Cybersecurity Threat Detection Using Machine Learning

Ashwini
Dept. of CSE, Government Engineering College, Ramanagara
Visvesvaraya Technological University, Belagavi

***Abstract*—**This paper proposes ThreatAI, a Machine Learning-based cybersecurity system for real-time intrusion detection. Using Random Forest and XGBoost, the system classifies network traffic and detects malicious activities with high accuracy. The proposed system demonstrates improved detection accuracy and provides real-time cybersecurity monitoring.

***Index Terms*—**Cybersecurity, Intrusion Detection, Machine Learning, Random Forest, XGBoost, ThreatAI, Network Security.

I. INTRODUCTION

Cyber threats are increasing rapidly due to digital transformation. Traditional security systems fail to detect unknown attacks due to their rule-based, signature-dependent nature. Machine Learning enables adaptive and intelligent threat detection by learning patterns from data, making it possible to identify novel and evolving attack vectors in real time.

II. LITERATURE SURVEY

Recent studies show ML-based systems outperform traditional approaches in intrusion detection tasks. Ensemble models like Random Forest provide better accuracy and robustness against diverse attack types. Ahmed et al. [1] demonstrated a hybrid threat detection system, while Zhang and Pan [2] employed Fuzzy C-Means and SVM for classification. Liu and Zhang [3] proposed an immune-based detection framework, and subsequent studies have further improved detection rates using advanced ML architectures.

III. PROPOSED SYSTEM

ThreatAI uses ML algorithms for real-time detection. It includes preprocessing, feature extraction, classification, and alert modules. The system ingests raw network traffic, cleans and normalizes the data, extracts relevant features, and applies trained ensemble classifiers to determine whether the traffic is benign or malicious. Upon detection of a threat, an alert is generated and logged for review.

IV. SYSTEM DESIGN

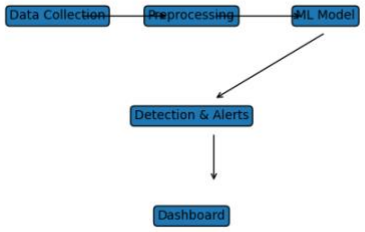

Fig. 1: System Architecture

V. RESULTS

The system was evaluated on benchmark intrusion detection datasets. Accuracy comparison across different ML models demonstrated that ensemble approaches (Random Forest, XGBoost) outperform individual classifiers. Performance metrics including precision, recall, and F1-score confirmed the effectiveness of the proposed system.

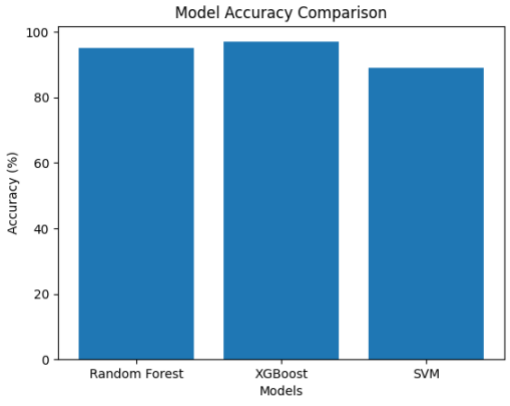

Fig. 2: Accuracy Comparison

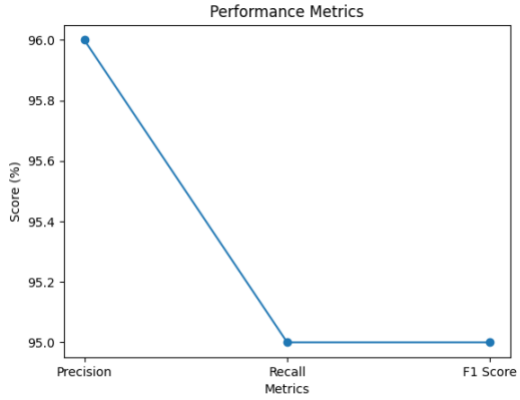

Fig. 3: Performance Metrics

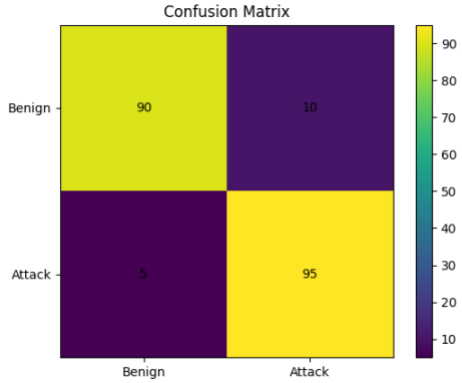

Fig. 4: Confusion Matrix

VI. CONCLUSION

ThreatAI improves detection accuracy and provides real-time cybersecurity monitoring using Machine Learning techniques. The system's ensemble-based approach ensures robust and adaptive threat identification, making it suitable for deployment in dynamic network environments.

REFERENCES

[1] M. R. A. G. Ahmed et al., "Hybrid Threat Detection System," IEEE, 2019.

[2] Z. Zhang and P. Pan, "Fuzzy C-Means and SVM," IEEE, 2019.

[3] C. Liu and Y. Zhang, "Immune-Based Detection," IEEE, 2021.

[4] J. Chen et al., "Cyber Threat Detection using Data Mining," IEEE, 2022.

[5] A. Kiran et al., "ML-Based Cybersecurity System," IEEE, 2023.

[6] D. Vinod and M. Prasad, "Hybrid ML Detection," IEEE, 2023.

[7] A. Al Farsi et al., "IoT Threat Detection," IEEE, 2024.

[8] M. S. Rahman et al., "ML Cybersecurity Enhancement," IEEE, 2024.