Requirements Specification

Project Title: Packet Sniffer with Biometrics for Secure Network Monitoring

Team: Byte Builders
Members: Thong Dang, Oluwatosin Omiteru, Christian Mandujano Brojas

1. Introduction

The purpose of this document is to record the functional and non-functional requirements of the **Packet Sniffer with Biometrics for Secure Network Monitoring project**, which will analyze and track network traffic in real time along with secure access through biometric verification.

2. System Overview

The system integrates two principal components:

1. **Packet Sniffer** – Sniffs and examines network traffic for monitoring purposes.
2. **Biometric Authentication** – Protects sniffer capabilities and network logs from being accessed by only authorized individuals.

The project will enhance network security by utilizing real-time monitoring, secure data storage, and alerts on unusual activity.

3. Functional Requirements

The system will implement the following functions:

3.1. Packet Sniffing Functionality

- The system will record network packets in real time.
- The system will parse useful information such as source IP, destination IP, protocol type, and payload data.
- The system will filter traffic based on predefined rules (e.g., HTTP, FTP, or DNS packets).
- The system will log network traffic for future analysis and provide secure storage for logged data.

3.2. Biometric Authentication

- The system shall use a fingerprint scanner or facial recognition camera for user authentication.
- The system shall store biometric data securely for verification.
- The system shall restrict access to packet sniffer functionalities unless authentication is successful.

3.3. Secure Data Storage & Logging

- The system will encrypt packet data that has been captured before it is stored.
- The system will maintain a secure log of network activity for future use.
- The system will allow retrieval of historical network traffic data.

3.4. User Interface (UI) for Monitoring

- The system will possess a web-based dashboard or LCD display for real-time traffic analysis.
- The UI will be accessible only upon successful biometric authentication.
- The UI will display network statistics, security alerts, and logged traffic.

3.5. Real-Time Alerts & Notifications

- The system detects suspicious activities such as abnormal data transfer rates or unauthorized access attempts.
- The system generates alerts and log security incidents for network administrators.

4. Non-Functional Requirements

4.1. Performance

- The system will process and analyze network traffic in real time with minimal latency.
- The biometric authentication process shall not exceed 2 seconds for user verification.

4.2. Security

- All biometric and network traffic data shall be encrypted using secure encryption algorithms (e.g., AES-256).
- Unauthorized access attempts shall be logged and flagged.

4.3. Reliability

- The system maintains continuous packet monitoring without interruptions.
- The biometric authentication module shall have an accuracy rate of at least 95%.

4.4. Scalability

- The system will support multiple network protocols for packet sniffing.
- The storage system shall allow scalable logging of historical network data.

4.5. Usability

- The UI shall be designed to be user-friendly and intuitive for administrators.
- Alerts and logs shall be easily accessible and understandable.

5. System States and Operation Flow

5.1. Initial State

- The packet sniffer is inactive and requires biometric authentication.
- The system is waiting for an authorized user.

5.2. Authentication Phase

- User inputs fingerprint or facial recognition.
- If authentication fails, access is denied, and an attempt is logged.
- If authentication succeeds, access to the sniffer and monitoring dashboard is granted.

5.3. Packet Capturing and Analysis

- The sniffer captures real-time packets.
- Extracts source IP, destination IP, protocol type, and payload data.
- Encrypts and logs the data for security.

5.4. Monitoring and Alerting

- Displays real-time traffic statistics on the UI.
- Detects suspicious activities and triggers alerts.
- Logs alerts and unauthorized access attempts.

5.5. System Shutdown

- Logs out the user after a timeout period.
- Stores all session logs and encrypts the stored data.

6. Hardware and Software Components

6.1. Hardware Requirements

- **Packet Sniffer Device**: Raspberry Pi or Microcontroller
- **Biometric Authentication Sensor**: R307 Fingerprint Sensor or Raspberry Pi Camera
- **Display Interface**: LCD Screen or Web-based Dashboard
- **Storage**: Local or Cloud Storage with Encryption

6.2. Software Requirements

- **Packet Sniffer Libraries**: Wireshark, Scapy, or custom sniffing scripts
- **Biometric Software**: OpenCV for facial recognition or Fingerprint Processing SDK
- **Encryption Libraries**: AES-256 or RSA for securing stored data
- **User Interface Framework**: HTML, CSS, JavaScript for a web-based dashboard

7. Constraints & Assumptions

- The system assumes users have enrolled biometric data ahead of authentication.
- The packet sniffer only sniffs permitted traffic to comply with ethical and legal requirements.
- The system must function on low-power embedded hardware successfully.

8. Expected Outcomes

- A dedicated packet sniffer with biometric login.
- A secured and encrypted traffic logging process.
- A security alarm displaying intranet portal on real-time dashboards.
- An entity capable of capturing and reporting suspicious behavior.

9. Conclusion

The Packet Sniffer with Biometrics for Secure Network Monitoring will provide a superior security solution through the integration of real-time network traffic analysis and biometric authentication. The system will block unauthorized network analysis while maintaining sensitive network data protected.