**REPUBLIQUE DU CAMEROUN REPUBLIC OF CAMEROON**

**PAIX - TAVAIL- PATRIX PEACE – WORK – FATHERLAND**

**MINISTERE DE L’ENSEIGNMENT SECONDAIRE MINISTRY OF HIGHER EDUCATION**

P. O Box 63, Buea, South West Region Cameroon

Tel : (237) 674354327

Fax: (237) 3332 22 72



# UNVERSITY OF BUEA

**FACULTY OF ENGINEERING AND TECHNOLOGY COMPUTER ENGINEERING DEPARTMENT**

# CEF 440: INTERNET PROGRAMMING AND MOBILE PROGRAMMING REQUIREMENT GATHERING

***COURSE INSTRUCTOR : DR KEMENI VALERY***

# GROUP 13

|  |  |
| --- | --- |
| **NAMES OF GROUP MEMBERS** | **MATRICULE NUMBER** |
| CHO WESLEY MUNGO | FE21A160 |
| ANANFACK ZANGO ANGELA CARINE | FE21A137 |
| NKWETI MANGEM ANCELIA | FE21A280 |
| ALAIN NKEH MBUNKUH | FE21A133 |
| NTUI RAOUL NTUI NJOCK | FE21A288 |

**TABLE OF CONTENT**

1. [INTRODUCTION… 1](#_TOC_250031)
   1. [Stakeholders… 1](#_TOC_250030)
2. [USER REQUIREMENTS… 1](#_TOC_250029)
   1. [User Requirement(Instructor)… 1](#_TOC_250028)
   2. [User Requirement(Student) 2](#_TOC_250027)
   3. [User Requirement(Administrator). 2](#_TOC_250026)
3. [FUNCTIONAL REQUIREMENTS… 3](#_TOC_250025)

3.1. User Login Management… 3

* 1. Attendance Management… 4
  2. [Data Synchronization… 4](#_TOC_250024)
  3. [Attendance tracking and reporting… 4](#_TOC_250023)
  4. [User Management… 4](#_TOC_250022)
     1. [Admin User Functionality… 4](#_TOC_250021)
     2. [Account Recovery… 4](#_TOC_250020)
  5. [Biometric Authentication… 5](#_TOC_250019)
     1. [User Authentication… 5](#_TOC_250018)

[3.6.2. Authentication Feedback… 5](#_TOC_250017)

* 1. [User Registration… 5](#_TOC_250016)
     1. [User Account Creation. 5](#_TOC_250015)
     2. [Biometric Enrollment… 5](#_TOC_250014)
     3. [Biometric Data Storage… 5](#_TOC_250013)
  2. [Error Handling and Support… 5](#_TOC_250012)
     1. [Error Messages… 5](#_TOC_250011)
     2. [Customer Support… 6](#_TOC_250010)

1. [Non-Functional Requirements… 6](#_TOC_250009)
   1. [Security Requirements… 6](#_TOC_250008)
   2. [Performance Requirements… 6](#_TOC_250007)
   3. User Interface (UI). 6
   4. Scalability 6
   5. Offline Functionality… 6
   6. Compatibility… 6
2. [Business Requirement… 6](#_TOC_250006)
   1. [Enhance student accountability 6](#_TOC_250005)
   2. [Increase Instructor Productivity… 6](#_TOC_250004)
   3. [Improve Attendance Management Efficiently… 7](#_TOC_250003)
   4. [Increase student Engagement… 7](#_TOC_250002)
   5. [Enhance institutional reputation… 7](#_TOC_250001)
   6. [Enhance institutional decision-making… 7](#_TOC_250000)

6 Other requirement… 7

# Introduction:

The Biometric Student's Attendance Mobile Application is designed to streamline attendance tracking in academic settings. By leveraging biometric technology, specifically fingerprint recognition, this mobile application ensures secure and reliable attendance recording for students in higher educational institutions. This document outlines the requirements for designing and implementing this system.

Requirement gathering refers to the description of the functions, features, constraints and qualities that a software system must possess to fulfill its intended purpose and meet stakeholders’ need. It simply explains how the system needs to be developed. The application aims to address the limitations of traditional attendance methods by providing a secure, efficient, and user-friendly solution for educational institutions.

There are 3 types of requirement gathering namely:

Business requirements, User requirements, System requirements.

# Stakeholders

* Students
* Instructors
* System Administrators
* Educational Institution

# User Requirements

# User Requirement(Instructor)

* + **User Friendly Interface:** The application should have an intuitive and user-friendly interface that require minimal training for the instructor to use it conveniently.
  + **Real-time Visibility:** Instructor should have instant access to attendance records and be able to monitor student’s participation in real-time.
* **Report and Analytics:** the instructor should be able to generate attendance reports, view statistics and analyze attendance date for individual students.
* **Attendance Exception:** Instructor should be able to mark attendance for a student who was not in class and has a valid reason for not coming.
* **Offline mode:** The application should support offline functionality allowing the system to still perform well in areas of limited internet connection.
* **Attendance list management:** The ability to view and management the attendance list of students for various classes and the option to add, remove or edit students from the attendance list including manually entering student information.

# User Requirement (Student)

* **Biometric enrollment:** The students should be able to enroll their biometric data within the application.
* **Attendance History:** Student should be able to view their attendance history including dates, time-laps etc
* **User Profile Management:** Students should be able to update and manage their personal information such as class preferences or contact details within the application.
* **User Interface:** The application should have an intuitive and user-friendly interface that require minimal training for the instructor to use it conveniently.

# User Requirement(Administrator)

* **Administrative Dashboard:** The administrator should have access to a centralized dashboard too monitor the attendance across multiple classrooms and departments.
* **Role-based Access:** The system should support role-based access control allowing the administration to define different levels of access and permission for instructors, students and other staff members.
* **Data Backup and recovery:** The system should include regular backup so as to avoid permanent lost of information.
* **Manages Classes:** He creates the class, edit existing class and can delete class and put additional information like the data of a class, the lecturer.
* **User management:** The administrator manages the instructors and student including adding new instructor or student, editing and deleting if necessary.

# Functional Requirements

* 1. **User Login and Management**
* Students: Login using a secure mechanism (e.g, username/password, student ID).
* Instructors: Login using a secure mechanism with appropriate access control.
* System Administrators: Manage user accounts (students, instructors) and assign roles.

# Attendance Management Students:

* Check-in attendance using fingerprint recognition.
* View their attendance history.

# Instructors:

* Initiate attendance sessions for classes.
* View real-time attendance data for ongoing sessions.
* Access historical attendance records for classes.
* Export attendance data to various formats (e.g, CSV, PDF).

# Data Synchronization:

Anytime a student puts his finger on the finger print device, his name should instantly be ticked.

# Attendance tracking and reporting:

The system take and maintain a record of student, if the student attendance with date and time, instructor and administrator should be able to generate attendance reports and view attendance statistics.

# User Management

# Admin User Functionality:

* + - * Authorized administrators shall have access to a separate interface for managing user accounts and system settings.
      * Admin users shall be able to create, update, or delete user accounts as needed, with appropriate validation checks and confirmation prompts.
      * Administrators shall have the ability to view detailed logs of user activities, including account creation, authentication attempts, and modifications.

# Account Recovery:

* The system shall support account recovery mechanisms for users who forget their passwords or encounter login issues.
* Users shall be able to initiate the account recovery process by providing necessary identifying information (e.g, email address or phone number).
* Upon initiating account recovery, the system shall send a verification code or link to the user's registered email or phone number for identity verification.

# Biometric Authentication

# User Authentication:

* Upon login, the system shall prompt users to authenticate themselves using biometric data previously enrolled during registration.
  + Users shall have the option to choose the preferred biometric modality for authentication, based on available options.
  + The system shall perform real-time comparison of captured biometric data with stored templates to verify the user's identity.
* Authentication shall be deemed successful if the captured biometric data matches the stored template within an acceptable margin of error.

# 3.6.2. Authentication Feedback:

* The system shall provide immediate feedback to users regarding the outcome of the authentication attempt (e.g, "Authentication Successful" or "Authentication Failed").
* In case of authentication failure, the system shall provide clear instructions for users to retry the authentication process or use an alternative authentication method.

# User Registration

# User Account Creation:

* + - * The system shall provide a user-friendly interface for individuals to create a new account.
        + Users shall provide the following information during registration: full name, matricule number, institutional email and email address
        + The system shall enforce password strength requirements, including a minimum length and a combination of alphanumeric characters.
      * Upon successful registration, the system shall assign a unique identifier (user ID) to the user.

# Biometric Enrollment:

- During account creation, the system shall prompt users to enroll their biometric data using supported modalities (e.g, fingerprint, facial recognition).

- The enrollment process shall guide users through capturing high-quality biometric samples, ensuring sufficient detail and accuracy for authentication.

- Users shall have the option to enroll multiple biometric modalities for enhanced flexibility and reliability.

# Biometric Data Storage:

* The system shall securely store biometric templates generated during the enrollment process.
* Biometric data shall be encrypted using strong cryptographic algorithms to protect sensitive information from unauthorized access.
* Access to biometric templates shall be restricted to authorized personnel with appropriate privileges.

# Error Handling and Support:

# Error Messages:

* + - * The application provides clear and concise error messages to guide users in case of authentication failure or other issues.
      * Error messages offer actionable steps for users to resolve authentication errors or technical issues.

# Customer Support:

* + - * Users have access to customer support services within the application for assistance with account- related queries or technical issues.
      * Customer support options may include FAQs, live chat support, or email support for escalated issues.

# Non-Functional Requirements

# Security Requirements

Secure storage of student biometric data (fingerprint templates). Implement industry-standard encryption for data transmission. User authentication mechanisms to prevent unauthorized access. Audit logs to track user activity and maintain accountability.

# Performance Requirements

Fingerprint recognition should be fast and reliable (less than 5 seconds per student).

The application should function smoothly on various mobile devices with different specifications. Efficient data synchronization between the mobile app and central server.

* 1. **User Interface (UI):** Intuitive and user-friendly interface for both students and instructors. Design that caters to different screen sizes and resolutions. Accessibility features for users with disabilities.
  2. **Scalability:** The application should be scalable to accommodate a growing number of users and classes.
  3. **Offline Functionality:** Allow students to check-in attendance even in areas with limited internet connectivity (data will be synced later).
  4. **Compatibility:** The application should be compatible to run on multiple versions of iOS and Android devices, also it should ensure consistent functionality and user experience across different devices and screen sizes. It should also be able to be integrated to other applications and can integrate some services from other applications.

# Business Requirement

This defines what the business wants to accomplish and serve as a foundation for the design and development of solutions.

# Enhance student accountability:

Accurately record student attendance using biometric verification hence minimize risk of attendance fraud. Provide students with a clear understanding of their attendance records.

# Increase Instructor Productivity:

Enable instructor to mark attendance quickly and easily using biometric modality so reduce time spent on administrative task related to attendance management, provide instructor with real-time insights into student attendance patterns.

# Improve Attendance Management Efficiently:

Automate attendance tracking reducing manual effort and errors associated with traditional methods. Eliminates the need for paper attendance sheets and manual date entry. Provide real-time attendance date for immediate analysis and decision-making.

# Increase student Engagement:

Provide students with immediate feedback of their attendance, encourage students to take ownership of their attendance work. Promote a culture of accountability and responsibility among students.

# Enhance institutional reputation:

Demonstrate a commitment to using Technology to improve student success and accountability. Increase students satisfaction and improve the overall educational experience.

Strengthen the institution’s reputation for innovation and efficiency.

# Enhance institutional decision-making:

Provide administration with comprehensive attendance reports and analysis, identify trend and patterns in student attendance.

Inform data-driven decision related to academic intervention, resource allocation and policy development.

# Other Requirements:

* 1. **Legal and Regulatory Requirements**

- The application must comply with relevant laws and regulations regarding biometric data usage and privacy.

# Documentation Requirements

* The application must provide comprehensive documentation for installation, configuration, and usage.

# REFERENCES

Vaibhavi desai, Yugandhara Gore, Shital Jakar, S.V .Patil, Attendance Management using Biometrics with SMS Alerts 2001

Aniket Bansal, Satyam Humar, Ashutosh Pandey, Kaushal Kishor Attendance Management System through print 2002