REPORT ON REQUIREMENT ANALYSIS

PRESENTED BY

GROUP 3

MEMBERS

ETHE ENAME CALUDE VIRGIL (SENG22SE015)

ETIKWE RAMPSON NQWESEPOH (SENG22TE004)

AGBOR TABE AYAMBA (SENG22TE002)

1. Review and Analysis of Gathered Requirements

Completeness

The requirements gathered cover key functionalities expected in a biometric student attendance system, including:

- Biometric login (e.g., fingerprint or facial recognition)
- Student profile management
- Attendance logging and reporting
- Admin dashboard for monitoring and reports

However, some requirements such as error handling mechanisms, offline mode support, and data synchronization are partially specified and need elaboration.

Clarity

Most requirements are clear and understandable. For example:

- “The system should allow students to mark attendance using fingerprint recognition.”
  This is concise and measurable.

However, some vague statements such as “The system should be user-friendly” require further elaboration into measurable non-functional requirements (e.g., response time, success rate of biometric scans).

Technical Feasibility

Technically, the app is feasible using:

- Mobile platforms (Android/iOS) with biometric APIs
- Cloud-based or local databases for storage
- Admin backend interface for attendance tracking

Considerations:

- Device compatibility with biometric sensors
- Security measures for storing biometric data
- Compliance with data protection regulations

Dependency Relationships

Some requirements depend on others:

- Biometric authentication depends on user registration.
- Attendance reporting depends on successful data logging.
- Admin features depend on real-time data synchronization.

2. Identification of Inconsistencies, Ambiguities, and Missing Information

Inconsistencies

- Conflicting statements about whether offline attendance is supported.
- Differing views on who can access historical attendance data (students vs. only admins).

Ambiguities

- “Should support multiple biometric types” — unclear if all must be implemented or just one.
- “Fast login” — no metric for what qualifies as “fast.”

Missing Information

- Backup and recovery protocols for biometric data
- Notification or alert system for irregular attendance

- Detailed user roles and access levels

3. Requirement Prioritization

Requirement	Priority	Reason
Biometric authentication	High	Core functionality
Attendance logging	High	Essential operation
Admin dashboard	High	Necessary for oversight
Student profile management	Medium	Supports main features
Notification system	Medium	Improves usability
Analytics and reports	Medium	Adds value
Offline attendance support	Low	Complex and optional

4. Classification of Requirements

Functional Requirements

- Register and authenticate students using biometrics
- Log attendance with timestamps
- Admin can view, edit, and export attendance data
- Generate attendance reports by class/date/student
- Student can view personal attendance history

Non-Functional Requirements

- Authentication success rate should be above 95%
- System should respond within 2 seconds for login
- App should work with Android 10+ and iOS 14+
- Biometric data must be encrypted in storage and transmission

- Uptime should be at least 99% monthly
- Comply with local data privacy laws (e.g., GDPR if applicable)

5. Software Requirements Specification (SRS)

A full SRS will be developed (refer to the next task), but at this stage, a summarized version includes:

Introduction

- Purpose: Provide a secure, reliable, and user-friendly biometric attendance system.
- Scope: Supports student and admin roles, biometric login, real-time attendance tracking.

Overall Description

- System interfaces: Biometric sensors, mobile device OS, database
- User classes: Students, Admins
- Constraints: Device compatibility, data storage, security

Specific Requirements

- FR1: The system shall allow students to authenticate via biometric input.
- FR2: The system shall log attendance with timestamp and student ID.
- FR3: The admin shall be able to generate class-wise attendance reports.
- NFR1: System shall encrypt biometric data using AES-256.
- NFR2: App shall respond to user input within 2 seconds.

6. Validation with Stakeholders

Validation Process

- Requirements were reviewed in stakeholder meetings including instructors, IT staff, and student representatives.
- Use cases were presented to illustrate typical interactions.
- Feedback was gathered on:
    - App interface expectations
    - Concerns over data privacy
    - Role definitions and permissions

Key Outcomes

- Agreement on mandatory biometric login
- Clarified that only admins should have edit access to attendance
- Added requirement for students to receive absence notifications