Intrusion Detection System (IDS) using Machine Learning

Advanced Computer Security CS 558
Project Proposal
By

Team 18

Ramya Arumugam
Arvind Sai Dooda
Atharva Bauskar
Sumedh Devaki

Intrusion Detection System (IDS) using Machine Learning

Overview

This project aims to develop a Hybrid Machine Learning-Based Intrusion Detection System (IDS) that integrates Network- based IDS (NIDS) and Host-based IDS (HIDS) to improve the detection of both known and unknown cyberattacks. By using machine studying (ML) techniques, the system will analyze both the network traffic and host information to offer extra comprehensive detection abilities. Key aspects of this project encompass designing the hybrid IDS architecture, where NLP strategies like BERT will convert host logs into a format suitable for ML processing. Various ML models, inclusive of Decision Trees, Random Forest, and AdaBoost, might be tested on datasets like CICIDS to hit upon assaults like SQL Injection and DoS. The project can even address the data imbalance through SMOTE and optimize model performance with the usage of hyperparameter tuning. Additionally, the system can be extended to help real-time detection and be tested in IoT environments to ensure scalability. Overall, the hybrid IDS ambitions to gain greater accuracy, decrease false positives, and better adaptability compared to traditional IDS processes.

Background

As cyberattacks become more state-of-the-art, traditional Intrusion Detection Systems (IDS) rely on signature-based detection to keep up. These systems, which match the known attack signatures in opposition to network traffic, often fail to discover evolving threats like zero-day attacks, Advanced Persistent Threats (APT), and encrypted traffic. Network-based IDS (NIDS), which monitors the network traffic, and Host- based IDS (HIDS), which examines host logs, each have limitations. NIDS struggles with encrypted or unknown attacks, even as HIDS provides computational overhead and might omit broader network-level attacks.

To conquer those boundaries, machine learning (ML) has come to be promising answers. These strategies analyze patterns of normal and malicious behavior, allowing them to detect unknown attacks that traditional IDS would omit. Combining NIDS and HIDS right into a hybrid IDS enhances detection competencies with the aid of leveraging both network traffic and host- based records, providing a more comprehensive protection method. Recent advances, like NLP-based fashions such as BERT, allow the transformation of host logs into numerical data, making them suitable

for machine learning models to stumble on anomalies.

Numerous ML models, together with Decision Trees (DT), Random Forest (RF), Logistic Regression (LR), Gaussian Naive Bayes (GNB), and Adaptive Boosting (AdaBoost), have proven strong performance in detecting plenty of attacks, along with SQL injection, Cross-Site Scripting (XSS), and Denial-of-Service (DoS). Ensemble techniques, which integrate more than one algorithm, have been especially effective in enhancing detection rates. However, demanding situations like information imbalance, wherein benign traffic hugely outnumbers malicious samples, stay. Techniques like SMOTE (Synthetic Minority Over-sampling Technique) are used to balance information and enhance schooling outcomes.

In addition to addressing information imbalance, cutting-edge IDS ought to manage real-time detection and be adaptable to environments with IoT traffic. The complexity of modern-day networks, along with bandwidth obstacles and congestion, offers further challenges. This project proposes to broaden a Hybrid Machine Learning-Based IDS that integrates NIDS and HIDS to provide robust detection across an extensive range of attack types, as well as enhancing accuracy, lowering false positives, and supporting real-time, scalable intrusion detection in complicated environments.

Project Outline

The project will be conducted in stages to thoroughly assess the proposed Hybrid Intrusion Detection System (IDS).

Phase I: Understanding the Hybrid IDS

Initially, we can outline the layout and format of the Hybrid IDS, which combines Network-based IDS (NIDS) and Host-based IDS (HIDS) to capture each network traffic and host activity information. This phase will concentrate on how machine learning (ML) algorithms can be used to detect malicious activities. We will also describe the feature extraction technique from network and host logs, along with the use of NLP-based methods (consisting of BERT) for converting textual host data into numerical representations.

Phase II: Performance Analysis of the Hybrid IDS

In the second phase, we will be able to conduct experiments to assess the effectiveness of the hybrid IDS using the NSL-KDD and CICIDS datasets. We aim to measure the

system's accuracy in detecting diverse kinds of attacks, which includes web-based attacks along with SQL Injection, Cross-Site Scripting (XSS), and Brute Force.

The evaluation will focus on:

- Binary classification for figuring out malicious vs. Benign traffic.
- Multi-class classification to identify different attack types (DoS, Probe, R2L, U2R).

Experiments will replicate previous studies and utilize performance metrics inclusive of accuracy, precision, recall, F1-score, and false positive rate (FPR).

Phase III: Balancing and Enhancing Data Assumptions

This phase will deal with issues related to statistics imbalance, that's commonplace in network traffic datasets. We will rent SMOTE (Synthetic Minority Over-sampling Technique) to stabilize the datasets, ensuring the truthfulness and strong efficacy of the machine learning model training. Additionally, we will be able to adjust certain parameters on network traffic, such as path length and bandwidth, to create more authentic network conditions. This will help evaluate the model's performance in scenarios with congestion or confined bandwidth.

Phase IV: Comparison of Different Machine Learning Models

In this phase, we will discover the performance of diverse supervised system learning algorithms, such as:

Decision Trees (DT)

Random Forest (RF)

Logistic Regression (LR)

Gaussian Naive Bayes(GNB)

Adaptive Boosting(AdaBoost)

These models could be tested for their capacity to hit upon malicious traffic, and their consequences might be compared primarily based on metrics like accuracy, F1-score, and fake positive rate. Special attention might be given to the performance of ensemble

strategies, which may additionally provide stronger detection capabilities over single-model strategies.

Optional Phase V: Hyperparameter Tuning and Model Optimization

This phase will focus on optimizing the system machine learning models through hyperparameter tuning. Techniques like GridSearchCV and RandomizedSearchCV will be used to fine-tune the parameters of the model, improving detection accuracy and minimizing false positives. The optimized fashions will then be compared to perceive the best-performing algorithm for the hybrid IDS.

Note: This phase is optional and can be included if time and resources permit. While it can significantly enhance model performance, basic model evaluation and tuning in earlier phases can be sufficient for the project.

Optional Phase VI: Real-Time Detection and IoT Traffic

In this phase, we will be able to extend the hybrid IDS to address real-time detection and examine its overall performance in environments with IoT based traffic. The machine may be examined towards a variety of IoT-specific attacks, with a focus on how well it can detect the attacks in an Internet of Things (IoT) environment. The purpose is to ensure the hybrid IDS can scale and adapt to the developing complexity of network environments, in particular as IoT gadgets grow to be more conventional.

Note: This phase is optional and could be considered a stretch goal. Real-time detection and IoT traffic handling can add complexity to the project and may require additional resources.

References

1. Zhiyan Chen, Murat Simsek, Burak Kantarci, Mehran Bagheri, Petar Djukic, Machine learning-enabled hybrid intrusion detection system with host data transformation and an advanced two-stage classifier, Computer Networks, Volume 250, 2024, 110576, ISSN 1389-1286, https://doi.org/10.1016/j.comnet.2024.110576.

2. Mynuddin, Mohammed & Khan, Sultan Uddin & Chowdhury, Zayed & Islam, Foredul & Islam, Md Jahidul & Hossain, Mohammad & Ahad, Dewan. (2024). Automatic

Network Intrusion Detection System Using Machine learning and Deep learning. 10.36227/techrxiv.170792293.35058961/v1.

3. Vadhil, Fatimetou & Salihi, Mohamed & Nanne, Mohamedade. (2024). Machine learning-based intrusion detection system for detecting web attacks. IAES International Journal of Artificial Intelligence (IJ-AI). 13. 711. 10.11591/ijai.v13.i1.pp711-721.

4. Amit Singh, Jay Prakash, Gaurav Kumar, Praphula Kumar Jain, and Loknath Sai Ambati. 2024. Intrusion Detection System: A Comparative Study of Machine Learning-Based IDS. J. Database Manage. 35, 1 (Jan 2024), 1–25. https://doi.org/10.4018/JDM.338276

5. Kunal, & Dua, Mohit. (2019). Machine Learning Approach to IDS: A Comprehensive Review. 117-121. 10.1109/ICECA.2019.8822120.