Cyber Threat Detection Using Machine Learning

1. Abstract

This project presents a machine learning–based intrusion detection system using Random Forest and Isolation Forest. The system processes large network datasets and provides visual dashboards including charts, 3D plots, and geo■maps.

2. Introduction

Cyberattacks continue to grow in complexity and frequency. Manual network monitoring is inefficient. Machine learning offers automated detection of malicious traffic.

3. Problem Statement

Traditional signature-based systems fail to detect unknown attacks. There is a need for a fast, ML■based system with visualization support.

4. Objectives

- Detect attacks using ML
- Provide visual analytics
- Support large CSV datasets
- Generate severity scores
- Map attacks globally

5. Methodology

Data preprocessing, feature alignment, Random Forest prediction, Isolation Forest anomaly detection, and visual dashboards.

6. Results

High accuracy, 3D threat visualization, and global attack mapping.

7. Conclusion

This system successfully detects attacks and provides powerful visual analysis tools.

8. Future Work

Deep learning, alerting, real-time packet inspection.