CAPSTONE PROJECT

– NETWORK INTRUSION DETECTION

Presented By:
1. Student name: HEENA MAKWANA
2. College name: Sigma university
3. department: B.TECH computer engineering

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**

PROBLEM STATEMENT

Network Intrution Detection:

The challenge: –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 purposed system aims to address the challenge of predicting the required. The system should be capable of analyzing network traffic data to identify and classify various types of cyber-attacks (e.g., DoS, Prob, R2L, U2R) and distinguish them from normal network activity. This involves leveraging data analytics and machine learning techniques to forecast demand patterns accurstely. The solution will consist of the following components:**
- Data Collection:
  - Gather historical data on Network intrution detection , including protocol type, service and other relevant factors.
  - Utilize real-time data sources, such as network detection condition, protocol types, and intrution of network, to enhance prediction accuracy.
- Data Preprocessing:
  - Clean and preprocess the collected data to handle missing values, outliers, and inconsistencies.
  - Feature engineering to extract relevant features from the data that might impact network intrurion demand.
- Machine Learning Algorithm:
- Implement a machine learning algorithm, such as a analyzing network trffic data model to identify and classify various types of cyber-attack (e.g., DoS, Prob, R2L, U2R), to predict to distinguish them from normal network activity.
- Consider incorporating other factors like analyzing network conditions, types of cyber-attacks, and special decection of network to improve prediction accuracy.
- Deployment:
  - Develop a user-friendly interface or application that provides real-time predictions for network intrution at different protocol types..
  - Deploy the solution on a scalable and reliable platform, considering factors like server infrastructure, cyber-attack dection, and distinguish normal network activity.
  - Evaluation:
  - Assess the model's performance using appropriate metrics such as Mean Absolute Error (MAE), Root Mean Squared Error (RMSE), or other relevant metrics.

- **Fine-tune the model based on feedback and continuous monitoring of prediction accuracy.**
- **Result:**

SYSTEM APPROACH

The "System Approach" section outlines the overall strategy and methodology for developing and implementing the Network Intrution Detection prediction system. Here's a suggested structure for this section:

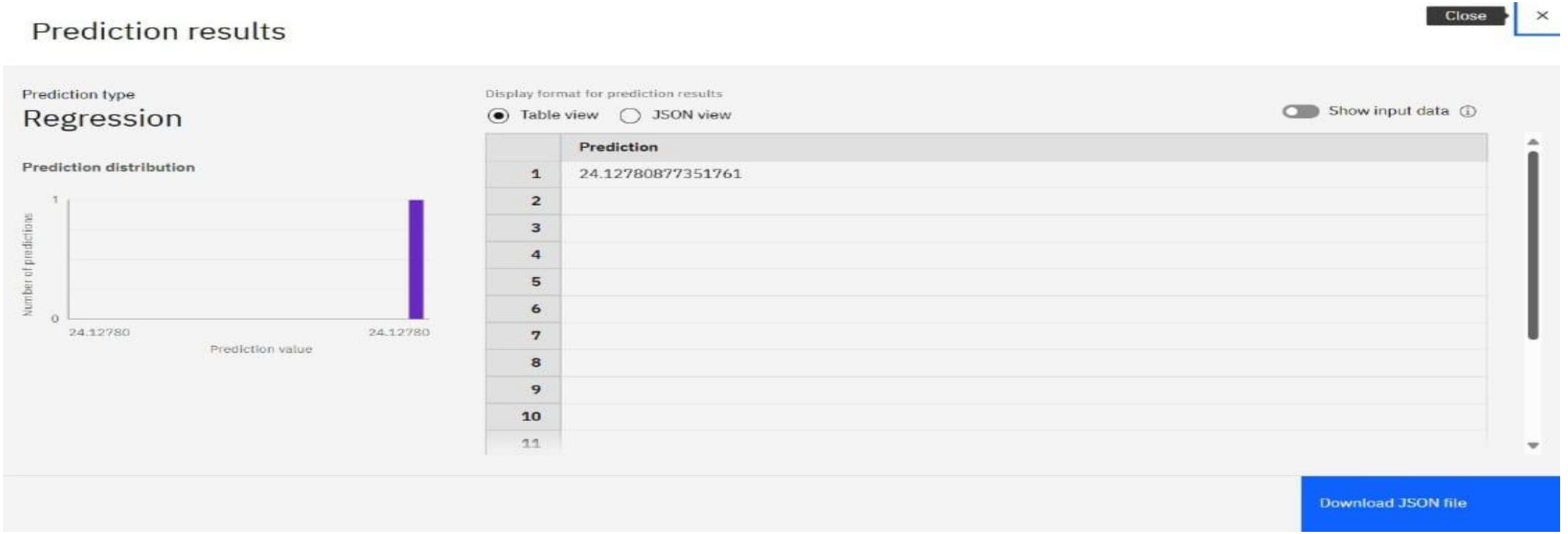
- System requirements
- Watsonx.ai studio
- Watsonx.ai Runtime
- Library required to build the model
- Build machine learning models automatically

ALGORITHM & DEPLOYMENT

- In the Algorithm section, describe the machine learning algorithm chosen for predicting network intrution. Here's an example types of cyber-attacks (e.g.,, DoS , Prob, R2L, U2R) structure for this section:
- Algorithm Selection:
  - Provide a brief overview of the chosen algorithm (e.g., network analyzing model, like Dos , prob , R2L , U2R) and justify its selection based on the problem statement and data characteristics.
- Data Input:
  - Specify the input features used by the algorithm, such as historical network traffic data, nework detection conditions, network cyber-attack , and any other relevant factors.
- Training Process:
  - Explain how the algorithm is trained using historical data. Highlight any specific considerations or techniques employed, such as cross-validation or hyperparameter tuning.
- Prediction Process:
  - Detail how the trained algorithm makes predictions for future network intrution. Discuss any real-time data inputs considered during the prediction phase.

RESULT

Present the results of the machine learning model in terms of its accuracy and effectiveness in predicting Network Intrution Detection. Include visualizations and comparisons between predicted and actual intrution to highlight the model's performance.



CONCLUSION

The implementation of a machine learning-based Network Intrusion Detection System(NIDS) demonstrates the effectiveness of intelligent algorithms in enhancing cybersecurity. By analyzing network traffic data, the system can accurately identify and classify various types of cyber-attacks—such as DoS, Probe, R2L, and U2R—while distinguishing them from normal activity. The model serves as a proactive defense mechanism, offering early warnings of malicious behavior and enabling timely response to threats. Ultimately, such a system contributes significantly to the security and resilience of communication networks in an increasingly digital world.

FUTURE SCOPE

There are several potential enhancements and expansions for this system:

Incorporating additional data sources (e.g., real-time traffic, IoT devices) to improve detection accuracy and cover broader threat landscapes.

Optimizing the machine learning algorithms for better speed, accuracy, and scalability in large or complex network environments.

Expanding the system to monitor and secure networks across multiple cities, regions, or enterprise-level infrastructures.

Integrating emerging technologies such as:

Edge Computing – for faster, decentralized data analysis closer to the source.

Advanced Machine Learning techniques – such as deep learning, reinforcement learning, or ensemble

models to enhance threat prediction and adaptability.

Building real-time intrusion response mechanisms to automatically alert or take action when threats are detected.

Incorporating self-learning features to adapt to new or unknown types of attacks (zero-day threats) without manual intervention.

REFERENCES

Datasets Used:

1. **Kaggle dataset link – https://www.kaggle.com/datasets/sampadab17/network_intrusion-detection**

Topics covered in the References

1. Cyber-attack types: DoS, Probe, R2L, U2R
2.Supervised and unsupervised machine learning
3.Model training, testing, evaluation (accuracy, precision, recall, F1-score)
4.Data preprocessing (normalization, feature selection)

- This could include academic papers on network intrution prediction, machine learning algorithms, and best practices in data preprocessing and model evaluation.

IBM CERTIFICATIONS

IBM CERTIFICATIONS

In recognition of the commitment to achieve professional excellence

Journey to Cloud: Envisioning Your Solution

IBM

Heena Makwana

Has successfully satisfied the requirements for:

Journey to Cloud: Envisioning Your Solution

Issued on: Jul 16, 2025
Issued by: IBM SkillsBuild

Verify: https://www.credly.com/badges/862b37a5-eef0-4e1c-afd4-14d661c52967

IBM

IBM CERTIFICATIONS

IBM **SkillsBuild** Completion Certificate

This certificate is presented to

Heena Makwana

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

edunet foundation

THANK YOU

edunet
foundation