**Network Packet Sniffer with Real-Time Anomaly Detection System**

**Introduction**

In modern cybersecurity, monitoring network traffic and detecting anomalies is critical for preventing attacks such as port scanning, flooding, and other suspicious activities. This project focuses on designing a **real-time network packet sniffer with an integrated alert system**, providing a visual and interactive dashboard for monitoring network traffic efficiently.

**Abstract**

The project implements a web-based network monitoring application that simulates real-time traffic and automatically detects anomalies. It visualizes packet flow, statistical metrics, and suspicious patterns through an interactive dashboard. The alert system notifies users when traffic thresholds or suspicious activity patterns are detected. This solution demonstrates the core principles of a network packet sniffer without requiring low-level network capture libraries, making it suitable for educational and professional demonstrations.

**Tools Used**

* **Frontend:** React, TypeScript, Tailwind CSS
* **Data Visualization:** Recharts, Chart.js
* **Data Processing:** Simulated network data with anomaly detection algorithms
* **Utilities:** Date-fns for timestamp handling
* **Version Control & Deployment:** Git, npm

**Steps Involved in Building the Project**

1. **Packet Data Simulation**
   * Simulated network traffic with various protocols (TCP, UDP, ICMP, HTTP, HTTPS)
   * Logged packet details including IP addresses, ports, packet length, and flags
2. **Anomaly Detection Engine**
   * **Port Scanning Detection:** Monitors multiple port connection attempts from a single IP
   * **Flood Attack Recognition:** Detects high-volume traffic spikes beyond configurable thresholds
   * **Suspicious Traffic Analysis:** Flags abnormal traffic patterns or connections to known risky ports
   * **Bandwidth Monitoring:** Tracks unusual data transfer patterns
3. **Data Processing & Logging**
   * Maintained statistical summaries of network traffic
   * Processed packets in real-time using efficient data structures (Maps, Sets)
   * Implemented sliding window algorithms for time-based analysis and memory optimization
4. **Interactive Dashboard & Visualization**
   * Live charts displaying traffic timelines, protocol distribution, top destination ports
   * Real-time alert panel with color-coded severity levels (low, medium, high, critical)
   * Modular UI with components for packet table, stats summary, and alert panel
5. **Alert System Implementation**
   * Configurable thresholds for each detection type
   * Alerts triggered instantly for detected anomalies
   * Severity-based notification and acknowledgment workflow
6. **Optimization & Performance**
   * Limited memory usage by maintaining only the most recent packets in memory
   * Throttled UI updates to ensure smooth real-time visualization
   * Modular codebase for future scalability

**Conclusion**

This project successfully demonstrates a **network packet sniffer with real-time anomaly detection** through a web-based dashboard. It highlights the core concepts of cybersecurity monitoring, anomaly detection, and alerting mechanisms. The modular design allows further enhancement, such as integrating machine learning-based threat detection, geolocation visualization, or exportable forensic reports. This project strengthens understanding of network protocols, threat patterns, and full-stack development in cybersecurity applications.