**UNIVERSITY OF BUEA**

**FACULTY OF ENGINEERING AND TECHNOLOGY**

****

**DEPARTMENT OF COMPUTER ENGINEERING**

**FET 598: FINAL YEAR PROJECT**

**SYSTEM REQUIREMENT SPECIFICATION DOCUMENT FOR A BIOMETRIC STUDENT’S ATTENDANCE APPLICATION**

BY:

ASONGNA FRANK TONGWA

FE20A012

SOFTWARE ENGINEERING

**Supervisor:**

Date: 01/05/2024 Dr. VALERY NKEMENI

**Table of Contents**

[1. Introduction 3](#_Toc165453500)

[1.1. Purpose 3](#_Toc165453501)

[1.2. Scope 3](#_Toc165453502)

[1.3. Definitions, Acronyms and abbreviations 3](#_Toc165453503)

[1.3.1. Definitions: 3](#_Toc165453504)

[1.3.2. Acronyms and abbreviations 3](#_Toc165453505)

[1.4. References 3](#_Toc165453506)

[2. Overall Description 4](#_Toc165453507)

[2.1. Product Perspective 4](#_Toc165453508)

[2.2. Product Functions 4](#_Toc165453509)

[2.3. User Classes and Characteristics 4](#_Toc165453510)

[2.4. Operating Environment 4](#_Toc165453511)

[2.5. Design and implementation constraints 4](#_Toc165453512)

[3. System Features 5](#_Toc165453513)

[3.1. Functional Requirements 5](#_Toc165453514)

[3.2. External Interface Requirements 5](#_Toc165453515)

[3.2.1. User Interfaces 5](#_Toc165453516)

[3.2.2. Hardware Interfaces 6](#_Toc165453517)

[3.2.3. Software Interfaces 6](#_Toc165453518)

[3.2.4. Communication Interface 6](#_Toc165453519)

[3.3. Non-functional Requirements 7](#_Toc165453520)

[4. Biometric systems 7](#_Toc165453521)

[4.1. Fingerprint Recognition 7](#_Toc165453522)

[4.2. Facial Recognition 8](#_Toc165453523)

[4.3. Iris Recognition 8](#_Toc165453524)

[4.4. Voice Recognition 9](#_Toc165453525)

# Introduction

## Problem Statement

The current manual method of recording and tracking attendance is slow and inefficient, wasting valuable time for students transitioning between classes.

## Purpose

The aim of this application is automate and efficiently record the attendance of students with an institution.

## Scope

* The scope encompasses the development of a software solution tailored for educational institutions to automate the process of tracking student attendance using biometric authentication.
* This includes the design and implementation of user-friendly interfaces for seamless registration of biometric data, real-time authentication during class sessions, and generation of detailed attendance reports.
* The application will integrate with existing student information systems (SIS) through APIs.

## Definitions, Acronyms and abbreviations

### Definitions:

**Student:** A student is an individual enrolled in an educational institution, such as a school, college, or university, who attends classes and is subject to taking attendance.

**Instructor:** An individual responsible for teaching and managing classes within an educational institution, who also tracks student attendance.

**Administrator:**  This is an authorized personnel responsible for managing and maintaining the system, overseeing its configuration, user management, and overall functionality.

### Acronyms and abbreviations

* API: Application Programming Interface
* GUI: Graphical User Interface
* SIS: Student Information System
* SSL: Secure Sockets Layer
* TLS: Transport Layer Security
* JSON: JavaScript Object Notation.
* XML: stands for Extensible Markup Language.
* GDPR: General Data Protection Regulation

## References

* How does Biometric Attendance System work with HCMS?

<https://pulsehrm.com/time-attendance-software/>

* Student biometric identification SRS

<https://www.slideshare.net/HassaanAfzal/student-biometric-identification-srs>

* SRS for attendance management system
* SRS documentation of a Market Management System

# Overall Description

## Product Perspective

The biometric student attendance application will function as a standalone system. It will interact with biometric devices for authentication and integrate with existing SIS through APIs for data synchronization.

## Product Functions

* **Student Registration**: Administrators can register students into the system by capturing and storing their biometric data (like fingerprints and facial patterns).
* **Attendance Tracking**: Students authenticate themselves using biometric data to record their attendance in classes.
* **Reporting**: The system generates attendance reports for administrators and instructors based on specified parameters such as date range and class/course.
* **Integration**: Integration with existing SIS allows for seamless data exchange between systems.

## User Classes and Characteristics

* **Administrators**: Manage system settings, view attendance reports.
* **Instructors**: Take attendance, view class rosters.
* **Students**: view personal attendance records.

## Operating Environment

The application will run on Windows/Linux servers with compatibility for various biometric devices and databases.

## Design and implementation constraints

* **Biometric Device Compatibility:** The application's functionality relies on the compatibility and proper functioning of biometric devices for data capture. Compatibility issues with specific devices may arise.
* **Data collection:** The accuracy and reliability of the system heavily rely on the quality of biometric data captured during enrollment.
* **Data Security:** The storage and transmission of biometric data must adhere to strict security protocols to prevent unauthorized access or breaches.
* **Scalability:** The system should be designed to accommodate the potential growth of student enrollment and increased usage over time.
* **Integration Complexity:** Integration with existing student information systems may present challenges due to variations in data formats and APIs.
* **Regulatory Compliance:** Compliance with legal and regulatory requirements related to data privacy and biometric data usage may impose constraints on system design and implementation.

# System Features

## Functional Requirements

* 1. **Student Registration**

Allows administrators to register students into the system by capturing their biometric data.

* 1. **Attendance Tracking**

Records student attendance by authenticating biometric data effectively and possibly at specified times.

* 1. **Reporting**

Generates attendance reports for administrators and instructors, for certain date ranges and class or course. Reports formats are to be diverse for different needs such as PDF, CSV, JSON and others

* 1. **Enhanced User Management**

Include detailed roles and permissions for administrators and instructors, such as the ability to delegate tasks and monitor user activities.

* 1. **Real-Time Alerts and Notifications**

Implement a system for real-time alerts and notifications to administrators and instructors for specific events like low attendance and device errors.

* 1. **Backup and Recovery:** Implement automated backup and recovery functionalities to ensure data integrity and availability.

## Non-functional Requirements

* 1. **Performance**
* The system should support concurrent authentication of multiple students within seconds.
* Ensure system response time for authentication is under 5 seconds.
* Optimize database queries and biometric data processing algorithms for faster performance.
  1. **Security**
* Biometric data should be encrypted and stored securely.
* Access to administrative features should be restricted based on user roles and permissions.
* All system communications should use SSL/TLS for secure data transmission.
* Multi-factor authentication should be implemented for administrators and instructors.
* Regular security audits and vulnerability assessments should be conducted.
  1. **Reliability**
* Ensure a failover mechanism and load balancing to maintain high availability.
  1. **Usability**
* GUI should be intuitive and user-friendly to facilitate ease of use for administrators, instructors, and students.
* Conduct usability testing with end-users to gather feedback and make iterative improvements.
* Provide comprehensive onboarding and help resources within the application.
  1. **Legal and Regulatory compliance**

The application should comply with data protection laws (LIKE GDPR) regarding the storage and usage of biometric data.

* 1. **Scalability**

The system should be capable of scaling, allowing it to easily adapt to changes in the number of users, attendance recording frequency, or system load. Scalability should be achieved through efficient resource utilization and distributed architecture.

* 1. **Integrability**
* Ensure that the biometric attendance system can seamlessly integrate with existing student information systems (SIS), databases, and other third-party applications used in educational institutions.
* Provide a well-documented API for third-party integrations.

## External Interface Requirements

### User Interfaces

1. **Administrative Interface**
   * + - * **Description**: The administrative interface is designed for system administrators to manage system settings, configure user roles and permissions, and access reports.
         * **Features**:
   * **User Management:** Allows administrators to add, modify, and delete user accounts with different roles (like admin and instructor).
   * **Settings Configuration:** Enables administrators to configure system settings such as biometric device integration, data retention policies, and email notifications.
   * **Report Access:** Provides access to attendance reports, allowing administrators to generate, view, and export reports.
2. **Instructor Interface**

* **Description**: The instructor interface allows instructors to take attendance, view class rosters, and access basic reporting functionalities.
* **Features**:
  + - **Attendance Management**: Enables instructors to take attendance for classes by authenticating students using biometric data.
    - **Roster Access:** Provides access to class rosters, allowing instructors to view enrolled students and their attendance history.
    - **Basic Reporting:** Allows instructors to generate simple attendance reports for individual classes or specific time periods.

1. **Student Interface**

* **Description**: The student interface is a web-based platform that allows students to view their attendance records.
* **Features**:
  + - **Attendance Records:** Displays a summary of attendance records for each enrolled course, including dates and percentage of attendance.

### Hardware Interfaces

* **Biometric Devices**: The application will interface with biometric devices for capturing and authenticating biometric data (links fingerprint scanners). These devices should support standard communication protocols for integration with the application.
* **Server Hardware**: The application will be deployed on Windows/Linux servers with adequate processing power, memory, and storage capacity to support concurrent user authentication and data processing.

### Software Interfaces

* **Student Information Systems (SIS) API**: The application will integrate with existing SIS through APIs for data synchronization. This integration will allow for seamless exchange of student information, course schedules, and attendance records between the biometric attendance application and the SIS.

### Communication Interface

* **Description:** The communication interface facilitates communication between the biometric attendance application and external systems, devices, or services.
* **Protocols:** The application will utilize standard communication protocols such as HTTP/HTTPS, TCP/IP, or WebSocket for communication with external systems, including biometric devices, servers, and APIs.
* **Data Formats:** Data exchanged through the communication interface will adhere to standard data formats such as JSON or XML to ensure compatibility and interoperability.
* **Security:** Communication over the interface will be secured using encryption protocols (like SSL/TLS) to protect sensitive data transmitted between systems.

# Other Requirements

## Documentation Requirements

* User manuals for administrators, instructors, and students.
* Technical documentation for system administrators and developers.

## Training Requirements

Training sessions for administrators, instructors, and students on system usage and maintenance.

## Maintenance Requirements

Regular updates and patches to ensure system security and stability.

# Biometric systems

For a biometric student attendance application, several biometric measures can be considered, each with its own advantages and challenges. The chosen system depends on different factors like accuracy, convenience, cost, and scalability. Here are the 4 of the most common ones.

## Fingerprint Recognition

* 1. **Definition and description:**
* Fingerprint recognition is a biometric technique that identifies individuals based on the unique patterns present in their fingerprints.
* It relies on capturing an individual's fingerprint image using a sensor, which then processes the image to extract distinctive features such as ridge endings, bifurcations, and ridge patterns. This is then converted in a mathematical representation called a template and stored in a database for comparison.
* During authentication, the system captures a fingerprint image from the user, processes it to create a template, and compares it with the templates stored in the database to determine a match.
  1. **Advantages**:
* Widely adopted and proven technology.
* High accuracy and reliability.
* Cost-effective biometric devices are available.
  1. **Challenges**:
* Requires clean and dry fingers for accurate recognition.
* May have hygiene concerns, especially in shared environments.
  1. **Suitability**: Fingerprint recognition is a popular choice due to its high accuracy and availability of affordable devices. It's suitable for small to large-scale implementations.

## Facial Recognition

* 1. **Definition and description:**
* Facial recognition is a biometric technique that identifies individuals based on their facial features.
* It involves capturing an image or video of a person's face using a camera, which is then analyzed to extract unique facial characteristics such as the distance between the eyes, the shape of the nose, and the contours of the face. These features are converted into a mathematical representation called a faceprint or facial template, which is stored in a database.
* During authentication, the system captures an image of the user’s face, extracts facial features, and compares them with the stored templates to verify the identity of the individual.
  1. **Advantages**:
* Non-intrusive and convenient for users.
* Can work at a distance, allowing for contactless authentication.
  1. **Challenges**:
* Vulnerable to variations in lighting conditions and facial expressions.
* Privacy concerns and ethical considerations regarding data collection and storage.
  1. **Suitability**: Facial recognition offers convenience and contactless authentication, making it suitable for applications where hygiene and convenience are paramount. However, it may require more sophisticated hardware and software for accurate performance.

## Iris Recognition

1. **Definition and description:**

* Iris recognition is a biometric technique that identifies individuals based on the unique patterns present in their iris, the colored part of the eye surrounding the pupil.
* It involves capturing a high-resolution image of the iris using a specialized camera, which then analyzes the intricate patterns such as furrows, freckles, and coronas. These patterns are converted into a digital template, which is stored in a database for comparison.
* During authentication, the system captures an iris image from the user, extracts iris patterns, and compares them with the templates stored in the database to authenticate the individual.

1. **Advantages**:

* High accuracy and uniqueness of iris patterns.
* Difficult to spoof.

1. **Challenges**:

* Requires specialized hardware for iris scanning.
* Users may feel uncomfortable with close-range scanning.

1. **Suitability**: Iris recognition offers high accuracy and security but may be less suitable for large-scale deployments due to hardware requirements and user discomfort with close-range scanning.

## Voice Recognition

1. **Definition and description:**

* Voice recognition, also known as speaker recognition, is a biometric technique that identifies individuals based on their unique vocal characteristics or features
* It involves capturing and analyzing various attributes of a person's voice, including pitch, tone, rhythm, and speech patterns. These attributes are used to create a unique voiceprint or vocal template, which is stored in a database.
* During authentication, the system captures the user's voice sample, analyzes it to extract vocal features, and compares them with the stored voiceprints to verify the identity of the individual.

1. **Advantages**:

* Convenient for users, as it does not require physical contact.
* Can be combined with other biometric measures for multi-factor authentication.

1. **Challenges**:

* Vulnerable to background noise and variations in speech patterns.
* Users with speech impairments may face difficulties.

1. **Suitability**: Voice recognition can be suitable for applications where hands-free operation is important. However, it may not be as reliable in noisy environments or with users who have speech variations.

Based on the requirements of the system outlined in the SRS document, **fingerprint recognition** seems to be the most suitable biometric measure. Additionally, the two technology are mature and widely adopted, with a range of reliable devices available in the market.