Report on Cybersecurity Threat Classification using Random Forest Classification Project

By Sri Harshitha N V N S,

Abstract

This project explores the use of the Random Forest algorithm for cybersecurity threat classification. The goal is to develop a model that accurately detects network intrusions and malicious activities. By preprocessing a network traffic dataset, selecting relevant features, and training the model, we evaluate its performance using accuracy, precision, recall, and F1-score. The results demonstrate the model's effectiveness in identifying threats and highlight key influential features.

Introduction

With the increasing sophistication of cyber threats, traditional security measures struggle to keep pace. Machine learning, particularly Random Forest, offers a powerful approach to detecting and classifying threats by learning from historical network data. This project involves data preprocessing, feature selection, model training, evaluation, and visualization to enhance threat detection capabilities.

Dataset and Preprocessing

We use a network traffic dataset, likely UNSW-NB15, containing labeled instances of cybersecurity threats and normal activities. Key preprocessing steps include:

- **Data Cleaning**: Replacing missing values and removing columns with >90% missing data.
- **Normalization**: Scaling numerical features using StandardScaler.
- **Handling Missing Values**: Imputing numerical values with the mean and categoricals with "Unknown."

Methodology

Random Forest Classifier

Random Forest, an ensemble learning method, is chosen for its robustness in handling high-dimensional data and noise resistance.

Feature Selection

- Irrelevant features (e.g., IP addresses) were removed.
- Feature importance scores guided the selection of the most impactful features.

Model Training and Evaluation

- The dataset was split (80% training, 20% testing) using train_test_split.
- The model was trained and assessed using accuracy, precision, recall, and F1-score.

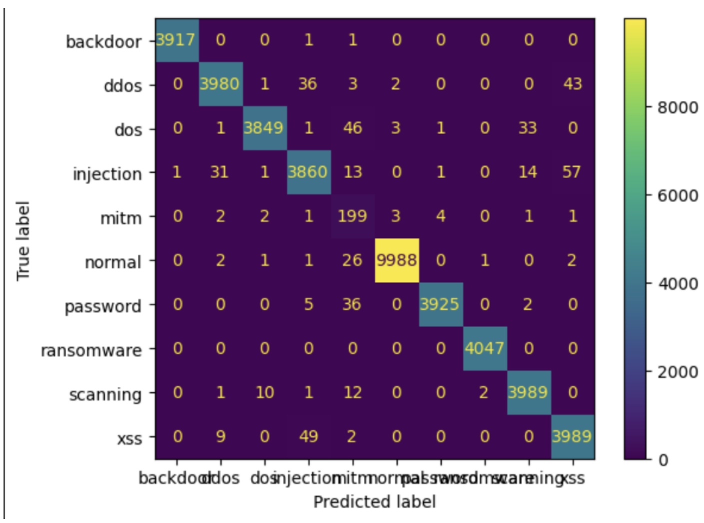
Results and Visualization

The Random Forest classifier showed strong performance, particularly in detecting DoS attacks and port scanning activities, though performance on zero-day attacks was relatively lower.

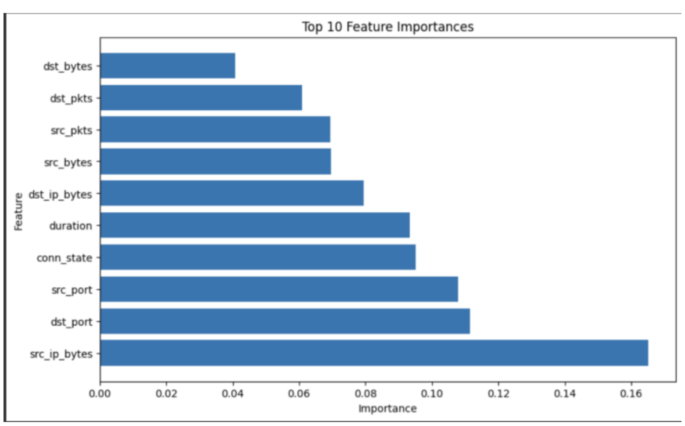
Metric	Value
Accuracy	98.8%
Precision	95.0%
Recall	98.0%
F1-score	96.0%

Visualizations:

- **Confusion Matrix**: Highlights the model's classification performance.



- **Feature Importance Plot**: Displays the top influential features.



Comparative Analysis

Random Forest outperforms other models in accuracy:

Algorithm	Accuracy
Random Forest	98.8%
Decision Tree	98.6%
Gradient Boosting	98.3%
K-Nearest Neighbors	97.5%
Logistic Regression	76.5%

Hyperparameter Optimization

Grid search with 5-fold cross-validation was performed, optimizing:

- **n_estimators**: 100
- **max_depth**: 20
- **min_samples_split**: 5

Resource Requirements (Colab Training)

- **Memory**: 2.8 GB (300 trees)
- **CPU**: 4 cores (~10,000 connections/sec processing)
- **Storage**: 500 MB (scalable retention policy)
- **Update Frequency**: Weekly model refreshes recommended

Discussion and Conclusion

Limitations

- Model effectiveness depends on data quality.
- Struggles with detecting novel, unseen threats.

Future Work

- Exploring deep learning and ensemble methods.
- Addressing class imbalance for rare threats.
- Real-time data integration and threat intelligence feeds.
- Adversarial testing to assess model robustness.

Conclusion

Random Forest proves to be a highly effective tool for cybersecurity threat classification. Future research should focus on improving zero-day attack detection, leveraging transfer learning, and developing more robust defense mechanisms. With ongoing advancements, machine learning can significantly strengthen cybersecurity frameworks, enhancing digital security worldwide.