NOV 2025

LEVERAGING EXTREME GRADIENT BOOSTING (XGBOOST) FOR HIGH-ACCURACY INTRUSION DETECTION IN CIC-IOMT 2024 NETWORKS

SECURING THE EDGE: ACHIEVING 98% ACCURACY IN IOMT INTRUSION DETECTION WITH XGBOOST.

Prepared by: Syed Tayyab Raza Tabassam

02

ABSTRACT

This project addresses the critical challenge of Intrusion Detection in IoT Networks using the CIC-IoMT 2024 dataset, with the primary objective of classifying network traffic as either benign or malicious (binary classification). A complete machine learning pipeline was implemented, starting with data preprocessing that included loading the training data, handling missing values via row deletion (dropna), and scaling numerical features using StandardScaler. The robust XGBoost Classifier was chosen as the core predictive model. In the initial implementation, the model was trained and evaluated as a multi-class classifier, correctly distinguishing between 18 distinct types of network traffic. This preliminary multi-class model demonstrated exceptionally strong performance, achieving an overall Accuracy of 97.99% on the validation set.

The results validate the feature set and the power of the XGBoost algorithm for this cybersecurity domain. The subsequent phase will involve the crucial refinement of adapting the model to the required binary classification format by merging all attack types into a single 'malicious' class (1). Final optimization will include incorporating class weighting and hyperparameter tuning to maximize performance and deliver a high-accuracy, submission-ready solution.

03

INTRODUCTION

The rapid expansion of Internet of Things (IoT) devices, especially in critical sectors like healthcare (IoMT), has created a vulnerable attack surface. Due to the high-stakes nature of these environments, the early and accurate detection of malicious activity is essential for maintaining network integrity.

This study utilizes the CIC-IoMT 2024 dataset, which contains realistic network flow data, to address the challenge of binary classification (benign vs. malicious) in network traffic. The project's success is evaluated based on the Accuracy Score.

A robust machine learning pipeline was implemented, including data preprocessing (handling missing values and feature scaling) followed by the deployment of the eXtreme Gradient Boosting (XGBoost) classifier. Initial experimentation with a multi-class setup demonstrated exceptional performance, achieving an overall 97.99% Accuracy. The subsequent effort focuses on adapting this high-performing model to the required binary format and optimizing its parameters to deliver a high-accuracy, submission-ready solution.

04

RESULTS

Model Performance (Multi-Class)

The initial model, which was trained to distinguish between 18 distinct classes of network traffic (a temporary multi-class approach before converting to binary), demonstrated exceptional overall performance:

- Overall Accuracy: The model achieved an accuracy of $\mathbf{0.97993}$ (or 97.99%) on the test set. This result confirms the robust feature set and the classification power of the XGBoost algorithm on this type of tabular network data.

Classification Metrics

The detailed Classification Report provides metric averages across all 18 classes, confirming the high level of performance across multiple evaluation criteria:

- Macro and Weighted Averages: Both the Macro Average and Weighted Average for Precision, Recall, and F1-score were consistently high, hovering around 0.98. This suggests the model performs well not only on the entire dataset but also handles smaller classes reasonably well, though specific class-level analysis reveals minor trade-offs.
- Class-Specific Performance: Most individual classes (e.g., 0, 1, 2, 3, 4) achieved near-perfect F1-scores of $\mathbf{1.00}$.

05

RESULTS

Confusion Matrix Analysis

The Confusion Matrix (18x18 matrix) provides granular insight into the model's predictive behavior.

- Strong Diagonal Concentration: The vast majority of predicted instances fall on the main diagonal, confirming the high Accuracy score and indicating that the model is generally excellent at correctly identifying the true class of traffic.
- Identified Misclassification Clusters: Specific areas of minor misclassification were identified:
  - Classes 6 and 7: A significant number of instances were misclassified between these two traffic types (e.g., 1151 instances of Actual 6 predicted as 7, and 776 instances of Actual 7 predicted as 6). This points to a high degree of feature overlap between these two specific traffic behaviors.
  - Classes 11 through 14: Several hundred misclassifications were distributed across the off-diagonal cells within this cluster, suggesting these four traffic types are difficult for the model to perfectly differentiate.