Identifying Cyber Threats Using Machine Learning

1. Domain Background

Cybersecurity aims to safeguard systems, networks, and data from cyber threats. With the increasing complexity of attacks, traditional security measures often fail to detect emerging threats in real time. This project explores the potential of using machine learning (ML) techniques to analyze network traffic and identify potential cyber threats.

2. Problem Statement

Traditional cybersecurity mechanisms, such as signature-based intrusion detection systems, struggle to detect novel and emerging cyber threats. With attackers continuously evolving their strategies, constantly adapting defences are required to combat this. ML provides a potential means to fight developing attacks as it is possible to adapt models to developing threats automatically using computer architectures. The challenge lies in developing ML models that can generalize well to detect known and emerging threats based on network traffic data.

This project aims to investigate whether ML can effectively distinguish between normal, malicious, and outlier network traffic. By leveraging advanced ML techniques, we seek to enhance cyber threat detection and improve response mechanisms.

3. Datasets and Inputs

The dataset used in this project is LUFlow, a flow-based network intrusion detection dataset from Kaggle. The dataset can be found here: https://www.kaggle.com/datasets/mryanm/luflow-network-intrusion-detection-data-set/data. It contains:

- Labeled network flow telemetry data captured from honeypots and production services.
- Data points labeled as malicious, normal, or outliers (unknown threats).
- Features derived from network traffic, including protocol types, IP addresses, packet sizes, and timing characteristics.

The dataset is continuously updated with real-world attack patterns, making it highly relevant for research in adaptive threat detection.

4. Solution Statement

This project proposes a machine learning pipeline to analyze network traffic data and classify flows into normal, malicious, or outlier categories. The approach consists of the following steps:

1. Data Preprocessing: Cleaning and transforming network flow data.
2. Exploratory Data Analysis (EDA): Understanding feature distributions, correlations, and trends.
3. Feature Engineering: Extracting relevant features.
4. Model Training: Implementing supervised machine learning models.
5. Evaluation and Optimization: Assessing model performance.

5. Benchmark Model

As this is a supervised, multi-class classification problem, I intend to employ the random forest classifier as the baseline model for this project, owing to its robustness and interpretability in multi-class classification problems. I will then use XGBoost and Neural Network classification as the comparative models. These models will be evaluated to determine their effectiveness in identifying cyber threats and generalizing to emerging attack vectors.

6. Evaluation Metrics

To measure the success of the threat detection models, accuracy, precision, recall, and the F1-score will be used as evaluation metrics. Among these, precision, which represents the proportion of correctly identified threats out of all instances predicted as threats, is the most critical metric for classification in cybersecurity. This is because false positives can lead to unnecessary alerts, while false negatives may result in undetected threats. Therefore, precision will be used as the main indicator of model effectiveness.

7. Project Design Outline

The project will be executed as outlined in the solution statement. Incorporating the algorithms and metrics outlined in Sections 5 and 6 of this document.

Conclusion

This project investigates the feasibility of using machine learning to identify cyber threats in network telemetry data. By leveraging the LUFlow dataset, we aim to assess how well ML models can generalize to emerging threats. The research will contribute to the development of more adaptive cybersecurity defenses, helping security teams respond more effectively to evolving threats.