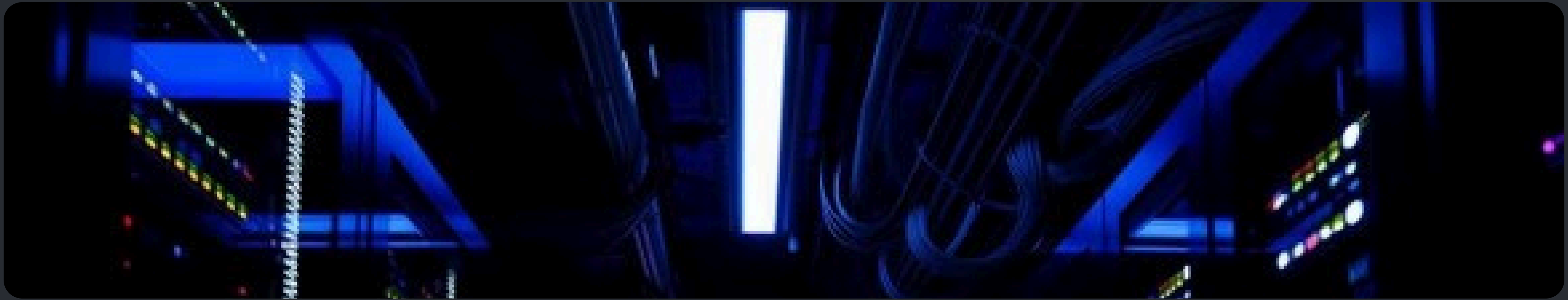
Advanced Intrusion Detection and Prevention System

Presentation by Lalithadithya, Thasif Vali, Uddhav Narasimharao, and Sreenivasulu, BESTIU (2024-2025).

Abstract



- **Heuristic + ML**: Combines to catch threats.
- **Real-time**: Sniffs packets, classifies, responds.
- **Framework**: Flask (UI) + Scapy (network analysis).
- **Random Forest**: Trained on NSL-KDD dataset.
- **Key Features**: Alerting, IP blocking, dashboard.

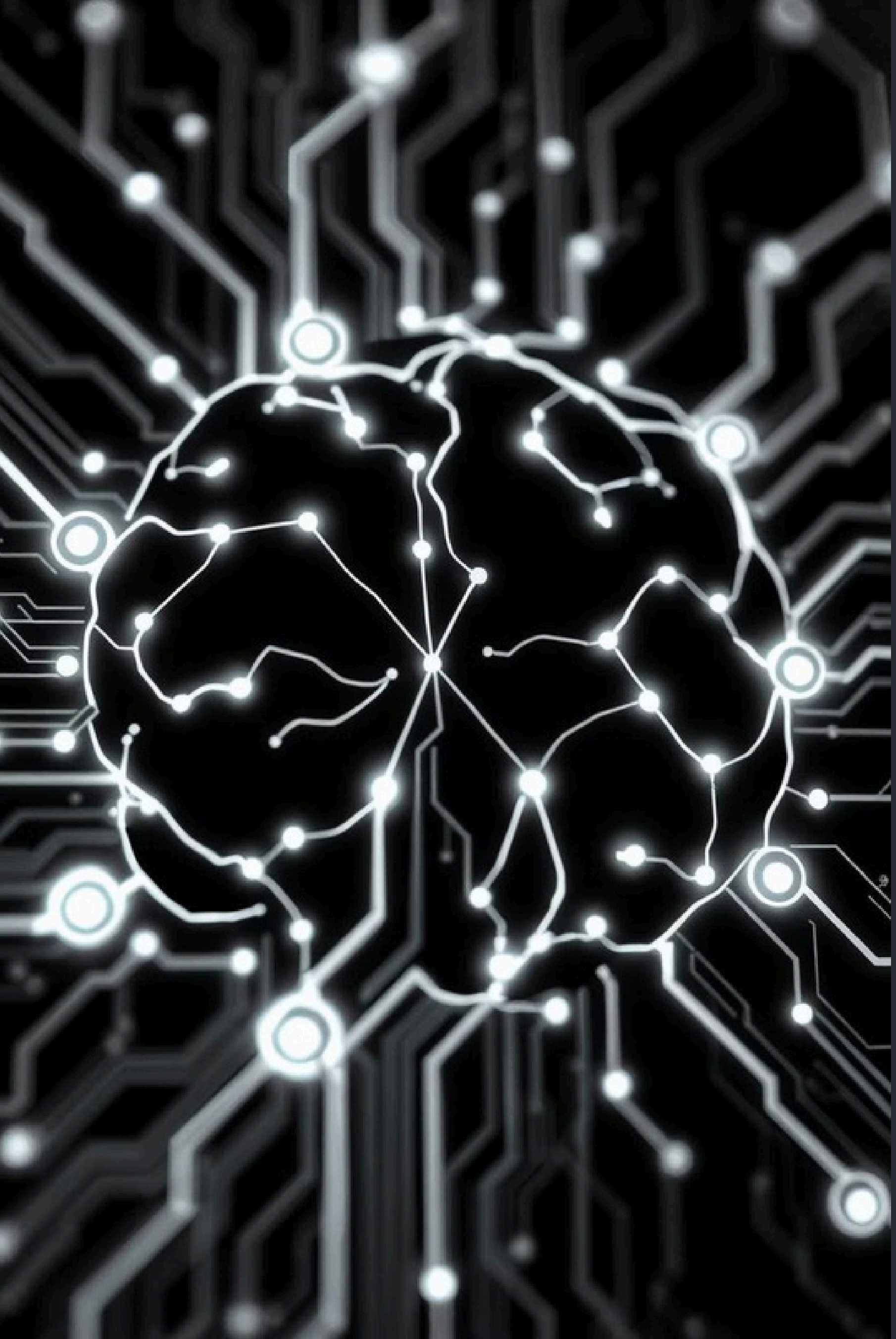
Problem Statement & Objectives

Problems Addressed

- Inefficient static rules.
- High false positive rates.
- Lack of real-time action.

Objectives

- Real-time threat detection.
- Automated IP blocking.
- ML-based anomaly detection.
- User-friendly dashboard.



Literature Survey Highlights

Title	Method	Accuracy
CNN-LSTM for IoT	Deep Learning	96% 97%
Graph Neural Networks	GNN	
Hybrid Signature & Anomaly	ML + Rules	+30% FP reduction

AI Trend: improves detection, reduces FPs, but increases resource usage.

System Architecture

- **Data Collection**: Live packets.
- **Preprocessing**: Cleaning & Feature Extraction.
- **ML Layer**: Random Forest.
- **Detection & Prevention**
- **Logging & Alerting**
- **Web Dashboard**

Real-time monitoring and IP blocking integrated.

Methodology

- Train Random Forest (NSL-
- KDD). Sniff packets (Scapy).
- Extract Features ^{3} Classify ^{3}
- Action.
- Visualize, Log Attacks.

  Update model periodically.

Dataset Overview

Primary Dataset

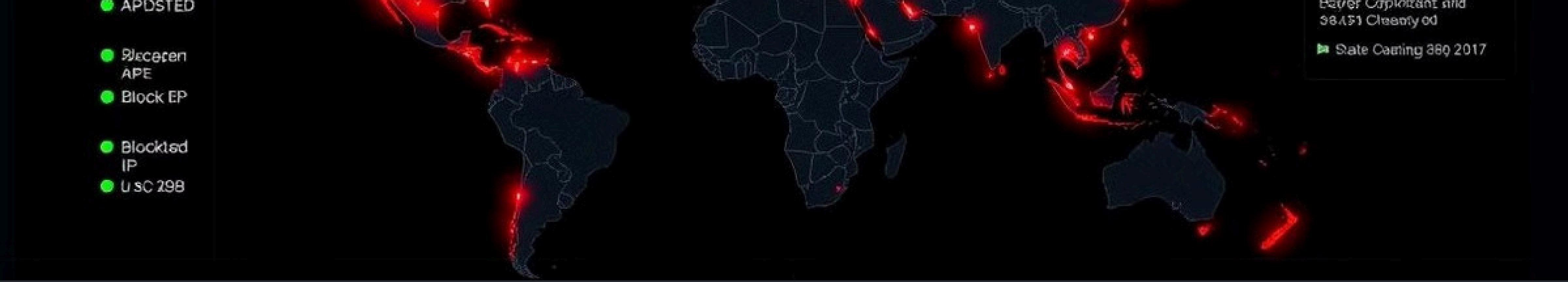
- NSL-KDD.
- 41 features + 1 label.
- Attack types: DoS, Probe, U2R, R2L.

Extended Datasets

- CIC-IDS2017: Botnets, XSS, SQLi
- UNSW-NB15: Worms, Exploits, Shellcode.
- Real-time & adversarial traffic.

Technologies Used

- **Python**: Core Development. **Flask**: Web
- Dashboard. **Scapy**: Packet Analysis.
- **Scikit-learn**: ML Model (Random Forest).
- **Pandas/NumPy**: Data Handling.
- **Matplotlib/Seaborn**: Visualization.
-



Output & Performance

- **Web Interface**: Logs, IP Blocking, Alert Suppression.
- **Detection Accuracy**: High, low false positives.
- **Detected Attacks**: DoS, TCP scans, Recon.
- **Real-time**: Alerts, dynamic firewall updates.

Conclusion & Future Work

Conclusion

Hybrid ML + Heuristics = efficient IDPS.

Real-time threat mitigation with automation.

Future Scope

- Deep learning models (CNN, RNN).
- Integrate with SIEM (Splunk).
- Enterprise deployment.

Thank you!

We sincerely thank our Mentor, Project Co-Ordinator,DEAN sir and peers for their support and guidance throughout this journey

THIS PROJECT HAS BEEN A COLLABORATIVE EFFORT FILLED WITH LEARNING, INNOVATION, AND TEAMWORK.