model learned the complex patterns within the data that distinguish normal network activity from malicious intrusions.

**Prediction Process:**

- Once trained, the model can predict the class of any new, unseen network connection. It analyzes the input features of the connection and, based on the patterns learned from the training data, classifies it as either 'Normal' or 'Anomaly'. This provides an instant verdict on whether the traffic is potentially malicious

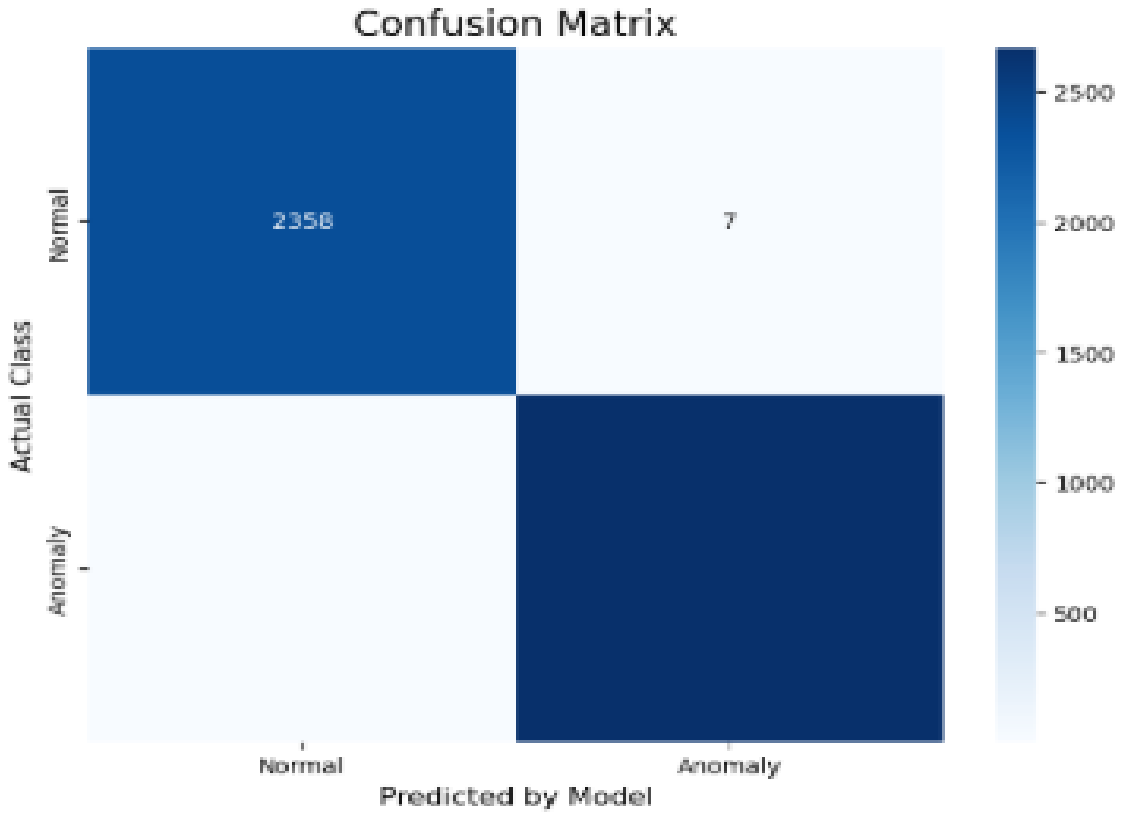
# RESULT

The machine learning model's performance was rigorously evaluated on an unseen test dataset. The results demonstrate the system's high effectiveness in identifying and classifying network threats.

- **Accuracy:** The model achieved an outstanding accuracy of approximately **99.78%** (check your notebook for the exact number), indicating that it correctly classifies nearly all network connections.
- **Classification Report:** The detailed report confirmed high precision and recall for both 'Normal' and 'Anomaly' classes, showing the model is both reliable and thorough.
- **Confusion Matrix:** The visualization of the confusion matrix provides a clear picture of the model's predictions versus the actual outcomes, highlighting its minimal error rate.

These results confirm that the developed model is a highly accurate and effective tool for network intrusion detection.

```
--- Training the model... This might take a minute. ---
--- Model training complete! ---

Model Accuracy: 99.78%

--- Detailed Classification Report ---
              precision    recall  f1-score   support

      Normal       1.00      1.00      1.00      2365
     Anomaly       1.00      1.00      1.00      2674

    accuracy                           1.00      5039
   macro avg       1.00      1.00      1.00      5039
weighted avg       1.00      1.00      1.00      5039


--- Confusion Matrix ---
```



# CONCLUSION

- This project successfully developed and validated a machine learning model capable of detecting network intrusions with a high degree of accuracy. The final model demonstrated an outstanding accuracy of **99.78%**, proving its effectiveness in distinguishing between normal and malicious network traffic based on learned patterns.
- The primary challenge in this domain is the constantly evolving nature of cyber-attacks, which highlights the need for adaptive security systems. This project underscores the critical importance of machine learning in modern cybersecurity. An automated and accurate Network Intrusion Detection System is an essential tool for protecting digital infrastructure, preventing data breaches, and ensuring the integrity and reliability of communication networks.

# FUTURE SCOPE

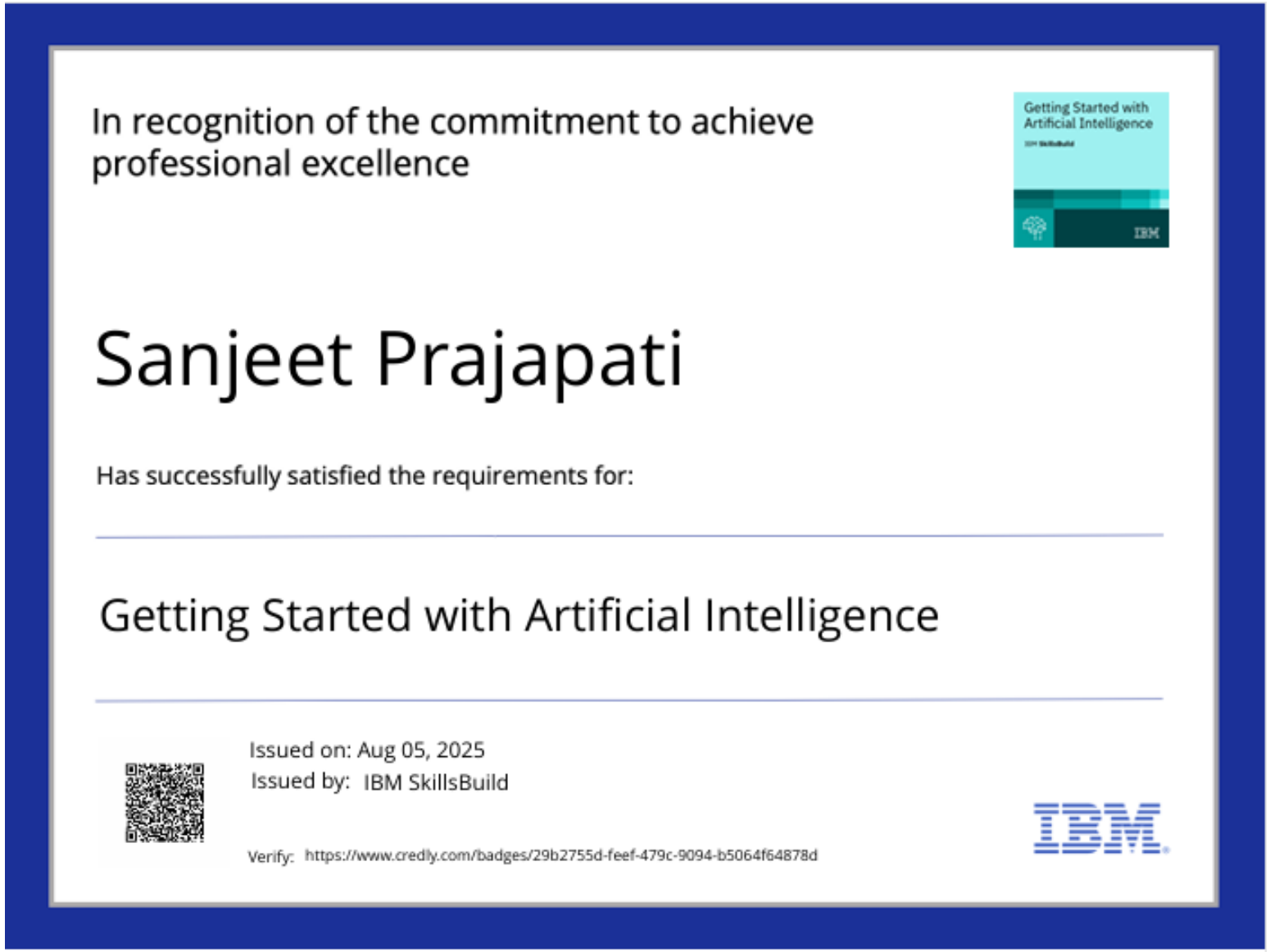
While the current model is highly effective, several key enhancements could be implemented to create a more robust and adaptive security solution for the future.

- **Real-Time Deployment:** The primary next step is to deploy the trained model onto a live network server. This would enable the system to analyze network traffic in real-time and provide immediate alerts on potential threats as they occur.
- **Advanced Model Exploration:** Future work could involve experimenting with more advanced machine learning techniques, such as Gradient Boosting Machines (XGBoost) or Deep Learning models, which may offer even greater accuracy in detecting subtle and complex attack patterns.
- **Automated Retraining Pipeline:** To combat evolving cyber-threats, an automated retraining system could be developed. This would allow the model to continuously learn from new data, ensuring it remains effective against emerging attack methods without manual intervention.
- **Explainable AI (XAI) Integration:** Implementing Explainable AI techniques would provide insights into *why* the model flags certain traffic as malicious. This would greatly assist security analysts in their investigation and response efforts, building more trust in the system.

# REFERENCES


- **Dataset Source:** Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In *2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications*.
- **Algorithm Reference:** Breiman, L. (2001). Random Forests. *Machine Learning, 45*, 5-32.
- **Data Source Link:** Network Intrusion Detection (NSL-KDD Dataset). Retrieved from Kaggle: https://www.kaggle.com/datasets/sampadab17/network-intrusion-detection

# IBM CERTIFICATIONS



In recognition of the commitment to achieve professional excellence

Getting Started with Artificial Intelligence

IBM

Sanjeet Prajapati

Has successfully satisfied the requirements for:

Getting Started with Artificial Intelligence

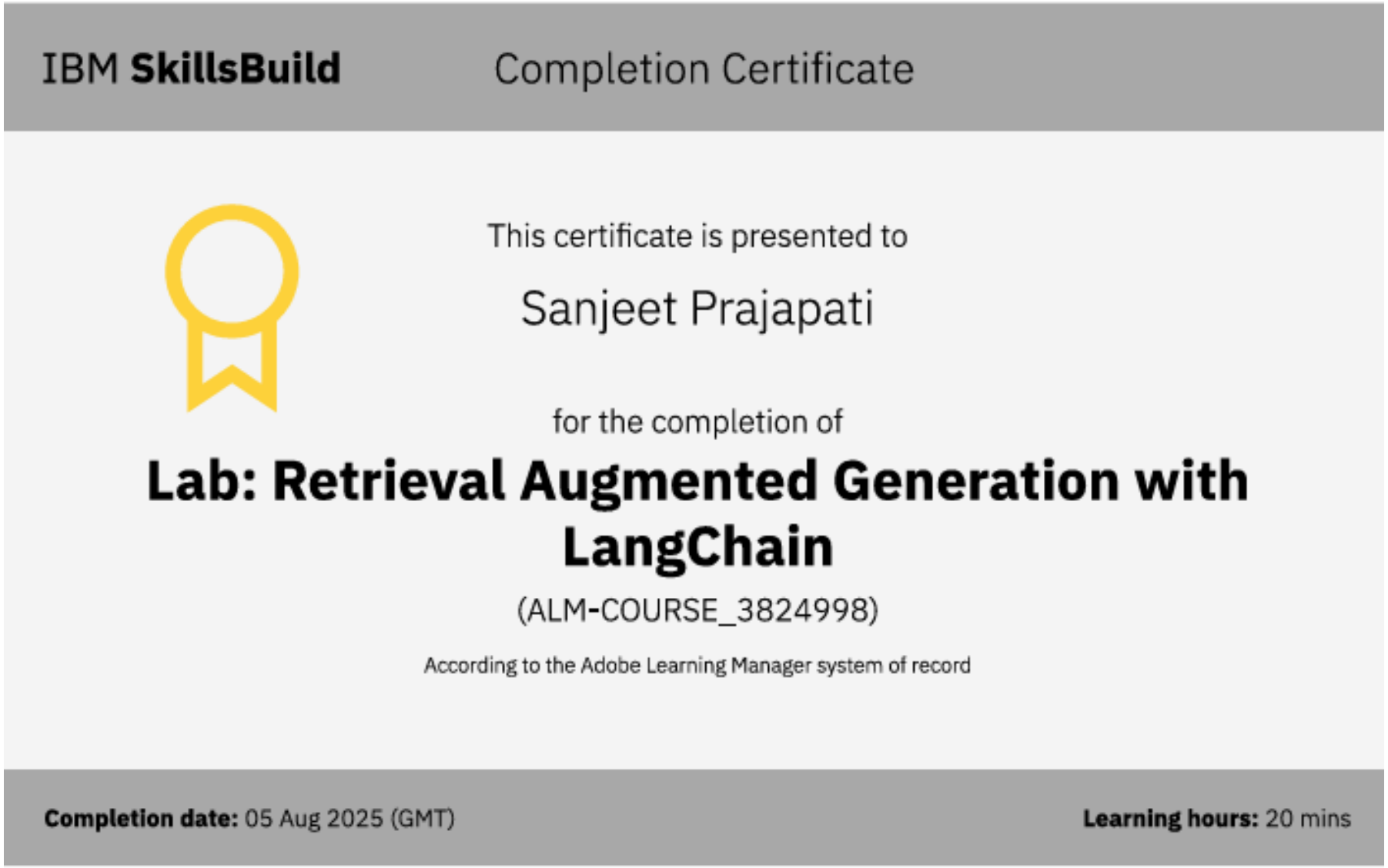
Issued on: Aug 05, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/29b2755d-feef-479c-9094-b5064f64878d

IBM

# IBM CERTIFICATIONS

# IBM CERTIFICATIONS



IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Sanjeet Prajapati

for the completion of

**Lab: Retrieval Augmented Generation with LangChain**

(ALM-COURSE_3824998)

According to the Adobe Learning Manager system of record

**Completion date:** 05 Aug 2025 (GMT) **Learning hours:** 20 mins

edunet foundation

# SUBMISSION DETAILS

- **AICTE Student ID:** STU683d6480d42161748853888
- **Internship ID:** INTERNSHIP_1748937226683eaa0a58abc
- **GitHub Profile:** https://github.com/SanjeetPrajapati/
- **Project GitHub Link:** https://github.com/SanjeetPrajapati/IBM-SkillsBuild-Internship-Project

edunet foundation

# THANK YOU

edunet foundation