AI-Driven Honeypot System for Detecting Network Attacks

Anna Chiu, Moina Vernon, May Barani Zaw

Abstract:

Traditional honeypot systems struggle to detect sophisticated network attacks because they rely on static detection methods. By automating and adapting the detection process, an AI-driven honeypot system can significantly enhance cybersecurity defenses against evolving threats.

Introduction

Honeypots serve as an early warning system. They gather intelligence on threats and limit damage. Traditional honeypots, which lures attackers into simulated environments, have limitations due to their static and reactive nature. The growing gap in cybersecurity defenses creates a need for innovative solutions.

Problem Statement: Traditional honeypot struggle to detect new, evolving threats due to their reliance on static rules and manual log analysis, leading to delayed and less accurate threat detection.

Objective: Utilizing machine learning to analyze attack logs and provide real-time detection of network threats with improved accuracy and response speed.

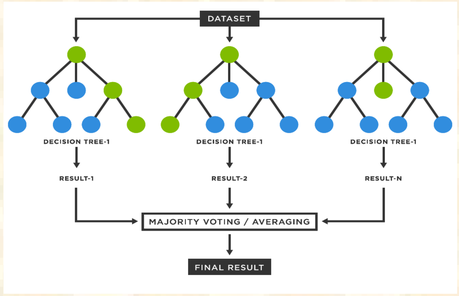
Hypothesis

We hypothesize that by integrating a combined machine learning approach using Random Forest and XGBoost in a hard-voting classifier into the honeypot system, we expect to enhance its detection capabilities. This AI-driven honeypot will more accurately detect novel and sophisticated network attacks by dynamically analyzing network traffic and identifying abnormal patterns. The system will significantly reduce false positives and negatives compared to traditional honeypot systems while adapting more effectively to evolving real time threats.

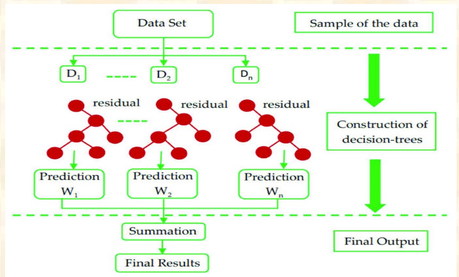
Methodology

We applied supervised machine learning models to detect network attacks and combined them using a hard-voting classifier to improve performance.

- **Random Forest** will be used for classification to identify known attack patterns and classify data accordingly.



- **XGBoost** will focus on anomaly detection to identify deviations from normal traffic patterns and uncover potential threats.

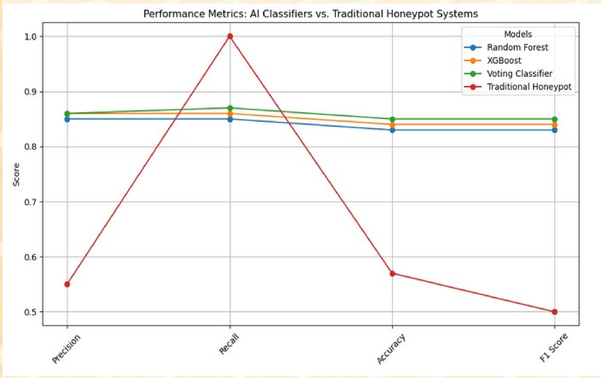


We used the **Network Anomaly Detection** dataset from Kaggle, which is widely recognized in network-based anomaly detection systems. The dataset contains traffic logs labeled as normal or malicious, including features such as protocol type, connection duration, and service requested.

Expected Results

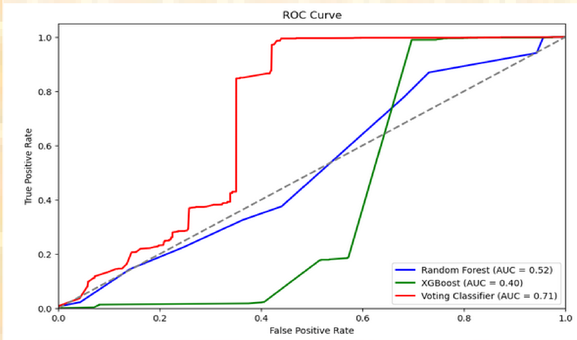
We expect the learning-enhanced honeypot to detect and classify network attacks more accurately than traditional systems. The use of algorithms supervised learning machines will lead to higher detection rates and fewer false positives. Our analysis showed improved performance in adapting to new attack patterns.

Final Performance Line Plot Graph



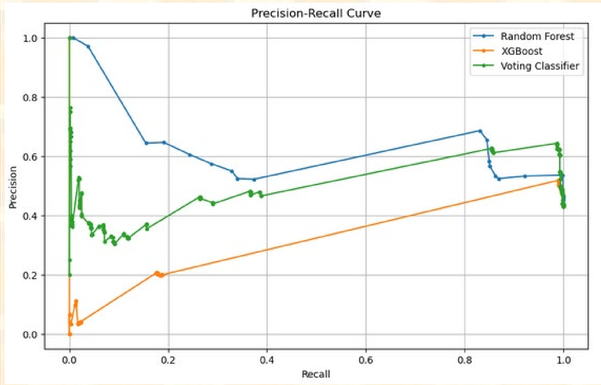
This graph compares **Precision**, **Recall**, **Accuracy**, and **F1-score** for various models (Random Forest, XGBoost, Voting Classifier) versus a traditional honeypot system. The Voting Classifier performs best in recall, demonstrating its capability to detect attacks while maintaining a balanced precision-recall tradeoff.

ROC Curve



The **ROC Curve** shows how each model distinguishes between legitimate and malicious traffic at various threshold levels. The **Voting Classifier** outperforms both Random Forest and XGBoost, demonstrating superior performance in distinguishing between malicious and normal traffic.

Precision-Recall Curve



This curve shows the tradeoff between **precision** and **recall** for each model. The **Random Forest** model shows a strong precision-recall relationship, indicating that it is very confident when predicting positive attack cases. **XGBoost** and the **Voting Classifier** also provide solid results, with the latter having a more balanced curve.

Expected Conclusions

Integrating machine learning models will significantly improve the honeypot's ability to detect and analyze network attacks. This approach is expected to yield more accurate threat detection and faster responses compared to traditional honeypot systems.

Research and Articles:

1. Network Analysis Detection https://www.kaggle.com/code/indhumalinib/nad-with-88-accuracy
2. Honey Models: Machine Learning Honeypots By Ahmed Abdou , Ryan Sheatsley, Yohan Beugin, Tyler Shipp and Patrick McDaniel
3. Honeypot with Machine Learning based Detection Framework A Honeypot with Machine Learning based Detection Framework for defending IoT based Botnet DDoS Attacks | IEEE Conference Publication | IEEE Xplore
4.New honeypot system and its application in the security of employment network https://ieeexplore.ieee.org/document/6219267
5. T-Pot All in One Multi Honeypot Platform https://github.com/telekom-security/tpotce