Network Intrusion Detection System Using Machine Learning

A comprehensive capstone project focused on developing a Network Intrusion Detection System leveraging IBM Cloud Lite and advanced machine learning techniques. Presented by an E&TC Department intern, this project aims to enhance network security through intelligent detection methodologies.

Nisha Khankure

Outline and Problem Statement of ML-based NIDS

Agenda and problem overview for NIDS using machine learning on real datasets

Intelligent Intrusion Detection Model Deployment

ML-based traffic classification and alert system for network security

Intrusion Detection Model

Develop an intelligent intrusion detection model leveraging advanced machine learning techniques to enhance network security and threat identification capabilities.

Dataset Source

Utilize Kaggle's Network Intrusion Detection Dataset, a comprehensive resource for training and validating the ML model on real-world network traffic data.

Classification Goal

Accurately classify network traffic into normal or attack categories to ensure precise threat detection and minimize false positives during monitoring.

Alert Mechanism

Implement a system to promptly raise alerts upon detection of suspicious activity, enabling timely response and mitigation of potential cyber threats.

Deployment Platform

Deploy the final ML model on IBM Cloud Lite using Watsonx or AutoAI for scalable, accessible, and efficient intrusion detection in cloud environments.

Scalability and Accessibility

Ensure the deployed solution supports scalability and easy access, allowing integration with existing security infrastructures and adaptability to evolving threats.

System Development Approach for NIDS ML Project

Key technologies and procedural steps in system development

Use of IBM Watson Studio and Watsonx.ai

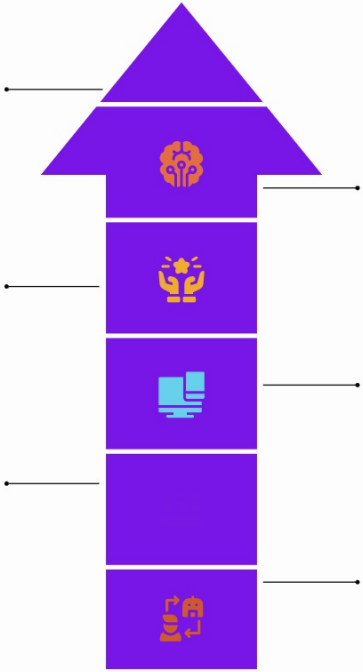
Leveraged IBM Watson Studio and Watsonx.ai platforms for efficient data science and machine learning model development.

Integration via IBM Cloud Functions

Integrated system components seamlessly using IBM Cloud Functions to enable scalable and serverless execution.

Feature selection and normalization

Applied feature selection and normalization methods to enhance model performance and reduce bias.



Automated model training with IBM AutoAI

Employed IBM AutoAI to automate training and comparison of multiple machine learning models for optimal results.

Data cleaning and preprocessing techniques

Performed thorough data cleaning and preprocessing to prepare quality input for accurate model training.

Model training and evaluation metrics

Trained models like Random Forest and XGBoost and evaluated them using accuracy, precision, recall, and F1-score metrics.

Algorithm Selection and Deployment for NIDS

Overview of models, features, and deployment process in NIDS

AutoAI Model Experiments →	AutoAI was utilized to experiment with Logistic Regression, Random Forest, Decision Trees, and Gradient Boosted Trees (XGBoost) for optimal performance.
Best Model Selection Criteria →	The best performing model was selected based on accuracy and recall metrics to ensure reliable intrusion detection.
Key Input Features →	Input features included network protocol, service type, byte size, duration, and flags to effectively characterize network traffic.
Deployment Architecture →	The trained model was deployed on IBM Watsonx.ai with a web service/API created for real-time network intrusion detection.

Network Intrusion Detection System Performance Results

Summary of accuracy, detection insights, and alerting features

High accuracy achieved across models

Models consistently reach over **95%** accuracy in detecting threats.

Confusion matrix shows clear attack separation

Confusion matrix visualizes excellent distinction between attack types.

Real-time alerts for abnormal behavior

System generates immediate alerts upon detecting unusual activity.

Dashboards visualize attack trends

Interactive dashboards display ongoing attack patterns and statistics.

Detection rates monitored continuously

Detection performance is tracked in real time via monitoring tools.

Effective differentiation of attack types

System accurately separates multiple intrusion types for response.

AI-Driven Network Intrusion Detection Success

Summary of enhanced cyber threat detection using IBM cloud tools

Machine Learning Integration

Successfully deployed NIDS with IBM cloud tools

Enhanced Threat Detection

Reduced risks of data breaches significantly

AI Improves Security

Demonstrates AI's role in network monitoring

Future Scope of NIDS Machine Learning

Enhancing detection and response with integration and automation

Live Packet Sniffers

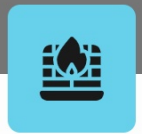
Integrate with **live packet sniffers** like Wireshark to enable real-time traffic analysis and improved threat identification capabilities.

Zero-Day Detection

Expand the detection model to support **zero-day attack detection** by implementing advanced anomaly detection techniques for unknown threats.

Visual Dashboards

Add **visual dashboards** to provide intuitive interfaces that allow security teams to monitor threats and system status efficiently.



Auto-Patching

Implement automated patching or firewall rule updates that respond dynamically to detected threats, enhancing system resilience.

Threat Response

Develop mechanisms for dynamic threat response that reduce manual intervention and accelerate mitigation in network environments.

Key References for Network Intrusion Detection

Essential sources underpinning NIDS ML project insights

Kaggle Dataset

Provides comprehensive network traffic data essential for training intrusion detection models effectively.

IBM Watsonx.ai

Offers detailed documentation and tools supporting AI-driven cybersecurity solutions.

Research Papers

Contain advanced studies on machine learning applications tailored for cybersecurity challenges.

MITRE ATT&CK

A structured framework detailing adversary tactics and techniques for threat analysis and defense.

JASA
TEKNOLOGI
INFORMASI
IBM

Thank you for your attention. Would you like me to convert this into a PDF or PowerPoint file next?

Thank you for your attention throughout this Network Intrusion Detection System Machine Learning Project presentation. Please let me know if you would like me to convert this into a slide-style PDF or PowerPoint file for your convenience.