UCS503 Software Engineering Project Report
B.E. Third Year COE
Group:- 3C43
Team Alpha

Members:

Dron Garg –	102303583
Aryan Singla –	102303586
Lakshya Arora –	102303591
Mannan Jain –	102303593

THAPAR INSTITUTE
OF ENGINEERING & TECHNOLOGY
(Deemed to be University)

Submitted to :-

Dr. BRAHMADESAM
VENKATARAMAIYER R

Dated:-3/10/2025

ABLE OF CONTENTS

Software Bid/ Project Teams

UCS 503- Software Engineering Lab

Group : 3C43_____ Dated: 3/10/2025

Team Name:
Alpha:

Please enter the names of your Preferred Team Members. :

- You are required to form **a three to four person** teams
- Choose your team members wisely. You will not be allowed to change teams.

Name	Roll No	Project Experience	Programming Language used	Signature
Dron Garg	102303583	Null	C++/python/ML/JAVASCRIPT	Dron
Aryan Singla	102303586	Null	HTML/CSS/ReactJS	Aryan
Lakshya Arora	102303591	Null	C++/IOT/JavaScript/Python	Lakshya
Mannan Jain	102303593	Null	C++/Flutter/Dart/Python	Mannan

Choices of Projects:
Please select **4 projects** your team would like to work on, by order of preference: *[Write at-least one paragraph for each choice (motivation, reason for choice, feasibility analysis, etc.)]*

	Project Name	Unique Selling Point
First Choice	College ID-Based Attendance System	A system that uses barcode scanning of student ID cards to automatically record attendance, reducing manual effort and ensuring accuracy.
Second Choice	University Student Marketplace Platform	An online platform where students can easily buy and sell used items like books, calculators, and furniture within the university community.
Third Choice	University Society Recruitment and Events Portal	An online portal where students can view open recruitments for societies, apply using stored personal information, and stay updated on upcoming society events.
Fourth Choice	Campus Placement Info and Application Platform	A centralized web portal that provides students with up-to-date placement information, application forms, deadlines, and auto-filled forms using pre-stored student data.

Additional Remarks/ Inputs

Please tell us about any other factors that we should take into consideration (e.g., if you really would like to work on a project for some particularly convincing reason).

Problem Statement

The current methodologies for managing student attendance—both manual and basic electronic—suffer from critical, interlocking deficiencies that erode operational efficiency and academic integrity. The need for a modernized solution is immediate and pressing.

The Failure of Current Systems

1. Manual Marking: Operational Cost and Data Risk

Traditional manual attendance (roll calls) is inefficient and fundamentally flawed, consuming valuable resources and introducing high risk:

- **Time Loss:** Current methods **consume significant lecture time** (an estimated **10-15 minutes of valuable teaching time lost per lecture**)
- **Data Reliability:** Manual processes are **prone to human error**, which leads to **inaccurate and unreliable attendance records**. These errors compromise the integrity of institutional data and negatively impact administrative decisions.

2. Single-Factor Systems: The Proxy Fraud Vulnerability

Any system relying on a **single physical credential** for authentication—such as an ID card, key fob, or simple QR code—suffers from a fundamental security flaw that directly enables academic misconduct.

- **The Problem of Proxy:** The core vulnerability is the **shareability of the physical credential**. Because **Student ID cards can be easily shared or borrowed**, a high volume of **proxy attendance** is facilitated. This allows students to register as present without ever physically attending the lecture.
- **The Failure to Verify:** These single-factor systems offer **No Verification of Physical Presence**. They lack the robust, critical mechanism required to confirm that the individual presenting the credential is the legitimate student on record.
- **Integrity Risk:** This fraudulent activity directly **undermines academic honesty** and compromises student fairness. The integrity of all recorded attendance data is immediately rendered unreliable.

Conclusion: The SmartAttend Mandate

Current methodologies are inefficient, consume significant lecture time, and are highly vulnerable to academic misconduct, compromising data integrity

The **SmartAttend system** aims to mitigate these deficiencies by providing **verifiable student presence** and streamlining administrative tasks through a **Dual-Verification** approach.

Proposed Solution

The **SmartAttend Dual-Verification Attendance System** is the solution designed to eliminate the critical issues of proxy attendance, data inaccuracy, and time loss inherent in current methodologies. Its **Core Objective** is to modernize the attendance process through an automated, secure, and user-friendly system that eliminates fraud whilst respecting student privacy.

1. System Workflow: How SmartAttend Works

SmartAttend replaces manual roll calls and vulnerable single-factor scans with a rapid, secure, four-step verification process, achieving a processing speed of under **4 seconds per student**.

A. Student Enrollment & Verification

The process begins when the student arrives at the classroom or lecture hall:

1. **Student Arrives:** The student approaches the SmartAttend station (equipped with a scanner and camera).
2. **Scan ID & Face:** The student simultaneously **scans their ID card** (via the Barcode Module) and looks at the **high-resolution camera** (for Facial Verification).
3. **Dual-Match Confirmation:** The system instantly verifies two things:
   - **Credential Check:** Is the ID card valid?
   - Identity Check: Does the face match the encrypted biometric record for that ID? The system only records attendance if both checks pass, ensuring 100% authentication and eliminating proxy attendance.
4. **Record Attendance:** Attendance is instantly confirmed, timestamped, and secured in the central PostgreSQL database.

B. Faculty Access and Data Management

Faculty gain immediate access to clean, real-time data, freeing them from administrative burdens:

- **Real-Time Dashboard Access:** Faculty can access a secure web interface to view the attendance record for their current and past classes **in real-time**.
- **Actionable Insights:** This access allows faculty to identify students who are nearing the minimum attendance threshold, enabling **proactive intervention** instead of reactive reporting.
- **Zero Manual Effort:** The system eliminates the need for faculty to manually mark, collect, or upload attendance sheets, contributing to the projected **52% reduction in attendance verification time**.

Need Analysis

The design and justification of the SmartAttend Dual-Verification Attendance System are driven by a comprehensive analysis of needs across all critical institutional stakeholders: students, faculty, and administrators. Current attendance methodologies fail each group in distinct ways, creating a universal mandate for an integrated, secure, and efficient solution.

The primary objective is to **Modernise the attendance process through an automated, secure, and user-friendly system that eliminates fraud whilst respecting privacy**.

---

1. Student Needs and the Requirement for Fairness

Students are the end-users of the system, and their primary requirements revolve around **academic fairness, minimal disruption, and personal data protection**. The existing system severely compromises these needs:

A. Academic Fairness and Integrity (Integrity Risk)

Students require an assurance that the academic environment is honest. When proxy attendance is rampant, it fundamentally undermines the value of hard work and regular attendance for compliant students.

- **Verifiable Attendance:** Students need a system that ensures their accurate, verifiable attendance is recorded instantly and reliably, eliminating any risk of manual data error.
- **Fair Competition:** Proxy fraud erodes **Student Fairness** by allowing non-attending peers to achieve minimum attendance thresholds. The SmartAttend system directly addresses this by providing the **high prevalence of proxy attendance undermines academic honesty**.

B. Speed and Minimal Disruption (Time Loss)

Students' time during a lecture is dedicated to learning, and they require administrative tasks to be completed as quickly as possible.

- **Elimination of Wait Time:** Students are currently forced to wait while **10-15 minutes of valuable teaching time is lost per lecture** due waiting for manual roll calls or standing in line for slow single-factor systems.
- **High Throughput:** The system must ensure rapid processing to maintain class flow. SmartAttend is designed for a target processing time of under **4 seconds per student**, plus a 2-second buffer, ensuring minimal disruption to the class schedule.

C. Data Privacy and Ethical Use

As a biometric system, student trust hinges on responsible data handling. Students require transparency and compliance with the highest ethical standards.

- **Privacy-First Design:** Students need assurance that sensitive biometric data is protected. SmartAttend meets this by using a **Privacy-First Design** where **Mathematical embeddings replace photograph storage**, making the system ethically sound and GDPR-compliant. Raw images are not stored, minimizing the risk footprint.
- **Clear Policies:** Students require clear, transparent policies on how their attendance data is used, stored, and eventually deleted, fostering a culture of trust between the institution and its student body.

---

2. Faculty Needs and the Requirement for Efficiency

Faculty are the direct daily users of the attendance system and require tools that enhance their efficiency and accuracy in their core role: teaching.

A. Reclaiming Instructional Time (Faculty Efficiency)

Faculty are currently burdened by administrative overhead that diminishes teaching capacity.

- **Time Savings:** The most urgent faculty need is to eliminate the **Wasted time on repetitive tasks** associated with attendance management. By automating the process, SmartAttend aims to achieve a projected **52% reduction in attendance verification time** (Feasibility Study Data), allowing the instructor to reclaim the 10-15 minutes per lecture currently lost.
- **Focus on Pedagogy:** Faculty members need to focus their energy on course delivery and student engagement, not on manual data entry and managing attendance disputes. The automated, hands-off nature of SmartAttend meets this need.

B. Absolute Data Accuracy (Data Accuracy)

Faculty rely on attendance data to correlate with performance, assign grades, and comply with reporting requirements.

- **Reliable Records:** They need records that are guaranteed accurate and free from human error. The current methods compromise data integrity, as **Errors compromise institutional decisions**.
- **Immediate Access:** Faculty need real-time dashboards to view attendance trends and identify students at risk of falling below the minimum threshold, enabling proactive intervention rather than reactive reporting.

3. Administrative and Institutional Needs

The administration and the institution as a whole require a system that safeguards operational integrity, enables strategic decision-making, and ensures legal compliance.

A. Data Integrity and Operational Control

The highest administrative need is eliminating fraud and securing the integrity of institutional records.

- **Elimination of Proxy Fraud:** The **High prevalence of proxy attendance** creates **Integrity Risk** for the entire institution. The dual-verification methodology—which ensures **No Verification** failure by requiring both credential and identity—is the only way to establish reliable records.
- **Actionable Data:** Administrators require highly reliable attendance data to track student engagement, correlate it with academic success, and inform resource allocation decisions. SmartAttend's automated, centralized data stream is key to this.

B. Compliance and Strategic Positioning

Institutions must meet legal obligations and maintain a competitive edge.

- **Auditing and Compliance:** Accurate attendance data is critical for **compliance with auditing requirements** and reporting to government bodies and funding agencies. Automating data collection and reporting streamlines this compliance, **fostering greater trust and operational integrity**.
- **Innovation Leadership:** Adopting an advanced solution like SmartAttend demonstrates the institution's commitment to **innovation and technological leadership**. This forward-thinking stance **attracts prospective students and faculty**, providing a competitive edge in the educational market.

By addressing the distinct yet interconnected needs of these three stakeholder groups, the SmartAttend system provides not just an attendance solution, but a strategic investment in academic integrity, operational efficiency, and institutional excellence.

Comprehensive Feasibility Analysis

This report section details the feasibility of the SmartAttend Dual-Verification Attendance System across technical, operational, and economic dimensions, demonstrating its viability for full institutional deployment.

Technical Feasibility Assessment

Technical feasibility evaluates the availability of hardware, software, and necessary technical skills to implement the SmartAttend system successfully. The analysis concludes the project is **highly technically feasible**, relying on mature, established, and scalable technologies.

1.1 Dual-Verification Architecture

The system's core viability is based on combining two distinct layers of authentication in parallel, ensuring **100% authentication assurance** and effectively neutralizing the threat of proxy attendance.

1.1.1 Barcode Scanning Module

This component handles the rapid identification of the student credential.

- **Technology:** Utilizes standard, commercially available **2D barcode scanners** compatible with common university ID formats (e.g., Code 39 or QR codes).
- **Performance:** Barcode processing must be near-instantaneous, contributing minimal latency. The goal is **50–100 scans per minute** per station.

1.1.2 Biometric Facial Verification

This module provides the critical security layer by confirming the identity of the person presenting the card.

- **Technology:** Integrates **high-resolution webcams** strategically positioned to capture the student's face. Processing relies on specialized **Machine Learning (ML) facial recognition libraries** (e.g., based on deep learning architectures).
- **Process:** The ML model extracts mathematical representations (**embeddings**) of the face, comparing this vector against the stored, encrypted vector linked to the scanned student ID.
- **Performance:** The core technical requirement is high accuracy, with a specified target of **98% accuracy** for the facial recognition algorithm.

1.2 Software and Data Architecture Stack

The solution requires a robust, scalable, and secure software environment designed for high-volume transactions:

Layer	Technology/Component	Rationale
Frontend (User Interface)	Secure Web Dashboard (e.g., React/Angular)	Provides faculty and administrators with **real-time access** to attendance data and configuration.
Backend/API	Node.js or Python Backend Framework	Manages all API requests, controls hardware I/O, performs verification matching, and handles secure data logging, favoring **asynchronous handling** for concurrency.
Biometric Processing	Specialized ML Libraries	Manages complex feature extraction from the live camera feed and the distance calculation between the captured and stored embeddings.
Database	**Encrypted PostgreSQL Database**	Chosen for high reliability, transactional integrity, and **scalability**, essential for managing high-volume, sensitive attendance records.

1.3 Performance and Scalability Requirements

For institutional adoption, the system must maintain high throughput to avoid bottlenecks during peak entry times:

- **Processing Speed Goal:** The end-to-end verification process (scan + capture + match + record) must be completed in **under 4 seconds per student**, with an additional **2 seconds buffer** for student transition.
- **Scalability Design:** To accommodate large cohorts (e.g., 150 students), the design mandates the deployment of **three concurrent, parallel SmartAttend stations** at entry points. This configuration allows for the rapid processing of a large class, successfully reclaiming the 10–15 minutes previously lost to manual methods.
- **Concurrency:** The backend must be specifically engineered to handle multiple simultaneous verification attempts across all deployed stations without latency degradation.

Operational Feasibility Assessment

Operational feasibility confirms the system can be successfully integrated, used, and maintained within the institution’s existing environment and policies without creating undue burden.

2.1 System Workflow and Process Integration

The system’s workflow is designed to maximize ease of use for students and eliminate manual tasks for faculty.

2.1.1 Student Verification Workflow

The process is simple, requiring minimal training:

1. **Approach & Action:** The student simultaneously **scans their ID card** and presents their face to the **camera**.
2. **Result:** Upon successful **Dual-Match**, a confirmation is displayed, and attendance is instantly recorded.
3. **Efficiency:** The automated workflow contributes directly to the projected **52% reduction in attendance verification time** (Feasibility Study Data).

2.1.2 Faculty and Administrative Access

- **Real-Time Dashboards:** Faculty access a secure, role-based dashboard to monitor attendance **in real-time** for their classes.
- **Zero Manual Entry:** The system completely eliminates the administrative burden on faculty, allowing them to focus entirely on teaching. This ensures a high level of **Faculty Efficiency** and user acceptance.

2.2 Resource and Skill Availability

The project is operationally sound given the available resources:

- **Development Skills:** The team possesses the requisite skills in **C++, Python, ML/JavaScript**, and database management, aligning perfectly with the technical requirements for development and initial deployment (as per team skills listed in final_se (1).docx).
- **Maintenance:** Long-term maintenance requires skilled IT staff capable of managing the centralized database and network infrastructure. This knowledge is standard within an institutional IT department and can be acquired through targeted training.
- **Integration:** The system is designed to seamlessly integrate its data outputs with existing **Student Information Systems (SIS)** to maximize data utility and reduce redundant entry points.

2.3 Policy, Privacy, and Security Feasibility

Operational success is contingent upon strict adherence to privacy standards, which is feasible through design choices:

- **Privacy-First Design:** The system is designed to be **GDPR-compliant** and ethically sound. Crucially, **no raw image files are stored**. Only **AES-256 encrypted mathematical embeddings** are retained and used for verification.
- **Security Measures: Mandatory Multi-Factor Authentication (MFA)** will secure administrative and faculty access, and **Role-Based Access Control (RBAC)** will ensure data is only viewed by authorized personnel. This addresses the highest level of institutional security needs.

Economic Feasibility Assessment

Economic feasibility confirms the project is financially viable, demonstrating a positive Return on Investment (ROI) based on efficiency gains and cost avoidance.

3.1 Estimated Initial Investment (One-Time Costs)

The initial capital outlay is calculated based on procurement necessary for widespread deployment (estimated 48 stations).

Category	Item	Unit Cost (₹)	Quantity	Total Cost (₹)
Hardware: Verification Stations	High-Resolution Webcams	5,000	48	2,40,000
Hardware: Verification Stations	2D Barcode Scanners	3,000	48	1,44,000
Hardware: Infrastructure	Central Server/Main Computer	70,000	1	70,000
Software/Labor	Initial Development & Licensing (Year 1)	30,000	1	30,000
Total Initial Investment				**4,84,000**

3.2 Quantifiable Benefits and ROI

The economic benefits of SmartAttend are tangible, derived from efficiency gains and the recovery of lost instructional time.

- **Recovered Instructional Time:** The system directly reclaims the **10–15 minutes of valuable teaching time lost per lecture**. This is projected to be a **52% reduction in attendance verification time**, saving approximately **6.5 minutes** per large lecture, which translates into significant recovered instructional value over a semester.
- **Reduced Administrative Costs:** A projected **55% reduction in administrative processing** is achieved by eliminating the labor associated with correcting manual data errors, resolving attendance disputes, and compiling audit reports.
- **Return on Investment (ROI):** Based on the cumulative value of recovered instructional time and reduced administrative labor, the projected **ROI is estimated to be achieved within 18–24 months** of full institutional deployment.

Cultural and Social Feasibility Assessment

This assessment addresses the potential impact of the SmartAttend system on user behavior, ethical expectations, and acceptance within the academic community.

4.1 Ethical Acceptance and Privacy Assurance

The introduction of biometric technology requires a proactive strategy to address privacy concerns.

- **Privacy-First Design as Social Contract:** The system's **Privacy-First Design** serves as a vital social contract. The explicit policy that **no raw image files are stored** and that only **AES-256 encrypted mathematical embeddings** are used ensures the project is ethically sound and assuages student fears regarding data misuse. This measure is crucial for achieving cultural acceptance.
- **Transparency and Consent:** The implementation strategy must include a clear communication plan detailing *what* data is collected, *how* it is secured, and *how long* it is retained. This transparency builds the necessary trust for social feasibility.

4.2 User Adoption and Behavioral Change

The system must demonstrate clear superiority over manual methods to encourage its adoption.

- **Motivator: Eliminating Proxy Fraud:** The most significant social motivator is the system's ability to eliminate **proxy attendance**. Students who attend regularly will support the system because it restores **Student Fairness** and **academic honesty**, addressing a major cultural pain point.

- **Low Barrier to Entry:** The system's simplicity (4-second verification time) minimizes behavioral change. It replaces a long wait (10–15 minutes) with a quick action, driving positive user adoption.
- **Accessibility:** The system must be accessible and robust enough to handle diverse lighting conditions and various face shapes/hairstyles, ensuring it does not unfairly exclude any student demographic.

4.3 Institutional Image and Innovation

- **Competitive Positioning:** Adopting SmartAttend positions the institution as a leader committed to **innovation and technological leadership**. This forward-thinking stance positively influences the institution's public image, helping to **attract prospective students and faculty**.
- **Data Trust:** By guaranteeing the integrity of its attendance records, the institution strengthens its relationship with auditing bodies and funding agencies, fostering greater external **trust and operational integrity**.

Risk Assessment and Security Analysis

A robust security framework is paramount for the SmartAttend system, given its role in academic integrity and its handling of sensitive biometric data. This section details the comprehensive security protocols, risk mitigation strategies, and the phased approach required for successful implementation.

Proposed Security Framework Overview

The SmartAttend security framework is designed to ensure data integrity, confidentiality, and availability while proactively addressing vulnerabilities and achieving regulatory compliance (GDPR).

1.1 Data Confidentiality Protocols

Confidentiality is the highest priority for the SmartAttend system, focusing specifically on securing biometric data.

- **Encryption at Rest and in Transit:** Biometric facial embeddings are secured using industry-standard **AES-256 encryption** both during transmission (in transit) and when stored on the server (at rest). This prevents unauthorized parties from intercepting or accessing the data in a readable format.
- **Minimal Data Exposure:** The system employs a "Privacy-First Design" by storing only **mathematical vectors (embeddings)**—not raw image files. Since the stored data is a non-reversible numerical representation of the face, it minimizes direct exposure risks and cannot be used to recreate the student's face.
- **Rigorous Algorithm Testing:** The security integrity of the facial recognition algorithms (e.g., resistance to presentation attacks/spoofing) must undergo **rigorous testing** during the pilot phase to ensure only live, legitimate students can register.

1.2 Access Control and User Authorization

A multilayered control system is essential to prevent internal misuse and unauthorized data viewing.

- **Role-Based Access Control (RBAC):** A strict RBAC system governs access to attendance data. Permissions are explicitly assigned based on defined user roles (Administrator, Faculty, Student). For example, faculty can only view attendance for the courses they teach.
- **Mandatory Multi-Factor Authentication (MFA): MFA is mandatory** for all administrative access accounts. This critical security layer prevents unauthorized system configuration changes or data exports, even if a password is compromised.

- **Comprehensive Audit Trails:** A detailed audit trail is maintained for all system access, queries, and data modifications. Logs record user activities, timestamps, and data changes for complete transparency. These logs are regularly reviewed for anomalous activity.

1.3 Secure Infrastructure Architecture and Compliance

The infrastructure must be isolated and regularly assessed to protect against external threats.

- **Network Isolation:** The SmartAttend platform operates in **isolated network segments** separate from general campus traffic. This compartmentalization limits the potential spread of any security breaches.
- **Vulnerability Management:** The system undergoes continuous security evaluation via **routine penetration testing and vulnerability assessments**. All identified weaknesses and zero-day threats must be addressed promptly.
- **Regulatory Compliance:** The system is explicitly designed for full **GDPR compliance**. Compliance includes mandatory data protection impact assessments (DPIAs) and adhering to automated data retention policies to purge information upon academic necessity expiry. Regular independent **third-party audits are planned** to confirm ongoing compliance.

Validation, Verification, and Implementation Strategy

Mitigating risk requires a structured plan that moves the project from development through to full deployment, validating performance and security at every stage.

2.1 Validation and Verification Requirements

Before broad deployment, the system must prove its reliability and security through external and internal testing.

- **Pilot Testing Requirements:** A pilot program is crucial for validating performance, security, and user acceptance in a live, controlled environment. It should be limited to specific courses or a small student cohort to facilitate iterative improvements and early issue identification. Success is measured by high system uptime, **98% accuracy**, and positive user feedback.
- **Independent Validation & Verification (IV&V):** Independent validation & verification (IV&V) ensures all functional and non-functional requirements are met impartially. Successful IV&V is a mandatory prerequisite for broader deployment.
- **Third-Party Security Audits:** External **third-party security audits and penetration testing** are required to confirm the robustness of the security architecture and the integrity of the encryption and access controls

.

2.2 Phased Implementation Plan

Risk is mitigated by dividing the project into four distinct phases, with clear decision points required before proceeding to the next stage.

Phase	Focus Area	Key Objectives and Deliverables	Risk Mitigated
Phase 1	**Development & Testing**	Finalize architecture, integrate hardware, complete alpha and beta testing of core verification modules.	Technical integration risk, algorithm error risk.
Phase 2	**Pilot Program**	Deploy to a controlled cohort/department, gather performance data (speed, accuracy, latency).	User acceptance risk, performance degradation risk.
Phase 3	**Iterative Refinement**	Optimize system based on pilot feedback, conduct IV&V and security audits.	Security vulnerability risk, non-compliance risk.
Phase 4	**Full Deployment**	Gradual, institution-wide rollout with comprehensive training and ongoing support.	Scalability risk, training/adoption risk.

Each phase has defined objectives, deliverables, and decision points, ensuring that the system is only scaled once critical risks have been successfully contained and validated.