Tab 1

Ghana-India Kofi Annan Centre of Excellence in ICT
(GI-KACE)

GI-KACE
Ghana - India Kofi Annan Centre of Excellence in ICT

CSD46.5

BIOMETRIC INTEGRATION IN ATTENDANCE

Lecturer: Prescott
Date of submission: 4th October, 2025

DECLARATION

We, the undersigned, hereby declare that this project work titled “BIOMETRIC INTEGRATION IN ATTENDANCE” is the result of our own original research and effort. It has not been submitted whether in whole or part, for any other academic purpose in this or any other institution. All sources of information have been fully acknowledged.

Group Members:

1. Hector Kelvin Quarshie ID: A2025CSD46.5M024
2. Name:Selasi Afi Agorsor ID: A2025CSD46.5M020
3. Bright Emmanuel Darkwa ID: A2025CSD46.5M019
4. Solomon Kok Nanleeb ID: A2025CSD46.5M021
5. Lucky Dunya ID: A2025ScD46.5M022
6. Denis Pappoe ID: A2025CSD46.5M023

Date: 29th September, 2025

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to everyone who supported us throughout the completion of this project. First and foremost, we thank the Almighty for granting us the strength, focus, and perseverance to carry out this work

successfully.Our heartfelt appreciation goes to our lecturer, **Mr. Presscot**, for his guidance, encouragement, and insightful feedback, which greatly shaped the direction of this project. We also acknowledge the support of the **GHANA-INDIA KOFI ANNAN CENTER OF EXCELLENCE IN ICT** for providing the academic environment and resources necessary for this work.Special thanks to our classmates and friends for their collaboration, motivation, and constructive discussions. Finally, we are deeply grateful to our families for their unwavering support and understanding during this academic journey.

DEDICATION

We would like to dedicate this project to God, whose grace and guidance carried us through every step of the journey.We also dedicate this work to our families, for their constant support, patience, and encouragement. Your belief in us kept us going, even when things got tough.To Mr. Presscot, our lecturer, thank you for your dedication, your wisdom, and for pushing us to think deeper and do better.And finally, to our classmates and the entire GI-KACE community — this is for all of us. Your teamwork, ideas, and shared energy made this experience truly memorable.

INTRODUCTION

In the rapidly evolving landscape of digital transformation, educational institutions and organizations worldwide are placing increasing emphasis on security, accuracy, and operational efficiency in their daily activities. One critical area where these priorities converge is attendance and access management. Traditional methods such as manual sign-in registers, identity cards, and password-based login systems, though historically effective, are becoming increasingly inadequate in modern environments. These conventional approaches are often plagued by significant limitations, including susceptibility to human error, data manipulation, impersonation, and unauthorized access. Moreover, manual processes consume valuable administrative time, lack scalability, and are inefficient in handling large volumes of records. As institutions expand and integrate advanced technologies into their operations, there is a pressing need for a secure, reliable, and automated identity management solution capable of addressing these challenges comprehensively.

Biometric authentication technologies have emerged as one of the most promising solutions to these limitations. By leveraging unique physiological or behavioral characteristics — such as fingerprints, facial features, iris patterns,

or voice recognition — biometric systems offer a higher level of security and accuracy compared to traditional methods. Unlike passwords or ID cards, biometric traits cannot be easily lost, stolen, or duplicated, thereby significantly reducing the risk of identity fraud. However, single-modality biometric systems are not without their drawbacks. They may encounter issues such as false acceptance or rejection rates under certain conditions, environmental influences, or variations in user appearance. As a result, researchers and system designers have turned toward **multimodal biometric systems**, which integrate two or more biometric modalities to improve reliability, accuracy, and robustness.

This project proposes the design and implementation of a **Hybrid Biometric Sign In/Sign Out System** that integrates **facial recognition** and **fingerprint verification** into a unified authentication framework. By combining these two biometric modalities, the system leverages the strengths of each while mitigating their individual limitations. Facial recognition offers a fast and contactless verification process, ideal for efficient crowd handling, whereas fingerprint recognition provides a highly reliable and unique identification factor with minimal error rates. Together, they form a robust two-factor biometric authentication system capable of significantly enhancing security and reducing false acceptance and rejection rates.

The system's operational workflow is designed to be straightforward yet highly effective. Upon arrival at an entry or exit point, a student approaches a dedicated biometric device, enters their name or student identification number, and undergoes facial recognition followed by fingerprint verification. Once authenticated, the system automatically records the sign-in or sign-out event, including a timestamp and optional device information such as laptop or tablet details. All records are securely stored in a centralized database, which supports a wide range of administrative functionalities. These include real-time attendance monitoring, advanced search and filtering capabilities, automated report generation, and data correction features — all of which significantly reduce administrative burden and human intervention.

Furthermore, the system offers several practical advantages that extend beyond traditional attendance management. It enhances accountability by ensuring that only authenticated individuals can access institutional premises or services. It minimizes paperwork and eliminates the inefficiencies associated with manual attendance processes. It also provides a scalable solution that can accommodate institutional growth and can be adapted for

use in other contexts such as workplaces, government facilities, or secure research environments.

In summary, this project demonstrates how modern biometric technologies can be harnessed to create a **secure, accurate, and scalable identity management solution** tailored to the evolving needs of educational and organizational environments. By integrating facial recognition and fingerprint verification into a hybrid model, the system offers a reliable, future-ready solution that not only strengthens security and improves operational efficiency but also transforms the way attendance and identity verification are managed. This work contributes to the growing body of research on biometric-based security systems and presents a practical implementation framework that aligns with the increasing demand for advanced, automated, and technology-driven institutional operations.

Problem Statement

1. Background of the Current System

In our institution, student attendance and device declaration are currently managed through
a manual process. Upon arrival, each student is expected to write their name, the devices
they bring (such as laptops, phones, or tablets), the time of arrival, and provide their
signature in a physical logbook. Similarly, when leaving, students sign out and record their
departure time. This method was introduced to promote accountability, discipline, and to
ensure proper tracking of students and their belongings.
While the manual system may appear straightforward and cost-effective, it is no longer
sustainable in a modern educational environment. As the number of students has grown
significantly, this approach has exposed a number of critical weaknesses that affect both
efficiency and accuracy. In an era where institutions are adopting digital systems for
academic and administrative functions, relying solely on handwritten records limits the ability
of administrators to manage student activities effectively.

2. Challenges of the Manual System

Inaccuracy of Records

One of the most significant issues with the manual method is its vulnerability to inaccuracy.
Handwritten entries are often unclear, incomplete, or even deliberately falsified. A common
practice among students is **proxy attendance**, where one student signs in on behalf of an
absent colleague. This creates false records and undermines discipline within the institution.
In addition, poor handwriting and spelling mistakes further reduce the reliability of the
records.

Time-Consuming Process

The signing in and signing out process is slow and inefficient. During busy periods such as morning arrival and afternoon dismissal, long queues often form as students wait their turn to enter their details into the logbook. What should ideally be a quick process of seconds turns into several minutes per student. This wasted time not only affects punctuality but also interrupts the smooth flow of academic activities.

Weak Security in Device Management

The institution requires students to declare the devices they bring on campus for accountability in cases of loss, theft, or unauthorized use. However, since the declaration is done manually, administrators have no reliable way to verify the accuracy of the information.In the event of a stolen laptop or mobile device, administrators must search through dozens

or even hundreds of paper entries to track ownership. This is highly inefficient and prone to errors. Furthermore, dishonest students can deliberately provide false information about their devices, making investigations even more difficult.

Difficulty in Data Retrieval and Analysis

Physical registers do not support quick data access or long-term analysis. Whenever
administrators need to confirm attendance, prepare reports, or investigate disciplinary
issues, they must manually flip through pages of logbooks. This process is slow, stressful,
and highly inefficient. Moreover, without a centralized digital record, it is impossible to track
trends such as patterns of absenteeism, late arrivals, or suspicious device usage. This lack
of analytical power leaves the institution at a disadvantage compared to modern schools that
rely on digital data for decision-making.

Consequences of the Current System

The continued reliance on manual attendance and device declaration has far-reaching
consequences:

- **Reduced Administrative Efficiency:** Staff waste valuable time maintaining, organizing, and searching through logbooks.
- **Loss of Accountability:** Proxy attendance and inaccurate entries reduce discipline
among students.
- **Security Risks:** Device theft or loss becomes harder to investigate due to unreliable
data.
- **Lack of Data for Decision-Making:** Administrators cannot easily generate reports,
identify attendance trends, or enforce accountability measures.
- **Negative Institutional Image:** In a digital era, persisting with outdated methods can
create an impression of stagnation and limit the institution’s appeal to prospective
Students.

The Need for a New System

Given the challenges of the manual system, it is clear that a transformation is urgently

required. The institution needs a **modern, automated attendance and device**
management system that eliminates inaccuracies, strengthens security, and improves
efficiency.The proposed solution is a **biometric-driven system** that integrates **facial recognition,**
fingerprint authentication, and device declaration. With this system:

- Students will be able to sign in quickly by first entering their name, confirming their
identity through face recognition, and recording attendance using their fingerprint.
- Device details can be stored securely and linked to each student's biometric profile,
ensuring accountability in cases of theft or loss.
- All records (time in, time out, student ID, device information, and biometrics) will be
automatically stored in a central digital database.
- Administrators will have real-time access to accurate, structured data, making it easy
to monitor attendance, track punctuality, and generate reports.
- The system will save time, reduce fraud, and enhance the overall image of the
institution as a technology-driven environment.

Objectives of the Project

General Objective

The overarching objective of this project is to design, develop, and implement a secure, efficient, and reliable Hybrid Biometric Sign In/Out System for the Ghana-India Kofi Annan Centre of Excellence in ICT (GI-KACE). At present, the institution relies on a manual logbook system where students and visitors sign in and out at the entrance. While this system has been in place for many years, it presents several limitations, including the ease of impersonation, the potential for missing or inaccurate records, and the difficulty of retrieving historical attendance data.

The hybrid biometric system being proposed combines facial recognition technology with fingerprint verification to provide a dual-layer authentication process. This ensures that only the rightful student or visitor is able to complete the sign-in or sign-out process. The integration of biometrics eliminates opportunities for fraud, strengthens institutional security, and provides administrators with reliable and tamper-proof records.

Furthermore, the general objective of this project goes beyond merely replacing the manual logbook. It aims to transform the way attendance and access management are conducted at GI-KACE, aligning the institution with modern technological trends and promoting a culture of accountability, efficiency, and security. In doing so, the project directly supports the institution's broader goals of becoming a model ICT hub, where innovation and digital transformation are applied in practical, everyday scenarios.

Specific Objectives

1. To eliminate proxy sign-ins and sign-outs

One of the most significant challenges of the manual system is the possibility of students signing in or out on behalf of others. This practice undermines the credibility of attendance records and creates opportunities for dishonesty. The proposed biometric system directly addresses this issue by requiring both face recognition and fingerprint verification before an individual can be recorded in the system.

By eliminating proxy sign-ins, the system ensures that every attendance record reflects the actual presence of the student or visitor. This not only improves accountability but also fosters a culture of personal responsibility. Students will no longer have the opportunity to manipulate records, and administrators will be able to trust the integrity of the data collected. In the long term, this objective supports accurate academic reporting, security enforcement, and institutional planning.

2. To automate the attendance tracking process

Currently, security personnel are required to manually supervise the sign-in and sign-out process, while students must wait in queues to write their names in logbooks. This process is inefficient, prone to errors, and time-consuming.

The hybrid biometric system automates this process by instantly capturing the identity and timestamp of each student or visitor.

Automation significantly reduces the time required for each transaction. Instead of taking 20–30 seconds to write in a book, the biometric system will complete the process in less than 5 seconds. This efficiency is especially important during peak periods, such as class start times or institutional events. Beyond efficiency, automation also ensures consistency, as the system records information in real-time without relying on human handwriting or memory.

The automation of attendance tracking creates an environment where administrative staff and security officers can redirect their efforts toward higher-value tasks, while students experience smoother entry and exit procedures.

3. To enhance institutional security at entry and exit points

The safety and security of students, staff, and visitors are critical priorities for any academic institution. GI-KACE is no exception, particularly because it operates as a national ICT hub that hosts a variety of programs, training, and public events. A manual logbook system does little to deter unauthorized access since individuals can easily provide false information or impersonate registered students.

The hybrid biometric system provides a robust solution by ensuring that only individuals who are properly authenticated can gain access. Face recognition technology serves as the first line of verification, while fingerprint authentication serves as an additional safeguard. Unauthorized persons will therefore be unable to pass through the system undetected.

This objective is vital not only for monitoring attendance but also for strengthening campus security. In the event of emergencies or security breaches, administrators will have access to real-time records of all individuals present within the facility. This greatly improves the institution’s capacity to respond quickly and effectively to crises.

4. To provide a centralized and efficient data management platform One of the weaknesses of the manual logbook system is the scattered and unstructured nature of its data. Physical records can easily be misplaced, damaged, or rendered illegible. Moreover, retrieving attendance data from logbooks often

requires significant time and effort, especially if the information dates back several weeks or months.

By contrast, the proposed biometric system will store all attendance data in a centralized digital database. This database will serve as a single source of truth for all records, ensuring consistency, accuracy, and security. Administrators will be able to search, filter, and retrieve information with just a few clicks, saving time and improving overall efficiency.

Centralized data management also supports transparency and accountability. Since all records are timestamped and securely stored, they cannot be easily altered or erased. This creates a reliable audit trail, which is essential for both academic and administrative purposes.

5. To generate insightful administrative reports for decision-making

Beyond simply collecting data, the biometric system will provide tools for analyzing attendance patterns. Administrators will be able to generate daily, weekly, or monthly reports to monitor student punctuality, class attendance, and visitor trends. These reports will be presented in clear, structured formats, enabling administrators to quickly identify irregularities or patterns.

The ability to generate reports supports evidence-based decision-making. For instance, if attendance rates in a particular program are consistently low, the administration can investigate and address the issue. Similarly, visitor logs can help management understand peak periods of institutional activity and allocate resources accordingly.

To guide development, the project adopts the **Waterfall Model of Software Development**, which is well-suited for projects with clearly defined requirements and a need for structured documentation. The Waterfall approach ensures that each phase—requirements gathering, design, implementation, testing, deployment, and maintenance—is fully completed before moving to the next. This is especially critical for a security-sensitive project where errors at later stages would be costly to fix.

Chapter 2: Software Methodology

The methodology selected for this project is the **Waterfall Model**, a sequential approach to system development. Each stage of development is executed in order, with deliverables from one phase serving as inputs to the next. This linear approach is appropriate for the biometric sign-in system because the requirements are well established, and the system involves sensitive data where strict compliance and verification are mandatory.

The phases of the Waterfall model—Requirements, Design, Implementation, Testing, Deployment, and Maintenance—directly align with the needs of this project. For example:

- In the **Requirements phase**, the biometric features and security needs were outlined.
- The **Design phase** translated those requirements into layered system architecture, covering the client interface, authentication APIs, and secure databases.
- During **Implementation**, coding and biometric integration will be executed systematically.
- **Testing** will emphasize accuracy, security, and resistance against spoofing attempts.

- **Deployment** will occur in phases, starting with controlled pilot testing before full rollout.

- Finally, **Maintenance** ensures the system remains secure, reliable, and optimized through regular updates.

The choice of Waterfall also reflects the academic context of this project. With multiple contributors, the methodology provides clear task boundaries, making it easier for each team member to focus on one stage of development. Additionally, the heavy documentation that accompanies the Waterfall model supports compliance with **data protection standards** and ensures that system validation can be demonstrated clearly.

System Development Life Cycle (SDLC) Overview

The development of the Biometric Integrated Sign-In System follows the **System Development Life Cycle (SDLC)** as its guiding framework. The SDLC provides a structured process for creating reliable, secure, and maintainable systems. Since the project involves sensitive biometric data, it is critical that every stage is executed systematically, with careful validation before moving forward.

The SDLC in this project is aligned with the **Waterfall methodology**, meaning the phases are carried out in a linear, sequential order. Each phase produces deliverables that feed into the next stage. This ensures thorough documentation, reduces risks of overlooking security requirements, and provides clear checkpoints for evaluation.

The six phases of the SDLC applied in this project are:

1. **Requirements and Planning** – Identifying and documenting system needs, functional goals, and security requirements.

2. **System Design** – Translating requirements into architecture, workflows, and database schemas.

3. **Implementation / Development** – Writing the code, integrating biometric APIs, and setting up databases.

4. **Testing** – Validating functionality, security, and performance through rigorous evaluation.

5. **Deployment** – Delivering the system in controlled phases, from pilot testing to institution-wide rollout.

6. **Maintenance** – Monitoring performance, applying patches, updating features, and ensuring compliance.

Figure 2: SDLC Framework for the Biometric Integrated Sign-In System (Insert diagram here)

The structured flow of the SDLC is particularly important for this project because:

- **Biometric accuracy must be tested and validated** before deployment.

- **Data security and compliance checks** need to be embedded at multiple stages.

- **Institutional adoption requires reliability**, so errors or failures cannot be tolerated.

SDLC Phases in Detail

Requirements and Planning

The first and most critical stage of the SDLC is **Requirements and Planning**. In this phase, the goals, scope, and expectations of the Biometric Integrated Sign-In System are clearly defined. For this project, requirements gathering was essential because the system involves not just attendance automation but also **biometric authentication**, **device registration**, and **data security**. Any

mistake or oversight at this stage would affect all subsequent phases of the project.

Objectives of the Requirements Phase

The main objectives during this phase include:

- To identify **functional requirements** (what the system should do).
- To establish **non-functional requirements** (how the system should perform).
- To evaluate constraints, risks, and compliance needs.
- To plan resources, responsibilities, and timelines for development.

Functional Requirements

Functional requirements define the specific operations that the system must perform. For this project, they include:

1. **Biometric Authentication**
    - The system should capture and verify student identity using **face recognition** and **fingerprint scanning**.
    - Multi-modal verification (both face and fingerprint) must be required for successful sign-in or sign-out.
2. **Automated Attendance Tracking**
    - Once authentication is successful, the system should log the student's **sign-in/sign-out time** in a secure database.
    - The system should also store associated details such as student ID, name, and device information.
3. **Device Information Capture**

- The system should prompt users to declare any devices (laptops, tablets) brought into the institution for security tracking.

4. **Administrative Dashboard**

    - Administrators should be able to log into a separate dashboard to view attendance records, search and filter data, generate reports, and override entries when necessary.

5. **Reporting Features**

    - The system should provide **daily, weekly, and monthly attendance reports** in exportable formats (e.g., PDF, Excel).

Non-Functional Requirements

Non-functional requirements address **system quality, performance, and constraints**. For the biometric sign-in system, they include:

1. **Security Requirements**

    - All biometric templates must be **encrypted** in storage and transmission.

    - Liveness detection must be applied to prevent spoofing attempts using photos or fake fingerprints.

    - Access to the system should be controlled via **role-based authentication** (students vs. administrators).

2. **Performance Requirements**

    - The system must process authentication requests within **3–5 seconds**.

    - The system should support at least **100 concurrent users** without delays.

Reliability Requirements

- The system must achieve **at least 95% biometric accuracy**.
- Daily backups should be scheduled to ensure data recovery.

3. **Usability Requirements**
    - The user interface should be **simple and intuitive** for students.
    - Clear error messages should be displayed when authentication fails.
4. **Compliance Requirements**
    - The system must comply with data protection standards and relevant national or institutional regulations on biometric data.

Outcome of the Requirements Phase

By the end of this phase, the project has:

- A **clear definition** of what the system should do.
- A list of **functional and non-functional requirements**.
- A requirements document that will guide the **System Design phase**.
- A realistic plan with defined roles, risks, and deliverables.

This ensures that the project begins with clarity, reducing chances of misinterpretation during design and implementation.

System Design

The **System Design Phase** translates the requirements gathered during the Requirements and Planning phase into a structured **blueprint** for building the Biometric Integrated Sign-In System. This stage focuses on **how** the system will be built, what components will be involved, and how they will interact.

The design phase is divided into two key parts:

1. **High-Level Design (HLD)** – focuses on system architecture and overall structure.

2. **Low-Level Design (LLD)** – focuses on specific modules, database schemas, and detailed workflows.

High-Level Design (HLD)

The high-level design provides an overview of the entire system's structure and its main components.

System Architecture

The proposed biometric sign-in system follows a **three-tier architecture**:

1. **Presentation Layer (Frontend)**

    - This layer consists of the **user interface** where students and administrators interact with the system.

    - Built with technologies such as **React.js** or plain HTML/CSS/JavaScript.

    - Provides login forms, biometric prompts, dashboards, and reporting pages.

2. **Application Layer (Backend/Business Logic)**

    - Implements the **authentication logic**, biometric verification, and attendance recording.

    - Manages communication between frontend and database.

- Built using **Python (Django/Flask)** or **Node.js**.

3. **Data Layer (Database & Storage)**
    - Stores biometric templates, attendance logs, and device information.
    - Uses **relational databases** such as MySQL or PostgreSQL.
    - Provides secure, encrypted storage with daily backup routines.

Low-Level Design (LLD)

The low-level design focuses on the internal structure of the system, defining **modules, database design, and workflows**.

System Modules

1. **Student Module**
    - Register students with a unique ID.
    - Capture biometric details (face & fingerprint).
    - Log attendance during sign-in/sign-out.
2. **Biometric Verification Module**
    - Capture live biometric input.
    - Compare against stored template using recognition algorithms.
    - Accept or reject authentication requests.
3. **Attendance Module**
    - Generate logs of sign-in/sign-out times.

    - Associate attendance with specific courses/schedules.

4. **Device Information Module**
    - Allow students to declare devices during sign-in.
    - Save device information in database for security tracking.
5. **Administration Module**
    - Provide admin login.
    - Allow search, filtering, and report generation.
    - Manage student and device records.

Design Principles Considered

- **Modularity:** Each module (attendance, biometric, device) is independent for easier updates.
- **Scalability:** The system can expand to handle thousands of students.
- **Security:** Data encryption, liveness detection, and restricted access.
- **Reliability:** Backup and recovery procedures included.

Outcome of Design Phase

At the end of this phase, the project team has:

- A **clear architecture diagram**
- Defined **modules and workflows**.
- A **database schema**.

- Documented **design principles** that will guide the implementation phase.

This ensures a smooth transition into coding, with no ambiguity about how the system should function internally.

ALGORITHM

1. START

2. Input

· Student enters their name or ID.

3. VERIFY: Face Recognition.

· System will capture student's face via camera connected to the system.

· if the face is verified:

  · move on to fingerprint verification

· ELSE:

  · Display "Face not recognized. Please try again or contact the administration."

  · END.

4. VERIFY: Fingerprint.

· Student scans fingerprint on the scanner.

· IF fingerprint is verified:

  · Proceed to Step 5.

· ELSE:

  · Display "Fingerprint not recognized. Please try again."

  · Return to Step 4.

5. Input the device to be used

· Prompt student to enter device brought (e.g., laptop, tablet).

6. RECORD: Sign In / Sign Out Event.

· System timestamps the event (Sign In or Sign Out).

· Save record to database with:

  · Student name/ID

  · Face recognition result

  · Fingerprint verification status

  · Device info (if provided)

  · Timestamp

7. CONFIRM: Success Message

· Display "Sign In Successful" or "Sign Out Successful".

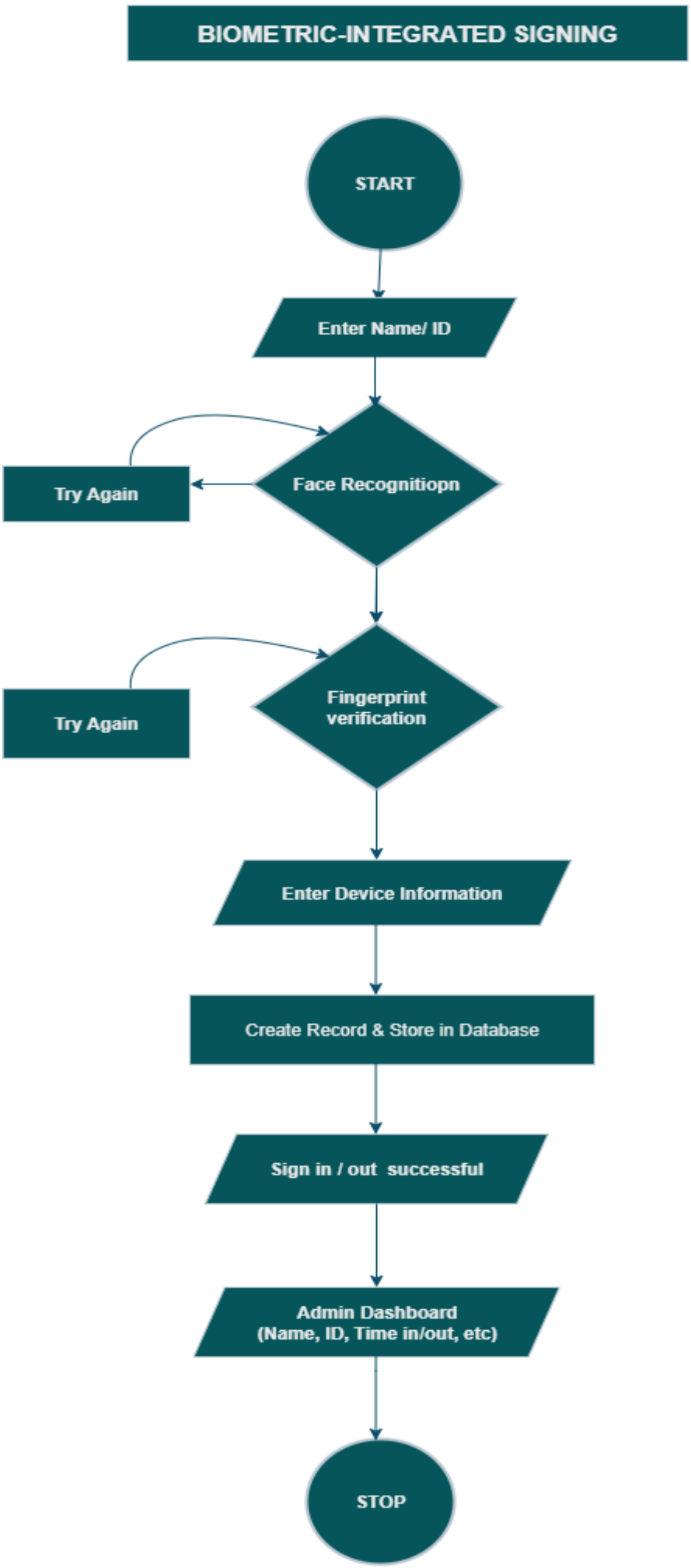
8. ADMIN ACCESS (Separate Process)

· Admin logs into dashboard.

· Can view, search, filter records, generate reports, and edit entries.

9. END

FLOWCHART


BIOMETRIC-INTEGRATED SIGNING
START
Enter Name/ ID
Face Recognitiopn
Try Again
Fingerprint verification
Try Again
Enter Device Information
Create Record & Store in Database
Sign in / out successful
Admin Dashboard (Name, ID, Time in/out, etc)
STOP

Implementation

The **Implementation Phase** is where the system is actually developed, coded, and configured according to the design specifications. This stage translates the **blueprints from the Design Phase** into a functional biometric sign-in system that can be tested and eventually deployed.

Goals of Implementation Phase

- Build the biometric sign-in system according to the **waterfall methodology**.
- Ensure all modules (student, biometric, attendance, admin) are properly coded and integrated.
- Set up a secure database for biometric data, attendance records, and device information.
- Apply encryption, authentication protocols, and security best practices.

Development Environment

The system will be developed using a combination of **backend, frontend, database, and biometric technologies**:

- **Programming Languages:**
    - Python (for backend & biometric integration using Django or Flask).
    - JavaScript (React.js for frontend).
- **Frameworks & Libraries:**

    - Django REST Framework (API endpoints).
    - React.js (UI).
    - OpenCV / TensorFlow (for face recognition).
    - Fingerprint SDK (e.g., Neurotechnology or open-source libraries).
- **Database:**
    - PostgreSQL / MySQL (relational database for attendance, biometrics, and devices).
- **Security Tools:**
    - JWT (JSON Web Tokens) for secure sessions.
    - AES Encryption for biometric templates.
    - SSL/TLS for secure client-server communication.

Implementation of Core Modules

1. Database Setup

- Create tables for **STUDENT, ATTENDANCE, DEVICE, BIOMETRIC_DATA**.
- Apply **high-level encryption** to biometric templates.
- Enable **backups & recovery system**.

Biometric Enrollment Workflow

- Students register with unique ID.

- Face & fingerprint data captured via hardware sensors.
- Biometric templates processed, encrypted, and stored in the **BIOMETRIC_DATA** table.

3. Authentication & Attendance

- **Step 1:** Student inputs ID → system triggers face recognition.
- **Step 2:** If face verified → system requests fingerprint scan.
- **Step 3:** If fingerprint verified → student is signed in, and time is stamped.
- **Step 4:** Attendance record saved in **ATTENDANCE** table with timestamp + device info.

4. Admin Dashboard Implementation

- Admin login with secure authentication (JWT or OAuth).
- Dashboard to:
    - View attendance records.
    - Generate reports (daily/weekly/monthly).
    - Override entries in special cases.

Security Features

- **Liveness Detection:** Prevents spoofing with photos, videos, or fake fingerprints.

- **Anti-Spoofing Measures:** Detects anomalies in face/fingerprint input.
- **Rate Limiting:** Prevents brute-force attempts.
- **Data Protection Compliance:** Ensures biometric data handling aligns with GDPR/ISO standards.

PSEUDOCODE

```
START
DISPLAY "Biometric-Integrated Signing System"

Step 1:
  ASK student to enter Name or ID
  READ student_name

Step 2:
  PERFORM Fa
      ce Recognition
  IF face match = TRUE THEN
      CONTINUE
  ELSE
      DISPLAY "Face not recognized, try again"
      GO BACK to Step 1
  ENDIF

Step 3:
  PERFORM Fingerprint Verification
  IF fingerprint match = TRUE THEN
      CONTINUE
  ELSE
      DISPLAY "Fingerprint not recognized, try again"
      GO BACK to Step 3
  ENDIF

Step 4:
  ASK students to enter Device Information (Laptop, Tablet, etc.)
  READ device_info
```

Step 5:
  CREATE record with:
      - Student Name/ID
      - Face recognition result
      - Fingerprint result
      - Device info
      - Time and Date
  STORE record in database

Step 6:
  DISPLAY "Sign In/Out Successful"

Step 7:
  ADMIN logs into dashboard
  ADMIN can:
      - View records (Name, ID, Time In, Time Out, Fingerprint)
- Search or edit records

END

Deliverables of Implementation Phase

At the end of this phase, the team will have:

- A **functional biometric sign-in system** (prototype or full version).
- Configured **database** with sample student/attendance records.
- Secure **frontend and backend modules** integrated.
- Documented **source code** and API endpoints.

Testing Phase

The **Testing Phase** ensures that the biometric integrated sign-in system works as expected, meets user requirements, and is secure against failures or attacks. Since this system manages sensitive biometric data (fingerprints and

facial features), **rigorous testing** is required to verify both functionality and data protection compliance.

Objectives of Testing

- Verify that the system meets all functional and non-functional requirements.
- Validate the accuracy of biometric recognition under different conditions.
- Detect and fix bugs before deployment.
- Ensure the system resists spoofing, unauthorized access, and performance bottlenecks.
- Confirm usability for both students and administrators.

Types of Testing Applied

1. Unit Testing

- Focus: Testing individual components of the system (e.g., face recognition module, fingerprint verification, database queries).
- Tools: PyTest (Python), Jest (JavaScript for frontend), SQL query validators.
- Example: Verify that the function `verify_face(student_id)` returns the correct match for enrolled students.

2. Integration Testing

- Focus: Testing how modules work together (e.g., face + fingerprint verification → attendance database entry).

- Example: Student provides ID → system matches face → system matches fingerprint → attendance record saved.

- Goal: Ensure data flows seamlessly from **biometric capture** → **verification** → **database storage** → **admin dashboard**.

3. System Testing

- Focus: Testing the entire system end-to-end.

- Example scenarios:

    - The student tries to sign in with correct biometrics (should succeed).

    - Students try with wrong biometrics (should fail).

    - Multiple students attempt sign-in at the same time (system must not crash).

4. Security Testing

Since biometric systems are vulnerable to spoofing, strong **penetration testing** is applied:

- **Spoofing Attempts:** Testing with high-quality photos, masks, or fake fingerprints.

- **Liveness Detection Validation:** Ensures the system detects real vs. fake biometrics.

- **Data Encryption Check:** Ensures biometric templates are securely encrypted in the database.

- **Rate Limiting:** Ensures multiple failed login attempts trigger alerts or lockouts.

5. Performance Testing

- Simulate **100+ students signing in simultaneously**.
- Check system response time (< 3 seconds per authentication).
- Ensure **database queries and attendance updates** are handled without delays.
- Stress testing under peak load conditions (exam days, class starts).

6. User Acceptance Testing (UAT)

- Conducted with a **pilot group of students and administrators**.
- Collect feedback on usability, accuracy, and speed.
- Example: Pilot test with one faculty before full rollout.
- Adjustments made based on feedback (e.g., improving UI, adjusting camera placement).

Testing Tools and Frameworks

- **Frontend:** Jest, Cypress (UI testing).
- **Backend:** PyTest, Postman (API testing).
- **Database:** SQLMap (security testing), pgAdmin/MySQL Workbench.

- **Biometric Testing:** OpenCV test datasets, fingerprint sensor SDK test suite.

- **Load Testing:** Apache JMeter, Locust.

Deployment Phase

The **Deployment Phase** marks the transition of the biometric integrated sign-in system from development and testing to real-world use. Since the system involves sensitive biometric data, deployment must be gradual, secure, and carefully monitored. Any errors at this stage could compromise trust, security, and usability.

Objectives of Deployment

- Introduce the system in a **controlled and monitored environment**.

- Minimize risks by rolling out in **phases** instead of all at once.

- Collect user feedback early to make refinements.

- Ensure system stability, reliability, and compliance before full adoption.

Deployment Strategy (Waterfall Approach)

The system deployment follows **four progressive phases**:

Phase 1: Internal QA Environment

- Deploy the system on an internal server accessible only by developers and QA team.
- Conduct a full testing cycle again (unit, integration, security).
- Verify all features work as intended outside the development machine.

Phase 2: Staging Environment

- Deploy system in a **staging server** that mirrors the production environment.
- Run **load tests** (e.g., 100+ concurrent authentications).
- Perform **integration testing** with institutional network, student management system, and attendance databases.

Phase 3: Product Pilot

- Deploy the system to a **limited pilot group** (e.g., one faculty or one lecture hall).
- Monitor sign-in accuracy, response times, and admin dashboard performance.
- Gather **student and staff feedback** for improvements.
- Apply patches before scaling.

Phase 4: Gradual Rollout

- Deploy system institution-wide but in **stages** (e.g., faculty by faculty).
- Monitor system health and biometric accuracy during each rollout.
- Provide **support staff and training sessions** for smooth adoption.
- Establish a **rollback plan** (ability to revert to manual attendance if system issues arise).

Security & Compliance in Deployment

- Configure **SSL/TLS** to secure communication between devices and server.
- Enforce **role-based access control** for admin dashboard.
- Ensure **data protection certificates** (local equivalents of GDPR/ISO compliance) are in place.
- Conduct final **penetration testing** before full rollout.

Post-Deployment Activities

- **Training:** Provide administrators and faculty staff with user manuals and hands-on training.
- **Monitoring:** Activate real-time monitoring of system health, sign-in accuracy, and failed authentications.
- **Feedback Loop:** Open communication channels (emails, forms, meetings) for user feedback.

- **Transition Plan:** Ensure students are aware of how to use the system (clear instructions at sign-in stations).

Deliverables of Deployment Phase

- Deployed biometric system (production environment).
- Deployment checklist and documentation.
- User training materials (manuals, guides).
- Feedback and monitoring reports from pilot rollout.
- Final confirmation of readiness for **Maintenance Phase**.

Maintenance Phase

The **Maintenance Phase** is the final stage of the SDLC, focused on keeping the biometric integrated sign-in system reliable, secure, and up-to-date after deployment. Since the system deals with sensitive biometric data, continuous monitoring and timely updates are crucial to prevent downtime, security breaches, or data corruption.

Objectives of Maintenance

- Ensure continuous availability and reliability of the biometric system.
- Fix issues discovered after deployment (bug fixing, error correction).
- Release patches and updates to strengthen security.
- Upgrade features to meet new institutional needs.

- Track performance metrics for system optimization.

Key Maintenance Activities

1. Monitoring

- Real-time monitoring of:
    - System uptime.
    - Failed authentication attempts.
    - Database performance.
- Automated alerts for unusual activities (e.g., repeated failed logins, spoofing attempts).

2. Backups

- Daily automatic backups of biometric database, attendance records, and system configurations.
- Point-in-time recovery options for disaster recovery.
- Secure storage of backups in encrypted formats (both on-site and cloud).

3. Updates

- **Monthly security patches** to fix vulnerabilities.
- **Quarterly feature updates** (e.g., adding support for new devices).
- Upgrade of biometric algorithms for higher accuracy.
- Regular updates to comply with evolving **data protection regulations**.

4. Support

- Tiered support model:
    - **Level 1:** Student-facing helpdesk (basic login issues).
    - **Level 2:** IT support team (software/hardware troubleshooting).
    - **Level 3:** Developers (complex bugs, API updates).

5. Analytics & Reporting

- Continuous tracking of biometric accuracy (False Accept Rate vs False Reject Rate).
- Performance metrics on sign-in speed and load handling.
- Regular reports for administrators on system usage and trends.

Maintenance Challenges

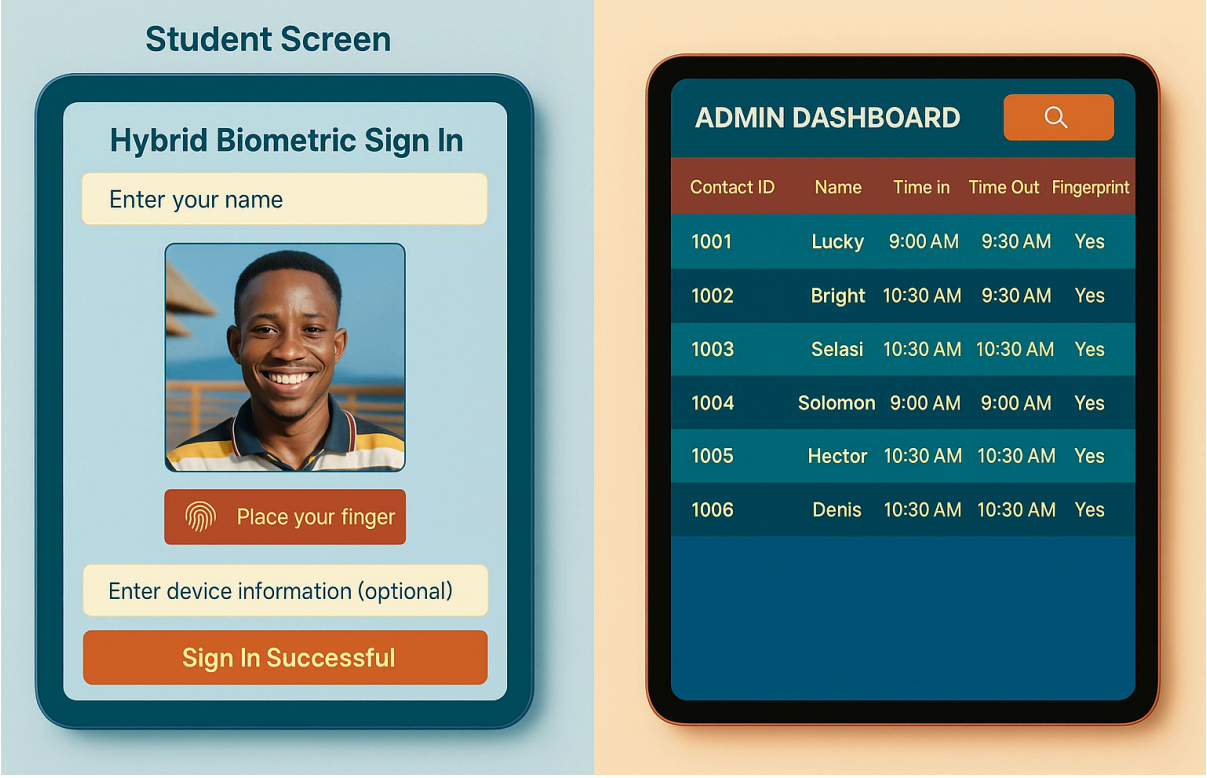
- Preventing **system downtime** during academic peak times.
- Managing **growing biometric data storage** as student enrollment increases.
- Ensuring compatibility with **new hardware or operating systems**.
- Keeping compliance with changing **data privacy regulations**.

Deliverables of Maintenance Phase

- Maintenance logs (bug fixes, updates applied).
- Backup and recovery procedures.

- Security patch reports.
- Regular performance and accuracy reports.
- Documentation of upgrades and new features.

STUDENTS SCREEN AND ADMIN DASHBOARD



CONCLUSION

In conclusion, the proposed attendance system provides an efficient, reliable, and modern solution to streamline the entire process of attendance tracking within our school. Unlike the traditional manual approach, which is often slow, and inconvenient, this system introduces a smart, automated method that significantly reduces the burden on both students and administrators. By integrating a robust algorithm with an intuitive and user-friendly interface, it ensures that attendance can be recorded quickly and accurately, thereby saving valuable time that would otherwise be wasted on paperwork or verification. The automation also minimizes human error, eliminates duplication, and prevents manipulation, ensuring that every record stored in the system is authentic, secure, and tamper-proof.

Moreover, the system is not just about marking attendance; it also plays a critical role in improving accountability and discipline among students. With features that allow real-time tracking and reporting, administrators can easily identify patterns such as absenteeism or lateness, which makes it easier to address issues before they become widespread. Parents and guardians can also benefit from timely updates and notifications, thereby strengthening the connection between home and school. This level of transparency ensures that all stakeholders,students, teachers, and administrators are actively involved in maintaining academic discipline.

Another important advantage of this innovation is its ability to promote convenience. For students, the system eliminates the need to sign paper registers or waste time searching for their names in long lists. For teachers, it reduces the workload of manually checking, collating, and submitting attendance sheets. Administrators also benefit from faster access to well-organized data, making reporting and decision-making more straightforward. This not only enhances efficiency but also allows the school to focus more on its core mission of delivering quality education rather than being bogged down by repetitive administrative tasks.

Furthermore, the attendance system positions the school as forward-thinking and technologically driven. In today’s digital age, adopting modern tools such

as this app shows that the institution is not only keeping up with global trends but is also committed to creating an environment that embraces innovation. This strengthens the reputation of the school and makes it more attractive to prospective students and parents who value modern, tech-enabled learning environments. By integrating technology into everyday operations, the school demonstrates adaptability, progressiveness, and readiness for the future.

Ultimately, this system does more than just track attendance—it contributes to the overall improvement of the learning environment. With accurate data, better accountability, and efficient management, teachers and administrators can dedicate more time and energy to academic excellence and student development. Students, on the other hand, learn the importance of responsibility and punctuality. Taken together, these benefits foster a culture of discipline, transparency, and efficiency. Therefore, the proposed attendance system is not merely a tool but a long-term investment in the growth, productivity, and technological advancement of the school.