College of Technology and Built Environment
School of Information Technology and Engineering
Fundamentals of Software Engine

Biometric(Faceprint) Attendance System

Software Requirements Specification

Team Members
1. Abraham Nigatu — UGR/7532/16
2. Hermela Teklegebriel — UGR/5174/16
3. Manuhe Habtamu UGR/2808/16
4. Naomi Mesfin —UGR/8207/16
5. Tsedeniya Fiseha — UGR/9263/16
6. Yordanos Teshome —- UGR/0489/16
7. Zenebu Melaku — UGR/6058/16

Advisors: Nuniyat Kifle

November 14, 2025 G.C

.

Revision History

Date	Description	Author	Comments
November 4, 2025	<Version 1>	All Members	First Draft
November 8, 2025	<Version 2>	All Members	Second Draft
November 12, 2025	<Version 3>	All Members	Final Draft

Document Approval

The following Software Requirements Specification has been accepted and approved by the following:

Signature	Printed Name	Title	Date
	Nuniyat Kifle	Instructor	

Table of Contents

List of Tables

List of figures

Definitions, Acronyms, and Abbreviations

Term/Acronym	Definition
Faceprint	"A digital representation of the features of an individual's face, extracted as a numerical vector (embedding) used for identification in biometric systems. Also referred to as facial embedding."
Facial Embedding	A 128 or 512-dimensional float vector that is generated from a facial image using deep models, such as FaceNet or dlib. Used for comparison during recognition.
Host	"A user with administrative privileges who is an instructor, lecturer, or admin creates subjects, schedules events, starts attendance sessions, and generates reports."
Attendee	user who signed up for a subject/event and records attendance via face recognition.
Subject	"A course, class, meeting, or organizational unit (e.g., "Intro to Programming") under which attendance events are organized."
Event	"A scheduled instance of attendance-taking (e.g., lecture on Nov 15, 2025, at 9:00 AM)".
Enrollment	The process by which an Attendee registers their faceprint for a given Subject.
Check-in/Check-out	A timestamp of when someone arrives or leaves an event.
Late Threshold	The maximum allowable delay (default: 15 minutes) after event start time to still be marked "Present" instead of "Late".
OpenCV	Open Source Computer Vision Library - a Python library used for real-time image processing and face detection.
dlib	A C++ library containing machine learning algorithms. It's used here for detecting facial landmarks and generating embeddings.
PostgreSQL	is an "open-source relational database management system used to store user data, facial embeddings, and attendance logs."
GUI	Graphical User Interface: the web-based dashboard accessed via browser.

FPS	Frames Per Second – smoothness of video stream, measured in frames per second. System requires ≥20–30 FPS.
HTTPS/TLS	Secure communication protocols that provide encrypted data transfers between client and server.
SMTP	Simple Mail Transfer Protocol - used to send email notifications: reminders, confirmations.
RESTful API	Representational State Transfer API - used for internal module communication, in case microservices are implemented.
WebSocket	A protocol providing full-duplex communication channels over a single TCP connection; used optionally to provide real-time dashboard updates.
GDPR	General Data Protection Regulation: EU regulation with regard to the handling of biometric data and user rights, such as the right to delete face data.
UPS	Uninterruptible Power Supply - Optional hardware zu_override power outages to keep the system available
CSV/PDF	File types for downloadable attendance reports.
Original photo	Original image provided during enrollment; deleted immediately after embedding extraction for privacy.
Manual Override	" Ability of the host to correct automatically marked attendance, for example, changing "Absent" to "Present".

DECLARATION

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included. We have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Group 2 Team

Name	ID
Abraham Nigatu	UGR/7532/16
Hermela Teklegebriel	UGR/5174/16
Manuhe Habtamu	UGR/2808/16
Naomi Mesfin	UGR/8207/16
Tsedeniya Fiseha	UGR/9263/16
Yordanos Teshome	UGR/0489/16
Zenebu Melaku	UGR/6058/16

Date: 11-14-2025

1. Introduction

This SRS project is prepared for the biometric faceprint attendance we will be developing as our course project. It will cover all the necessary issues to be addressed throughout the development of the app.

1.1 Purpose

The purpose of this Software Requirements Specification (SRS) is to provide a detailed description of the requirements for the "The Biometric Faceprint Attendance System" This document is intended for a wide audience, including:

●The Development Team: To understand the exact features, functionalities, and constraints of the system they are required to build.

●The Clients (Teachers and Students): To serve as a formal agreement on the system's capabilities, scope, and limitations.

●The Project Advisor: To evaluate the project's completeness, feasibility, and adherence to academic and technical standards.

●Testers and Quality Assurance: To provide a basis for creating test plans, test cases, and verifying that the implemented system meets all specified Requirements.

This document will define the system's purpose, scope, and specific requirements, ensuring all stakeholders have a clear and common understanding of the final product.

1.2 Scope

The software product to be developed is called The Biometric Faceprint Attendance System. The main purpose of this project is to record the attendance of students, employees, staff or any individual within an organization or where the attendance has been taken. The system will focus on face recognition to recognize individuals and store their attendance on the central database. The system using facial recognition biometric will keep historical data making it easier for the lecturers to access.

Upon arrival the system checks students' faces using the system developed. Then the system will recognize the individual's facial features and store it in the central database for the purpose of comparing the facial features in future use and providing a user-friendly interface to manage the database. Once recognized the record will be automatically logged with the real time. Administrators will be able to view detailed information of students, record time and generate reports.

The system aims to:

- Enhance real-time security measures.
- Automate attendance management
- Enable seamless access control through accurate face recognition

This system does not include remote attendance system, payroll management whatsoever. The system's efficiency is highly dependent on the lighting of the environment and image quality for the purpose of clear facial image. Sudden change in a person's appearance over time like aging, facial hair, glasses etc can affect the accuracy.

This SRS documentation covers all the functional aspects of our project and the features it will incorporate.The requirements and possible constraints will be extensively discussed in the following sections. All effort has been made to ensure that this document creates a holistic picture of the project.

1.3 <u>Overview</u>

This SRS document is organized into four main sections:

- Section 1: Introduction: Provides the purpose, scope, and an overview of this document.
- Section 2: General Description: Describes the overall product perspective, its main functions, the characteristics of its intended users, and the high-level constraints and assumptions that affect its development.
- Section 3: Specific Requirements: Details all specific requirements, including external interfaces (UI, hardware, software), functional requirements (features), use cases, non-functional requirements (performance, security, etc.), and any design constraints.
- Section 4: Change Management Process: Outlines the procedure for making, approving, and tracking changes to the requirements defined in this document. Appendices and references are included at the end.

2. General Description

2.1 Product Perspective

The Facial Recognition Attendance System uses a face recognition approach to prevent forgeries of attendance and to automate signing in. The captured and confirmed faces of employees/students by webcam store their biometric data within the system. The system also keeps track of check-in/check-out hours and displays reports to the admins. In this regard, the paperless attendance management is fully accurate and time-saving both for the employees and admins. The image processing and face detection are done using OpenCV, while the database holds the details of the employee, facial data, and attendance records.

2.2 Product Functions

The system will:

- Allow admins to create an employee's account with name, ID, department, and face data.
- Identify and recognize employees' faces, from the real-time stream of a camera.
- Automatic recording of attendance-both check-in and check-out time.
- Generate attendance reports daily, weekly, or monthly.
- Allow the admin to manage user accounts, employee data, and reports.
- Send notifications for missed check-ins.

2.3 User Characteristics

Admin/Host: Creates and runs the system, registering employees, updating or deleting records in it. Basic computer knowledge is required.

Employee/Student: Uses the system for attendance simply by standing in front of the camera for facial verification.

2.4 General Constraints

- The camera quality and lighting conditions determine how accurate the system is.
- Facial recognition can fail if the employee's face is partially covered-for example, masks or sunglasses.
- Requires a continuous flow of power supply, webcam functional.
- Facial data must be handled and kept secure to protect user privacy.
- Performance depends upon computer processing power and memory capacity.
- Security and privacy are critical: facial data should be encrypted and access-controlled, with regulatory policies in place to protect user information.

2.5 Assumptions and Dependencies

Assumptions

- Employees have to provide their biometric data
- The camera has to be positioned correctly in order to capture faces.
- The admin will have basic computer knowledge to operate the system.

Dependencies

- OpenCV for face detection and recognition.
- PostgreSQL to store data.
- This requires a stable power supply and functioning camera hardware.
- Other Python packages for data handling and analysis.

3. Specific Requirements

3.1 External Interface Requirements

In this part, the interaction of the Biometric (Faceprint) Attendance System with all external interfaces is explained. The external interfaces include user, hardware, software, and communication. These interfaces define the interaction of users, devices, and external systems with the software.

3.1.1 User Interfaces

The system shall feature an interface that is easy to use, intuitive, and secure from any Host (Admins/Instructors) and Attendee (Students/Employees) perspectives.
The following types of User Interface must be supported:
Web-Based Graphical User Interface (GUI)
Supported on the most commonly used web browsers (Chrome, Firefox, Edge, Safari).
Responsive design created for desktop and laptop viewing.
Provides different dashboards according to user roles:

- Host Dashboard: control over subject creation, scheduling of events, running of sessions for attendance, generating reports.
- Attendee Dashboard: registering, enrolling and viewing schedules, and managing personal data.

The interfaces should provide a clear indication of:
- Profile settings
- Attendance status
- Alerts and notifications
- Subject/event list

- Camera Interface (Real-Time Attendance Window)
- During the attendance sessions, it will show the live camera feed.
- The status of the detection will be shown in real time as: "Face Detected", "Match Found", "Unknown Face".
- Confirms attendance by sound (beep) and visual confirmation.

Accessibility Requirements
- The font must be large and easy to read for visibility purposes.
- UI mode with high contrast
- The keyboard can be used to navigate through the form fields.
- The system should be compatible with the screen reader.

UI/UX Mock Design Collection
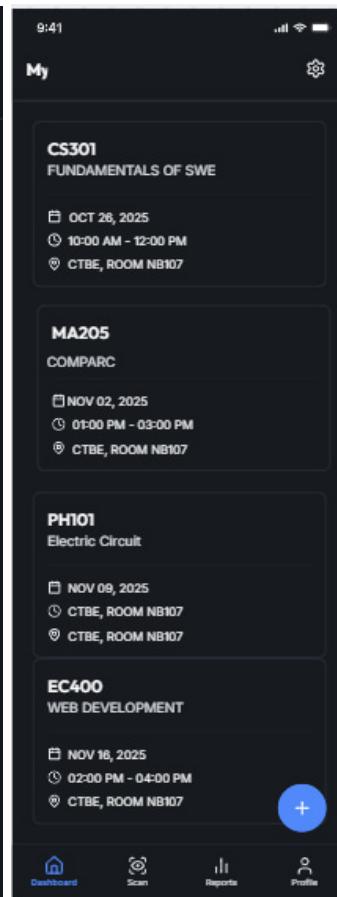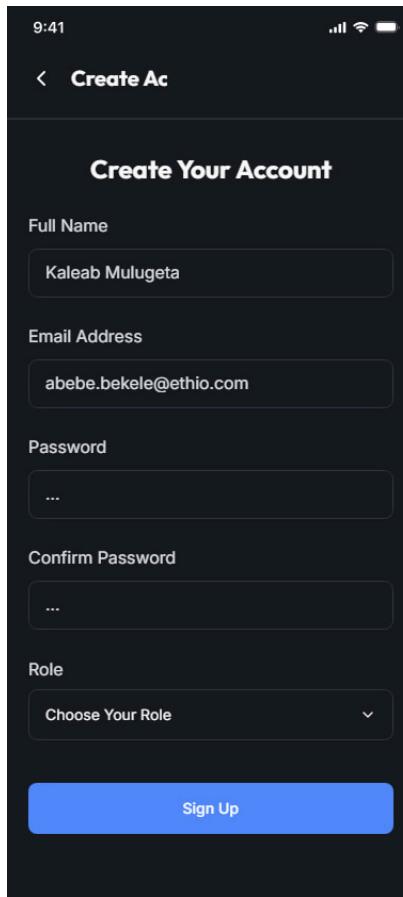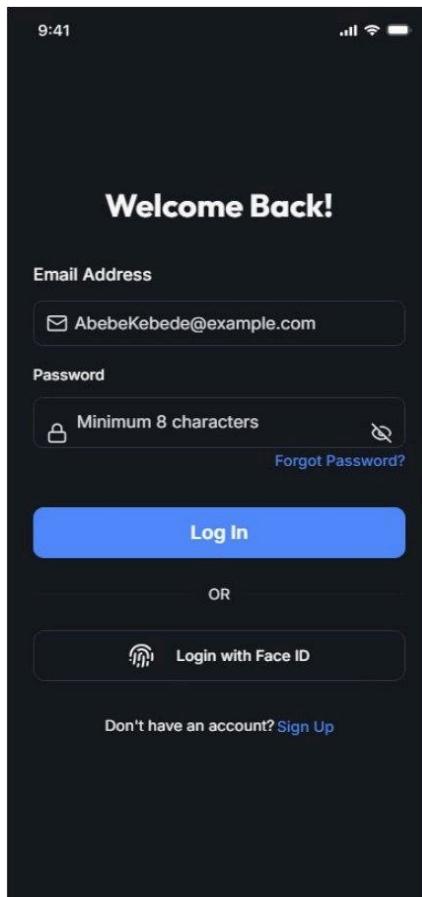
Fig 3.1 Login Screen   **Fig 3.2 Sign Up Page**   **Fig 3.3 Host Dashboard**
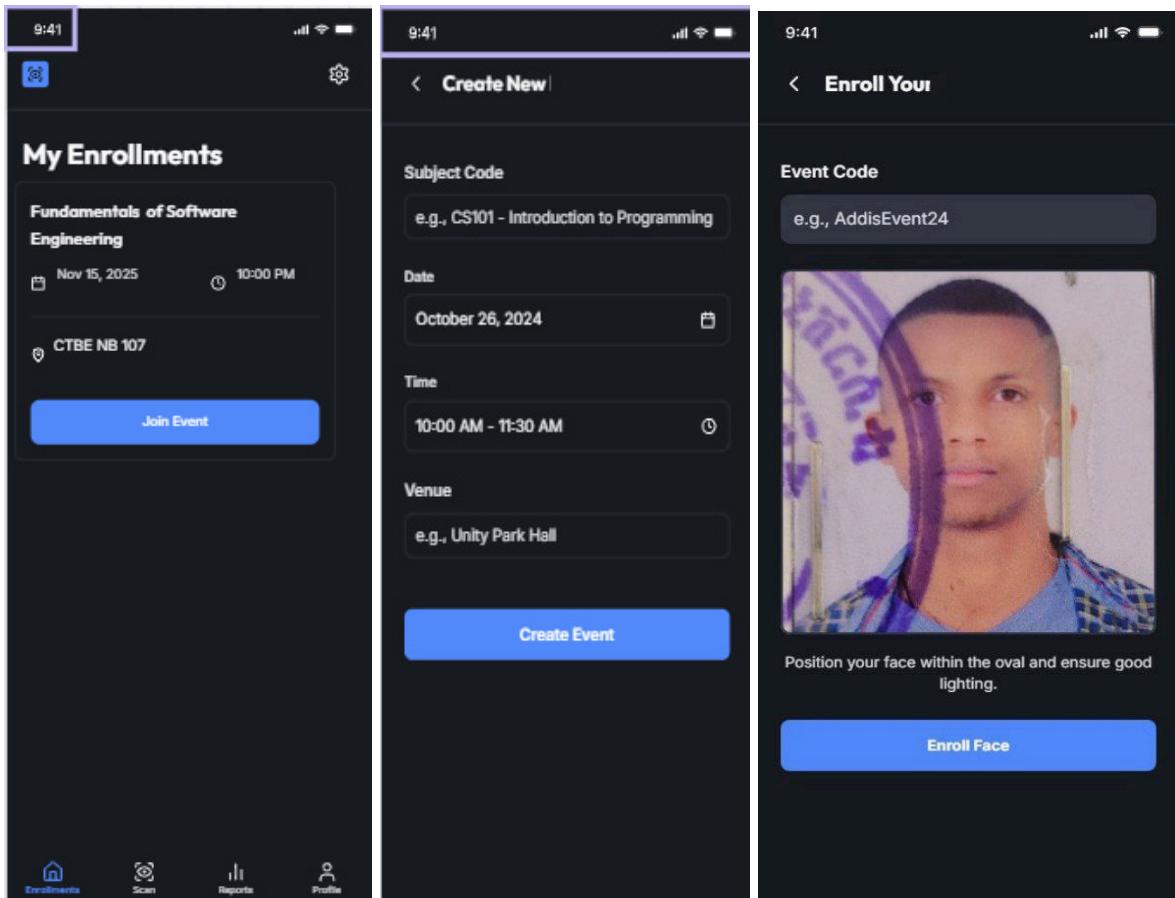
Fig 3.4 Attendee Dashboard   Fig 3.5 Create Event   Fig 3.6 Enroll Face
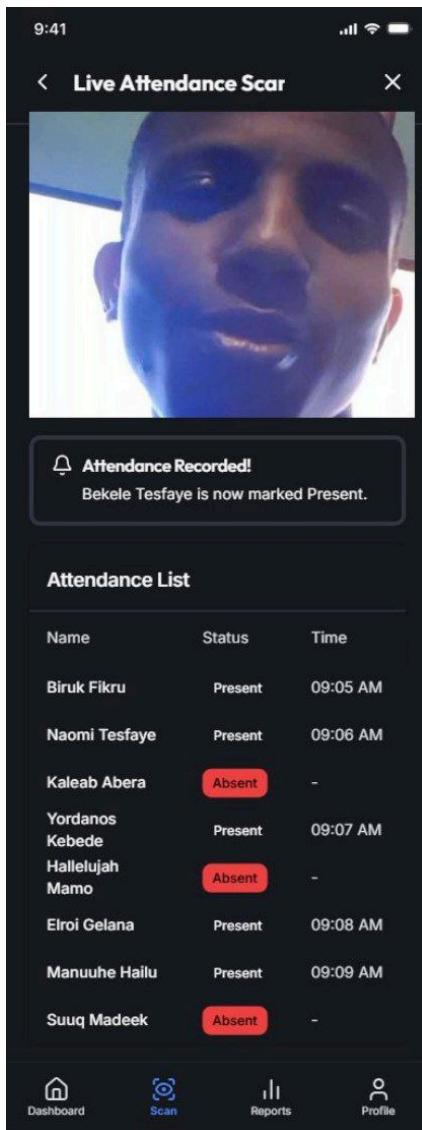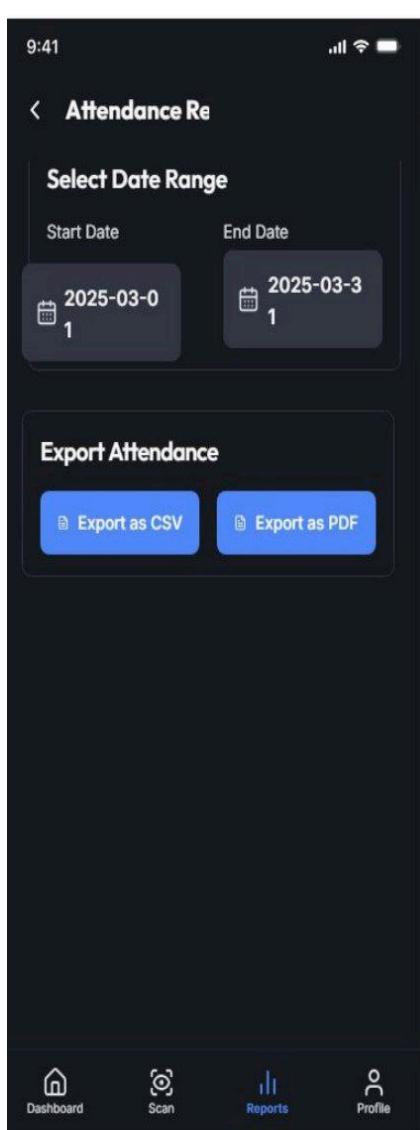
Fig 3.7 Live Scan   **Fig 3.8 Report Generation**   **Fig 3.9 Privacy**
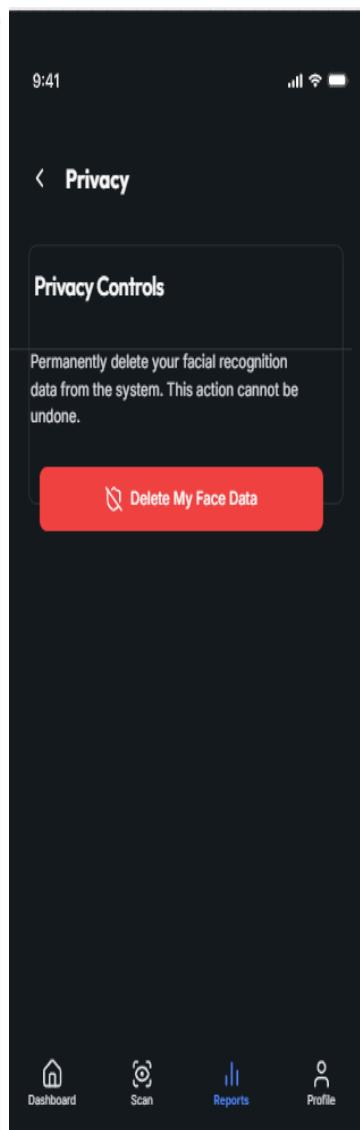
3.1.2 Hardware Interfaces

The system interacts with hardware required for capturing facial images and supporting system operation.

Supported Hardware

- **Standard HD Webcam (720p or higher)**

  - Used for capturing facial images for enrollment and attendance.
  - The system must detect when the webcam is unavailable or malfunctioning.

Camera Interface Specifications

- Video input must maintain at least **20–30 FPS** for smooth face detection.
- Accepts USB webcams commonly used in offices and classrooms.
- Must integrate with the OS camera services (Windows, Linux, macOS).

Optional Hardware

- **UPS (Uninterruptible Power Supply)**

  - Ensures continuous operation during power interruptions.
  - Not controlled by the system but supports availability requirements.

3.1.3 Software Interfaces

The Biometric Attendance System interacts with required third-party libraries, frameworks, and database systems.

Table 3.1.0 Mandatory Software Components

Software	Purpose	Version	Interface Type
Python 3.9+	Core application language	3.9 or later	Execution environment
OpenCV	Face detection and image processing	4.x	Used via Python API
Face Recognition Library (dlib or similar)	Facial embedding extraction	Latest stable	Embedding generation

PostgreSQL	Database backend	v12+	Via psycopg2 or SQLAlchemy
Email Service Provider (SMTP)	Notification delivery	Standard SMTP	Email protocol

Database Interface

- Communications performed through secure SQL queries.
- Inputs/outputs:
  - User account data
  - Facial embeddings (encrypted)
  - Attendance logs
  - Subject + event information

File Handling Interface

- Accepts uploaded images (JPG/PNG) for enrollment.
- Maximum file size: **2 MB**.

3.1.4 Communications Interfaces

The system requires reliable communication protocols to support user authentication, data retrieval, and notifications.

Network Requirements

- System operates over standard TCP/IP networks.
- All communication between client and server must be encrypted using **HTTPS (TLS 1.2+)**.

Email Notification Interface

- Uses SMTP protocol to send:
  - Event reminders
  - Enrollment confirmations
  - Face data deletion confirmations
  - System alerts (e.g., failed attempts)

Real-Time Attendance Data Updates

- Optional use of WebSockets or long polling for live dashboard updates.
- Ensures hosts see live attendance status during sessions.

3.2 Functional Requirements

Table 3.2.1 Sign up

ID	FR-01
Name	Signup
Input	Email, password, confirm password, full name, role (Host / Attendee)
Processing	The system makes sure email format and unique email.
Output	Account created → redirect to login. Email verification sent.
Dependency	None
Error Handling	Email already exists, Invalid email format , Passwords don't match, Weak password
Reference	UC-01

Table 3.2.2 Logging in

ID	FR-02
Name	Login
Input	Email, password
Processing	System should allow the user to sign in after checking with the encrypted db.
Output	Login successful
Dependency	FR-01 (Signup should be done)
Error Handling	Wrong Email/Password, Account Not Verified
Reference	UC-02

Table 3.2.3 Profile Edit

ID	FR-03
Name	Profile Edit
Input	Full name, email, contact number, profile photo (non-biometric)
Processing	System validates and updates profile.
Output	Profile updated and saved. Confirmation message.
Dependency	FR-02 (Login)
Error Handling	Invalid email, File too large (>2MB)
Reference	UC-03

Table 3.2.4 Subject creation and Session scheduling

ID	FR-04
Name	Subject Creation + Event Scheduling
Input	Subject: Name (e.g., "Intro to Programming", "Senate Meeting") Event: Title, date, start time, venue (optional) and instructions (optional)
Processing	System generates unique subject code and automatically sends email to enrolled Attendees.
Output	Subject created. Event scheduled. Email sent with: subject, title, date, time, venue, "Don't be late more than 15 minutes." Event appears on both dashboards.
Dependency	FR-02 (Login as Host)
Error Handling	Subject name required, Date must be future
Reference	UC-04

Table 3.2.5 Attendee Registration with Faceprint Enrollment

ID	FR-05
Name	Attendee Registration with Faceprint Enrollment
Input	Subject code, one clear frontal facial photo
Processing	System validates code. Captures face → extracts facial embeddings → encrypts and stores linked to Attendee + subject.
Output	Enrollment confirmed. Attendee added to subject roster.
Dependency	FR-04 (Subject should exist), FR-02 (Log in as Attendee)
Error Handling	Invalid or Expired Code Face Not Detected Poor Image Quality Already Enrolled
Reference	UC-05

Table 3.2.6 Automated Reminders & Notifications

ID	FR-06
Name	Automated Reminders & Notifications
Input	Auto-activated 30–60 min prior to event
Processing	System sends: Email reminder, In-app dashboard banner, Push notification (mobile)
Output	Host and Attendees receive: event details + "Event starts in X minutes"
Dependency	FR-04 (Event must be scheduled) FR-05 (Attendees enrolled)
Error Handling	"Email failed" (logged, retry)
Reference	UC-08

Table 3.2.7 Attendance Session Management + Marking & Manual Override

ID	FR-07
Name	Attendance Session Management + Marking & Manual Override
Input	Click "Start Session" → camera feed

Processing	Processing System turns on the camera:
	1. Activates camera
	2. Captures live face
	3. Compares with stored embeddings
	4. On match: Beep + record timestamp + name
	5. If ≤15 min late → Present
	6. If >15 min → Late
	7. No match → Absent
	8. The status can be manually edited by the host.
Output	Real-time attendance list. Beep on success. Final status: Present / Late / Absent
Dependency	FR-04(Event scheduled) FR-05 (Faceprints enrolled) FR-02 (Login as Host)
Error Handling	Camera not accessible , Face not clear — retry , Session ended
Reference	UC-06

Table 3.2.8 Report

ID	FR-08
Name	Report Generation
Input	Select event or date range → format (CSV / PDF)
Processing	Processing System generates the report containing the following: Event details, list of attendees with their name, status, and timestamp
Output	Downloadable CSV/PDF.
Dependency	FR-07 (Attendance must be taken)
Error Handling	No data for the selected Range
Reference	UC-07

Table 3.2.9 Face data privacy

ID	FR-09
Name	Face Data Privacy & Deletion
Input	Click "Delete My Face Data" → confirm

Processing	System: 1. Deletes facial embeddings 2. Removes from all subjects 3. Logs deletion 4. Sends confirmation email
Output	Face data erased. Confirmation: "Your biometric data has been deleted."
Dependency	FR-05 (Faceprint must be enrolled), FR-02 (Login as Attendee)
Error Handling	Deletion failed — contact support
Reference	UC-09

3.3 USE CASES

Use Case 1: Sign Up (UC-01)

Field	Description
ID	UC-01
Actor	Guest User
Trigger	Clicks "Sign Up"
Precondition	Not logged in
Postcondition	Account created, verification email sent
Main Course	1. Enter email, password, confirm password, full name, and role Host/Attendee 2. System checks email format, uniqueness, password strength 3. System is creating account and sending verification email 4. Redirect to login or auto-login if enabled
Exceptions	Invalid email, weak password, duplicate email, passwords don't match
Extension	Log sign-up attempt + analytics
Failure Scenario	Creation of account fails due to a server/database error.
Reference	FR-01

Use Case 2: Log In (UC-02)

Field	Description
ID	UC-02
Actor	Host / Attendee
Trigger	Clicks "Log In"
Precondition	There exists an account and it is verified
Postcondition	Session started, role-based dashboard shown
Main Course	1. Login Email & password 2. System validates credentials against encrypted DB 3. Redirect to role-based dashboard
Alternative	1. Forgot password flow
Exceptions	Invalid credentials, account not verified
Extension	Audit log of login attempts
Failure Scenario	DB inaccessible, authentication fails
Reference	FR-02

Use Case 3: Edit Profile (UC-03)

Field	Description
ID	UC-03
Actor	Host / Attendee
Trigger	Opens profile settings
Precondition	Logged in
Postcondition	Profile updated and saved
Main Course	1. Edit full name, email, contact number, non-biometric profile photo 2. System checks email format and file size ≤2MB 3. System saves updates and gives confirmation

Exceptions	invalid email, uploaded file too big
Extension	Log profile edits
Failure Scenario	DB error prevents saving changes
Reference	FR-03

Use Case 4: Create Subject & Schedule Event (UC-04)

Field	Description
ID	UC-04
Actor	Host
Trigger	Clicks "Create Subject / Schedule Event"
Precondition	The host is logged in
Postcondition	Subject and event saved; notifications sent
Main Course	1. Enter subject name → system generates unique subject code 2. Schedule event: title, date, start time, optional venue/instructions 3. Validate future date and check time conflicts 4. Save event and send notification email to enrolled attendees
Alternative	1. Schedule event without optional venue/instructions
Excluded	Missing subject name, past date, event conflict
Extension	The system sends reminders (see UC-08)
Failure Scenario	DB/server error prevents subject/event creation
Reference	FR-04

Use Case 5: Enroll with Faceprint (UC-05)

Field	Description

ID	UC-05
Actor	Attendee
Trigger	Clicks "Enroll in Subject"
Precondition	Logged in; subject code is valid
Postcondition	face print stored; enrollment successful
Main Course	1. Enter subject code → validate 2. Upload clear frontal facial photo 3. System detects face → extracts embeddings → encrypts → stores → deletes raw photo 4. System confirms enrollment
Exceptions	invalid/expired code, poor image, face not detected, already enrolled
Extension	Generate Enrollment Certificate + Log
Failure Scenario	Encryption/storage failure
Reference	FR-05

Use Case 6: Attendance by Face Scan (UC-06)

Field	Description
ID	UC-06
Actor	Host
Trigger	Clicks "Start Attendance Session"
Precondition	Event scheduled; attendees enrolled
Postcondition	Attendance marked in real time - present, late, or absent
Main Course	1. Camera on 2. Capture live face → compare with stored embeddings 3. Record name, timestamp, status (≤15 min = Present, >15 min = Late) 4. Allow override manually 5. Close session

Alternative	1. Manual entry for attendees not detected
Exceptions	Camera not available, blurry face, interrupted session
Extension	Update live dashboard for both Host & Attendees
Failure Scenario	Records of attendance not saved due to system crash
Reference	FR-07

Use Case 7: Manage Reports (UC-07)

Field	Description
ID	UC-07
Actor	Host (Report)
Trigger	Host: Clicks "Generate Report"
Precondition	Attendance taken.
Postcondition	Report downloaded
Main Course	1. Select event/date range + output format (PDF) 2. System compiles event details, attendee list, status, timestamp 3. System allows download and shows analytics
Exceptions	Data unavailable
Failure Scenario	DB/server error prevents report generation

Use Case 8: Automated Reminders (UC-08)

Field	Description
ID	UC-08
Actor	System
Trigger	30–60 min before event start

Precondition	Event scheduled; attendees enrolled
Postcondition	Notifications sent - email, dashboard, push
Main Course	1. Scan upcoming events 2. Send reminders to the Host and Attendees - email, in-app banner, and push notification 3. Log delivery status
Exceptions	Delivery failure → retry
Extension	Analytics on notification open/read rates
Failure Scenario	Notification service down
Reference	FR-06

Use Case 9: Face Data (UC-09)

| Field	Description
ID	UC-09
Actor	Attendee (Delete)
Trigger	Attendee: Clicks "Delete My Face Data"
Precondition	Delete: Faceprint enrolled
Postcondition	face data deleted
Main Course	1. Confirm deletion 2. System deletes embeddings and removes attendee from all subjects, logs deletion, sends confirmation email
Exceptions	Deletion failure
Extension	Audit logs
Failure Scenario	DB/server error prevents deletion
Reference	FR-09

USE CASE DIAGRAM
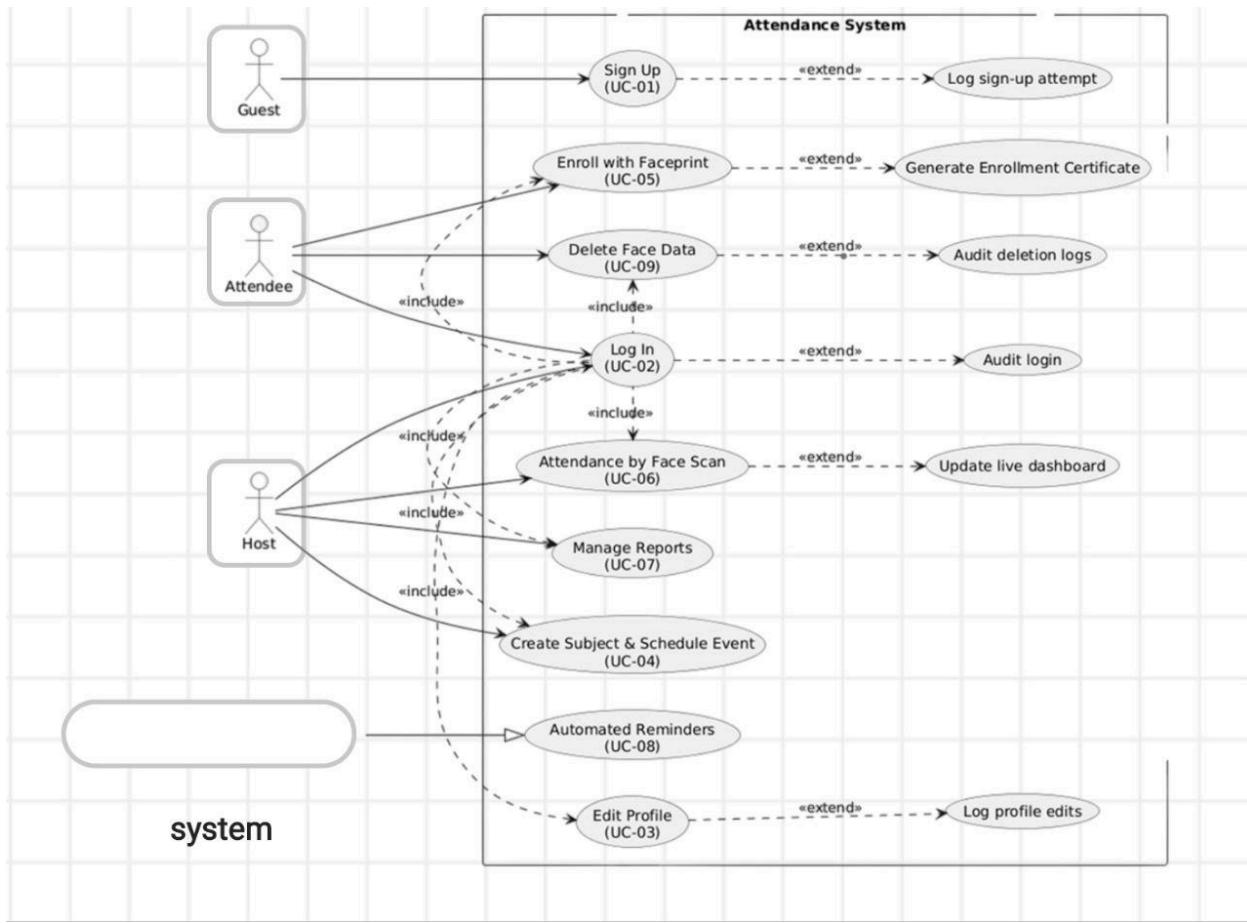
Fig 3.10 UC Diagram

3.4. Non-Functional Requirements

3.4.1. Portability

The system should be deployable on both desktop and mobile devices with camera support, requiring only facial recognition software but no special hardware.

3.4.2. Security

The system shall encrypt all faceprint data and attendance records. Only authorized administrators can view or modify records.

3.4.3. Maintainability

The system should allow easy software updates and database changes without affecting stored data or daily operation.

3.4.4. Reliability

The system shall maintain 95% reliability, automatically saving data and recovering from issues like camera failure, network loss, or app freezes to ensure continuous operation.

3.4.5. Scalability

The system shall support small-to-medium deployments without significant performance degradation.

3.4.6. Performance

On a 3G or faster internet connection, the system shall detect and record a user's face within 2–3 seconds after scanning and display confirmation within 5 seconds.

3.4.7. Reusability

The system modules are specifically designed for face recognition and are not intended for reuse in other types of biometric systems

3.4.8. Flexibility

The system shall allow integration of additional biometric types or attendance categories without major structural changes.

3.5 Inverse Requirements

- The system will not support fingerprint or card-based attendance methods.
 - The system will not allow attendance marking without face detection.
 - The system will not function without camera access permissions.

3.6. Design Constraints

-The system shall be developed using modern web technologies.
 -It must comply with data protection and privacy standards related to biometric information.
 -The system depends on camera-enabled devices; hence, it cannot function on devices without cameras.

3.7. Logical Database Requirements

Table Db Requirements

Table	Description	Attributes
1. Users	The main table for users. Allows login, role-based access, and profile management.	- User ID (Primary Key) - Full Name - Email (Unique) - Password (Hashed) - Role (Host / - Attendee) - Contact Number - Profile Photo URL (non-biometric) - Registration Date - Last Login Date - Is Verified (Email)

2. Subjects	One Host can create multiple subjects. This is used to organize events and registrations.	- Subject ID (Primary Key) - Host ID (Foreign Key → Users) - Subject Name (e.g., "Intro to Programming") - Subject Code (6-char, Unique) - Created At
3. Events	One subject can have many events. Attendance is tied to events in real-time.	- Event ID (Primary Key) - Subject ID (Foreign Key → Subjects) - Title - Event Date - Start Time - Venue (Optional) - Instructions (Optional) - Late Threshold (Default: 15 min) - Status (Scheduled / Ongoing / Completed) - Created At - Started At - Ended At
4. Enrollments	Associates Attendees with Subjects. Stores faceprint for recognition. The raw photo is immediately deleted after embedding.	- Enrollment ID (Primary Key) - Subject ID (Foreign Key → Subjects) - Attendee ID (Foreign Key → Users) - Facial Embedding (512-float vector, encrypted) - Enrolled At - Is Active (Boolean)
5. AttendanceRecords	A real-time attendance log that has both manual override and auditing features.	- Attendance ID (Primary Key) - Event ID (Foreign Key → Events) - Enrollment ID (Foreign Key → Enrollments) - Timestamp - Status (Present / Late / Absent) - Is Manual Override (Boolean) - Recorded By (Host ID → Users) •

		• Recorded At
6. Admins	Admins are the staff users that have complete access to monitoring, management, and reporting.	• Admin ID (Primary Key) • User ID (Foreign Key → Users)
7. AuditLogs	A tamper-proof log that is required for GDPR compliance, debugging, and trust building.	• Log ID (Primary Key) • User ID (Foreign Key → Users) • Action (e.g., Login, Enroll Face, Delete Face Data, Start Session) • IP Address • Device / User Agent • Timestamp

3.8 Other Requirements

3.8.1 Training-related Requirements

Users will not be subjected to any formal training as the web-based biometric attendance system is equipped with a very user-friendly and straightforward interface. A very minimal technical skill like just web navigation (like logging in, filling forms, and clicking buttons) can allow the user to operate the system efficiently. Nonetheless, the users will be given a very short onboarding assistance or a help page along with the main system to navigate the first time users through the system.

3.8.2 Packaging Requirements

As a web application, the system does not need any physical packaging, and it can be easily accessed by any modern browser installed on any desktop computer or mobile device. The user interface, database, and face recognition services are online and can be securely accessed through the institution's domain or local intranet.

3.8.3 Legal Requirements

All data gathered, including facial biometric templates and attendance logs, will belong to and be managed by the organization. Users will have the right, by the Face Data Privacy Policy (FR-09), to request the deletion of their biometric data. The organization promises to meet the

requirements of the data protection laws, thus, facilitating the safe storage and access to facial data, and sharing it with third parties only when allowed. Moreover, the company will have the right to use the materials submitted, photos taken during events, reports, etc. for administrative purposes only.

4. Change Management Process

This section details the process that will be followed whenever there is a need for changes in either the project scope or requirements.

4.1 Submission of Change Request

A change request can be proposed by any project member, stakeholder, advisor, or supervisor.

Requests can be made by email or within the shared project repository. A valid request shall include:

- Description of the proposed change
- Reason for requesting the change
- Modules or features likely to be impacted
- Urgency level and expected impact

4.2 Review and Impact Assessment

Once submitted, the request is reviewed by the Project Manager. The PM reviews:

- Impact on the project timeline
- Additional resources required
- Possible implications for budget or workload
- Technical feasibility
- Risk level

If a change has a significant impact, then it is subject to the review and approval by the SteCo.

4.3 Approval or Rejection

Based on the assessment, the request is either:

- Approved — changes are incorporated into the development plan
- Rejected — requester is informed with a clear justification
- Deferred — reserved for future iterations

Every outcome is documented for traceability.

4.4 Implementation of Approved Changes

Once approved, the development team updates:

- Functional and non-functional requirements
- Supporting diagrams-use cases, data models, UI sketches
- Test cases involving the revised requirement

A Change Log is appended at the end of the SRS, documenting the following:

- Change ID
- Change description
- Author
- Date
- Sections affected
- Approval signatures

4.5 Traceability

Each updated requirement receives a revision number or unique identifier.

This allows to link the change back to: The original requirement Related design elements Test cases Validation procedures The traceability matrix is updated after every approved modification.

References

1. EmpMonitor. Implement Facial Recognition Attendance System.
   Available at:
   https://empmonitor.com/blog/implement-facial-recognition-attendance-system/

2. SlideShare. Fingerprint Attendance System Presentation.
   Available at:
   https://www.slideshare.net/slideshow/fingerprint-attendance-system/2503115

3. PulseHRM. What is a Biometric Attendance System?
   Available at: https://pulsehrm.com/what-is-a-biometric-attendance-system/

4. Additional academic papers, technical materials, and online resources consulted during the preparation of this SRS.
5. Kifle, N. (2021). SRS Template
6. Sommerville, I., & Sawyer, P. (1997, May 5). Requirements Engineering. Wiley.
7. Previous SRS Documentations Submitted by our seniors
   - Mebrat, R., Kahsay, S. and Mebrat, Z. (2021). Bet Yaferaw
   - Mubarek, F.,Umeta,T.,Tesfaye,Y. and Bogale,Y.(2021).Snap CSS:A CSS Optimizer SRS.

Appendices

Note: All the information present in the appendices is mainly meant for providing extra context, reference, and traceability. The contents of the appendices may not be treated as a part of the binding set of requirements unless they are explicitly referenced and incorporated into the main body of the SRS (e.g., through a normative statement in Section 3). Appendices are considered as the supporting documents to help the understanding, design, and the maintenance of the system in the future.

A.1 Appendix 1: UI/UX Mockup Collection

Status: Informative (Not Normative)

In this appendix, the very first low-fidelity wireframes and mockup designs are included, which are referred to in Section 3.1.1 User Interfaces. The visuals were produced during the requirements gathering phase to make sure that all stakeholders were on the same page and they are meant to direct the frontend development. The final implementation might, however, change depending on the results of usability testing and the technical limitations.

Figure	Description
Fig 3.1	Login Screen
Fig 3.2	Sign Up Page
Fig 3.3	Host Dashboard
Fig 3.4	Attendee Dashboard
Fig 3.5	Create Event
Fig 3.6	Enroll Face
Fig 3.7	Live Scan (Real-Time Attendance)
Fig 3.8	Report Generation
Fig 3.9	Privacy & Data Control Panel

Note: If you want to see high-fidelity prototypes and interactive versions, you can find them in the project repository at the location of /design/mockups/. The annotations for accessibility (WCAG 2.1 AA compliance) are inserted in the comments of the Figma file.

A.2 Appendix 2: Use Case Diagram (UC Diagram)

Status: Informative (Not Normative)

Referenced in Section 3.3 Use Cases as Fig 3.10 UC Diagram.

Use Case Diagram – Biometric Faceprint Attendance System

(Diagram created using draw.io / Lucidchart)

Actors:

- **Host (Admin/Instructor)**
- **Attendee (Student/Employee)**
- **System (Automated Processes)**

Use Cases Included:

- UC-01: Sign Up
- UC-02: Log In
- UC-03: Edit Profile
- UC-04: Create Subject & Schedule Event
- UC-05: Enroll with Faceprint
- UC-06: Attendance by Face Scan
- UC-07: Manage Reports
- UC-08: Automated Reminders
- UC-09: Face Data Privacy Management

A.3 Appendix 3: Functional Requirement Traceability Matrix (Initial)

Status: Informative (Will become normative upon formal approval)

FR ID	Requirement Description	Use Case	Source	Priority
FR-01	User Sign Up with Role Selection	UC-01	Section 3.2.1	High
FR-02	Secure Login with Session Management	UC-02	Section 3.2.2	High
FR-03	Profile Editing (Name, ID, Photo)	UC-03	Section 3.2.3	Medium
FR-04	Subject Creation & Session Scheduling	UC-04	Section 3.2.4	High
FR-05	Faceprint Enrollment (Multi-Angle Capture)	UC-05	Section 3.2.5	High
FR-06	Real-Time Face Detection & Matching	UC-06	Section 3.2.7	Critical
FR-07	Manual Attendance Override (Host Only)	UC-06	Section 3.2.7	Medium
FR-08	Generate Attendance Reports (PDF/CSV)	UC-07	Section 3.2.8	High
FR-09	Face Data Deletion on Request	UC-09	Section 3.2.9	High (Legal)
FR-10	Automated Email/SMS Reminders	UC-08	Section 3.2.6	Medium

To be expanded and linked to test cases during the testing phase.

A.4 Appendix 4: Glossary of Terms

Status: Normative (for consistent interpretation)

Term	Definition
Faceprint	A mathematical vector representation (embedding) of a person's facial features, generated using deep learning models (e.g., FaceNet, VGGFace). Not a raw image.
Enrollment	The process of capturing and storing a user's faceprint in the database for future recognition.
Host	Synonymous with Admin/Instructor; has elevated privileges.
Attendee	Synonymous with Student/Employee; end-user taking attendance.

Check-in / Check-out	Timestamped events marking arrival and departure.
Embedding	128–512 dimensional numerical vector representing facial identity.
Liveness Detection	(Future scope) Mechanism to prevent spoofing using photos or videos.

A.5 Appendix 5: Meeting Minutes with Advisor (Excerpt)

Status: Informative

Date: November 12, 2025, in-class.

Attendees: Group 2 Team, Advisor Nuniyat Kifle

A.6 Appendix 6: References (Full Citations)

Status: Informative

1. EmpMonitor. (n.d.). *How to Implement Facial Recognition Attendance System*. Retrieved from empmonitor.com
2. SlideShare. (n.d.). *Fingerprint Attendance System Presentation*.
3. PulseHRM. (n.d.). *What is a Biometric Attendance System?*
4. Kifle, N. (2021). *SRS Template for Capstone Projects*. Addis Ababa Institute of Technology.
5. Sommerville, I., & Sawyer, P. (1997). *Requirements Engineering: A Good Practice Guide*. Wiley.
6. Mebrat, R., et al. (2021). *Bet Yaferaw – Student Attendance System SRS*. AAiT Senior Project.
7. Mubarek, F., et al. (2021). *Snap CSS: A CSS Optimizer SRS*. AAiT Senior Project.

End of Appendices