TED UNIVERSITY

SENG 484 Ethical Hacking and Countermeasures

Project Initial Report

IoTGuard: AI-Based Intrusion Detection and Prevention for IoT Networks

Ateş Öztürk

Mehmet Alp Demiral

Ozan Alp Sarıdoğan

,

1. Introduction

The IoTGuard project is a cybersecurity solution that aims to detect and prevent attacks occurring in IoT networks using artificial intelligence-based methods. Within the scope of the project, an additional artificial intelligence layer is built on top of the open-source network security system Suricata, with the goal of dynamically detecting both known and new-generation attacks. This approach aims to enhance the security of IoT devices by overcoming the limitations of signature-based systems.

In the first phase of the project, the focus was on data collection and analysis preparation processes. Within this scope, a dataset provided by the University of New Brunswick (UNB) containing attack logs targeting IoT traffic was identified. The team downloaded and examined this dataset, conducting a preliminary analysis of its folder structure, content format, and labeling methods. Model training has not yet been performed; the evaluation of the dataset's characteristics, size, and usability is still ongoing.

At the same time, attempts were made to capture real network traffic on Suricata. However, due to Suricata's current configuration being set to a high security level, the system struggled to detect real attack packets, and the captured data contained very limited examples of attacks. This situation led the project team to decide to work primarily with recorded (offline) data sets rather than real-time traffic.

The project is currently in the data discovery and preliminary preparation phase. The team is continuing technical planning regarding the detailed examination of the UNB dataset, understanding Suricata's data flow structure, and how machine learning algorithms such as LightGBM will be integrated in later stages.

2. Project Progress Summary

2.1 Dataset Analysis

Dataset: CIC-IoT-2023 (Canadian Institute for Cybersecurity, UNB)
Source: https://www.unb.ca/cic/datasets/iotdataset-2023.html

The dataset contains 33 distinct attack categories organized in separate folders:

Attack Categories Identified:

- Backdoor_Malware
- Benign_Final (Normal Traffic)
- BrowserHijacking
- CommandInjection
- DDoS-ACK_Fragmentation
- DDoS-HTTP_Flood
- DDoS-ICMP_Flood

- DDoS-ICMP_Fragmentation
- DDoS-PSHACK_FLOOD
- DDoS-RSTFINFLOOD
- DDoS-SlowLoris
- DDoS-SYN_Flood
- DDoS-SynonymousIP_Flood
- DDoS-TCP_Flood
- DDoS-UDP_Flood
- DDoS-UDP_Fragmentation
- DNS_Spoofing
- DictionaryBruteForce
- DoS-HTTP_Flood
- DoS-SYN_Flood
- DoS-TCP_Flood
- DoS-UDP_Flood
- MITM-ArpSpoofing
- Mirai-greeth_flood
- Mirai-greip_flood
- Mirai-udpplain
- Recon-HostDiscovery
- Recon-OSScan
- Recon-PingSweep
- Recon-PortScan
- SqlInjection
- Uploading_Attack
- VulnerabilityScan
- XSS

2.2. Data Preprocessing Pipeline

2.2.1. Feature Engineering

Extracted Features:

Flow-based features: bytes_in, bytes_out, packets_in, packets_out, duration
Protocol information: TCP, UDP, ICMP flags
Temporal features: inter-arrival times (mean, std, min, max)
Statistical features: packet size distribution, flow rate
Behavioral patterns: connection states, flag ratios

2.2.2. Data Cleaning

Removed duplicate records
Handled missing values using median imputation
Removed zero-variance features

Normalized numerical features using StandardScaler
Encoded categorical variables (protocol types, attack categories)

2.3. Machine Learning Model Development

In the machine learning model development section, two models are outlined for attack detection and classification. The unsupervised Isolation Forest model, with its design completed and training pending, aims to detect novel or unknown attack patterns using a planned configuration of 0.1 contamination rate (to be optimized), 100 estimators, auto maximum samples, and a random state of 42 for reproducibility; next steps include training on a preprocessed dataset, validating anomaly detection, and tuning the contamination threshold. Complementing this, the supervised LightGBM model, with its architecture designed and training also pending, is intended for multi-class attack classification, configured with 100 estimators, a 0.1 learning rate, max depth of 7, balanced class weights to address imbalance, and multi_logloss as the metric; preparations are complete, including a ready feature engineering pipeline, stratified train-test split, and class balancing strategy via SMOTE combined with class weights.

3. Team Organization and Contributions

Member	Role
Part A - Data & ML Lead	Dataset collection, preprocessing, feature engineering, model training and evaluation, ML documentation
Part B - Network & Capture Engineer	Suricata setup, eve.json parsing, packet capture configuration, system integration testing
Part C - System & Response Engineer	Decision engine, blocking policy implementation, integration with OS-level firewall, Raspberry Pi optimization
Part D - Dashboard & Integration Lead	Flask API development, Grafana dashboard, front-end integration, final presentation and demo

4. Conclusion

The IoTGuard project has made significant progress in the foundational stages of implementing an AI-based intrusion detection and prevention system for IoT networks. We have successfully acquired and analyzed the CIC-IoT-2023 dataset, implemented a comprehensive data preprocessing pipeline, and designed the machine learning architecture.

5. References

[1] IoT-23 Dataset, Stratosphere Laboratory, 2020.
[2] BoT-IoT Dataset, University of New South Wales, 2019.
[3] S. M. H. Bamakan et al., “Cyber Threat Detection for IoT Using Machine Learning,” *IEEE Access*, 2022.