Real-Time Attack Detection System for Cyber-Physical Systems (CPS)

Summary of the System

The system is built in Python and uses Scapy for packet capturing, psutil for process monitoring, and Streamlit + Plotly for a modern web dashboard.

It consists of 5 layers:

1. Monitoring Layer

2. Detection Layer

3. Alert Layer

Sends alerts through:

4. Active Defense (IPS) Layer

5. Visualization Layer

How It Works (Simple Flow)

1. **Listen: Sniffer captures packets + monitors logs/processes**
2. **Analyze: Detection modules inspect patterns & event behavior**
3. **Detect: If an attack matches a rule or anomaly → alert triggers**
4. **Respond: System optionally blocks attacker or stops malicious processes**
5. **Display: Dashboard updates in real time with attack data**

Conclusion

This project successfully demonstrates a complete Intrusion Detection + Intrusion Prevention System (IDS/IPS) tailored for both IT networks and Cyber-Physical Systems.
It offers real-time monitoring, intelligent detection, instant alerts, and automated defense, all wrapped inside a clean, modern dashboard.

The system proves that a lightweight, Python-based security framework can effectively detect and respond to complex cyber attacks — making it valuable for learning, research, and real-world security enhancement.