MACHINE LEARNING DRIVEN CYBER INCIDENT DETECTION AND RESPONSE SYSTEM

Rahul.R, Samson Jebaseelan.C, Suraj M

Affiliation:K.Ramakrishnan College of Technology.

Email: samsonjebaseelan170@gmail.com

This project focuses on evaluating and identifying the best machine learning model for detecting cyber incidents in real time, utilizing five popular algorithms: Random Forest, XGBoost, Decision Tree, Logistic Regression, and LightGBM. The primary goal is to compare these models based on key performance metrics, including accuracy, precision, recall, and F1 score, to determine the most effective approach for detecting cyber threats. Once the best-performing model is selected, it will be deployed to analyze large datasets such as network traffic, system logs, and user behavior to identify potential security incidents. The selected model will then be integrated into an automated response framework, enabling the system to swiftly mitigate detected threats without requiring manual intervention. This approach aims to enhance the accuracy, speed, and efficiency of cyber incident detection and response, providing a more proactive defense mechanism against evolving cybersecurity threats.

This study explores the integration of multiple machine learning models—Random Forest, XGBoost, Decision Tree, Logistic Regression, and LightGBM—to develop a robust, adaptive system for cyber incident detection and response. By leveraging the strengths of these models, the system can effectively identify anomalous behaviors and potential security threats across large datasets. The combination of models ensures improved accuracy, scalability, and adaptability to emerging threats, while the automated response feature reduces the need for manual intervention, allowing for quicker threat mitigation and enhancing overall security efficiency. This multi-model approach paves the way for more proactive and intelligent cybersecurity solutions.

Keywords: Machine Learning, Cyber Incident Detection, Automated Response, Model Evaluation, Random Forest, XGBoost, Decision Tree, Logistic Regression, LightGBM, Threat Detection, Cybersecurity, Incident Response, Model Performance.