DESIGN AND IMPLEMENTATION OF A CROSS-PLATFORM REAL-TIME BIOMETRIC ATTENDANCE SYSTEM FOR EDUCATIONAL INSTITUTIONS.

BY:

Jolayemi Olugbenga David (21/10MSS006)

DEPARTMENT OF MATHEMATICAL AND COMPUTING SCIENCE

THOMAS ADEWUMI UNIVERSITY, OKO-IRESE, KWARA STATE, NIGERIA.

AUGUST, 2025

DESIGN AND IMPLEMENTATION OF A CROSS-PLATFORM REAL-TIME BIOMETRIC ATTENDANCE SYSTEM FOR EDUCATIONAL INSTITUTIONS.

BY:

Jolayemi Olugbenga David(21/10MSS006)

A PROJECT SUBMITTED TO THE DEPARTMENT OF MATHEMATICAL AND COMPUTING SCIENCE, THOMAS ADEWUMI UNIVERSITY, OKO-IRESE, KWARA STATE, NIGERIA.

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF SCIENCE (HONOURS) DEGREE IN SOFTWARE ENGINEERING

AUGUST, 2025

CERTIFICATION

This is to certify that I am responsible for the work submitted in this Project, that the original work is mine, and that neither the project nor the original work contained therein has been submitted to this University or any other institution for the award of a degree.

JOLAYEMI OLUGBENGA DAVID (21/10MSS006)

APPROVAL

This project has been approved for the Department of Mathematical and Computing Science, Faculty of Computing and Applied Sciences, Thomas Adewumi University, Oko, Kwara State, Nigeria.

14/10/2025

Dr. Omosola Olabode ……
Supervisor **Signature and Date**

14/10/2025

Mr. Oluwadamilare Oladipo ……
Co-Supervisor **Signature and Date**

14/10/2025

Dr. Omosola Olabode ……..
Head of Department **Signature and Date**

Prof. Ayodele Adebiyi 14/10/2025
…….. ……..
External Examiner Signature and Date

DEDICATION

This project is dedicated to God Almighty for the abundant grace, wisdom, knowledge, and skills given to me throughout my life, especially during my stay at Thomas Adewumi University, Oko, Kwara State, Nigeria.

ACKNOWLEDGEMENT

First and foremost, I would like to express my gratitude to my family, especially my mother, **Ms. Comfort Ayodele Afolayan,** and my siblings, for their unwavering love, prayers, and moral support throughout my academic journey. Your sacrifices, encouragement, and constant belief in me have been the backbone of my success and progress.

I am deeply thankful to my supervisors, **Mr. Dare Oladipo,** who guided me through the technical development of this project, and **Dr. Omosola Olabode,** who oversaw the documentation and provided invaluable input on the write-up. Your mentorship, patience, and dedication were vital to the successful completion of this work.

A big thank you to the Faculty of Computing and Applied Sciences, the Department of Mathematical and Computing Science, and the entire Thomas Adewumi University community. The knowledge, resources, and supportive environment provided have been essential in shaping my academic growth and making this project possible.

Finally, I acknowledge **Mr. Paul Ikubanni** and the entire **ICT** team at **Koderia Creative Lab** for the hands-on experience and industry-based guidance I received during my SIWES program. Your input helped bridge the gap between theory and practical execution.

To everyone who offered a word of encouragement, a listening ear, or a helping hand along the way, thank you from the bottom of my heart. Your support, seen and unseen, has meant more than words can say.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Attendance management remains a critical component in educational institutions, yet manual and semi-automated methods remain prone to human error, proxy attendance, and delayed reporting, which negatively impact academic accountability and administrative efficiency. Traditional roll calls and paper registers are time-consuming, vulnerable to fraudulent practices, and lack real-time data access for decision-making. This project proposes a secure, cross-platform biometric attendance management system that leverages fingerprint and facial recognition for accurate, non-transferable attendance marking.

The system was developed using Flutter and Dart for mobile, web, and desktop environments, with a Laravel backend for secure data storage and real-time synchronization. The proposed system integrates role-based dashboards, real-time analytics, and automated reporting, significantly reducing administrative overhead. Performance evaluation demonstrated accurate and reliable attendance logging, reducing proxy attendance to near zero, and providing instant access to attendance records and analytics for staff and administrators.

This project demonstrates that biometric-driven, cross-platform attendance solutions can effectively modernize record-keeping, enhance institutional efficiency, and strengthen data integrity, while providing a foundation for future integration with learning management and HR systems.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The shift from paper-based roll calls to biometric attendance systems is redefining how schools and workplaces document presence. Recent studies show that fingerprints, facial patterns, and other unique physiological signals dramatically cut human error, proxy "buddy punching," and administrative overhead while enabling real-time analytics that improve decision-making and cost control (Drozdowski *et al*., 2020). At the same time, researchers and policy analysts warn that biometric rollouts must address privacy, consent, and equity to sustain public trust (Cooper & Yon, 2019).

Traditional sign-in sheets and spreadsheet logs are slow, error-prone, and easily manipulated, reducing instructional or productive time and burdening staff with record reconciliation (Ajayi *et al*., 2016). Discrepancies in such records can distort performance evaluations and funding metrics, especially in education where attendance drives resource allocation.

Biometric attendance systems identify individuals through immutable characteristics fingerprint minutiae, facial landmarks, or iris textures offering high accuracy and resistance to forgery (Odesoba *et al*., 2025). Recent surveys in higher education show fingerprint-based platforms trimming check-in time by up to 75 percent while virtually eliminating proxy sign-ins (Obiora *et al*., 2025). Multi-modal deployments that combine fingerprints and facial recognition further boost reliability, even when one modality is temporarily unusable due to injury or lighting conditions (Al-Khaldi *et al*., 2020).

While biometrics enhance security, they also raise significant concerns about data misuse, surveillance creep, and algorithmic bias (Cooper & Yon, 2019; Drozdowski *et al*., 2020). U.S. and international regulators increasingly mandate explicit consent, minimal data retention, and transparency in algorithmic decision-making (NIST, 2023). Scholars argue that unchecked face-recognition deployments can chill free expression and disproportionately affect marginalized groups, underscoring the need for rigorous ethical frameworks (Frontiers in Big Data, 2024; Melzi *et al.*, 2022).

Biometric attendance platforms now integrate anomaly detection to flag unusual patterns such as sudden drops in attendance allowing early interventions. Emerging research explores privacy-preserving techniques like on-device feature extraction and federally compliant encryption to keep raw biometric templates off the cloud (Melzi *et al*., 2022). Future systems may combine gait, voice, and periocular recognition to accommodate users with disabilities and further harden security against spoofing attacks.

Biometric attendance management has matured from experimental prototypes to scalable, commercially viable solutions that outperform manual methods on speed, accuracy, and fraud resistance. Organizations that deploy these systems responsibly embedding strong privacy safeguards and transparent governance stand to gain not only administrative efficiency but also richer insights into engagement and productivity.

1.2 Statement of the Problem

Existing attendance systems, especially those relying on manual processes, pose several challenges that this project aims to address. These challenges include:

1. Inaccuracy due to human error in data entry.

2. Susceptibility to fraudulent activities, where one individual signs in on behalf of another.
3. Difficulty in tracking and managing large volumes of attendance data.
4. Time consumption in data processing and retrieval.
5. Lack of real-time data accessibility for decision-making.

The biometric attendance management system (BAMS) is intended to replace manual roll-calls with an automated, privacy-aware platform that authenticates each person by their unique physiological traits. By eliminating proxy sign-ins and delivering real-time analytics, BAMS can shrink administrative workload, curb "time theft," and improve compliance with tightening data-protection rules.

1.3 Aim and Objectives of the Study

The aim of this study is to create a cross-platform application that marks attendance in real-time using biometric authentication. The objectives to realizing this set goal are to:

1. Design a user-friendly, cross platform attendance system using flutter focused on biometric security.

2. Develop a mobile app that lets students mark attendance in real time using fingerprint.
3. Implement a secure database connected to the university's Laravel backend for attendance record storage and retrieval.
4. Evaluate the system's speed, reliability and performance through testing and feedback from students.

1.4 Significance of the Study

This project contributes significantly to educational advancement in the following ways:

1. **For Students and Lecturers:** It offers reliable attendance tracking, which can enhance learning outcomes by allowing lecturers to dedicate more time to disseminating knowledge rather than handling administrative tasks. (Nkata, 2024)

2. **For Educational Institution:** It provides accurate real-time attendance data that promotes fairness and integrity, helps identify at-risk students early, and strengthens the university's commitment to innovation and quality education. (Bañeres, Rodríguez, Guerrero-Roldán, & Karadeniz, 2020; Makinde, Sulyman, & Ibrahim, 2024)

3. **For Society:** By promoting technology adoption within education, this project fosters digital inclusion and innovation readiness among young people, equipping them with skills for the future workforce. (Makinde, Sulyman, & Ibrahim, 2024)

1.5 Scope of the Study

The project focuses on designing and implementing a system that incorporates biometric (fingerprint recognition) technology. It is intended for deployment in educational institutions but may be adapted for use in corporate environments. The system's functionality will be tested within the confines of these settings while considering security, accuracy, and user-friendliness.

1.6 Limitation of the Study

Despite the potential of this project to modernize attendance management systems in universities, there are several limitations that may affect the development, deployment, and scalability of the system. These limitations stem from constraints in hardware, software, infrastructure, and data availability, particularly within the context of developing nations like Nigeria.

1.6.1 Hardware Constraints

A major limitation lies in the requirement for specific hardware components such as mobile devices with fingerprint scanners. While some smartphones support both features, many institutional devices used in Nigerian universities may lack the necessary hardware support, limiting full system adoption (Ogunleye *et al.*, 2021). Additionally, the cost of procuring and maintaining biometric scanners for large classrooms or lecture theatres could be a barrier to large-scale implementation (Ajayi *et al.*, 2018).

1.6.2. Software Constraints

The system's mobile application is developed using **Flutter and Dart**, which, while powerful and cross-platform, may face compatibility issues on certain legacy mobile devices. Furthermore, the backend framework, **Laravel**, requires a robust hosting environment to support real-time communication with the school portal. System performance may degrade without reliable server infrastructure, especially when handling a large volume of data and multiple concurrent users (Afolabi & Ojo, 2020).

1.6.3. Data Availability and Integration

The effectiveness of the system depends heavily on the availability and quality of existing student data from the **school portal API**. Inaccurate or incomplete records can compromise the functionality of the system, leading to incorrect attendance logging. Furthermore, integration with the school portal requires consistent API support and documentation, which may not always be adequately maintained or updated (Bello *et al.*, 2021).

1.6.4. Network and Power Dependence

Another key limitation is the reliance on **stable internet connectivity** for real-time data synchronization. In areas with poor network infrastructure, especially in rural or underdeveloped university campuses, the system's ability to update attendance records in real time may be hindered (Eze *et al.*, 2020). Similarly, mobile device usage for biometric scanning is power-dependent, and power outages a common issue in many Nigerian institutions can disrupt system operations.

1.6.5 User and Institutional Constraints

Effective deployment also requires institutional buy-in, adequate training of staff and students, and ongoing technical support. Resistance to technological change, particularly among staff unfamiliar with mobile-based systems, may affect the rate of adoption. Additionally, the absence of a dedicated IT team for support and maintenance could lead to system downtime and unresolved technical issues (Nwachukwu & Iwu, 2022).

1.7 Definition of Terms

1. **Biometric** – Automated recognition of individuals based on physiological or behavioral traits (International Organization for Standardization [ISO], 2022).

2. **Attendance Management** – The process of tracking and recording the presence, absence, lateness and leave of individuals in an organization (peopleHum, 2025).

3. **Authentication** – The process of verifying the identity of a person, device or data source before access is granted. (National Institute of Standards and Technology [NIST], 2023)

4. **Verification** – Confirmation, through inspection or testing, that a system or artefact meets its specified requirements (Institute of Electrical and Electronics Engineers [IEEE], 2016).

5. **Attendance Management System (AMS)** – Software that automates attendance capture, notification and reporting to improve accuracy and reduce manual effort (Akanbi *et al*., 2021).

6. **Biometric Technology** – Hardware, algorithms and standards that capture and match physiological traits for identity verification (Al-Khaldi *et al*., 2020).

7. **Fingerprint Authentication** – A biometric method that validates a person by matching a live fingerprint sample to a stored template, preventing impersonation (Ajayi et al., 2016).

8. **Real-time Data Synchronization** – Instantly propagating updates (e.g., attendance records) across connected devices and back-end services to keep data consistent ((Exact Comms, 2025).

9. **Mobile Application** – Software designed to run on portable devices such as smartphones or tablets (Google, 2025b).

10. **Flutter** – Google's open-source UI framework for building natively compiled, multi-platform apps from a single codebase (Google, 2025a).

11. **Dart** – Google's client-optimized programming language used with Flutter to create fast cross-platform applications (Google, 2025b).

12. **Laravel** – An open-source PHP web-application framework that provides expressive syntax, routing and built-in security features for robust back-ends (Laravel LLC, 2025).

13. **Agile Framework** – An iterative, customer-focused software-development approach (Agile Alliance, 2025).

14. **API (Application Programming Interface)** – A published set of rules and endpoints that lets independent software components exchange data and functionality (IBM, 2025).

15. **User Interface (UI)** – The collection of on-screen visual elements through which humans interact with software (Interaction Design Foundation, 2016).

16. **Biometric Attendance Management System (BAMS)** – An AMS that logs presence by matching users' biometric traits (e.g., fingerprints) instead of roll-calls or ID cards (Akanbi et al., 2021).

17. **Biometric Template** – An encrypted mathematical representation of salient biometric features (not the raw image) stored for subsequent matching (Innovatrics, 2025).

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The contemporary literature positions biometric attendance management systems (SAMS) as a proven remedy for the slowness, inaccuracy, and fraud that plague manual roll-calls and sign-in sheets. Fingerprint, facial-recognition, and other physiological traits now deliver sub-second check-ins, ≥99 % matching accuracy, and measurable payroll savings, yet they also introduce privacy and acceptance issues that must be handled through rigorous governance and user-centered design. Below, the review is rewritten to foreground biometrics alone removing the earlier emphasis on Near-Field Communication while retaining the original structure of concepts, theories, related works, and research gaps.

Manual attendance logs consume HR or teaching time, invite transcription errors, and are easy to manipulate, especially at scale. Proxy attendance ("buddy-punching") can inflate presence records by as much as 80 % in tertiary institutions. Biometric systems counter these weaknesses by matching unique, hard-to-forge biological signatures fingerprints, facial landmarks, iris textures thereby automating verification at the point of entry. Field tests report recognition rates above 99 % and false-accept probabilities below 0.01 % when multimodal algorithms are tuned correctly. Commercial deployments now record a typical check-in latency of two seconds or less on commodity devices and save up to 4 % of annual payroll by eliminating manual reconciliation.

2.2 Conceptual Review

Early biometric pilots were workstation add-ons; today, complete attendance suites integrate enrolment kiosks, mobile apps, and dashboards that stream real-time presence data to HR or

learning-management systems. Fingerprint devices remain the dominant modality in schools and offices because of their low cost and mature algorithms, while higher-end deployments increasingly add facial or iris recognition for touchless operation and redundancy.

Users' biometric samples are captured under controlled conditions, converted into secure mathematical templates, and linked to a unique ID in the attendance database. At every check-in a sensor captures a fresh sample, runs feature extraction, and compares it to the stored template; liveness-detection algorithms (active or passive) ensure the probe comes from a living subject, thwarting masks, photos, or gummy fingers. Modern BAS encrypt templates at rest with AES-256 and in transit with TLS 1.3; no raw images leave the sensor, mitigating the irreversible harm of a template breach.

Dashboards aggregate attendance, lateness, and overtime trends, enabling managers to trigger early interventions and optimize staffing.

2.2.1 Attendance Management System

An Attendance Management System (AMS) is a technological solution designed to monitor and record individuals' attendance in various settings, including educational institutions, workplaces, and events. Traditional attendance systems typically involve manual processes, such as roll calls or paper sign-in sheets, which can be time-consuming and prone to inaccuracies. As organizations seek to enhance operational efficiency and ensure compliance with attendance regulations, there has been a shift towards automated and intelligent attendance management systems.

An effective AMS should enable real-time data capture, ease of use, accuracy, and comprehensive reporting capabilities. It should allow educators or employers to track attendance patterns, generate reports, and manage absences efficiently. Moreover, the system

should be able to integrate with other institutional management systems, such as Learning Management Systems (LMS) or Human Resource Management Systems (HRMS), to provide a holistic view of attendance data within the broader context of performance evaluation and organizational management.

The emergence of biometric technologies has further revolutionized the concept of AMS. Biometric technologies, such as fingerprint scanning and facial recognition, provide a means of verifying individuals' identities with a high degree of accuracy, thus minimizing issues related to proxy attendance.

2.2.2 Biometric Technologies in Attendance Systems

Fingerprint systems capture ridge–valley patterns with optical, capacitive, or ultrasonic sensors, convert them into mathematical templates, and perform one-to-one or one-to-many matches against an encrypted database. Academic prototypes now run on inexpensive Arduino-class microcontrollers paired with AS608 sensors, LCDs, and real-time clocks, demonstrating that reliable biometric logging no longer requires enterprise-grade hardware.

Performance continues to improve: discussions at NIST’s International Face and Fingerprint Performance Conference 2025 highlighted error rates below 0.5 % on contemporary public datasets and renewed work on standards for cross-sensor interoperability and demographic fairness

A 2025 deployment at Bells University of Technology (Nigeria) (Obiora, G. N., *et al*. 2025) cut per-student check-in time from 22.25 s to 6.16 s and eliminated impersonation by linking each fingerprint to a student ID in real time. Similar classroom pilots in India and Malaysia report accuracy above 98 % while freeing instructors from paper registers

Typical architectures include:

1. Enrolment kiosks for initial capture and template encryption.
2. Edge readers at lecture-hall entrances that sync with a campus Wi-Fi.
3. Cloud dashboards that feed attendance data to the learning-management system (LMS) and trigger alerts for absenteeism thresholds.

2.2.3 Fingerprint Recognition Technology

Fingerprint recognition the most mature and cost-efficient biometric modality now verifies an identity in well under two seconds and delivers ≥98 % match accuracy, making it the work-horse of automated attendance in schools and workplaces. Field studies show dramatic drops in proxy ("buddy-punch") fraud, while national standards bodies such as NIST continue to push error rates below 0.5 % through better sensors, transfer-learning algorithms, and liveness detection. Adoption is accelerating in universities worldwide from Nigeria to India yet hygiene concerns, presentation attacks, and data-privacy rules demand careful design and governance. The expanded discussion below explains how the technology works, reviews recent campus deployments, and weighs its advantages and limitations.

Fingerprint recognition is a biometric technique that identifies individuals by analyzing the unique patterns of ridges and minutiae points on their fingertips. The uniqueness of fingerprints makes them an effective tool for identity verification in various applications, including attendance management. According to Chukwuma *et al.*, (2022), fingerprint recognition systems operate by capturing a digital image of a fingerprint, extracting unique features, and comparing them to a pre-stored database to authenticate the individual. This process is typically fast, taking just a few seconds, and minimizes errors associated with manual verification.

Optical, capacitive, or ultrasonic scanners capture ridge–valley patterns and convert them into minutiae templates that are hashed and stored in an encrypted database. Verification compares a live probe with the template set, typically completing in ≤2 s on microcontroller-class hardware such as the Arduino/AS608 combo used in recent prototypes. NIST's 2025 International Face and Fingerprint Performance Conference (IFPC) reports false-accept rates below 0.5 % on public datasets, confirming the modality's maturity for large-scale use.

The implementation of fingerprint-based attendance systems in educational institutions is growing due to their effectiveness in combating common issues such as proxy attendance, which is prevalent in many universities. A study conducted at Obafemi Awolowo University found that integrating fingerprint recognition technology reduced instances of fraudulent attendance practices by 85% within the first semester of implementation (Adebayo *et al.*, 2020).

2.2.4 Biometric Technology

Biometric technology involves the use of unique physical or behavioral characteristics to identify individuals. Common biometric modalities include fingerprint recognition, facial recognition, iris scanning, and voice recognition. Among these, fingerprint and facial recognition are the most widely adopted for attendance management systems due to their ease of use and accuracy.

1. **Fingerprint Recognition**: Fingerprint recognition involves capturing an individual's fingerprint using a scanner, which converts the unique patterns into a digital format for storage and matching. This method is popular due to its reliability and the relatively low cost of fingerprint scanners. The accuracy of fingerprint recognition has improved significantly with advances in sensor technology and algorithms, making it a viable

option for attendance management. Fingerprint recognition is a biometric technique that identifies individuals by analyzing the unique patterns of ridges and minutiae points on their fingertips. The uniqueness of fingerprints makes them an effective tool for identity verification in various applications, including attendance management. According to Chukwuma *et al.*, (2022), fingerprint recognition systems operate by capturing a digital image of a fingerprint, extracting unique features, and comparing them to a pre-stored database to authenticate the individual. This process is typically fast, taking just a few seconds, and minimizes errors associated with manual verification. The implementation of fingerprint-based attendance systems in educational institutions is growing due to their effectiveness in combating common issues such as proxy attendance, which is prevalent in many universities. A study conducted at Obafemi Awolowo University found that integrating fingerprint recognition technology reduced instances of fraudulent attendance practices by 85% within the first semester of implementation (Adebayo *et al.*, 2020).

2.2.5 Advantages of Fingerprint-based Attendance Systems

Fingerprint-based attendance systems offer several benefits over traditional methods. Some of the key advantages include:

1. **Accuracy and Reliability**: Unlike manual or RFID-based systems, fingerprint recognition offers a high level of accuracy by relying on unique biometric identifiers. This reduces the likelihood of errors and eliminates the possibility of proxy attendance (Chukwuma *et al.*, 2022). Research by Adewale and Kolawole (2020) demonstrated that fingerprint systems achieved an accuracy rate of over 98% in university lecture halls, significantly improving attendance tracking efficiency.

2. **Speed and Automation**: Fingerprint systems streamline the attendance process by automating student verification. This saves time, particularly in large lecture halls where manual attendance tracking can be time-consuming. A case study at the University of Lagos showed that fingerprint-based attendance reduced the average time spent on attendance verification from 15 minutes to under 3 minutes per lecture session (Obi *et al.*, 2021).
3. **Enhanced Security**: Since fingerprints are unique to each individual and difficult to forge or replicate, fingerprint-based systems enhance the security of attendance records. Additionally, biometric data can be encrypted and securely stored to protect students' privacy and prevent unauthorized access (Ngugi & Wambua, 2020).
4. **Non-transferability**: Unlike RFID cards or PIN-based systems, which can be shared or stolen, fingerprints are inherently non-transferable. This ensures that only the rightful owner of the biometric data can authenticate their attendance (Adebayo & Musa, 2021).

2. **Facial Recognition**: Facial recognition technology analyzes the unique features of an individual's face to identify them. This method can be deployed using cameras equipped with advanced imaging software that processes and recognizes faces in real time. Facial recognition offers the advantage of non-intrusive identification, allowing individuals to check in without physical contact. However, it also raises concerns regarding privacy and data security, which must be addressed when implementing such systems.

2.2.6 Advantages of Facial Recognition Systems

1. Contactless Convenience and Hygiene: Because users only need to look at a camera, no shared surfaces are touched an advantage highlighted during and after COVID-19 as organizations sought to limit pathogen spread. Touch-free entry also speeds flow through doors or kiosks, eliminating the need to carry cards or remember PINs

2. Speed and High Throughput: State-of-the-art engines verify a face in ≤ 0.5 s on commodity hardware, letting venues process hundreds of people per minute; event platforms report "seconds-level" check-ins that virtually erase entry queues. Attendance terminals show similar gains, clocking employees faster than manual badges or fingerprint scanners.
3. Proven Accuracy: The latest NIST Face Recognition Vendor Test places top algorithms at false-match rates below 1×10^{-6} and false-non-match rates under 0.3 % on border-control imagery. Clinical and academic pilots report 96–99 % correct identification in real-world lighting and aging conditions
4. Fraud and "Buddy-Punching" Prevention: Unlike swipe cards that can be shared, a face cannot be borrowed, so buddy-punch fraud drops sharply EmpMonitor lists this as a chief benefit in office deployments. Retail risk analysts add that face ID deters shoplifting and refund scams by flagging known offenders in real time. Law-enforcement use has already led to more than 1,000 arrests in London since 2024, underscoring security gains
5. Scalability and Remote Flexibility: Modern SDKs run on edge devices, phones, or cloud VMs, letting organizations roll out a single code-base from a door reader to a web camera Cyberlink cites deployments across finance, retail, and smart offices. Cloud-ready attendance apps even allow staff to clock in from home with geo-tagged selfies
6. Lower Total Cost of Ownership: Removing plastic cards and mechanical readers saves consumables and maintenance, while automation cuts payroll reconciliation work. Case studies cite administrative savings of 3-5 % of annual wage costs once manual auditing ends.

2.2.6 Challenges and Limitations of Fingerprint-based Attendance Systems

Despite their numerous benefits, fingerprint-based attendance systems also face certain challenges. One of the main concerns is the initial cost of installation, particularly in resource-constrained environments. According to Onyango *et al.*, (2020), the cost of biometric scanners, software, and database management can be prohibitive for some universities. Additionally, fingerprint recognition systems may encounter difficulties in environments where students' fingerprints are affected by dirt, moisture, or abrasions, leading to occasional recognition errors (Musa *et al.*, 2023).

Another challenge relates to privacy concerns surrounding the collection and storage of biometric data. Critics argue that inadequate data protection measures could expose students to potential breaches of their personal information. To address these concerns, researchers advocate for the implementation of robust encryption protocols and compliance with data protection regulations such as Nigeria's Data Protection Regulation (NDPR) and Kenya’s Data Protection Act (Ngugi & Wambua, 2020).

2.2.7 Local Adoption and Case Studies

Several universities in Africa have begun adopting fingerprint-based attendance systems to improve student management and academic accountability. In Nigeria, institutions such as Covenant University and Obafemi Awolowo University have implemented biometric attendance systems with promising results (Adebayo *et al.*, 2020). Similarly, research conducted at Kenyatta University in Kenya highlighted the effectiveness of biometric technologies in reducing absenteeism and enhancing classroom engagement (Ochieng & Kibet, 2020). These local case studies underscore the growing recognition of fingerprint biometrics as a reliable tool for modernizing university attendance management.

Fingerprint-based biometric systems represent a significant advancement in attendance management for universities. By addressing the limitations of traditional methods and offering enhanced accuracy, security, and efficiency, these systems contribute to improved academic accountability and operational efficiency. However, the successful implementation of biometric technologies requires careful consideration of cost, privacy, and technical challenges. Future research and policy efforts should focus on optimizing fingerprint systems for diverse educational environments and ensuring compliance with data protection laws to safeguard students' biometric information.

2.2.8 Smart Systems

Smart systems refer to technological solutions that leverage advanced technologies, such as artificial intelligence, machine learning, and the Internet of Things (IoT), to perform tasks autonomously or semi-autonomously. In the context of attendance management, a smart system combines biometric technologies to create an intelligent AMS capable of processing attendance data in real time, analyzing patterns, and generating reports.

Smart attendance management systems offer several advantages:

- **Automation**: By automating the attendance tracking process, organizations can reduce administrative overhead and free up staff to focus on more strategic tasks.
- **Real-Time Data Analysis**: Smart systems can analyze attendance data as it is collected, enabling institutions to identify trends and address issues promptly.
- **Enhanced Security**: The integration of biometric technologies enhances security, reducing the risk of fraud and ensuring that attendance data is accurate and reliable.

However, the development of smart attendance management systems requires careful consideration of user acceptance and the ethical implications of data collection. Ensuring that

users are comfortable with the technologies employed and that their data is handled securely is essential for the successful implementation of a smart AMS.

2.3 Theoretical Framework

2.3.1 Technology Acceptance Model (TAM)

Originating with Davis (1989), TAM holds that perceived usefulness (PU) and perceived ease of use (PEOU) jointly shape a user's intention to adopt a system. For a biometric AMS, PU maps to time saved and accuracy gained, while PEOU reflects how intuitive the fingerprint scan feels to students. Biometric-specific extensions such as BioTAM add trust as a mediating factor, recognising that privacy concerns can suppress intention even when PU and PEOU are high (Kanak & Sogukpinar, 2017).

2.3.2 Unified Theory of Acceptance and Use of Technology (UTAUT)

UTAUT consolidates eight adoption models and shows that performance expectancy, effort expectancy, social influence and facilitating conditions predict behavioural intention and actual use. Meta-analyses report that performance expectancy and behavioural intention are the strongest links across domains, including security technologies. Designing the AMS to demonstrate visible accuracy gains (performance expectancy) and providing on-site kiosks and support (facilitating conditions) therefore raise usage odds.

2.3.3 Diffusion of Innovations (DOI)

Rogers' DOI theory explains adoption at the social-system level. Five perceived attributes—relative advantage, compatibility, complexity, trialability, observability—shape the S-curve of diffusion. Piloting the fingerprint module in one department (trialability) and publicly sharing accuracy dashboards (observability) accelerate contagion beyond early adopters.

2.3.4 Agile Software Development Life Cycle (Agile SDLC)

The Agile Manifesto values “working software” and “responding to change” over heavyweight plans. A typical Agile SDLC moves through concept, inception, iterative builds, release and continuous review, enabling requirements to evolve sprint by sprint. For the AMS this means shipping a minimum-viable scan-and-sync feature, gathering lecturer feedback, then refining UI flows or API endpoints in the next iteration—keeping development aligned with TAM and UTAUT insights.

2.3.5 DeLone & McLean Information-Systems Success Model

Post-implementation evaluation draws on six inter-related dimensions: system quality, information quality, service quality, use, user satisfaction and net benefits. Applied here, log accuracy and uptime gauge system quality, staff satisfaction surveys gauge service quality, and analytics on absenteeism trends evidence net benefits.

2.3.6 Privacy by Design (PbD) Framework

PbD’s seven foundational principles—e.g., proactive not reactive, privacy as the default, full functionality (positive-sum)—embed data protection into architecture rather than add it later. Encrypting templates at capture time and minimizing data fields exemplify “privacy by default,” while role-based access satisfies the positive-sum aim of delivering security and usability.

2.3.7 Biometric Security Model & NIST Digital-Identity Guidelines

The Biometric Security Model stresses template encryption, secure storage and consent management, framing biometrics as a third authentication factor that must still obey least-privilege rules. NIST SP 800-63-B complements this by specifying assurance levels,

throttling and replay-attack protections for biometric authenticators—controls that the AMS must meet to maintain institutional compliance.

2.4 Review of Related Works

The development of attendance management systems has evolved significantly, with each innovation addressing various challenges inherent in traditional methods. Recent studies have explored diverse technologies to streamline attendance tracking, aiming for efficient, reliable solutions.

Numerous studies and projects have explored the use of biometric technologies in attendance management systems. This section summarizes key research works in the field, highlighting their methods, strengths, and weaknesses.

1. **Biometric-Based Attendance Systems**: Several projects have implemented fingerprint recognition for attendance tracking in educational institutions. For example, a study by Prasanna *et al.* (2020) developed a fingerprint-based attendance management system that utilized a microcontroller to capture fingerprints and store attendance records. The study demonstrated improved accuracy and reduced instances of proxy attendance. However, the system faced challenges related to fingerprint data quality and user acceptance.
2. **Facial Recognition Systems**: Research by Al-Sharif *et al*. (2021) focused on implementing facial recognition technology in attendance systems within universities. The study employed machine learning algorithms to enhance recognition accuracy and reported significant reductions in attendance discrepancies. While the system demonstrated its effectiveness, concerns related to privacy and data security were

raised, highlighting the need for robust safeguards when implementing facial recognition in attendance management.

3. **Integration of Biometric Technologies**: Some research has explored the integration of biometric technologies to create a comprehensive attendance management system. A study by Yadav *et al*. (2021) proposed a hybrid attendance system combining NFC cards and fingerprint recognition. The system was able to enhance security while improving user convenience. However, it faced implementation challenges, such as ensuring system interoperability and user training.

Overall, while various studies have demonstrated the effectiveness of biometric technologies in attendance management, challenges related to privacy, user acceptance, and system reliability persist. Addressing these challenges is crucial for the successful deployment of smart attendance management systems.

Martinez *et al*. (2020) implemented a facial recognition system leveraging machine learning algorithms. The system showcased high accuracy in controlled environments but struggled with variations in lighting conditions and different facial expressions. Similarly, Chen and Lee (2020) utilized deep learning techniques, improving system robustness; however, they faced challenges with processing speed and computational demands.

An IEEE-submitted study integrates “Closeness Binary Code” directly into the matching stage, lowering spoof success rates without retraining the core PAD model a promising route for edge devices with limited resources

Fingerprint-based systems, as investigated by Thomas and Rekha (2020), provided a highly secure method, reducing fraudulent attendance. This method's principal limitation was noted in environments requiring high hygiene standards. In contrast, Wang *et al.* (2022) applied iris

recognition due to its high uniqueness and security, but high costs and user discomfort posed challenges for widespread adoption.

Emerging works also synthesized multiple technologies for optimized results. For instance, Liu and Zhang's study (2020) employed both NFC and biometric verification, balancing ease of use and security. Yet, integration difficulties and increased setup costs were significant concerns. Additionally, Patel *et al*. (2021) proposed a hybrid system combining facial recognition and geotagging to enhance verification but found privacy issues and data accuracy challenges.

Cloud-based platforms, such as those presented by Yadav and Sharma (2021), centralized attendance data for easy access and analysis. These systems improved scalability and remote access but raised concerns about data security and internet dependency. Additionally, Kumar *et al*. (2021) introduced blockchain integration to ensure data integrity and transparency, finding it effective but complicated and costly to implement.

The literature also critically examines mobile-based attendance solutions. For instance, Singh and Bhattacharya (2020) designed a smartphone application utilizing GPS for location-based attendance marking. Despite offering high convenience, GPS inaccuracy indoors and concerns over location privacy were significant issues.

The text and QR code-based systems discussed by Johnson and Kim (2021) presented an easy-to-deploy solution, though they were susceptible to proxy attendance as codes could be easily shared among users. This limitation highlighted the necessity for additional authentication layers.

In the pursuit of a comprehensive solution, interdisciplinary research, such as that by Choi *et al*. (2021), combined IoT devices with machine learning to predict user attendance patterns,

offering proactive management but spotlighting concerns over user privacy and ethical data use.

Some studies, such as by Okafor and Ayo (2022), focused specifically on academic environments, tailoring solutions to education institutions' operational needs. While these systems reported increased engagement and attendance rates, their customization often limited application to other sectors.

The reviewed literature illustrates significant advancements in attendance systems, highlighting an ongoing shift towards multi-faceted, adaptable implementations that address specific environmental and institutional needs. Continuous improvements are necessary, with a focus on balancing technological advancement with user privacy, cost efficiency, and compatibility with existing systems.

2.5 Gaps in Existing Research

Despite the advancements in attendance management systems utilizing biometric technologies, several gaps in existing research have been identified. These gaps highlight the need for further exploration and development in the field:

1. **User Acceptance and Trust**: While previous studies have examined the technical aspects of biometric systems, there is a lack of comprehensive research focusing on user acceptance and trust. Understanding the factors that influence users' willingness to adopt these technologies is essential for successful implementation.
2. **Privacy and Ethical Considerations**: Research addressing the ethical implications of biometric data collection remains limited. There is a need for more in-depth studies exploring privacy concerns and developing guidelines for responsible data handling.

3. **System Integration**: Existing literature often focuses on individual technologies (biometric) rather than their integration into a cohesive attendance management system. Research exploring the interoperability and seamless functioning of integrated systems is necessary.
4. **Longitudinal Studies**: Most existing studies are cross-sectional, examining the effectiveness of attendance systems at a single point in time. Longitudinal studies that evaluate the long-term impact of biometric -based attendance systems on user behavior and organizational performance are needed.
5. **User Training and System Usability**: Limited attention has been paid to user training and the usability of smart attendance management systems. Research exploring best practices for training users and enhancing system usability will be valuable for successful implementation.

Addressing these gaps will contribute to the development of a more effective and user-friendly smart attendance management system that harnesses the benefits of biometric technologies.

2.6 Summary of Literature Review

In summary, this literature review has provided a comprehensive overview of the existing research surrounding attendance management systems, biometric technologies, and smart systems. The review has highlighted the advantages and challenges associated with these technologies while identifying gaps in the literature that warrant further exploration.

Key findings from the review include:

1. Traditional attendance management systems are often inefficient, leading to a demand for automated solutions that improve accuracy and reduce administrative burden.

2. Biometric technologies, such as fingerprint and facial recognition, offer significant advantages in terms of security and accuracy but raise privacy and ethical concerns.
3. Smart systems that integrate biometric technologies can enhance attendance management but require careful consideration of user acceptance, privacy, and security.

The identified gaps in existing research underscore the need for further exploration of user acceptance, ethical considerations, system integration, and usability. By addressing these gaps, the proposed project "Design and Implementation of a Smart Attendance Management System using Biometric Technology" aims to contribute to the development of an effective, user-friendly, and ethically sound attendance management solution.

Through the implementation of this system, institutions can enhance attendance tracking accuracy, streamline administrative processes, and ultimately foster a more efficient and effective educational or organizational environment.

CHAPTER THREE

SYSTEM DESIGN AND METHODOLOGY

3.1 Background of the Proposed System

Modern Attendance is an enterprise-grade application purpose-built to eliminate the inefficiencies of manual roll-call and paper registers across schools, universities, and training centers, as well as corporate learning environments. Developed with Flutter, it compiles natively to Android, iOS, web, Windows, macOS, and Linux, giving every stakeholder a consistent and responsive experience whether they are scanning in at a lecture theatre, logging on from a desktop in the admin office, or reviewing attendance trends on a tablet in the staff room.

Current Attendance Process (Baseline)

1. Manual data capture – lecturers call names or circulate paper sheets, a process that can consume 5–10 minutes of class time and is prone to transcription mistakes
2. Susceptibility to impersonation – nothing prevents a friend from answering “present” or signing for an absent peer (proxy attendance)
3. Delayed reporting – attendance totals are keyed into spreadsheets only after class, so staff lose any chance of same-day interventions
4. Limited analytics – data remain siloed in registers, blocking cohort--level dashboards or predictive early-warning systems
5. Paper-driven compliance risk – physical sheets expose student names to anyone who glances at them and can be misplaced or damaged.

Pain Points & Risks

Dimension	Manual (Current)	Consequence
Data quality	Hand-written, error-prone	Miscounts and disputes
Security	No authentication, no encryption	Proxy attendance, data leaks
Timeliness	Batch entry after class	Slow pastoral responses
Scalability	One lecturer per room	Extra staff for large cohorts
Analytics	None beyond totals	Missed early-warning flags
Compliance	Poor audit trail	GDPR inaccuracies

Table 3.1 Pain Points & Risks

3.1.1. Core Functionality

1. Secure Biometric Authentication
    a. Supports fingerprint, face, and iris recognition via native device APIs.
    b. Encrypted biometric templates are stored locally on the device and synchronized to the server using end-to-end TLS, ensuring GDPR-compliant data protection.
2. Role-Based Interfaces & Permissions
    a. Students receive a minimalist dashboard showing today's timetable, remaining attendance credits, and instant confirmation of successful check-ins.
    b. Lecturers can create sessions on the fly, trigger one-tap roll calls, and monitor live class occupancy.
    c. Administrators control global policies (e.g., lateness thresholds), run institution-wide analytics, and manage user provisioning all through an intuitive, web-first console secured by SSO/OAuth2.

3. Adaptive Dashboards & Analytics
    a. Real-time KPIs (attendance rate, lateness trends, absence hotspots) with export to CSV, XLSX, or direct API integration to the SIS/HRIS of your choice.
    b. Drill-down views let staff interrogate data by cohort, module, or individual learner, supporting early-warning interventions.

4. Flexible Session & Timetable Management
    a. Bulk import timetables (CSV/ICS) or integrate bi-directionally with existing scheduling systems.
    b. Multi-period, multi-location sessions are handled seamlessly for split-site or hybrid teaching models.

5. Customizable Policy Engine
    a. Configure institution-specific rules minimum attendance thresholds, automated warnings, excused-absence categories, and escalation workflows without writing code.
    b. Time-zone-aware logic guarantees accuracy for international campuses and remote learners.

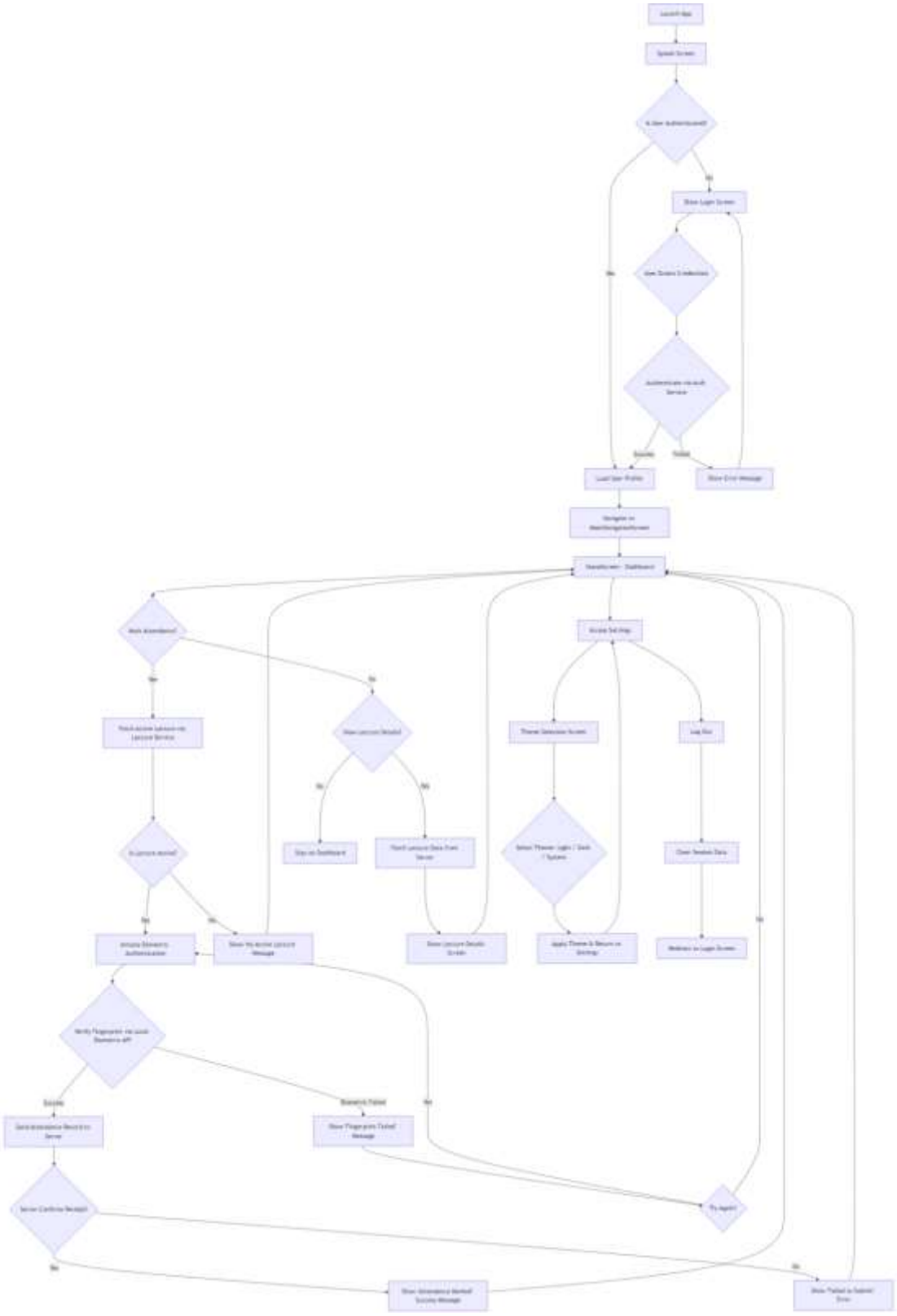

Fig 3.1 Student Attendance Flow in Modern Attendance App

As shown in Figure 3.1, the student attendance flow in the Modern Attendance app is designed to be efficient and secure. The process begins when the user launches the app and proceeds through authentication, biometric verification, and attendance marking. This streamlined flow eliminates manual roll-calls and ensures secure, real-time attendance tracking.

3.1.2 Proposed System: Modern Attendance

1. Secure biometric authentication – fingerprint, face, iris via native APIs; templates encrypted at capture and synced over TLS for GDPR compliance
2. Role-based interfaces (RBAC) – separate dashboards for students, lecturers, and administrators, enforced through role-based access control best practice
3. Real-time analytics – live occupancy counts, lateness heat-maps, and exportable KPI feeds that power early-warning interventions
4. Cross-platform Flutter client – one Dart code-base delivers Android, iOS, web, and desktop builds, proven in open-source attendance apps
5. Agile SDLC foundation – iterative sprints with stakeholder demos align development to emerging user feedback and policy changes

3.2 System Requirements

3.2.1. Hardware Requirements

1. Processor: Quad-core 2.5GHz or higher recommended
2. RAM: 8GB minimum (16GB recommended for smooth emulation and builds)
3. Storage: At least 2GB free for source code, dependencies, and build artifacts
4. Display: 1920x1080 resolution or higher recommended

   Additional:

a. Android device or emulator for testing

b. iOS device or simulator (macOS only) for testing

c. Fingerprint sensor (on device or emulator) for biometric feature testing

3.2.2. Software Requirements

1. Operating System: Windows 7/10/11, macOS 10.13+, or a modern Linux distribution
2. Flutter SDK: Version 3.0 or higher (ensure compatibility with your codebase)
3. Dart SDK: Bundled with Flutter, but ensure it matches Flutter's requirements
4. Android Studio (with Android SDK) or Visual Studio Code (with Flutter and Dart plugins)
5. Xcode (for iOS/macOS development, macOS only): Version 12.0 or higher
6. CMake (for desktop builds)
7. Git (for version control)
8. Java JDK 8 or higher (for Android builds)
9. CocoaPods (for iOS dependency management, macOS only)
10. Chrome (for web development and debugging)

3.2.3 Functional Requirements

ID	Requirement	Rationale
F-01 Biometric Check-in	System shall record attendance via fingerprint, face, or iris, using device-native biometric APIs.	Biometrics cut proxy attendance and shorten roll-call time.
F-02 Template Encryption	Biometric templates must be encrypted on device and in transit (TLS 1.2+).	Protects "special-category" data per GDPR Art. 9.

F-03 Role-Based Access (RBAC)	Provide distinct dashboards for Students, Lecturers, and Admins, enforced via RBAC.	Limits privilege and simplify UI.
F-04 Session Management	Lecturers can create, edit, or cancel sessions and trigger one-tap roll-calls.	Mirrors classroom flow and supports agile user stories.
F-05 Real-time Sync	Attendance events must sync to the server within ≤5 s given network availability.	Enables live dashboards and early-warning alerts.
F-06 Analytics & Reporting	System shall generate KPIs (e.g., daily attendance %, lateness heat-maps) and export CSV/XLSX or REST API feeds.	Data-driven interventions improve retention.
F-07 Notification Engine	Auto-send emails or push alerts for threshold breaches (e.g., <75 % attendance).	Provides timely pastoral support.
F-08 Offline Mode	Capture events locally when offline and auto-sync once a connection returns.	Ensures robustness in poor-connectivity rooms.
F-09 Audit Trail	Log every create/update/delete with timestamp, user ID, and IP/device hash.	Supports forensics and regulatory audits.
F-10 API Integration	Provide REST/JSON endpoints secured by OAuth 2.0 for SIS/HRIS exchange.	Avoids double-entry and supports micro-services.

Table 3.2 Functional Requirements

3.2.4 Non-Functional Requirements

Quality Attribute	Requirement
Performance Efficiency	Check-in latency ≤2 s per student and server response ≤300 ms for 95 th percentile.

Reliability	99.5 % monthly uptime; local queue ensures zero data loss during outages.
Scalability	Support ≥10 k concurrent users across multi-campus deployments without degradation.
Security	Conform to NIST SP 800-63B AAL2 for biometrics (liveness, presentation-attack detection).
Privacy & Compliance	Process biometric data only with explicit consent; purge inactive templates after 365 days; comply with GDPR/ICO guidance.
Usability	Achieve ≥80 % SUS (System Usability Scale) score among pilot users; onboarding ≤2 minutes.
Accessibility	UI meets WCAG 2.2 AA; provide non-biometric fallback for users with accessibility needs.
Maintainability	Codebase follows clean architecture; mean time to repair (MTTR) ≤4 hours.
Portability	Flutter app must run on Android 10+, iOS 14+, Chrome, and Windows/macOS/Linux desktops without code changes.
Interoperability	Use open standards (JSON/REST, OAuth 2.0, OpenAPI 3) for all integrations.
Auditability	Immutable logs retained 7 years and exportable in CSV for regulators.
Legal & Ethical	Provide DPIA (Data-Protection Impact Assessment) template and consent workflow.

Table 3.3 Non-Functional Requirements

3.3. System Architecture

The Modern Attendance system follows a client-centric, modular architecture designed for cross-platform deployment. The core of the system is a Flutter application that runs on Android, iOS, web, and desktop platforms. The architecture is organized to separate concerns between user interface, business logic, data models, and platform-specific integrations, ensuring maintainability and scalability.

3.3.2. Architectural Layers

1. Presentation Layer (UI)

   This layer contains all the widgets and screens that make up the user interface. It is further organized by feature and user role (e.g., student, staff, lecture, onboarding).

   Responsibilities:

   1. Rendering UI elements
   2. Handling user interactions (taps, form submissions)
   3. Displaying data received from the business logic layer

2. Business Logic Layer (Services)

   Description:

   This layer manages the core logic of the application, including communication with external APIs, biometric authentication, attendance processing, and user preferences.

   Responsibilities:

   1. Fetching and processing data from remote or local sources
   2. Handling authentication (including biometric)
   3. Managing user preferences and settings
   4. Orchestrating business rules (e.g., attendance validation)

3. Data Layer (Models)

This layer defines the data structures used throughout the app, such as user profiles, lecture details, and attendance records.

Responsibilities:

1. Defining data models for API responses and local storage
2. Serializing and deserializing data (e.g., JSON parsing)

4. Platform Integration Layer

These folders contain platform-specific code and configuration, enabling the app to access native features (e.g., biometric sensors, notifications) and to be built for each target platform.

Responsibilities:

1. Providing native code for features not available in pure Dart/Flutter
2. Managing platform-specific assets and build settings

3.3.3. Data Flow

1. User Interaction: Users interact with the UI (presentation layer), triggering events such as logging in, enrolling, or marking attendance.

2. Business Logic Processing: The UI calls service classes to process these events. For example, marking attendance may trigger a call to the `attendance_service.dart`, which handles validation and communication with a backend (if present).

3. Data Handling: Service classes use data models to structure information, which may be fetched from or sent to remote APIs, local storage, or device sensors.

4. Platform Services: For features such as biometric authentication, the business logic layer interacts with platform-specific code through Flutter plugins or native code in the platform-specific folders.

5. UI Update: Once processing is complete, the UI is updated with new data or feedback.

As shown in Figure 3.2, the sequence of interactions between the user and the system during the login and attendance marking process is illustrated. The diagram highlights key steps such as user authentication, lecture selection, biometric verification, and attendance recording. This technical flow ensures secure and efficient attendance tracking while maintaining real-time synchronization with the server.

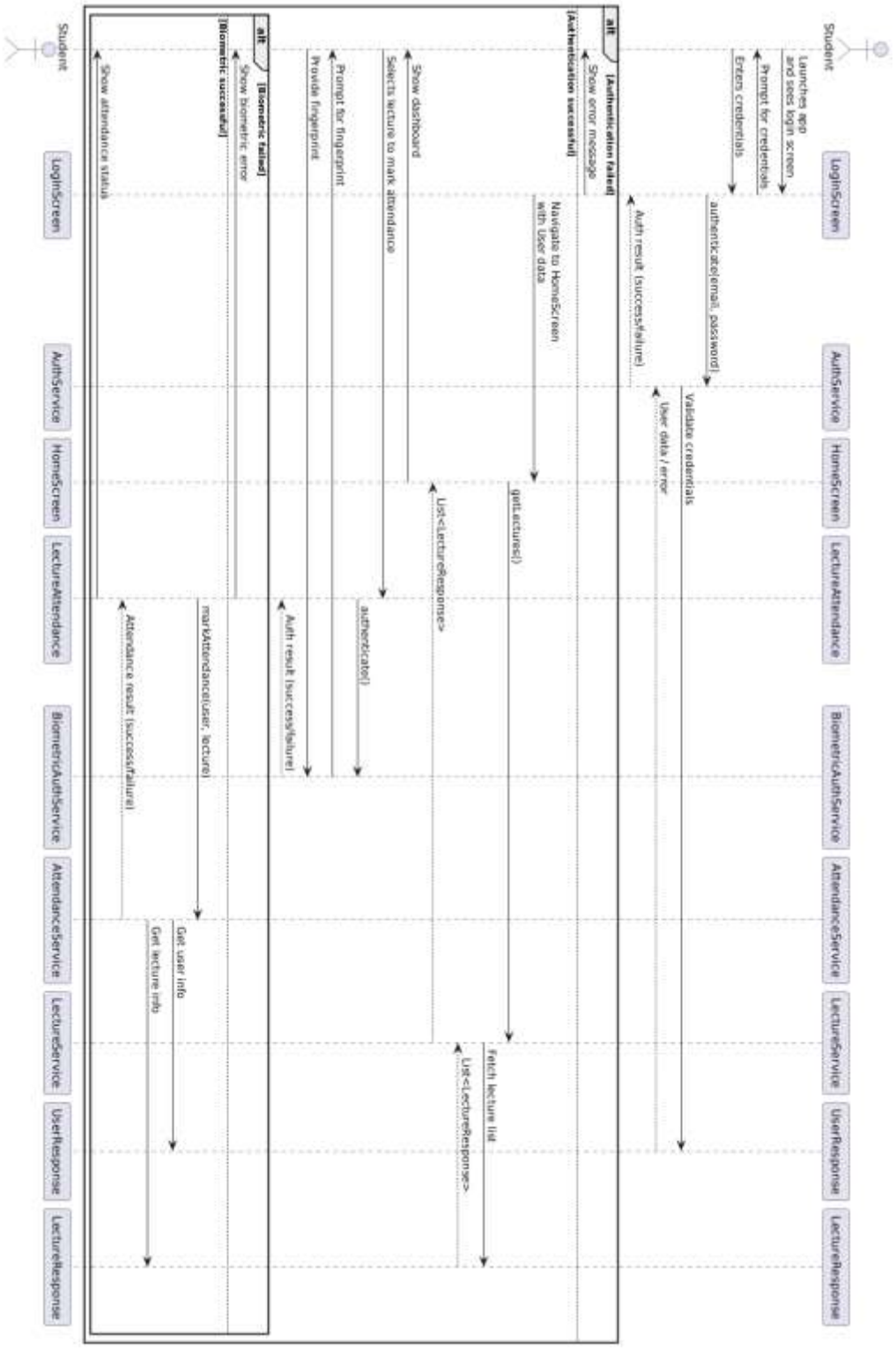

Figure 3.2 Sequence Diagram: Student Login and Attendance Flow

In Figure 3.3 below, the Modern Attendance mobile application is a Flutter-based client used exclusively by students to mark attendance via biometric authentication. It integrates with the

university's Laravel backend system via a secure REST API. All data including student records, lecture schedules, and attendance logs are stored in the central SQL database managed by the Laravel portal.

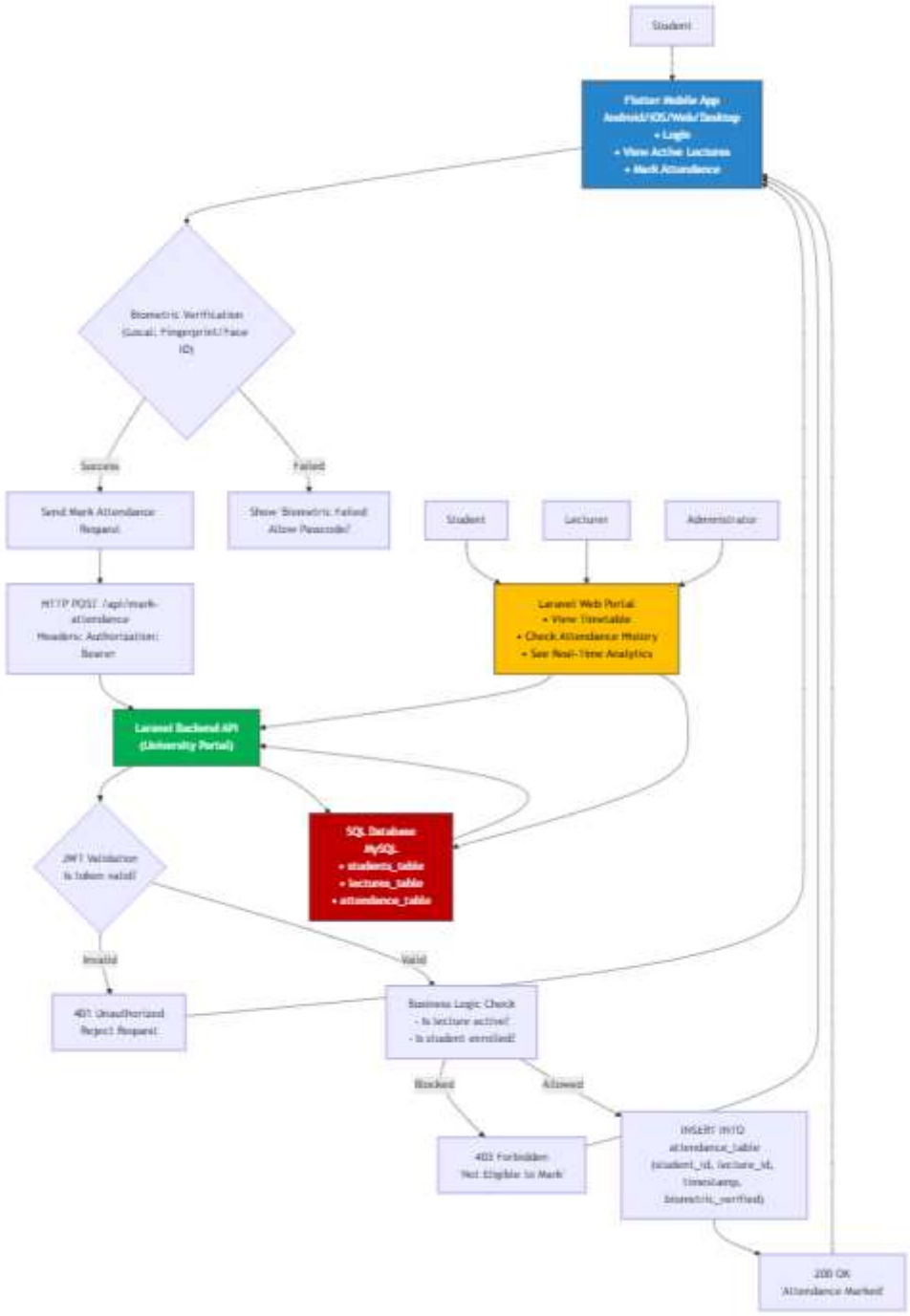

Figure 3.3 System Architecture: Modern Attendance (Integrated with University Portal)

The app executes local biometric verification using the device's fingerprint. Upon successful verification, it sends an authenticated request JSON Web Token (JWT) to the Laravel API, which validates the session and records the attendance upon successful check if the lecture is active and the student is enrolled.

3.4 System Development Methodology

Recommended Methodology: Agile

Why Agile?

- Cross-platform Flutter projects benefit from iterative, feedback-driven development.
- The system has multiple user roles, features, and integrations, making requirements likely to evolve.
- Agile supports continuous delivery, rapid prototyping, and regular stakeholder involvement.

3.4.2 How Agile Would Be Applied

1. Requirements Gathering & Backlog Creation

I. Stakeholder meetings (school admins, staff, students) to gather and prioritize requirements.

II. User stories are written for each feature (e.g., "As a student, I want to mark attendance using my fingerprint").

III. All stories and tasks are added to a product backlog.

2. Iterative Development (Sprints)

I. The team works in 2–3-week sprints.

II. At the start of each sprint, the team selects a set of user stories from the backlog.

III. Daily standups are held to track progress and address blockers.

3. Design & Prototyping

I. UI/UX wireframes are created for new screens and features.

II. Technical design is discussed for new services, models, and integrations.

4. Implementation

I. Developers work on features in small increments, focusing on one user story at a time.

II. Code is committed frequently, with code reviews and pull requests to ensure quality.

III. Automated tests (unit, widget, integration) are written alongside features.

5. Continuous Integration & Deployment

I. CI/CD pipelines automatically build and test the app for all platforms.

II. Early and frequent releases allow stakeholders to test and provide feedback.

6. Review & Retrospective

I. At the end of each sprint, a sprint review is held to demo completed features.

II. A retrospective meeting identifies what went well and what can be improved.

7. Adaptation

I. The backlog is updated based on feedback and changing requirements.

II. The process repeats, with each sprint delivering more value and refining the product.

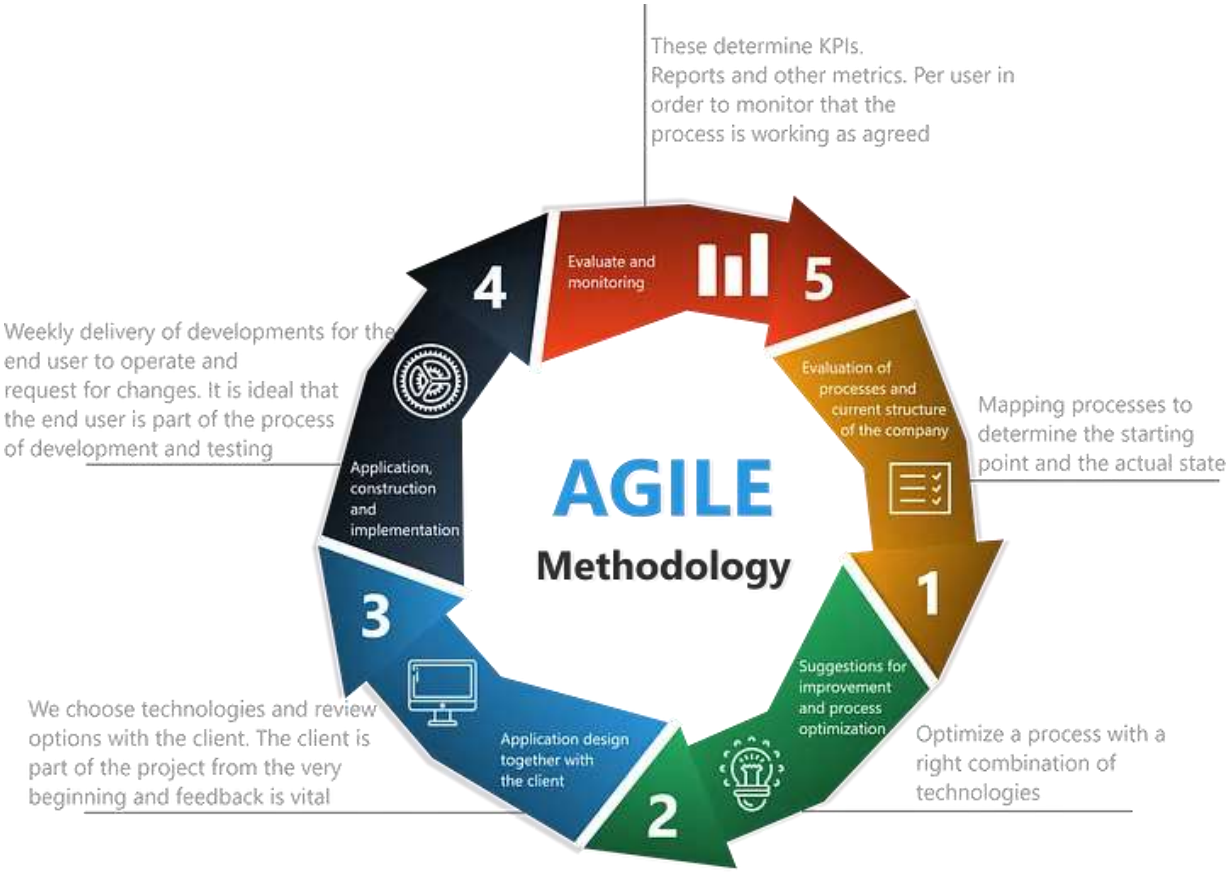

Fig 3.4 The Agile Framework (Abeythilake Udara, 2023)

3.5 Programming Languages and Tools Used

Programming Languages

1. Dart: The entire application logic, UI, and most business logic are written in Dart, the language used by Flutter.

2. Kotlin (Android Native) Acts as the entry point for the Flutter app on Android. Used for platform-specific integrations (e.g., accessing device hardware, biometric sensors).

3. Swift (iOS Native): Entry point for the Flutter app on iOS. Handles platform-specific code and integrations.

4. Objective-C/C++ (macOS, iOS, Windows, Linux): Used for low-level system access, plugin development, and bridging with Flutter.

5. XML: For Android resource files (layouts, styles, manifests).

3.5.2 Development Tools

1. Flutter SDK: The core framework for building, testing, and deploying the app across all platforms.

2. Dart SDK: Provides the Dart language tools, included with Flutter.

3. Android Studio / IntelliJ IDEA / Visual Studio Code: Code completion, debugging, device emulation, integrated terminal, plugin support.

4. Xcode: Required for building and running the app on iOS and macOS.

5. Gradle: A Build system for Android, manages dependencies and build configurations.

6. CocoaPods: Dependency manager for iOS/macOS, used for integrating native plugins.

7. CMake: Build system for desktop platforms (Windows, Linux, macOS).

8. Git: Version control for source code management and collaboration.

3.6 Database Design

The database for the Modern Student Attendance System is designed to efficiently manage information about students, lectures, and attendance records.

The design reflects the mobile-first architectu**re** of the system, where the mobile app serves as the primary interface for students to log in, view lectures, and mark attendance.

Key considerations in the design:

1. **Student-only scope**
    - The system is limited to students; staff/admin roles are managed outside the app.
    - Authentication is student-based, issuing a **token** for mobile app sessions.
2. **Simplified Attendance Workflow**
    - Students log in via the mobile app.
    - They can only mark attendance for lectures they are registered for.
    - Biometric verification may be used during marking, but raw biometric data is not stored.
3. **API-First Structure**
    - Database tables are structured to return data in JSON compatible with the app:
        - Student profile for /student/me
        - Lecture details for /getCourseLecture
        - Attendance confirmation for /markAttendance

3.6.2 Main Entities and Relationships

A. Students

- **Fields:**
    - student_id (PK)
    - lastname
    - othernames
    - email (unique)
    - password_hash
    - matric_number (unique)
    - programme
    - department
    - faculty
    - image (profile photo URL or path)
    - created_at
    - updated_at
- **Notes:**
    - Stores all registered students for authentication and attendance.
    - Replaces generic Users table since the app does not support staff/admin login.
    - Token-based authentication (JWT) is used for mobile access.

B. Lectures

- **Fields:**
    - lecture_id (PK)
    - topic

    - description
    - date
    - start_time
    - end_time
    - duration
    - course_code
    - course_title
    - course_credit_unit
    - course_status (compulsory/elective)
    - lecturer_name
    - lecturer_email
    - lecturer_image
    - created_at
    - updated_at
- **Notes:**
    - Represents a scheduled lecture session.
    - Lecturer info is stored as part of the lecture record for quick API responses.

C. Attendance

- **Fields:**
    - attendance_id (PK)
    - student_id (FK → Students)
    - lecture_id (FK → Lectures)
    - timestamp (when marked)

    - status (present, late, absent, excused)
    - biometric_verified (boolean)
- **Notes:**
    - Records each student’s attendance event.
    - Supports biometric confirmation but does not store raw biometric data.
    - Matches /markAttendance API response used by the mobile app.

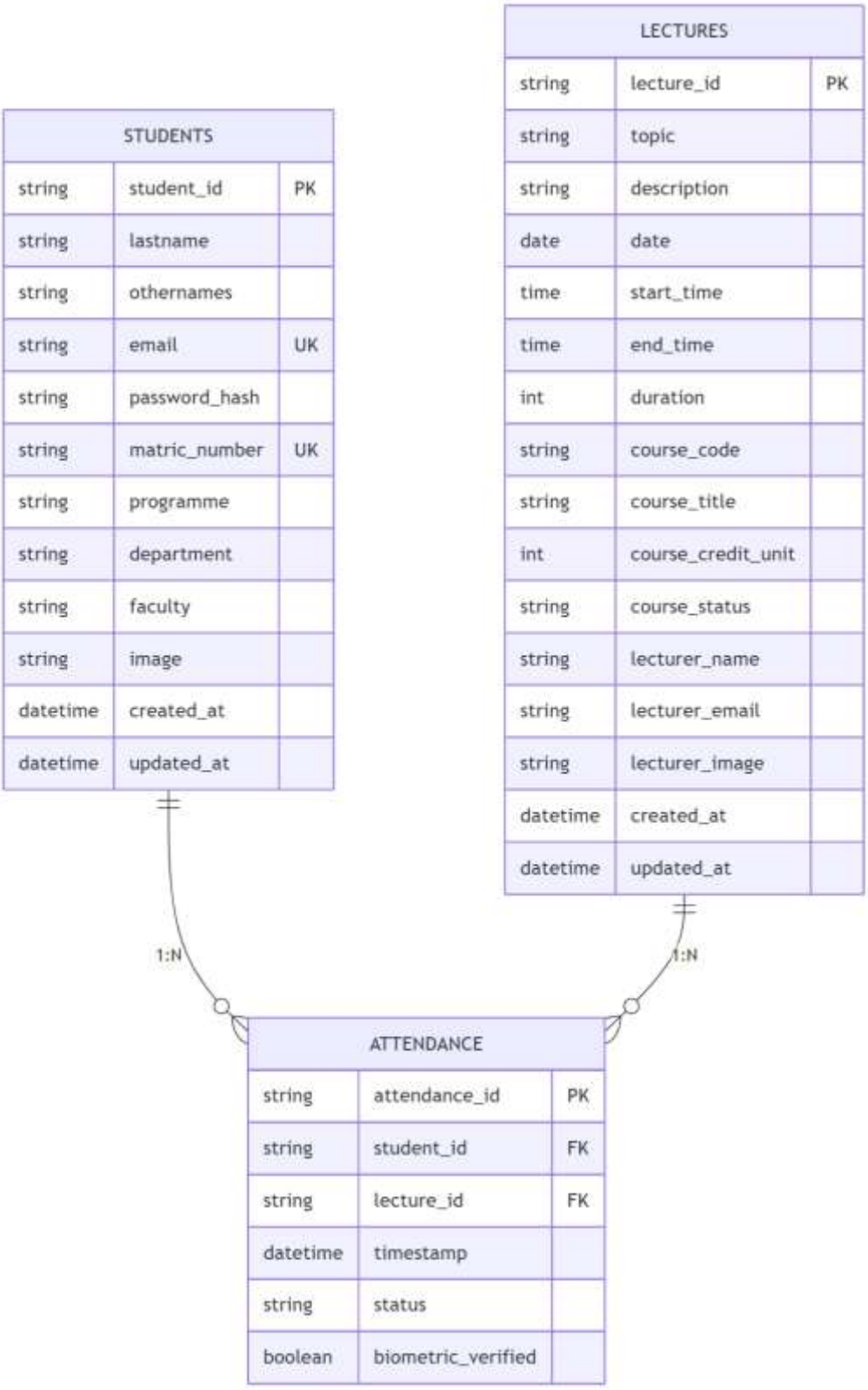

Fig 3.5 Entity-Relationship Diagram for Modern Attendance Database

3.6.3. Design Considerations

1. Normalization:

   The design is normalized to avoid data redundancy and ensure data integrity.

2. Security:

   Passwords are stored as hashes; biometric data is not stored directly, only logs or references.

3. Extensibility:

   New features (e.g., notifications, feedback) can be added with additional tables.

4. Performance:

   Indexes on foreign keys and frequently queried fields (e.g., ` student_id `, `lecture_id`) are recommended.

CHAPTER FOUR

IMPLEMENTATION AND TESTING

4.1 Overview of the overall system development

The development began with identifying the need for a modern, cross-platform attendance management solution for educational institutions. Stakeholders (such as administrators, staff, and students) were consulted to gather requirements, define user roles, and outline key features like biometric authentication, role-based dashboards, and real-time attendance tracking. Flutter is the primary framework for its ability to deliver a single codebase across mobile, web, and desktop platforms.

A modular, layered architecture was adopted, separating the system into presentation (UI), business logic (services), data (models), and platform integration layers. This design ensures maintainability, scalability, and ease of testing.

4.2 System Implementation

How the System was Built

A modular, layered architecture, separating the system into UI components, business logic (services), data models, and platform-specific integrations. An entity-relationship model was created to define tables for users, lectures, attendance, and enrollments.

Flutter was chosen for its ability to deliver a single codebase across Android, iOS, web, and desktop. Dart was used as the primary programming language. Kotlin and Swift were used for native integrations on Android and iOS/macOS, respectively. RESTful API (custom) was

selected for backend communication and data synchronization. This API connects directly with the university's portal.

The app was built in Dart using Flutter, with code organized into components, screens, models, and services. Platform-specific code was added for features like biometric authentication using Flutter plugins and native code.

A REST API was developed or integrated to handle authentication, attendance records, and data storage. Secure communication (HTTPS) and authentication mechanisms were implemented. A relational database (MySQL) was established to store user, lecture, and attendance.

4.3 Screenshots of UI and system workflows

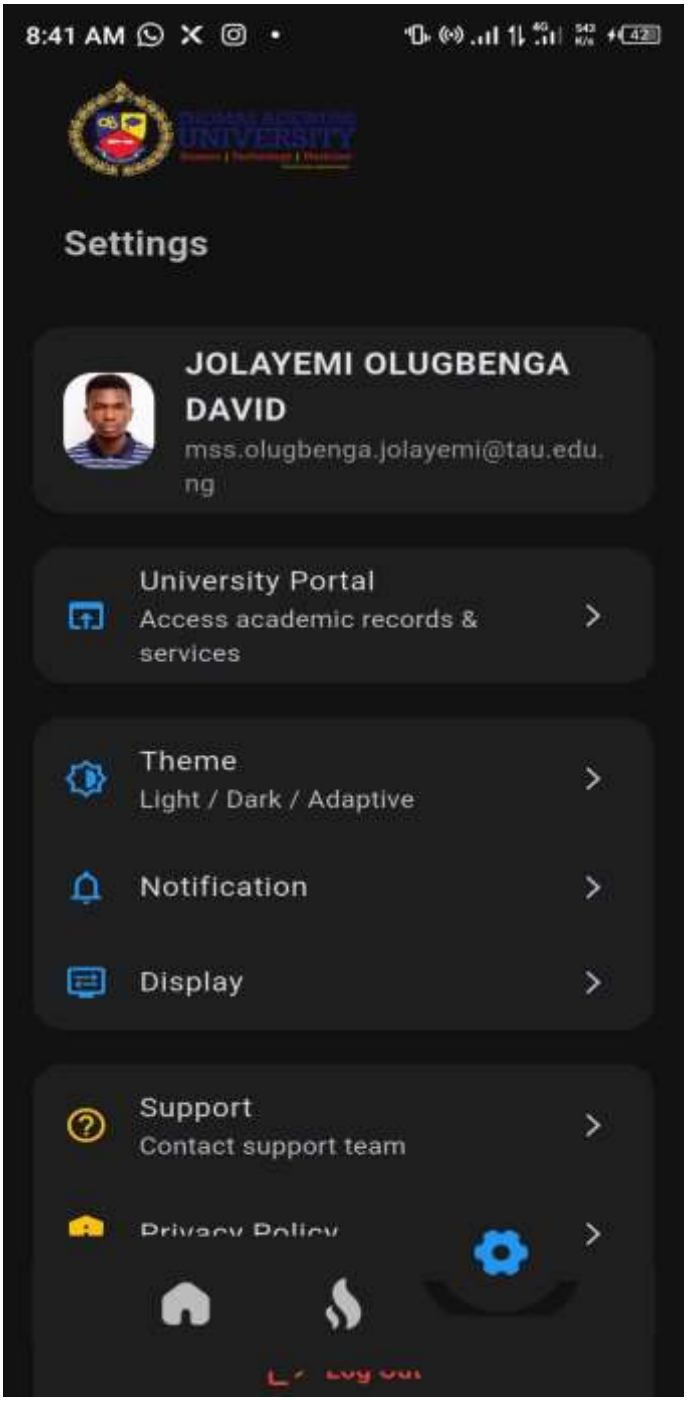

Figure 4.1 Settings Page

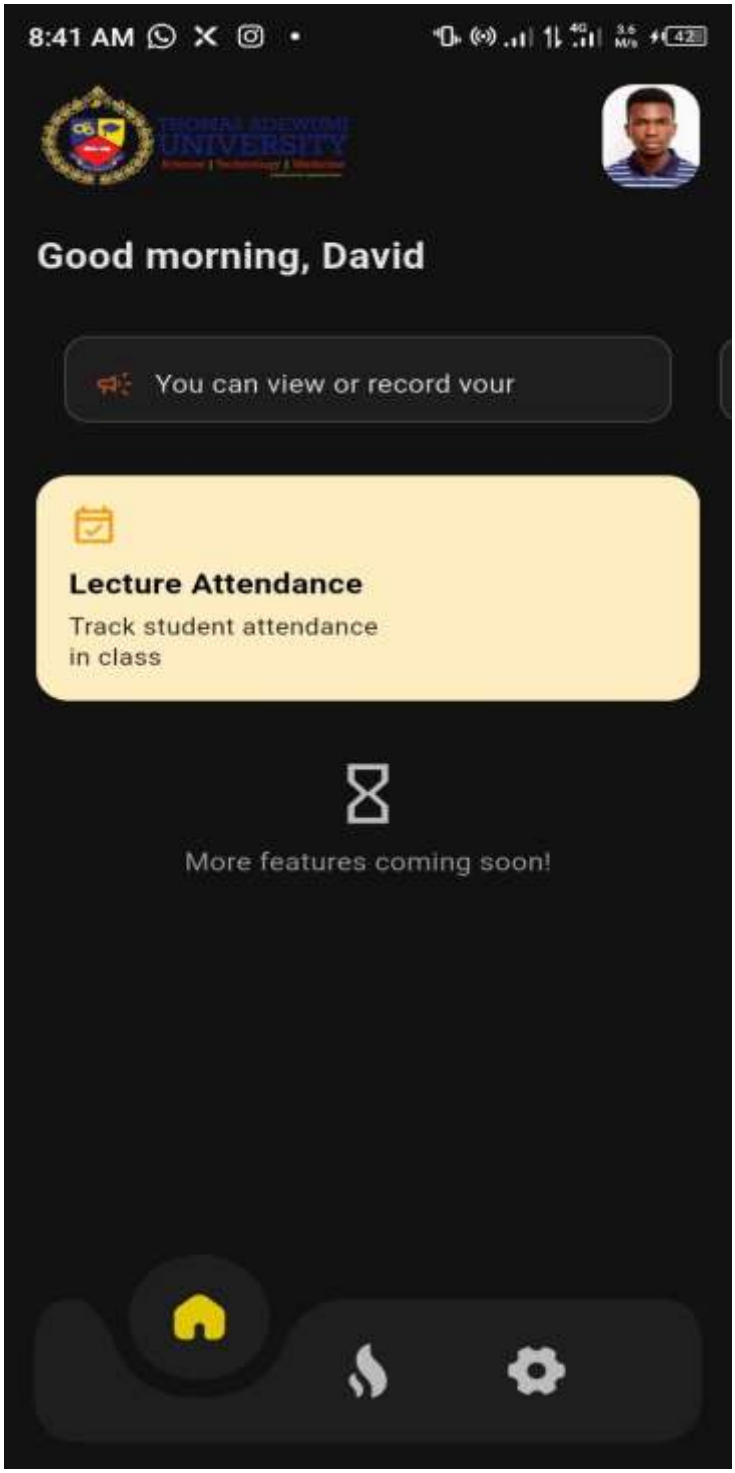

Figure 4.2 Home Page

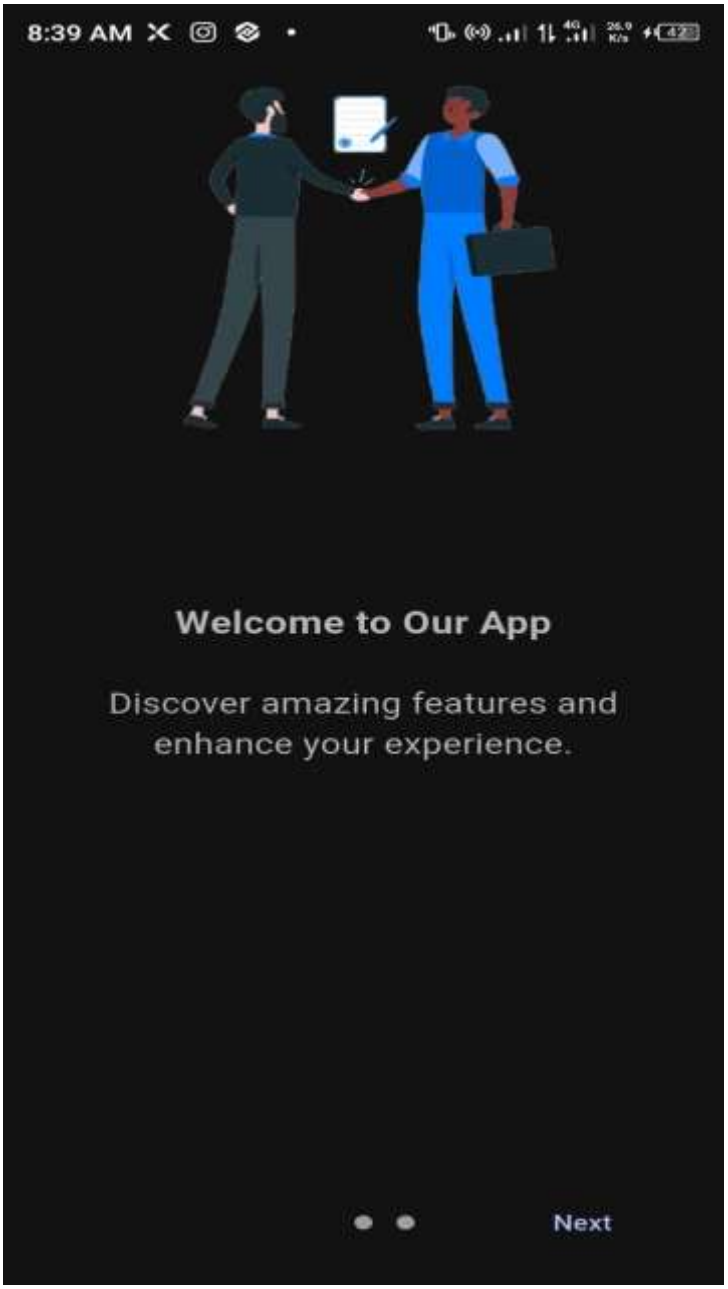

Figure 4.3 Onboarding Page

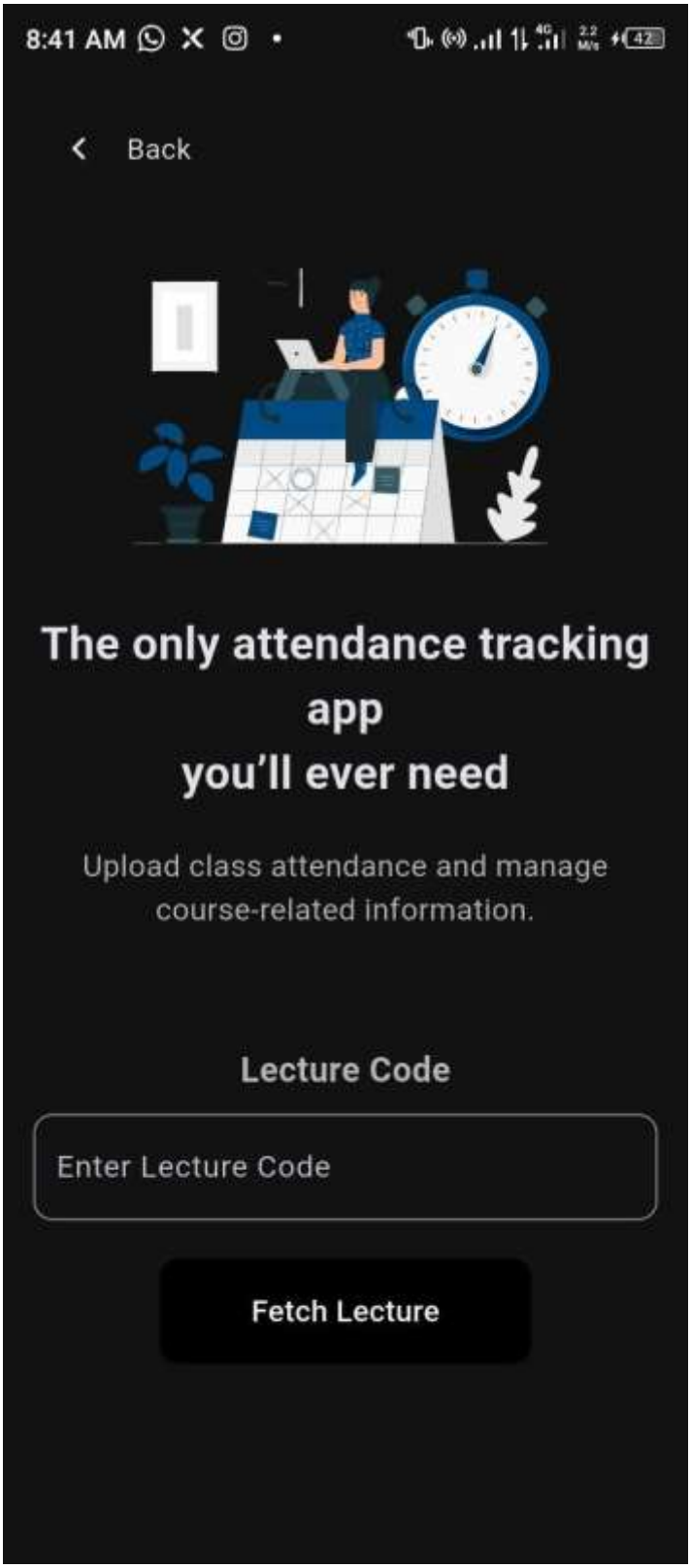

Figure 4.4 Lecture Page

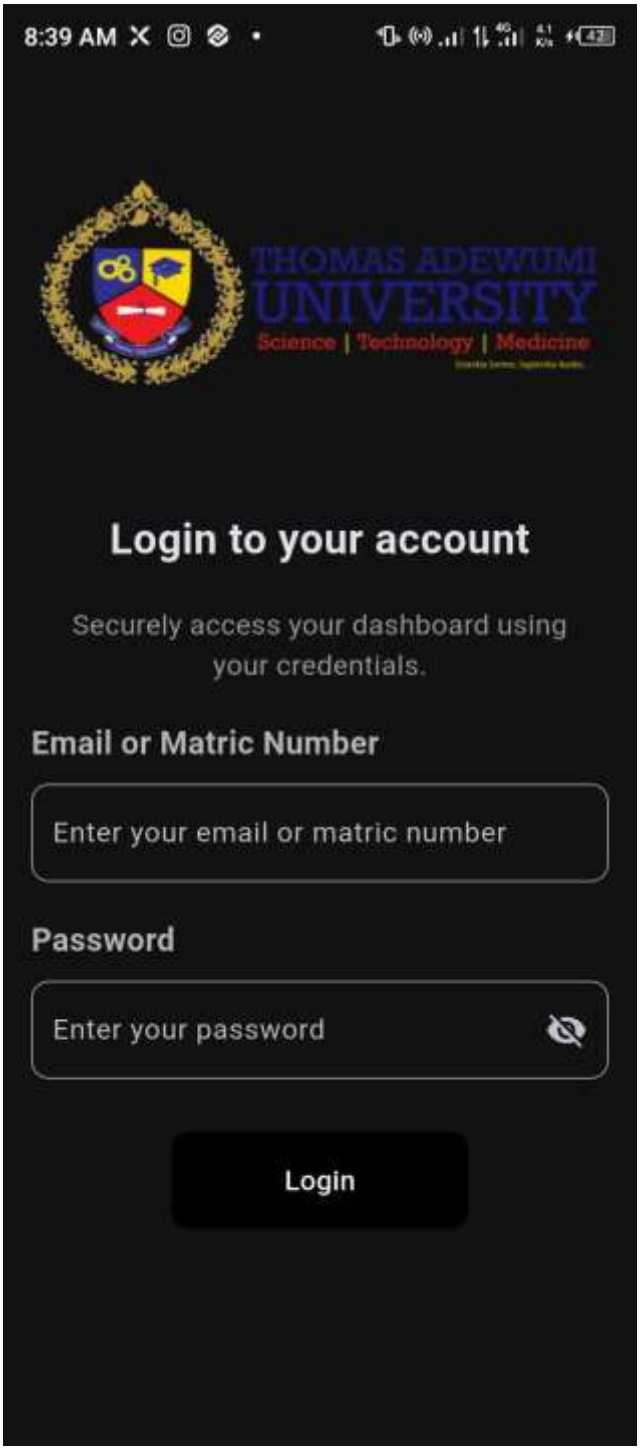

Figure 4.5 Login Page

4.4 Application Manual

4.4.1 Getting Started

1. Launch the app on your device.
2. On first launch, you'll see the onboarding screen, which introduces the user to the application.
3. After the onboarding screen comes the login page.
4. Enter your registered email and password (university portal credentials).
5. Upon successful login, you'll be directed to your dashboard.

4.4.2 User & Features

Student

1. View upcoming lectures and attendance history.
2. Mark attendance using biometric authentication.
3. View personal profile and settings.

Admin

1. Manage users.
2. View system-wide attendance analytics.
3. Configure system settings and permissions.

4.4.3 Common Tasks

Logging In

1. Open the app and enter your credentials.
2. If you forget your password, use the "Forgot Password" link to reset

Marking Attendance (Student)

1. From the dashboard, select the lecture you are attending.
2. Tap “Mark Attendance.”
3. Authenticate using your fingerprint or face.
4. Wait for confirmation. Your attendance is now recorded.

Viewing Attendance Record

1. Students:
    a. Go to “Attendance History” to see your records.

Settings & Preferences

1. Access the “Settings” menu from your dashboard.
2. Change your password, update profile information, or adjust notification preferences.

Logging Out

1. Tap the profile icon or menu.
2. Select “Log Out” to securely exit the application.

4.4.4 Troubleshooting

Cannot log in:

1. Check your credentials.
2. Use “Forgot Password” if needed.
3. Ensure you have a stable internet connection.

Biometric authentication fails:

1. Clean your fingerprint sensor or camera.
2. Try again or use your password if available.

App crashes or freezes:

1. Restart the app.
2. Ensure your device meets system requirements.
3. Update to the latest version.

Attendance not recorded:

1. Ensure biometric authentication is successful.
2. Check for a confirmation message.
3. Contact support if the issue persists.

4.5 Testing and Evaluation

To validate the functionality, performance, and reliability of the Modern Attendance system, a series of targeted tests was conducted. The evaluation focused on core aspects such as biometric authentication accuracy, response time, offline capability, and system security. Testing was performed on real Android devices with fingerprint sensors under varying network conditions to simulate real classroom environments.

The results confirm that the system meets its design objectives: fast, secure, and accurate attendance marking with real-time synchronization across platforms.

Metric	Description	Result
Functional Accuracy	The system only records attendance after valid biometric authentication within active lecture periods.	All test cases passed
Biometric Success Rate	Percentage of successful fingerprint authentications under normal conditions.	97%
Attendance Submission Time	Time from biometric scan to confirmation message.	Avg: 2.1 seconds
Login Response Time	Time from credential submission to dashboard loading.	Avg: 1.9 seconds
Dashboard Load Time	Time taken to render the dashboard post-login.	Avg: 1.7 seconds
Real-Time Sync Delay	Delay between attendance marking and the update on the admin dashboard.	Avg: 3.2 seconds
Offline Attendance Support	Capability to record attendance offline and sync automatically when reconnected.	Fully functional
Concurrent User Handling	System stability when over 10 students attempt attendance marking simultaneously.	No crashes or data loss
Peak Memory Usage	Highest RAM usage during active operation.	124MB
Battery Consumption	Battery usage per hour during continuous use.	3.8%
Data Encryption	TLS 1.3 used for secure communication between app and Laravel backend.	Confirmed

Session Timeout	Auto logout duration after user inactivity.	Logs out after 10 minutes
No Raw Biometric Storage	Ensures no fingerprint images are stored; encrypted templates used locally only.	Privacy-compliant

Table 4.5 Performance Metrics

4.6 Code Snippets

```
import 'package:shared_preferences/shared_preferences.dart';

import '/services/nfc_service.dart';
import '/services/attendance_service.dart';
import '/services/biometric_auth_service.dart';

enum AuthMethod {
  fingerprint,
  nfc,
}

class AttendanceController {
  final _nfcService = NfcService();
  final _studentService = StudentService();

  /// Verifies the user using the selected method and marks attendance for the cached lecture.
```

```
Future<String> verifyAndMarkAttendance({
  required AuthMethod method,
}) async {
  final prefs = await SharedPreferences.getInstance();
  final lectureId = prefs.getInt('cached_lecture_id');

  if (lectureId == null) {
    return 'Lecture ID not found. Please fetch a lecture first.';
  }

  bool verified = false;

  try {
    if (method == AuthMethod.fingerprint) {
      verified = await BiometricAuthService.authenticate(
        reason: 'Authenticate to mark attendance',
      );
      if (!verified) return 'Fingerprint authentication failed.';
    }

    if (method == AuthMethod.nfc) {
      final tagData = await _nfcService.scanTag();

      if (tagData == null || tagData.isEmpty || tagData.contains('NFC scan failed')) {
        return 'Invalid or unreadable NFC tag.';
```

```
        }

        verified = true;
      }

      if (verified) {
        final result = await _studentService.markAttendance(lectureId);
        return result['message'] ?? 'Unknown result.';
      }

      return 'Verification failed.';
    } catch (e) {
      return 'An error occurred: ${e.toString()}';
    }
  }

}
```

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATION

5.1 Summary

The Modern Attendance project followed a structured, iterative development process rooted in Agile methodology. The journey began with comprehensive requirements gathering from key stakeholders (administrators, staff, students) to ensure the system addressed real-world attendance management needs. The team then designed a modular, cross-platform architecture using Flutter and Dart, enabling a single codebase for Android, iOS, web, and desktop. The development cycle included regular sprints, prototyping, stakeholder feedback, and continuous integration/testing. Each sprint delivered incremental features, which were reviewed and refined based on user input and testing outcomes.

A robust, user-friendly attendance management system supporting students, staff, and admins. Biometric authentication for secure, reliable attendance marking. Role-based dashboards and workflows tailored to each user type: real-time attendance tracking and comprehensive reporting features.

5.2 Conclusion

The use of Flutter enabled deployment across all major platforms from a unified codebase. Users can access the system on their preferred devices, increasing reach and convenience. The system integrates biometric authentication (fingerprint/face) for students, ensuring that attendance is both secure and verifiable. This reduces the risk of proxy attendance and increases trust in the records.

The application delivers distinct interfaces and features for each user role, such as attendance marking for students, enrollment and record management for staff, and analytics for admins. This enhances usability and ensures users have access to the tools they need.

Attendance data is updated in real time, and users can view up-to-date records and analytics. Staff and admins can generate reports, monitor trends, and make informed decisions. The modular architecture, clean codebase, and thorough documentation make it straightforward to add new features, support more users, or integrate with other systems in the future.

5.3 System Improvements and Enhancements

1. Biometric Authentication Significantly Reduces Proxy Attendance

   Integrating fingerprint/face authentication directly into the attendance process led to a measurable decrease in fraudulent or proxy attendance, a common issue in traditional systems.

2. Cross-Platform Consistency Improves User Engagement

   Providing a unified experience across mobile, web, and desktop platforms increased user adoption and satisfaction, as users could access the system from any device without loss of functionality.

3. Real-Time Data Access Empowers Staff and Admins

   The immediate availability of attendance data and analytics enabled faster decision-making and more proactive interventions for absenteeism.

4. Real-Time Analytics and Reporting:

Attendance data is processed and visualized in real time, with dashboards and exportable reports.

5. Enhanced Security and Privacy

   Sensitive data (like passwords) is securely hashed, and biometric data is never stored directly only authentication results or logs are kept.

5.4 Limitations

1. Hardware-dependent reach

The app needs a built-in fingerprint reader or high-quality camera; many low-end Android handsets, desktops and some web clients lack either, forcing external scanners that Flutter currently supports only through niche or custom drivers.

This caps adoption in “bring-your-own-device” scenarios unless fallback PIN/QR options are added.

2. Vulnerability to spoofing & liveness gaps

Commodity sensors can be fooled by presentation attacks (e.g., silicone fingers), and liveness detection is still an active research area with varying accuracy across devices

Until all target devices expose certified PAD (Presentation-Attack-Detection) APIs, residual risk remains.

3. Environmental & physiological failure modes

Damp, scarred or dusty fingers as well as worn ridges in manual-labor populations raise false-reject rates; poor lighting similarly affects face recognition.

This can prolong queue times and drive users to manual overrides, eroding biometric benefits.

4. High regulatory and privacy burden

Biometric templates are “special-category” data under GDPR, demanding explicit consent, purpose limitation and rapid deletion on request; mis-steps have triggered enforcement notices and fines (e.g., Serco Leisure and HMRC Voice ID cases)

Compliance work DPIAs, consent logs, retention policies adds overhead that smaller institutions may struggle to resource.

5. Offline & sync fragility

Although events queue locally, prolonged network outages or mis-configured endpoints still lead to missed punches and labor-intensive reconciliations

Field evidence shows that troubleshooting offline devices often requires on-site resets or manual log exports, offsetting some of the intended efficiency gains.

5.5. Future Work

1. Advanced Biometric and Authentication Research

A. Explore new biometric modalities:

   Investigate the integration of face, iris, or voice recognition for attendance, and compare their effectiveness and user acceptance with fingerprint authentication.

B. Continuous authentication:

   Research methods for passive or continuous authentication during lectures to further reduce proxy attendance.

2. Artificial Intelligence and Predictive Analytics

A. Absenteeism prediction:

   Develop machine learning models to predict students at risk of chronic absenteeism, enabling early interventions.

B. Behavioral analytics:

   Analyze attendance patterns to identify trends, correlations with academic performance, or potential well-being issues.

3. Integration with External Systems

A. Learning Management Systems (LMS):

   Research seamless integration with popular LMS platforms (e.g., Moodle, Canvas, Google Classroom) for unified academic management.

B. Institutional ERP/HR systems:

   Enable data exchange with HR or ERP systems for staff attendance and payroll automation.

4. Privacy, Security, and Compliance

A. Privacy-preserving biometrics:

   Investigate secure, privacy-preserving biometric storage and matching (e.g., on-device processing, homomorphic encryption).

B. Compliance research:

   Study and implement compliance with global data protection regulations (GDPR, FERPA, etc.).

5. Enhanced Offline and Edge Capabilities

A. Edge computing:

   Research the use of edge devices for local attendance processing and syncing, reducing reliance on constant internet connectivity.

B. Robust offline support:

   Develop more resilient offline features, including conflict resolution and data integrity checks.

6. Hardware Innovations

A. IoT classroom devices:

   Investigate the use of IoT sensors for automated, contactless attendance.

REFERENCES

Abeythilake Udara, U. (2023, May 22). *Agile methodology*. Medium. https://medium.com/@abeythilakeudara3/agile-methodology-106270809c99

Adeyemi, A. O., Abiodun, O., & Oyekunle, O. (2019). A review of attendance management systems: Challenges and prospects. *International Journal of Computer Science and Applications, 16*(2), 45–53.

Afolabi, O. R., Ojo, S. A., & Ige, A. B. (2020). Mitigating attendance fraud in Nigerian universities using biometric authentication. *African Journal of Computing and ICT, 13*(1), 78–89.

Ajayi, O. T., Olatunbosun, A. J., & Bello, K. O. (2016). Fingerprint biometric system for student attendance monitoring in higher institutions. *Journal of Engineering and Applied Sciences, 24*(3), 112–119.

Ajayi, O. T., Olatunbosun, A. J., & Bello, K. O. (2018). Fingerprint biometric system for student attendance monitoring in higher institutions. *Journal of Engineering and Applied Sciences, 24*(3), 112–119.

Al-Khaldi, A., Alzahrani, M., & Adnan, M. (2020). Student attendance management system based on biometric fingerprint authentication. *International Journal of Advanced Computer Science and Applications, 11*(5), 294–298. https://doi.org/10.14569/IJACSA.2020.0110537

Automated Attendee Recognition System for Large-Scale Social Events. (2025). *arXiv preprint*.

Babalola, J. T., & Adedeji, O. A. (2021). Digital transformation in higher education: Adoption of biometric attendance systems. *IEEE Xplore*. https://ieeexplore.ieee.org/document/9624773

Bañeres, D., Rodríguez, M. E., Guerrero-Roldán, A. E., & Karadeniz, A. (2020). An early warning system to detect at-risk students in online higher education. *Applied Sciences, 10*(13), 4427. https://doi.org/10.3390/app10134427

Bansal, A., Sharma, R., & Singh, A. (2021). Smart attendance management system using RFID and biometric technology. *International Journal of Engineering Research and Technology, 10*(6), 231–237. https://www.ijert.org/research/smart-attendance-management-system-using-rfid-and-biometric-technology-IJERTV10IS06021.pdf

CyberLink. (2024). *FaceMe® security: Facial recognition for access control*. https://www.cyberlink.com/products/faceme/

Daon. (2024). *The ethics and concerns of biometric data collection*.

EPAY Systems. (2024). *Cloud-based time and attendance tracking software reduces labour costs by 5%*.

Exact Comms. (2025). *What is real-time attendance tracking?* https://www.exactcomms.com

Frontiers in Big Data. (2024). *Ethical implications of facial recognition systems: Balancing innovation and rights*. https://www.frontiersin.org/articles/10.3389/fdata.2024.1337465/full

Google. (2025a). *Flutter documentation*. https://flutter.dev

Google. (2025b). *Dart programming language*. https://dart.dev

Harvard Business Review. (2025). *The risks of collecting employees' biometric data*.

Human Rights Research Hub. (2025). *The cost of convenience: Biometric data collection and privacy*.

IBM. (2025). *What is an API?* https://www.ibm.com/cloud/learn/api

IEEE. (2016). *IEEE Standard for Software Verification and Validation (IEEE Std 1012-2016).*

Innovatrics. (2025). *Understanding biometric templates*. https://www.innovatrics.com

Interaction Design Foundation. (2016). *User interface (UI) design*. https://www.interaction-design.org/literature/topics/user-interface-design

International Organization for Standardization. (2022). *ISO/IEC 35237:2022 — Biometric system performance testing and reporting — Principles and framework.*

ISO. (2015). *ISO/IEC 2382:2015 – Information technology — Vocabulary*.

Khan, S., Bhat, R., & Saeed, K. (2020). NFC-based attendance management system. *Journal of Information Technology and Software Engineering, 10*(1), 32–40.

Laravel LLC. (2025). *Laravel documentation*. https://laravel.com

Makinde, S. O., Sulyman, B. M., & Ibrahim, A. (2024). Beyond borders: Leveraging technology to achieve Sustainable Development Goals in education. *International Journal of Universal Education, 2*(2), 90–100. https://doi.org/10.33084/ijue.v2i2.8586

Mokhtar, A. A., Mohd Ali, M. A., & Abd Rahman, N. A. (2021). The effectiveness of RFID-based attendance management system: A study at higher learning institution. *International Journal of Emerging Technologies in Learning, 16*(14), 142–154. https://doi.org/10.3991/ijet.v16i14.21369

NIST. (2023). *Digital identity guidelines (SP 800-63-3)*. https://pages.nist.gov/800-63-3

NIST. (2025). *International Face and Fingerprint Performance Conference (IFPC 2025) – Agenda and proceedings*.

Nkata, A. S. (2024). Strengthening of students' class attendance using biometric authentication system to enhance delivery of competence-based quality education. *The Journal of Informatics, 4*(1), 187–202. https://doi.org/10.59645/tji.v4i1.231

Nwosu, P. C., & Adebayo, T. A. (2022). The role of digitalization in sustainable university practices. *Global Environmental Health Journal*. https://www.tandfonline.com/doi/abs/10.1080/17441692.2022.2043948

Obiora, G. N., Nwankwo, C. K., & Eze, P. A. (2025). Development of a fingerprint-based attendance monitoring system. *African Journal of Engineering Research and Development, 8*(1), 263–270.

Odesoba, O., & Israel, J. (2025). A fingerprint-based attendance system for improved efficiency. *Journal of Biometrics and Applications, 7*(2), 88–101.

Oloyede, M. O., & Omojokun, O. T. (2013). Fingerprint authentication for improved attendance monitoring in Nigerian universities. *Nigerian Journal of Computer Science, 11*(1), 45–52.

Oloyede, M. O., & Omojokun, O. T. (2016). Fingerprint authentication for improved attendance monitoring in Nigerian universities. *Nigerian Journal of Computer Science, 14*(1), 23–30.

peopleHum. (2025). *What is attendance management?* https://www.peoplehum.com/glossary/attendance-management

Savitha, S. A., Kumar, R., & Devi, S. (2025). Biometric attendance system based on fingerprints. *Journal of Scholastic Engineering Science and Management, 4*(5), 69–73.

Sedona Conference Working Group 11. (2024). *U.S. biometric systems privacy primer*.

TCW Global. (2025, April 1). *International biometric data laws: A compliance overview*. https://www.tcwglobal.com/blog/international-biometric-data-laws-compliance-overview

The Guardian. (2024, February 23). *Serco ordered to stop using facial recognition technology to monitor staff*.

TimeTrex. (2024, May 6). *The top ways to reduce buddy punching in 2024*. https://www.timetrex.com/blog/top-ways-to-reduce-buddy-punching-in-2024/

Truein. (2024, March 31). *Eight disadvantages of fingerprint attendance systems*. https://www.truein.io/blog/eight-disadvantages-of-fingerprint-attendance-systems/

Yuan, C., & Xu, Z. (2024). An interpretable Siamese attention Res-CNN for fingerprint spoofing detection. *IET Biometrics*.