FINGERPRINT BIOMETRICS ATTENDANCE SYSTEM USING MOUNTAIN TOP UNIVERSITY AS A CASE STUDY

By

PAUL, GBENGA ELIJAH

18010301008

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE AND MATHEMATICS, COLLEGE OF BASIC AND APPLIED SCIENCES, IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE

2022

DECLARATION

I hereby declare that this project has been written by me and is a record of my own research work. It has not been presented in any previous application for a higher degree of this or any other University. All citations and sources of information are clearly acknowledged by means of reference.

_____

PAUL, GBENGA ELIJAH

_____

Date

CERTIFICATION

This is to certify that the content of this project entitled '**Fingerprint Biometrics Attendance System Using Mountain Top University as a case study'** was prepared and submitted by **PAUL GBENGA ELIJAH** in partial fulfillment of the requirements for the degree of **BACHELOR OF SCIENCE IN COMPUTER SCIENCE.** The original research work was carried out by her under by supervision and is hereby accepted.

_____ (Signature and Date)

Mr. J. A. Balogun

Supervisor

_____ (Signature and Date)

Dr. M.O. Adewole

Coordinator, Department of Computer Science and Mathematic

DEDICATION

This effort, as well as the success of the undergraduate program, is entirely devoted to God Almighty, my ever-present helper and lifter of my head. The ONE who created my life path from the beginning of time and has guided me through all of life's twists and turns. I give him all the credit.

ACKNOWLEDGEMENTS

I'd like to thank and acknowledge my family for being there for me throughout the journey: Dad and Mom, as well as my siblings, Titus Maxwell, Adeniran Israel, Adeoye Tofunmi, and Ojuroye Tobiloba, as well as all my friends and course mates, my Supervisor, Mr Jeremiah Balogun, all the Computer Science Academia, the Head of Department, and all other staff members who have influenced my life during my studies. Thank you very much.

ABSTRACT

The aim of this study was to develop an Attendance system for Mountain top university chapel which allows a smooth and running attendance in the chapel premises with the aid of using a fingerprint scanner. This study identified the various user and system requirements, also specify on the system design and implementation.

A review of the literature was been done to identify and understand existing attendance systems. The user and system requirements of the system were identified from researches done from existing systems. The system design was specified using UML diagrams which include uses case diagram, flowchart diagram, class diagram. The implementation of the system was done using HTML, CSS, JAVASCRIPT for the frontend AND PHP for the backend.

The results of the system showed the implementation of the attendance system for Mountain top university chapel by using the fingerprint scanner to carry out attendance the registration of student fingerprint marked with their Name and matriculation number thereafter they can now be scanned for each service attended.

The study concluded that using a Biometric base attendance system the university will be able to get a smooth and accurate attendance recording from each service and make it easier for attendance taking thereby eliminate the existing system in mountain top university.

Keywords: *Biometric-based, Fingerprint scanner, Mountain top university chapel, Registration, service.*

TABLE OF CONTENT

LIST OF FIGURES

CHAPTER ONE

INTRODUCTION

1.1 Background to the project

While not prehistoric, biometrics have been around for thousands of years. Biometrics have progressed from crude means of categorization to being authenticators of identification employing a variety of modalities throughout the previous few millennia. So, let us take a look back in time to see where biometrics has been and how far we've gone. (El-Abed, 2012). While the oldest descriptions of biometrics may be traced back to 500BC in the Babylonian kingdom, the first record of a biometric identifying system was in the 1800s in Paris, France. Alphonse Bertillon devised a technique of unique body measures for the categorization and comparison of convicts. While this technique was far from flawless, it was the first to use unique biological traits to authenticate. (Admin, 2021)

Fingerprinting followed suit in the 1880s, not only as a method of identifying criminals but also as a type of signature on contracts. It was realized that a fingerprint was a marker of a person's identity and that it might be used to hold someone accountable. While there are disagreements about who first used fingerprints for identification, Edward Henry is known for developing a fingerprinting standard known as the Henry Classification System. (Admin, 2021)

This was the first fingerprint-based identification system. The methodology was soon embraced by law enforcement, replacing Bertillon's methods as the norm for criminal identification. This sparked a century of research into what additional distinct physiological traits may be exploited for identification. (Admin, 2021). Biometrics evolved tremendously as a subject of study throughout the next century.

There were so many breakthroughs in the 1900s that it would be impossible to mention them all, so here are the highlights from the second half of the century.

Semi-automated facial recognition technologies were created in the 1960s, needing administrators to examine facial characteristics inside an image and extract useful feature points. Much more manual than the ones we may use to access our phones. By 1969, fingerprint and face recognition had become so common in law enforcement that the FBI allocated funds to the development of automated methods. This sparked the development of increasingly advanced sensors for biometric capture and data extraction. In the 1980s, the National Institute of Standards and Technology established a Voice group to explore and advance speech recognition technology processes. These experiments served as the foundation for today's voice command and recognition systems. In 1985, the idea that irises, like fingerprints, were unique to each individual was postulated, and by 1994, the first iris identification algorithm had been copyrighted. Furthermore, it was revealed that blood vessel patterns in the eyes were unique to each individual and could be utilized for authentication. In 1991, facial detection technology was invented, allowing for real-time recognition. While these techniques had numerous flaws, they sparked a surge of interest in facial recognition research.

Hundreds of biometric authentication recognition algorithms were functioning and patented in the United States by the 2000s. Biometrics were no longer being used just in huge corporations or the government. They were marketed commercially and used at large-scale events such as the 2001 Super Bowl. Biometric technology research has advanced at a remarkable pace in the last ten years alone. Biometrics has progressed from a revolutionary technology to an integral element of daily life. In 2013, Apple added fingerprint recognition to the iPhone, ushering in

widespread acceptance of biometric identification. Most smartphones now have biometric capabilities, and many applications employ biometrics as an authenticator for common activities.

Even with all of the progress, the development possibilities of biometric authentication and identity are far from exhausted. As biometrics research advances, we may expect it to be combined with artificial intelligence. The goal is to create biometric devices and systems that can learn and adapt to their users. Creating a smooth authenticating experience. As biometrics become increasingly ubiquitous, the usage of identity proxies may become obsolete. You no longer need to carry along keys, cards, or fobs when you can use yourself as proof of your identification. A future with a clearly defined society with frictionless transactions, interactions, and access control might be on the horizon. Don't fall behind on the times! Stay ahead of the curve and ensure your access control systems are up to date with biometric identity authentication (Admin, 2021).

1.2 Statement of Problem

As the student population grows, so does the number of names on the attendance list. Keeping these attendance papers becomes a difficulty, and no suitable backup is made. Most colleges still employ the conventional method, mostly in lecture halls and laboratories. The teacher or lecturer will hand out a sheet of paper with a list of students' names to sign, or in certain situations, the students must fill it out with their name, student ID, and matriculation number to demonstrate their attendance in a specific class. In this manner, fabrication of the student attendance list is prevalent. Assume a student is absent, but another student can sign in their place. To avoid this problem, it is required to create a fingerprint authentication

system for pupils. Biometric recognition will be utilized to track and maintain track of every student's attendance in a certain class.

1.3 Aims and objectives

The objective is to implement fingerprint recognition algorithm. The Region of Interest (ROI) for each fingerprint image is extracted after enhancing its quality. The Specific Objectives are to

i. identify existing relevant literatures on fingerprint recognition algorithm.
ii. identify the user and system requirements.
iii. design the system based on (ii)
iv. implement the system
v. test the system

1.4 Methodology of the Study

To fully accomplish the aforementioned objectives, the following methods were adopted.

a. Fingerprint Systems based on Attendance were compressively reviewed and observed
b. Users of the system and the system requirements were meticulously gathered
c. The user requirements for the proposed system involved the use of users biometric information. While the System requirements for the proposed system involves a device for capturing biometrics.
d. The design of the proposed system was based on the user and system requirements with comprehensive system architecture and relevant UML diagrams such as Sequence diagram and use case diagram.

e. The Implementation of the proposed system was done based on all the aforementioned processes.

1.5 Significance of the project

The range of pupils who use fingerprints Biometrics will completely eliminate the use of paper and pen to sign in and out of classes, exam halls, programs, and all other academic-related activities where attendance is required, which means we will no longer be at risk of losing data due to misplacing the attendance sheet or any other type of damage to the written records. Tracking and monitoring attendance time is time-consuming, and this project will automate that process and make the information available at all times and easy to access. Most importantly, it eliminates errors in attendance data and minimizes forgeries and fraud to a bare minimum.

This approach not only assists students but also management in detecting trends and swiftly correcting the problem, as well as exposing and apprehending imposters, so eliminating all of the disadvantages.

1.6 Scope and Limitation of the Study

The goal of this project is to create or create a Fingerprint Based Student Attendance Monitoring System that will enhance attendance by utilizing fingerprint as a means of verification for evidence of attendance in a class.

The limitations of the system are as follows:

i. The system will be a Windows-based application

ii. Microsoft Visual Basic.net will be the chosen programming language for creating the user interface

iii. Microsoft SQL Server for database architecture.

iv. It does not include other areas of biometrics.

1.7 Definition of terms

These refers to the terms that will be encountered in this report

a. Fingerprints (Biological): It is open to feature upgrades and is also incredibly versatile and reasonably priced. Fingerprints provide an ironclad way of personal identification since the ridge arrangement on each human finger is unique and does not change with growth or age. Fingerprints can disclose an individual's genuine identity despite personal denial, changed identities, or changes in physical appearance caused by age, sickness, plastic surgery, or accident. The method of using fingerprints to identify people, known as dactyloscopy, is a vital tool for modern law enforcement. (Edgar)

b. Fingerprints (Technological): Fingerprinting is a kind of biometrics, which is the science of identifying persons based on their physical or biological traits. Even identical twins do not have the same fingerprints. Unless the deep or 'basal' layer is lost or purposely altered by plastic surgery, fingerprints do not change as we age. Fingerprint patterns are classified into three types: arches, loops, and whorls. Each fingerprint is unique because of the form, size, quantity, and arrangement of minute minutiae in these patterns. (INTERPOL)

c. Biometrics: Biometrics is the measuring and statistical analysis of people's unique physical and behavioral features. The technology is primarily used for identification and access control, as well as identifying persons who are under observation. The underlying idea of biometric authentication is that every individual may be reliably recognized by intrinsic physical or behavioral attributes. The

term *biometrics* is derived from the Greek word's *bio*, meaning *life*, and *metric*, meaning *to measure*.

d. Attendance system: Is a system that can keep track of the people that are present in an organization, school, or workplace, and it may be applied in a variety of ways. (INTERPOL)

CHAPTER TWO

LITERATURE REVIEW

2.1 System overview

This proposed system incorporates fingerprint authentication into the attendance management process for both employees and students. It consists of two steps: enrollment and authentication. During enrollment, the user's biometrics are collected, and the minutiae data are extracted and saved in a database as a template for the topic, along with the user's ID. The enrollment module's goal is to accept a user into a database using his or her ID and fingerprints following feature extraction. These characteristics constitute a template that is utilized to identify the user's identity, hence forming the authentication process. An administrator of the attendance management system performs the enrolling procedure. During authentication, the user's biometrics are taken once more, and the extracted characteristics are compared to those already in the database to determine if there is a match. Following a successful match, attendance is recorded against the user id that was used to match the templates.

The study made use of a fingerprint reader as an input to gather photos, and it created a program with a fingerprint recognition and identification system, as well as a database to store user information. The database contains users' fingerprint templates and other bio-data, as well as attendance records. The database comprises the fingerprint templates and other bio-data of the users together with the attendance records made by the users. Figure 2.1 shows the architecture of the proposed attendance management system.

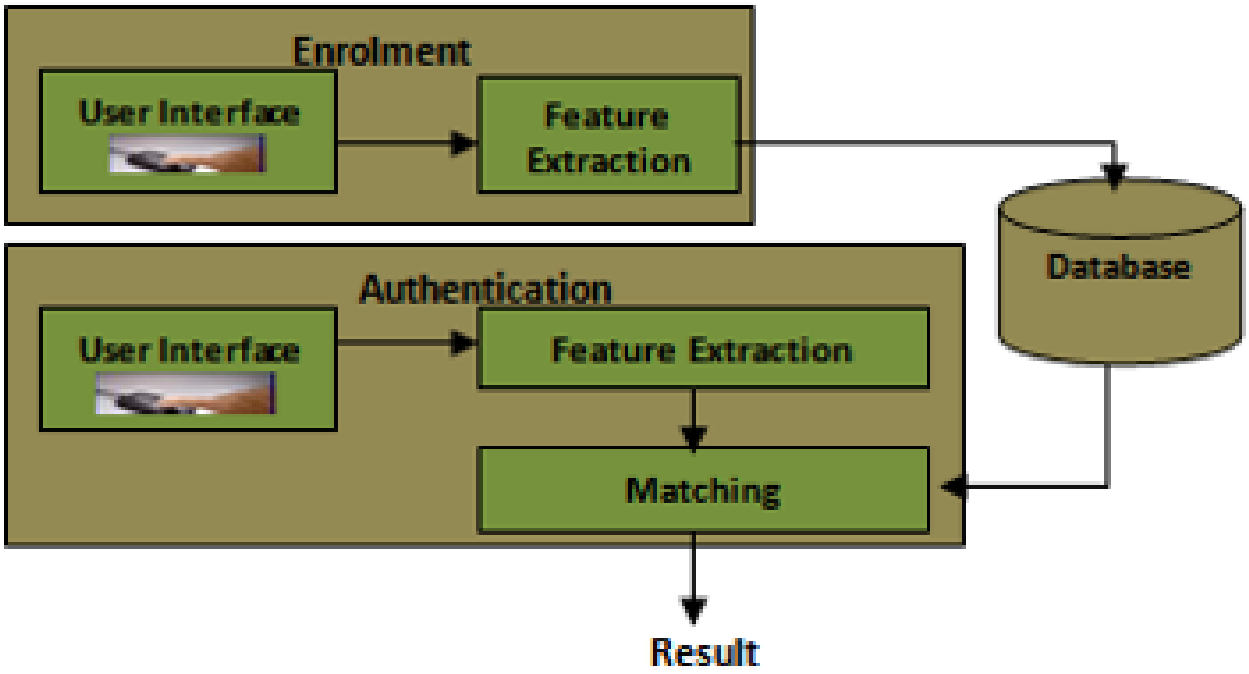

Figure 1.1: Architecture of the proposed attendance management system.

2.2 System architecture

The architecture can be broken down the designs and the way in which we want to implement and develop the fingerprint-based attendance management system in the following stages/modules:

a. Enrolment Stage

b. Authentication Stage

c. System Database

At the enrolment stage in the project, the primary role is to register users and their fingerprints in our system's database. The fingerprints and other bio-data of users are captured, and the unique features are retrieved and saved in our database as a template for the topic, including the user's ID. Matriculation Number, Surname, Other Names, Sex, Level and Course of Study, Department, College (Faculty), Phone Number, email, Department, and Passport Photograph are the bio-data to be captured for students, while those for staff may include: Employee Number, Surname, Other Names, Sex, Position, Staff Type, Phone Number, email, Department, and Passport Photograph. Two picture samples per fingerprint are taken to increase the quality of the kind of image obtained during registration and enrollment.

When fingerprint photos and the user's name of a person to be registered are supplied into the enrollment module, a minutiae extraction method is used to the fingerprint images and the minutiae patterns (features) are retrieved. These characteristics combine to build a template that is utilized to identify the user's identity, so forming the authentication process. An administrator of the attendance management system handles the enrollment process. The enrollment and registration phases are administrative in nature. For the first time, the user's fingerprint and other

bio-data are saved into the database for registration. Courses, practical's, tests, lecturers, and examinations are all registered at this stage. This module contains all of the data and information necessary for accurate attendance tracking.

2.2.1 Fingerprint recognition

Fingerprint recognition is the ability to differentiate between two human fingers. Several print pattern elements, such as ridges and minutiae points, are necessary to match two fingerprints. Ridges have three main patterns: arch, loop, and whorl. Fingerprint recognition has been one of the most essential and popular identifying techniques in recent years due to its high accuracy, and the present fingerprint recognition system is enough for identification and verification systems involving hundreds of users. (Anil K. Jain, 2004). There are three sub-domains in a fingerprint recognition system: enrollment, verification, and identification. Enrolment is the procedure by which a user's fingerprint data is captured using certain sensors and saved in a prepared database after some processing. The collected fingerprint will be compared to the template saved in the database during the verification process to authenticate a person's identification. This procedure is also known as a one-to-one comparison. The goal of confirming these data is to prevent several people from using the same identity.

In identification mode, the system will use a one-to-many comparison to determine the identity of a person. The collected fingerprint will be compared to everything in the system's database, and the only one that fits its record will be chosen.

2.2.2 Patterns of fingerprints

Biometric identification is a groundbreaking technique that identifies persons based on a variety of unique biometric data. Fingerprint recognition is one of these

biometric identifying systems, and it is also the most popular in the world. (Williams, 2019). The following are types of fingerprints

Figure 2:The Arch

i. The Arch

This is the most unusual sort of fingerprint. In reality, around 5% of the world's population has this fingerprint pattern. It is distinct due to the lack of cores, lines, or deltas. Within this pattern, two more sub-categories develop:

a. Plain Arch – This pattern is distinguished by raised ridges that run from one side of the finger to the other in a continuous line. This pattern accounts for only 5% of the total population, making it the rarest.

b. Tented Arch – The tented arch features elevated ridges that flow in the same direction as the plain arch. The pitch of the increased ridge makes a noticeable difference. When contrasted to the plain arch, the tented arch has a sharper edge and generates a tent-like shape.

ii. **The Whorl**

This fingerprint pattern accounts for around 25 to 35 percent of the overall population. Whorls, unlike the arch pattern, feature a core and two deltas. It is only comparable to the arch in terms of sub-categories; it has two:

a. Plain Whorl – A plain whorl will produce a circular pattern resembling a swirl or spiral. This circular pattern is continuous, and the revolution created in the middle is the result of at least one ridge.

b. Central Pocket Whorl – In this design, the center ridges will bend many times to produce a smaller inner whorl.

c. Figure 3: The Whorl

iii. The Loop

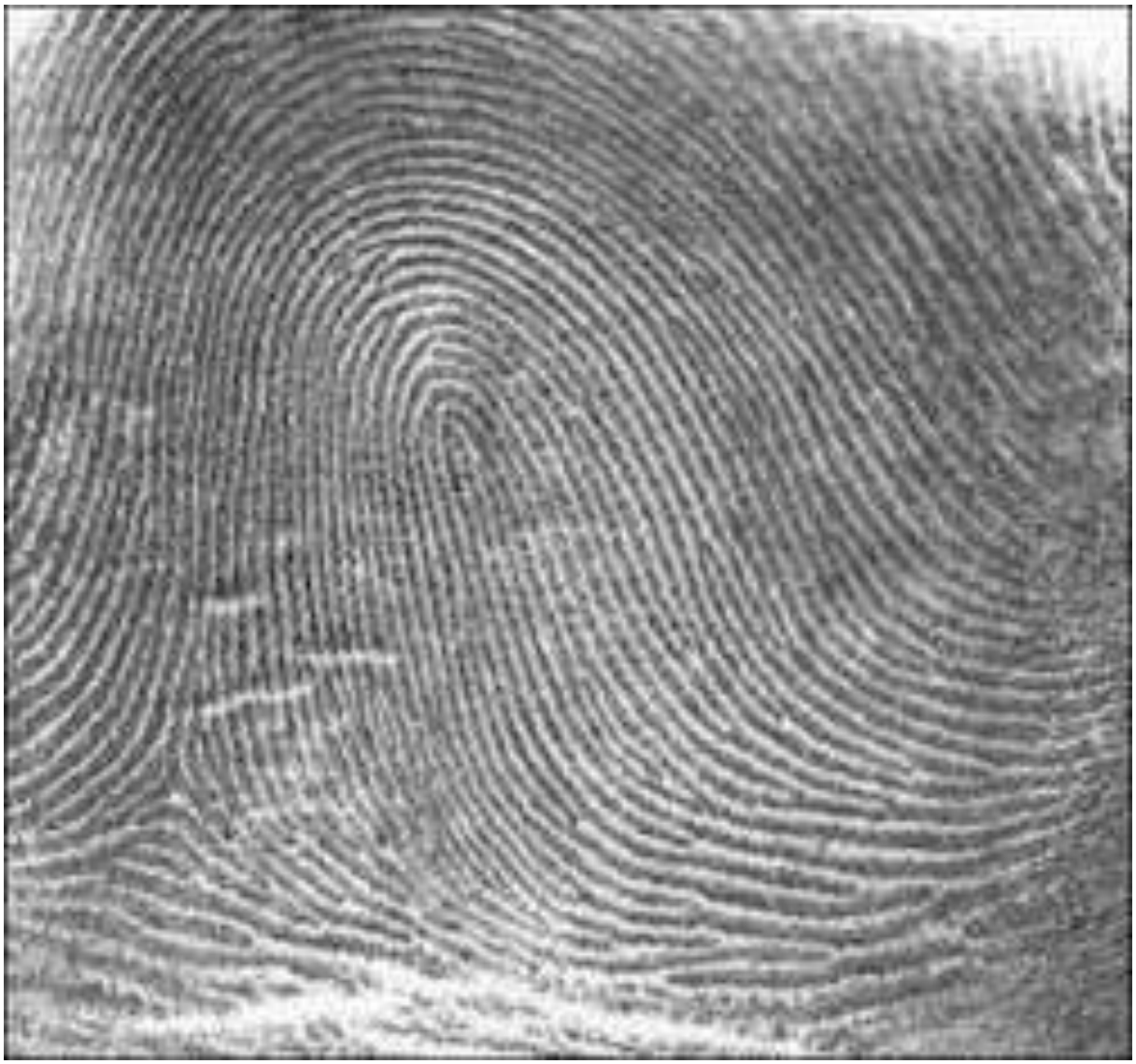

Figure 4: The Loop

The most common fingerprint pattern. Indeed, this trend is shared by 60 to 70% of the whole population. A single core and delta must exist in the loop pattern. Unlike the rest of the patterns, the loop has three sub-categories:

a. **Ulnar Loop** – The ridges turn backward in this design, but not completely. You'll see the loops traveling toward the tiny finger to identify an ulnar loop. These turns will be shown only if you view them on the hand rather than a card.
b. **Radial Loop** – This pattern is similar to the ulnar loop, but the difference is the turns point toward the thumb instead of the small finger.
c. **Central Pocket Loop** –The ridges in this pattern re-curve to surround the central whorl.

Apart from the three main fingerprint types, two more exist:

i. **Double Loop Whorl** – Close inspection reveals two distinct loops that encircle each other from opposing directions.
ii. **Accidental** – This category includes any pattern that does not match any of the other types listed here. These patterns contain two tented arch features: loop or whorl patterns.

2.3 Overview of attendance management

This solution we propose will offer a new automatic attendance management system that will integrate fingerprint authentication into attendance operations and will aid in the management of both staff and student attendance. It has two key processes: enrollment and authentication.

When enrolment is continuing, the biometrics of the user are acquired, and the minutiae data are collected and saved in a database as a template for the subject,

along with the user's ID. The primary goal of the objective module is to be able to admit a user into a database using their ID and fingerprints after extracting different attributes. These aspects contribute to the creation of a template that we will use to identify the identity of each user, forming the authentication process.

An administrator of the attendance management system handles the enrolling process. During authentication, the user's biometrics are recorded again, and the previous characteristics retrieved and saved in the database are compared to/against the one that was just captured. The database contains the user's fingerprint templates and other bio-data, as well as attendance records created by the users.

2.4 Review of related work

(Shoewu O., 2011) For attendance management, an embedded computer-based system is proposed. This system will have a single-chip computer-based subsystem (an electronic makeshift card reader), which will be serially connected to the digital computer's port. The electronic card is a form of smart card that carries the students identify, such as their name as the ID, their matriculation number, and a five-digit pin encrypted code. The card reader verifies the student ID. The card reader delivers data to the backend software system, which is interfaced with the card reader. The software then analyzes the data that has been received and matches the pin code that the card holder enters or inputs into the system with the code that was encrypted into the card. If it matches, the student is permitted entrance to the hall or venue; however, if the authentication fails, the card holder's access is refused. (Akinduyite C.O, 2017).

(V. & A, 2010) The development of real-time computer vision algorithms to be applied into an automatic attendance management system employing Computer Vision and Facial Recognition algorithms, both of which will be integrated into computer-based attendance management systems, is being offered. The systems will eliminate the need to use native methods of taking attendance, such as checking students' Identity Cards and calling their names one at a time from person to person, but the system still falls short of the ability to identify students who are present in class, and facial recognition images are subject to change between the time of enrolment and time of verification, and it later becomes a financial burden during installation and does not offer a financial guarantee.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

A requirement is a statement that describes the intended behavior. It is concerned with system objects or entities, the states that the objects can be in, and the functions that are used to modify the states or features of the objects. The requirements collection and analysis phase's purpose are to comprehend a user's issues and demands, which will serve as the foundation for their expectations of the proposed new system. It entails a thorough examination of the project problem statement, the elicitation of requirements from intended users and other stakeholders in order to create a requirements definition document, and the analysis of the requirements gathered in order to determine the specifications of the proposed new system.

3.2 Analysis of the existing MTU attendance system

Mountain top university's current attendance system is still controlled manually (paper and pen method). Users (students) are required to be at a certain area (the chapel), get themselves certified first by proving their eligibility during the chapel clearing at the beginning of the semester, and seat numbers are also provided to them. Students are to sit in their assigned seats depending on the group and seat number assigned to them, and attendance is taken according on what the administrators have on their list. The analysis of the manual system was looked into and the following benefits and demerits was identified.

3.3 Benefits of the Existing System

The benefits of the existing system are:

i. Students must be physically present.

ii. Familiarity of faces aids students' identification.

3.4 Limitations of the Existing System

Despite the claims of openness and system stability, the existing voting process is not without flaws. The findings listed below urge for changes in the way this entire procedure is carried out.

i. Low percentage of taking attendance.

ii. It is time and costly to produce report.

iii. It require more material (A4 paper).

iv. Lack of security.

3.5 Analysis of the proposed system

The new system authenticates users by using a biometric characteristic (fingerprint). Because fingerprint identification hardware is connected with the system, the manual system must be solved. The new system operates in an identification mode and performs the following:

i. Captures fingerprints, extracts the features and stores it in the database.

ii. Verifies the identification of users (students) upon registration by matching the fingerprint saved in the database with the fingerprint submitted when collecting attendance.

iii. It provides a user interface for registering and monitoring individual attendance rates.

iv. Allows administrators to view attendance for each service via an interface.

3.6 Design Goals for the Proposed System

i. Student authentication: Students should be who they are.

ii. Verifiability of attendance: Safe tracking of attendance system to ensure that students are registered and their information's are stored.

iii. Safe transfer of user's attendance from the fingerprint scanner to the server.

iv. Uniqueness of casting - Data cannot be tampered with.

3.7 Functional Requirements of the Proposed System

Functional requirements are the capabilities of the system and domain specific. The fingerprint biometric attendance system has the following functional requirement:

i. The system must provide the accurate data.

ii. The system must supply standard reports for decision making.

iii. The system should allow admins to make updates to student information in the database.

iv. The system must provide data integrity checks to ensure that data remains consistent and updated.

v. Audit trails of who made changes to the database must be maintained.

3.8 Non – Functional Requirements of the Proposed System

The non-functional requirements of the system include:

i. During the registration or attendance procedure, the system must operate at peak efficiency.

ii. Backup data restore capabilities should be granted.

iii. The system must conform to the requirements of the university chapel authorities.

3.9 Security Requirements

The fingerprint biometric attendance system would be required to enforce the following security rules or requirements in order to fully satisfy and build the trust of the attendance populace in the system. The security requirements are listed below:

i. The system should have zero-tolerant with regard to compromising.

ii. The system should provide accurate time and date setting.

iii. The system should not allow unauthorized users to interfere with the system database.

iv. The system should provide means for protecting and securing recounts of students.

v. The system should not allow improper actions by students or admins (chaplaincy unit workers).

3.10 Waterfall Development Method

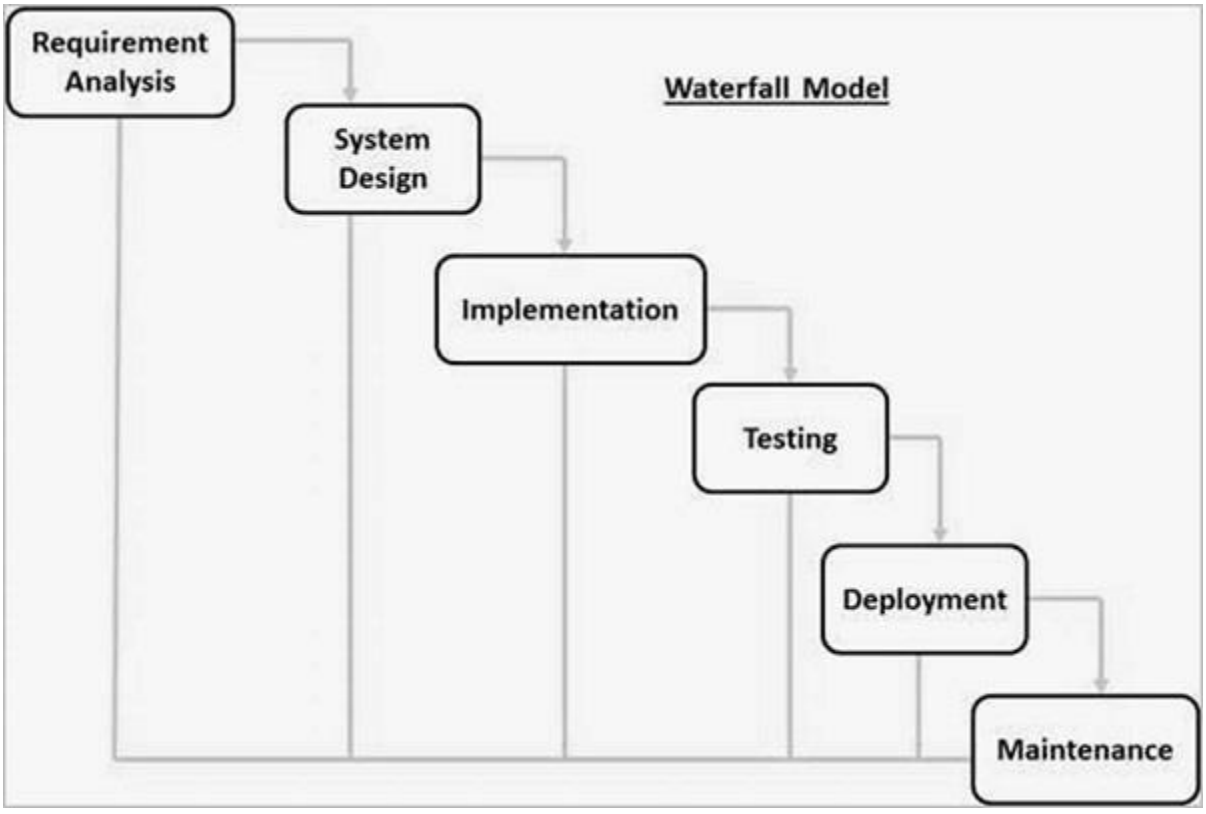

Figure 5:Diagram showing waterfall model

3.10.1 Steps for Waterfall Model

From figure 6 above, the steps for waterfall model can be briefly explained as:

i. **Requirement Gathering and analysis** - This phase captures and documents all conceivable system needs. The specifications of the input and output or end product are analyzed and marked here

ii. **System Design** - This phase studies the need specifications from the previous phase and prepares the system design. This system design aids in the specification of hardware and system requirements, as well as the definition of overall system architecture.

iii. **Implementation** - With input from the system design, the system is first built-in tiny programs called units, which are then combined in the following step. Unit Testing is the process through which each unit is designed and tested for functioning.

iv. **Integration and Testing** - After testing each unit, all of the units built during the implementation phase are merged into a system. Following integration, the complete system is tested for defects and failures.

v. Deployment of system - The product is deployed in the client environment or delivered to the market once functional and non-functional testing is completed.

vi. Maintenance - Some difficulties arise in the client environment. Patches are provided to address such concerns. Additionally, improved versions of the product are published in order to improve it. Maintenance is performed to ensure that these modifications are implemented in the client environment.

3.11 Design of the proposed system

After defining the needs of the proposed system, I will describe the system's architecture, which will include the use of software modeling tools to structure requirements. We may gain a complete understanding of needs by structuring them. It is critical to use standard notations when modeling, documenting, and conveying choices.

In this project work, use case models, data flow diagrams, entity - relationship models, and hierarchy chart, as well as input, process, and output (HIPO) diagrams, would be used to specify the functionality and non-functionality of the proposed attendance system with biometrics fingerprint authentication.

3.11.1 Entity Relationship (E-R) Diagram

An entity-relationship diagram is a data modeling approach that generates a graphical representation of the entities and their connections inside an information system. It provides a visual depiction of various data utilizing conventions that specify how these variables are connected to one another. It contains three notations: entity, relationship, and cardinality.

3.11.2 Data Flow Diagrams (DFDS)

A data-flow diagram is a model that depicts the graphical movement of data through an information system, the links between the data flows, and how data ends up in certain areas. Data-flow diagrams may depict the processes that modify or transform data. The data flow diagram focuses on the transit of data between processes, which are referred to as process models.

3.11.3 Context data flow diagram

The Context (Level 0) Data Flow Diagram provides an overall perspective of the system's core entities, processes, and data flow. It does not display a data storage.

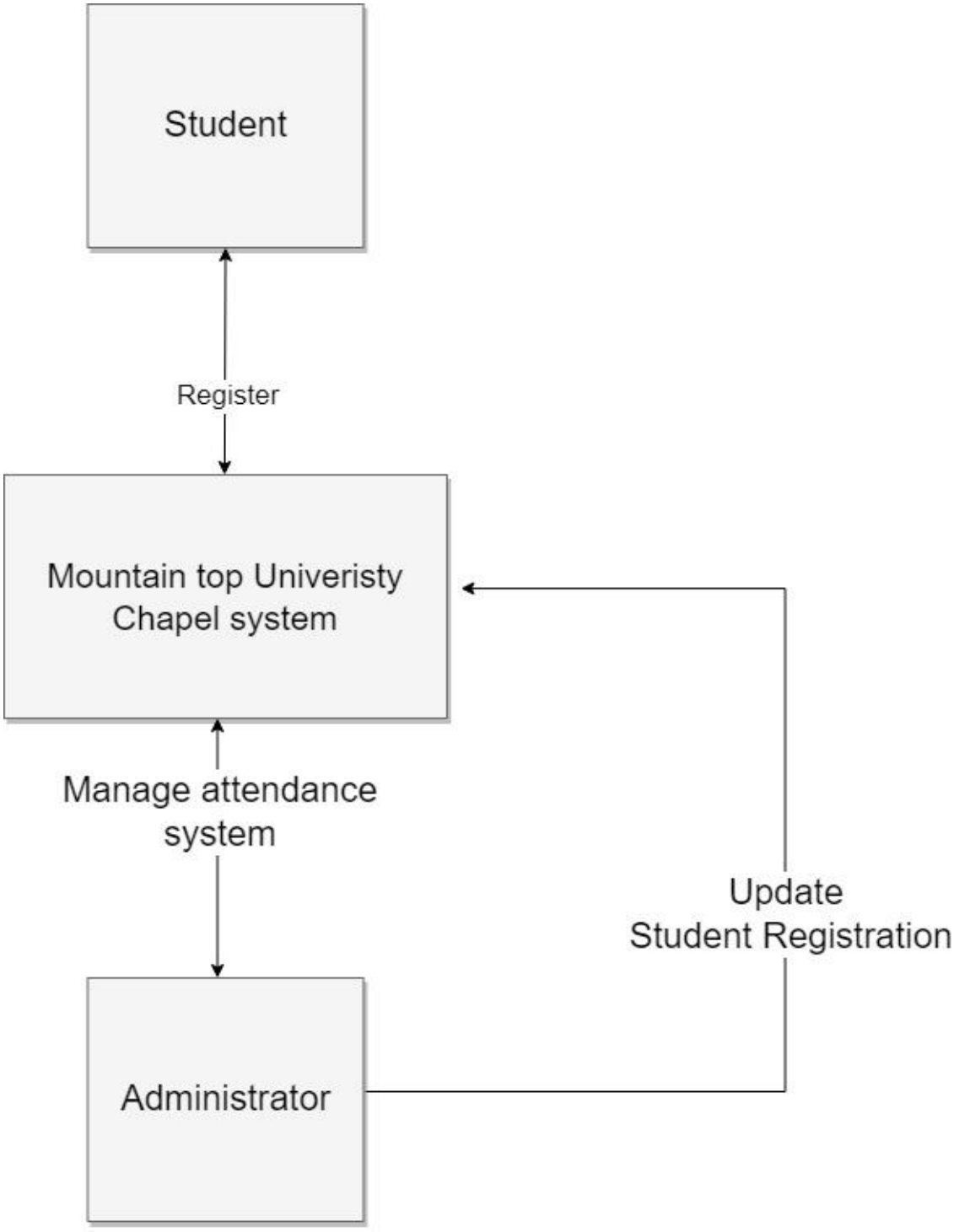

Figure 6:DIAGRAM SHOWING CONTEXT FLOW

The Offline (Desktop) module of the attendance system comprises of two major activities, which are the user Registration and Enrollment Process as well as the user Verification Process.

Their respective Data Flow Diagrams are shown below

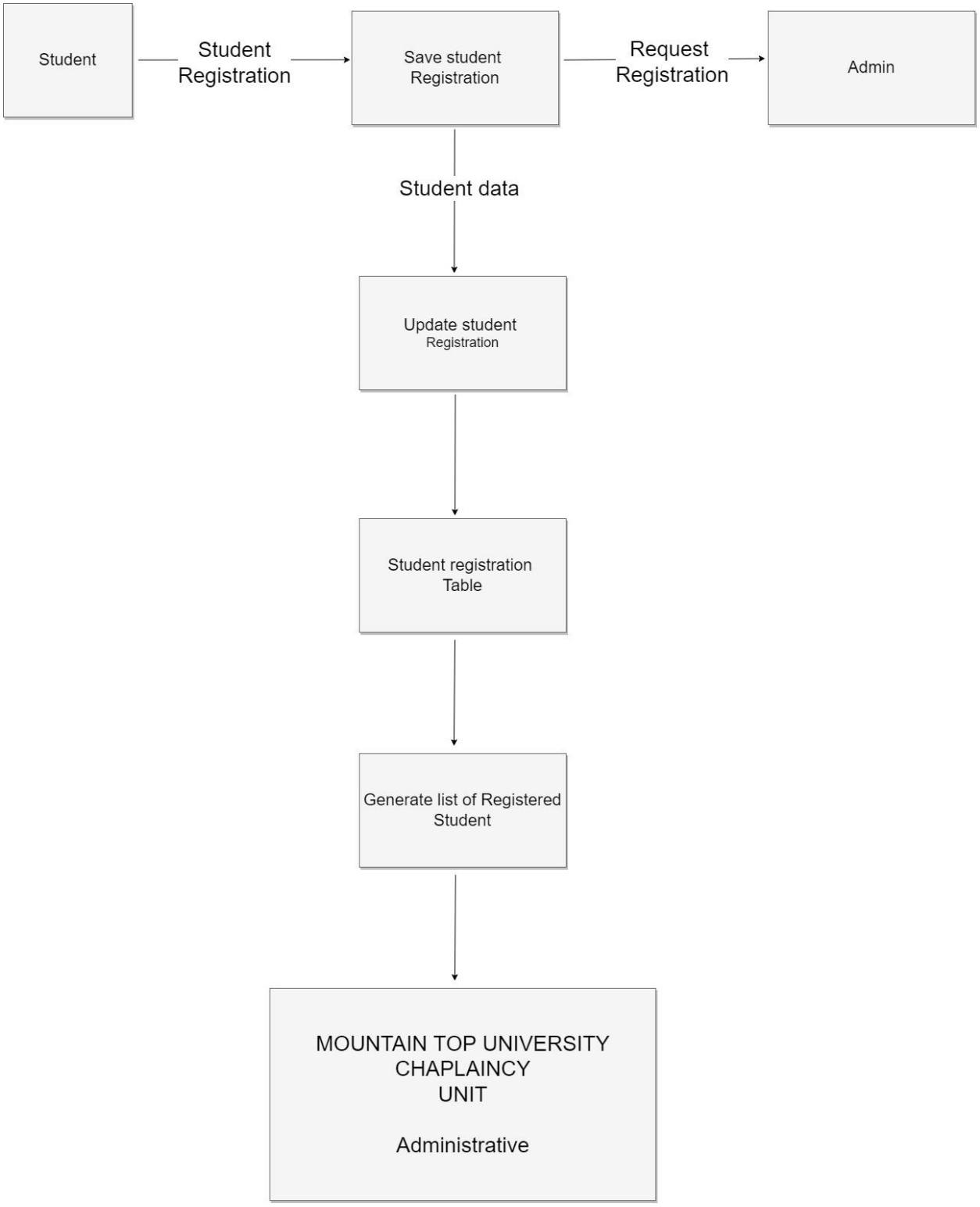

Figure 7:DIAGRAMS OF OFFLINE (DESKTOP) SUB-MODULE

3.12 PROCESS FLOW – CHARTS

Flowchart for fingerprint biometrics attendance system. Figure 9-10 shows the flowchart diagram.

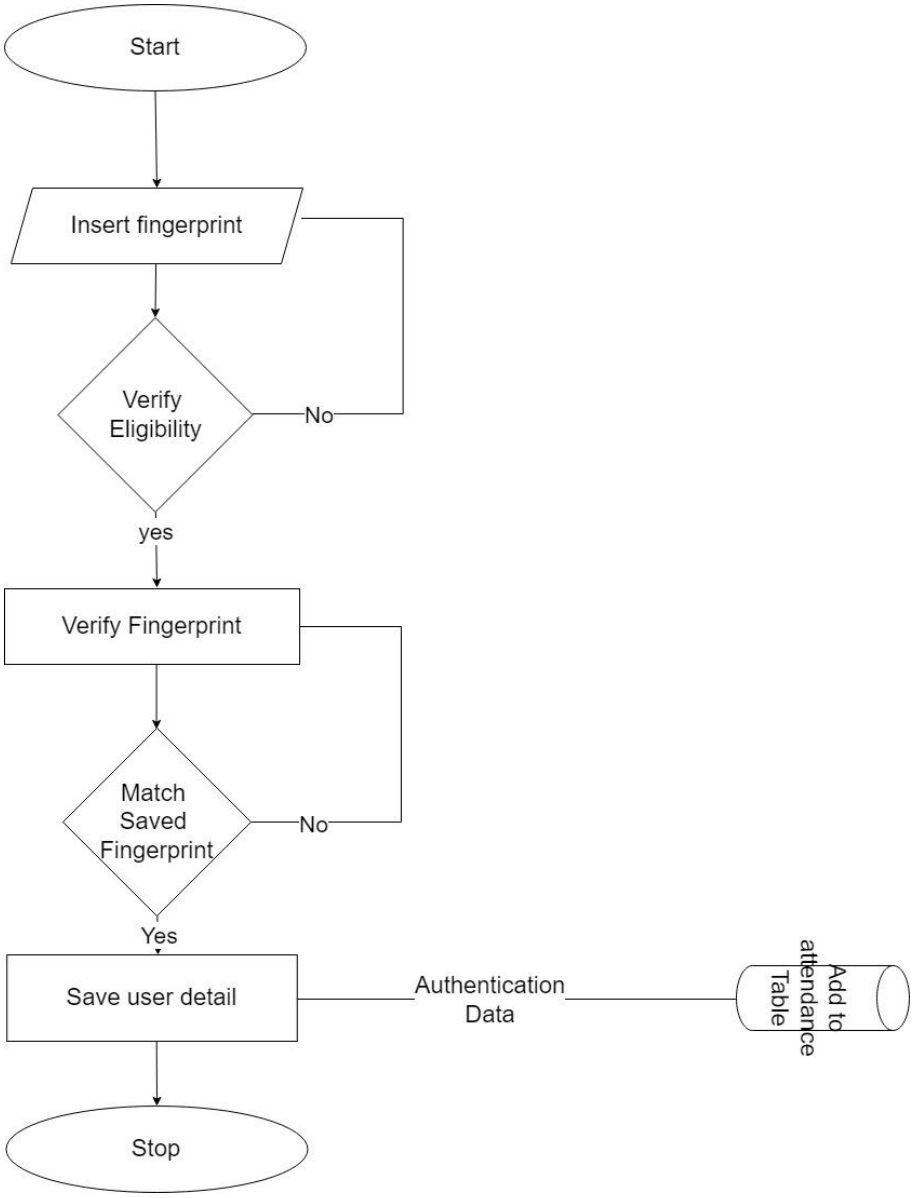

Figure 8:Flowchart for voter's verification and authentication

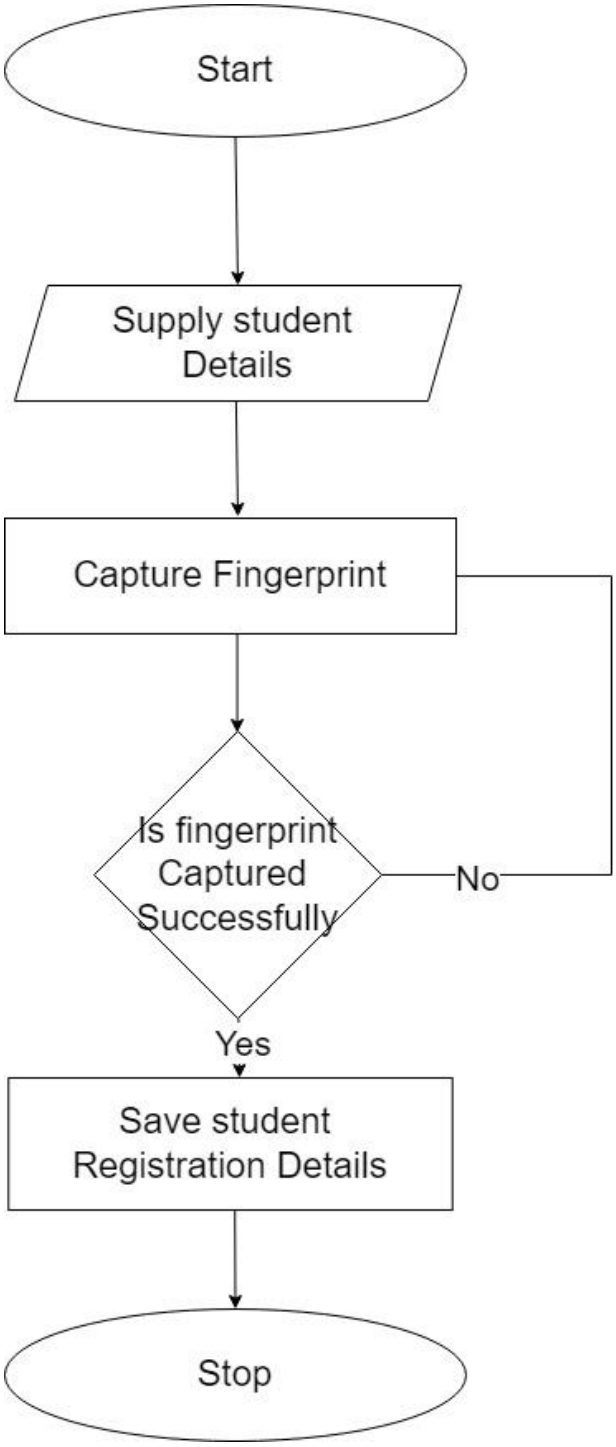

Figure 9:Student registration for attendance system flow chart

3.13 Use Case Diagram

The use case diagram is a graphical representation of the fundamental parts and operations that comprise a system. The fundamental pieces are referred to as "actors," and the procedures are referred to as "use cases." It demonstrates how actors interact with each use case. Figure 11 shows the Use case diagram below

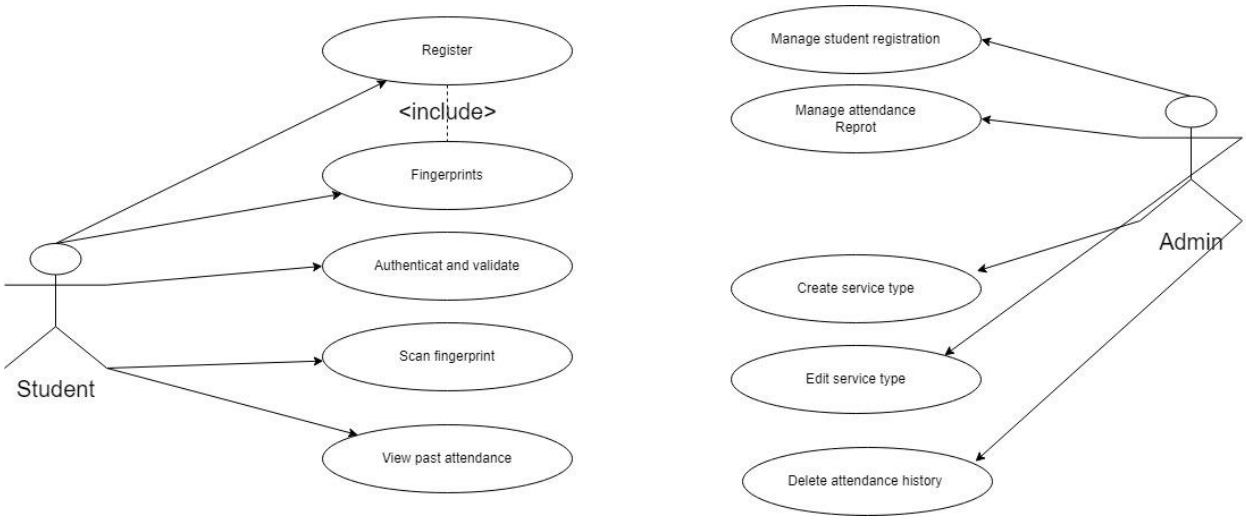

Figure 10:DIAGRAM SHOWING USE CASE

Following below are the breakdown of the individual Use Cases. Each showing the Actors, Input and Output respectively

Actors and their use cases

Actor: student

1. Register: This is a critical functional need of the system. The student's information as well as the fingerprint template are entered into the system and saved in the database.

2. Fingerprint: Students must register their fingerprints, which will then be used to track attendance.

3. Authenticate and validate: Fingerprints are confirmed and checked for correctness.

4. Scan Fingerprint: Fingerprints would be checked at the door post before students could enter the chapel.

5. View past attendance: Students can view their past attendance and keep check too.

Actor: Admin

The is an administrator who manages the operation of the Offline (or Desktop) module of the University chapel attendance system.

USE CASES:

Manage students' registration: Admin can edit and register students.

Manage student attendance report: Admin can be able to view the report of each attendance for each service.

Create service type: Admin can create service type for the attendance of that particular service.

Edit service type: Admin can edit and delete service type.

Delete past attendance: Admin can delete the past attendance which has been take and it's not really valid.

3.14 Entity Relationship (E-R) Diagram

An entity-relationship diagram (ERD) is a data modeling approach that generates a graphical representation of the entities in an information system as well as the interactions between them. It provides a visual representation of many data types by utilizing conventions that specify how these data types are connected to one another. Entity, Relationship, and Cardinality are the three notations.

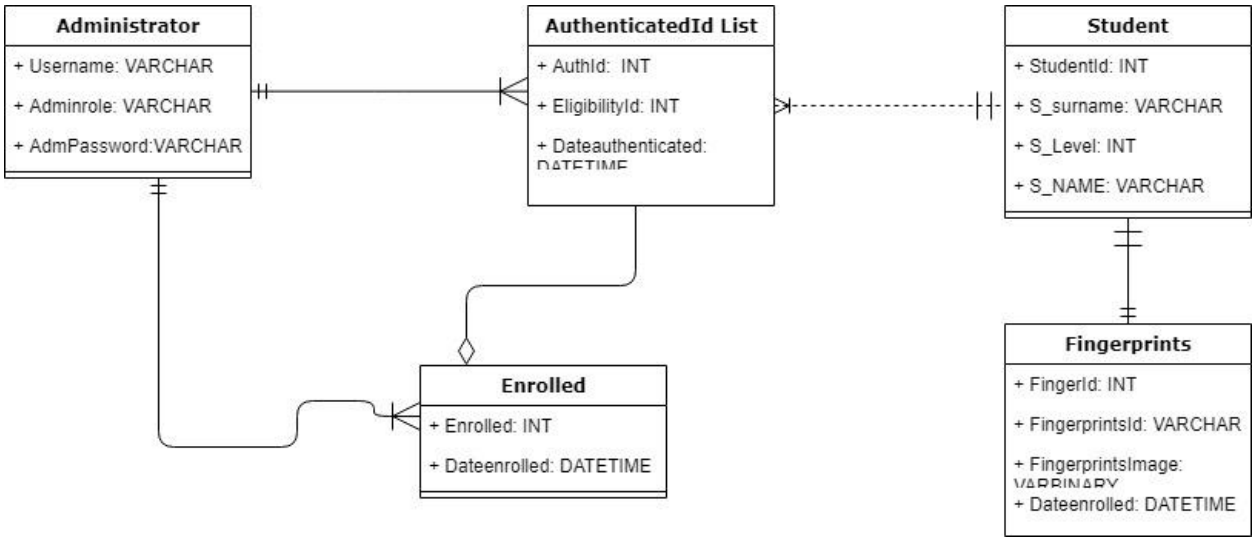

Figure 11:DIAGRAM SHOWING ER RELATIONSHIP

3.15 The fingerprint module

This module is used to gather user fingerprints. Several suppliers provide various types of fingerprint readers as well as their accompanying Software Development Kits. The DigitalPersona U.are.U 5000 fingerprint reader would be employed in the proposed new system. As shown in the table below, the aforesaid fingerprint reader has the following specifications:

Table 3.1 The DigitalPersona U.are.U 5000 reader specifications

Sensor Type	Optical
Resolution	512 PPI
Image size	355x390 pixels
Image Capture Area	14.6mm width at 18.1mm length
Colors	8-bit grayscale (256 levels of gray)
Device Connection	USB 1.0, 1.1 and 2.0 Full Speed
Supported OS	Windows 7/Vista/XP/2003/2000

Figure 12:DIAGRAM SHOWING FINGERPRINT MODULE (Adesua, 21 November 2016.)

3.16 Hierarchical (hipo) diagram

HIPO is a pictorial approach for describing a system. HIPO (Hierarchy plus Input-Process-Output) is a strategy for designing and/or documenting a computer program. A HIPO model consists of a hierarchy chart that graphically displays the program's control structure and a series of IPOS (Input-Process-Output) charts that explain the inputs to, outputs from, and functions (or processes) performed by each hierarchy chart module. Hierarchical input-process-output diagram showing student registration. Its shows the logical connection of registration authentication and to view all registered student.

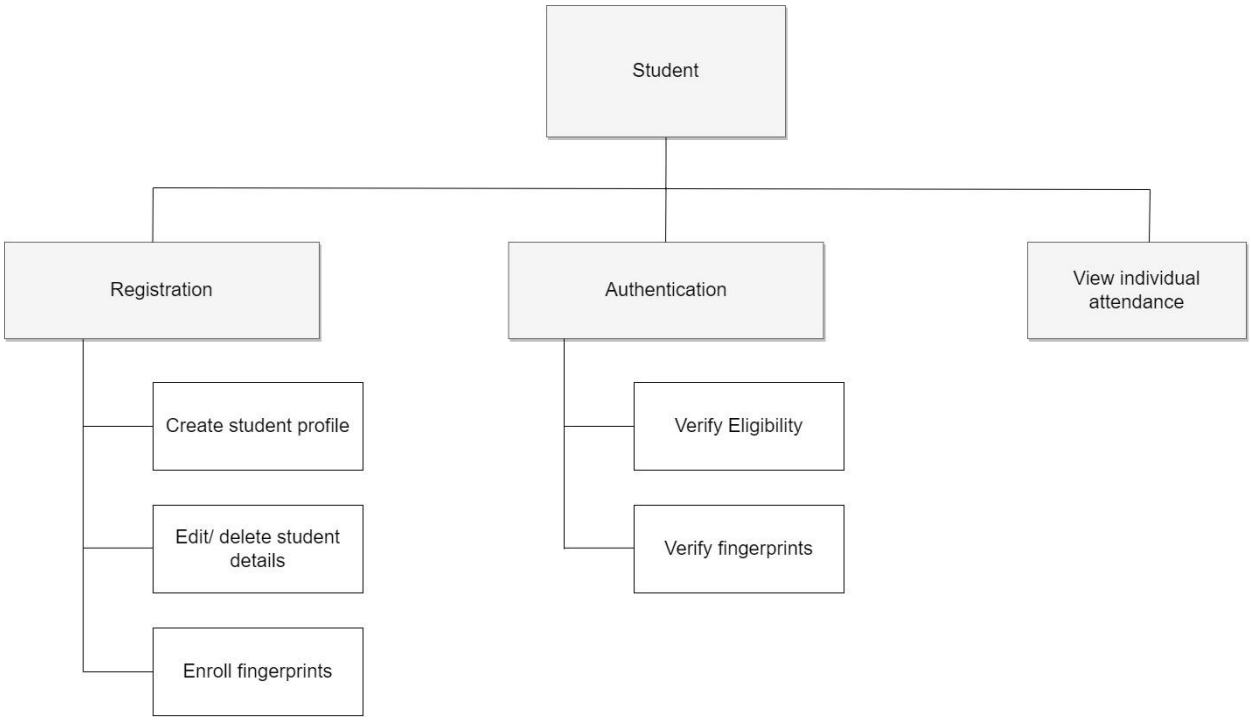

Figure 13:Diagram showing student registration

Hierarchical input-process-output diagram showing the attendance system. It shows the logical connection of the various processes that can be carried out by the two major entities on the attendance system, that is; the Student and the Administrator. It is worthy to note that both system users (student and administrator) have different interfaces from which they gain access into the system.

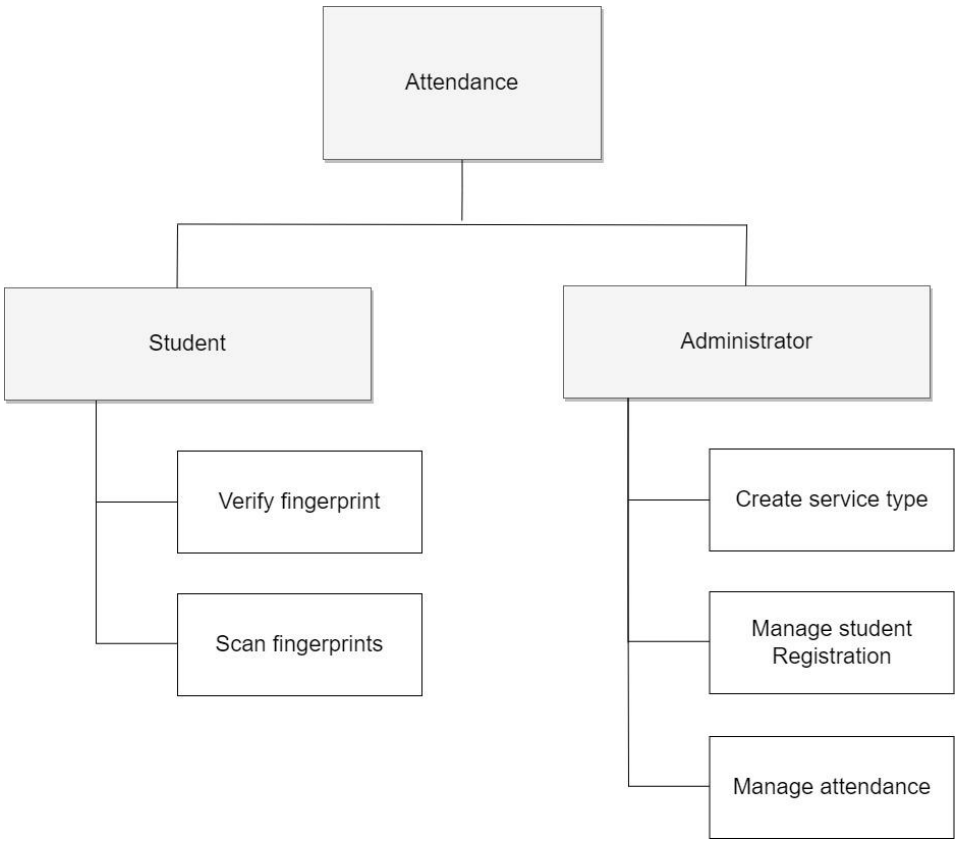

Figure 14:Diagram showing the attendance system

3.17 Fingerprint Enrolment

The first process of gathering fingerprint data from a user (student) and saving the obtained data as a fingerprint template for subsequent comparison is known as fingerprint enrolment. The technique described below is common for fingerprint enrolment.

3.18 Enrollment Workflow Procedure

i. Obtain the user's identification number (Student Identifier).

ii. Capture the user's fingerprint using the fingerprint reader.

iii. Take the fingerprint feature set for enrolment from the fingerprint sample.

iv. Repeat steps 2 and 3 until you have enough fingerprint feature sets to create a fingerprint template, typically four times.

v. Create a fingerprint template.

vi. Through the Subject Identifier, such as a user name, associate the fingerprint template with the person.

vii. Keep the fingerprint template and the Student Identifier for future comparison. Fingerprint templates can be saved in any form of repository, although a local database is utilized for this project.

3.19 Fingerprint verification

Fingerprint verification is the process of comparing fingerprint data to the fingerprint template generated during enrollment or registration and determining whether or not the two matches. The technique outlined below is usual for fingerprint verification.

Verification Workflow Procedure

i. Obtain the student Identification number of the person to be verified.

ii. Capture a fingerprint sample using the fingerprint reader.

iii. Extract a fingerprint feature set from the fingerprint sample for verification purposes.

iv. Get the fingerprint template for the Student Identifier from your repository.

v. Conduct a one-to-one comparison of the fingerprint feature set and the fingerprint template, and make a decision of match or non-match.

vi. Act on the decision accordingly.

3.20 System architectural design

The suggested architectural design system is a diagram that outlines the link between important structural aspects of the program, design patterns that may be utilized to accomplish the system's requirements, and restrictions that determine how architectural design patterns can be applied.

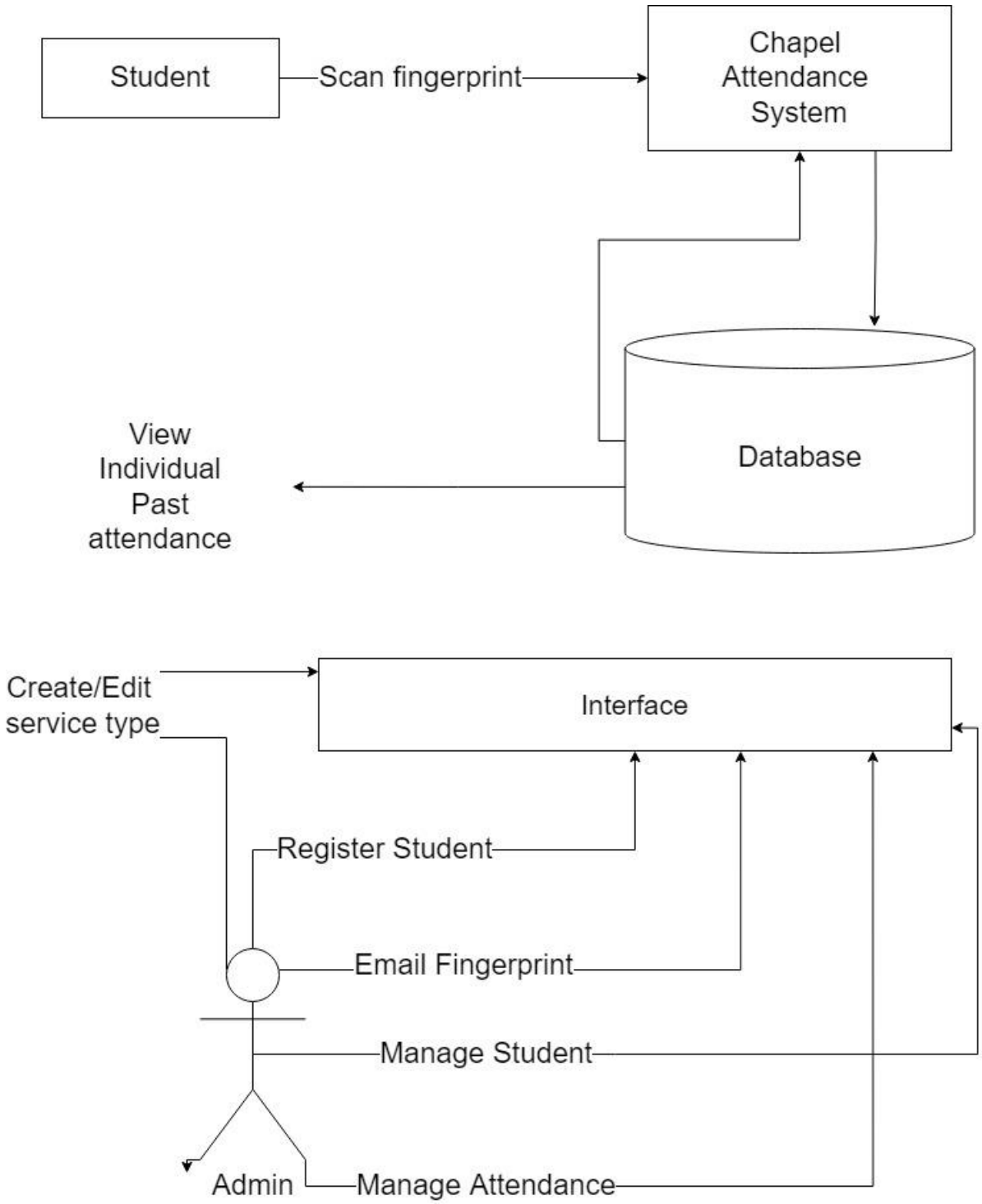

Figure 15:Diagram showing system architectural design

CHAPTER FOUR

IMPLEMENTATION AND RESULT

This chapter provides an overview of the attendance system's development and testing: it begins with program implementation specifics for the system, then moves on to a higher-level perspective of the system, and finally concludes with methods and requirements for deploying the attendance system.

4.1 Choice of programming languages

i. **CSS** stands for cascading style sheet, and it was used on this project to improve the design of the webpage by adding detailed CSS styles, making the webpages of this project more appealing and pleasant to read and use for both the user (students) and the administrators.

ii. **HTML** stands for Hyper Text Markup Language. It is used in this project to write explicit instructions on the style, type, format, structure, and makeup of a webpage before it is exposed to consumers. It facilitates in the structuring of this project's websites into sections such as paragraphs, sections, and headers.

iii. **JavaScript** is a programming language that allows webpages to think and behave in real time. It was utilized in this project to provide interactive functionality to webpages like as disclosing or hiding more information with the click of a button, cycling through a carousel of photographs on the main page, and leveraging a drop-down hamburger menu.

iv. **PHP** This program's online sub-system was constructed with PHP, which is now object oriented and hence excellently suited to the task of building this application. It is also less expensive to deploy online, thanks to the language's open-source nature and a large range of technical help.

4.2 System requirements

The system requirements under the headings of the hardware, and software requirements would be discussed below

4.2.1 Hardware Requirements

The hardware requirements of the system include the following:

i. A Fingerprint Reader: A Digital Persona Digital Persona 5000 fingerprint reader was used during the development of this application.

ii. A Compatible Computer: The application was ran on a computer with at least

the following configurations:

a. 4 GB RAM

b. 2.20 GHz Dual-Core CPU Processor

c. 500 GB HDD

4.2.2 Software Requirements

The software requirements of the application are as follows:

i. Windows 7/8/8.1 32/64-bit Operating System

ii. MySQL Server

iii. JAVA Development Kit

iv. Fingerprint SDK license

v. A compatible browser, for accessing the online module.

4.3 Personnel Training

It is necessary for the admins or personnel that would be handling the system to be well trained on how to properly and ethically use the system. They would need to be conversant with the system as well as the various of the system.

4.4 Development tools

i. Xampp server

ii. Visual studio code

4.5 System screenshots

The images below show the screenshots of the system from both the user's (students) and administrator perspective or account.

4.5.1 User Interface Attendance system for student

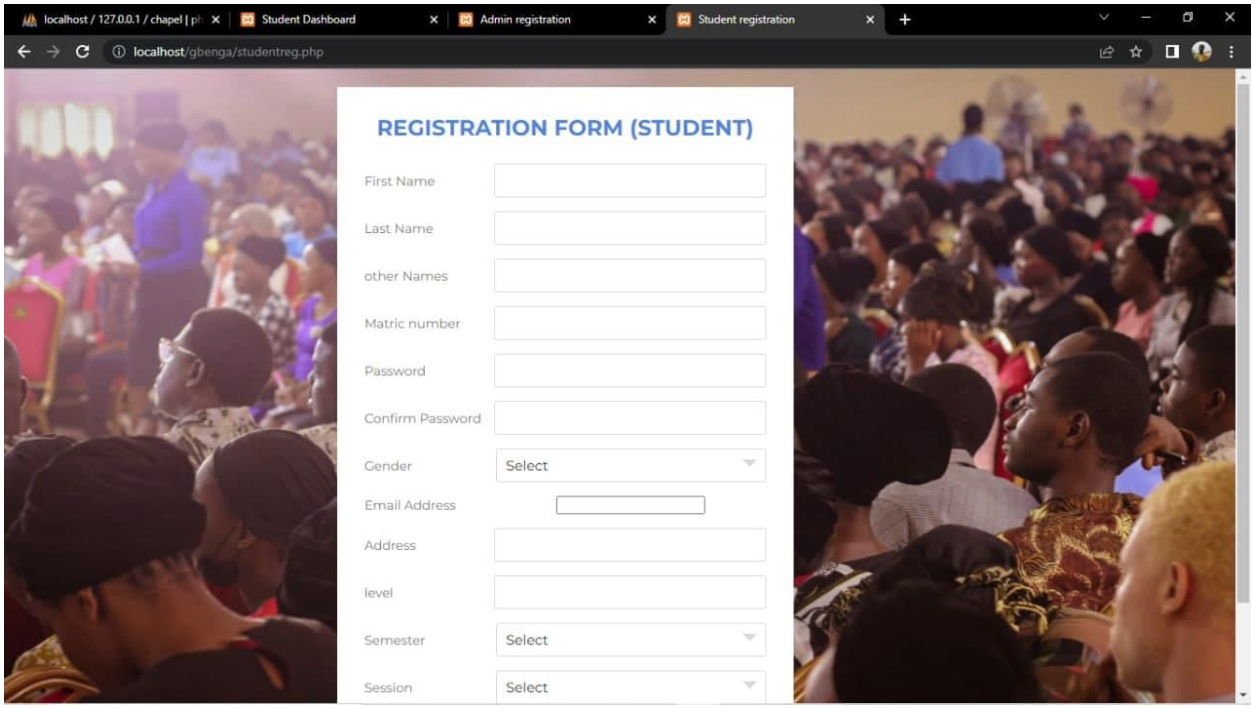

Figure 16:Student Login screen

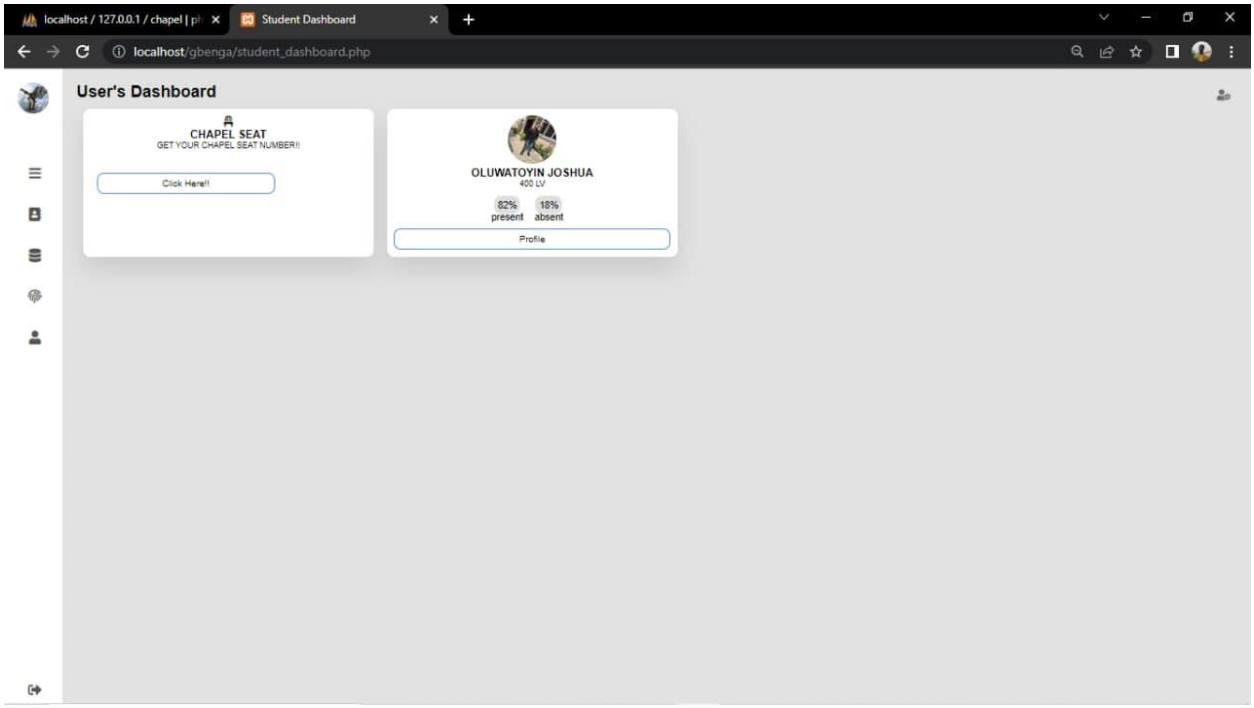

Figure 17:Student Dashboard

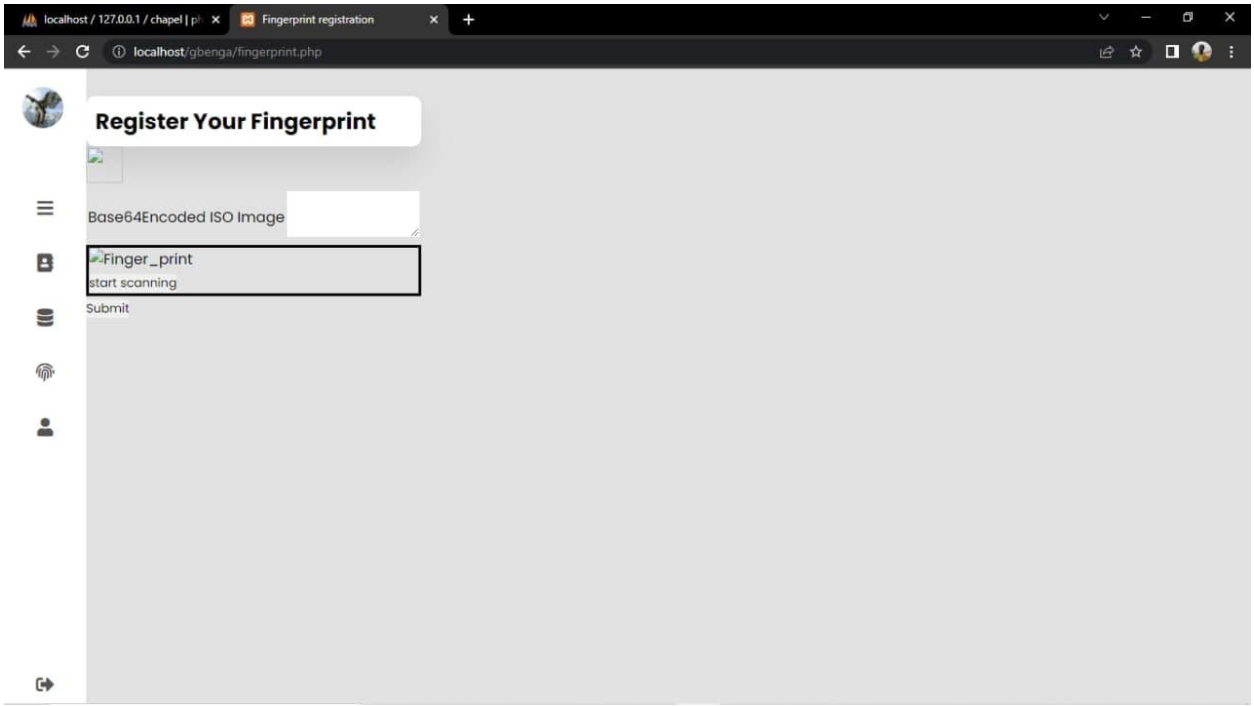

Figure 18:Student Fingerprint Registration

4.5.2 User Interface Attendance system for Administrator

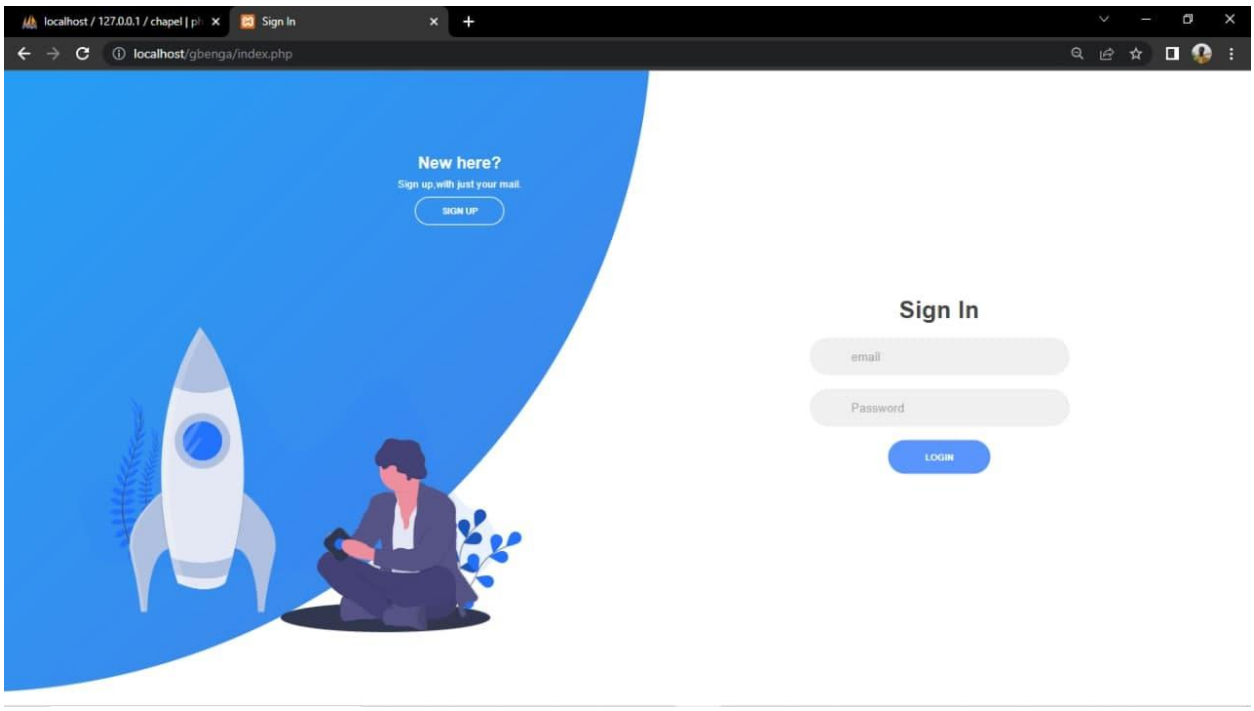

Figure 19:Administrator sign up and sign in screen

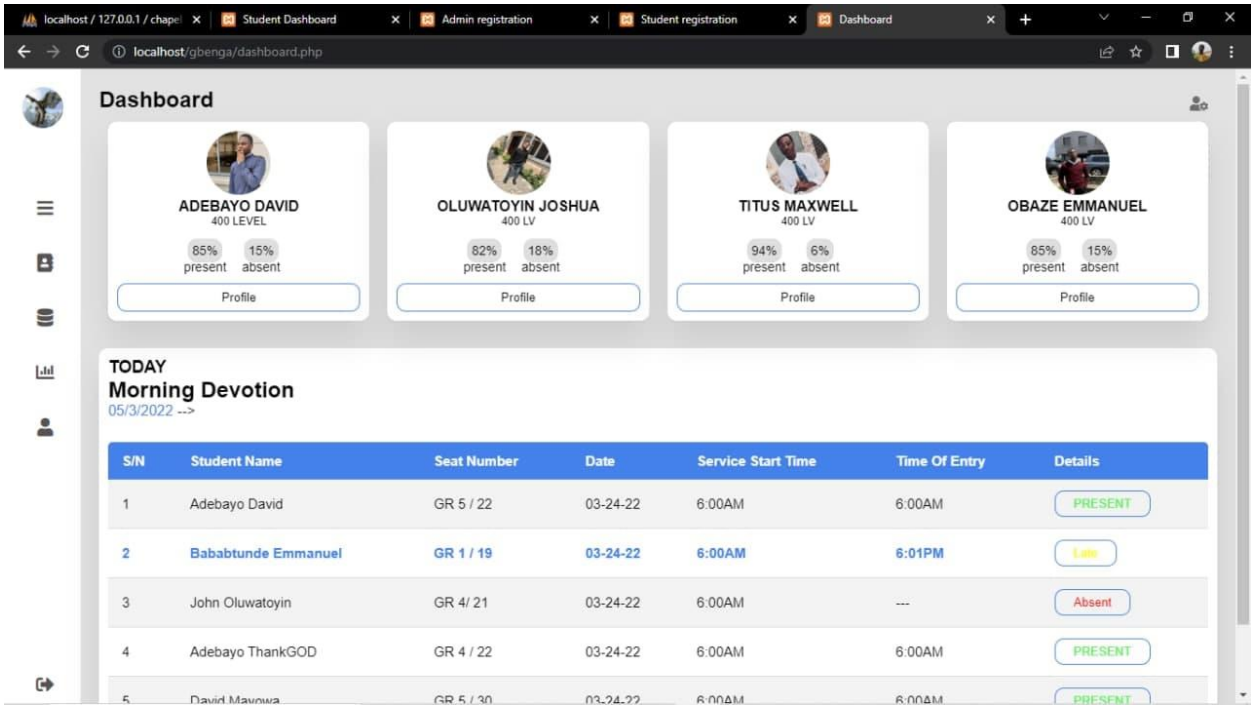

Figure 20:Administrator Dashboard

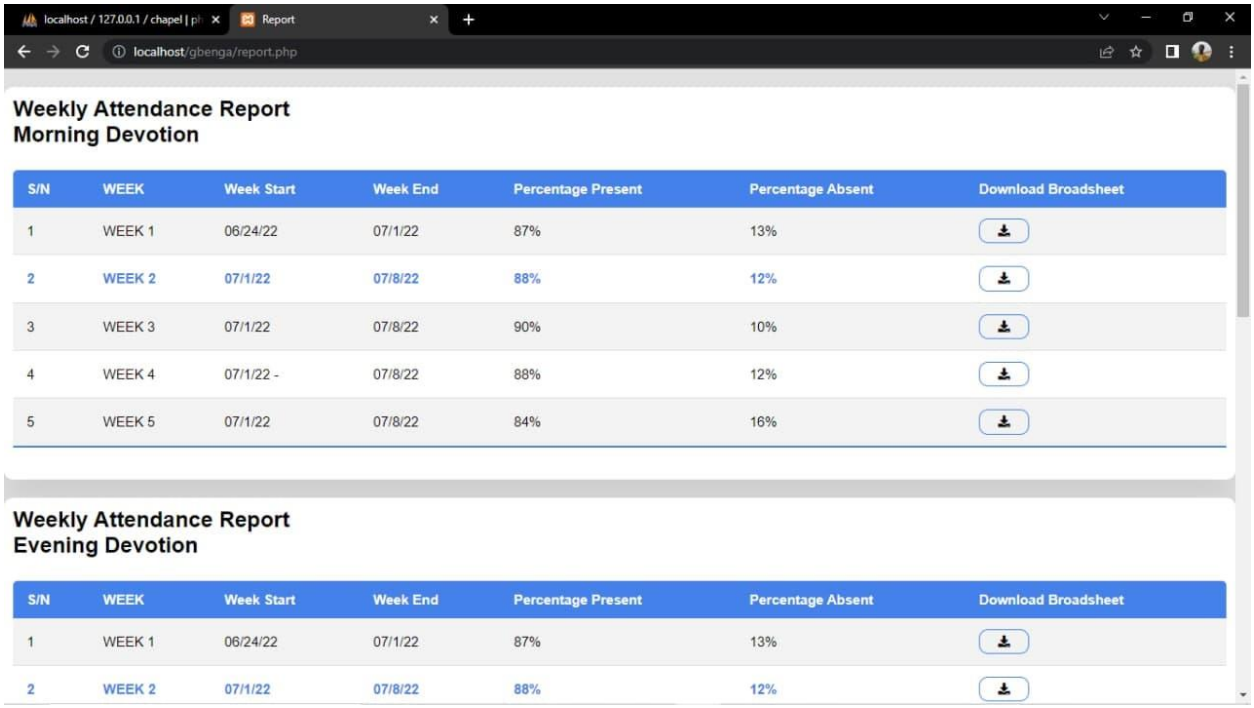

Figure 21:Attendance Weekly report

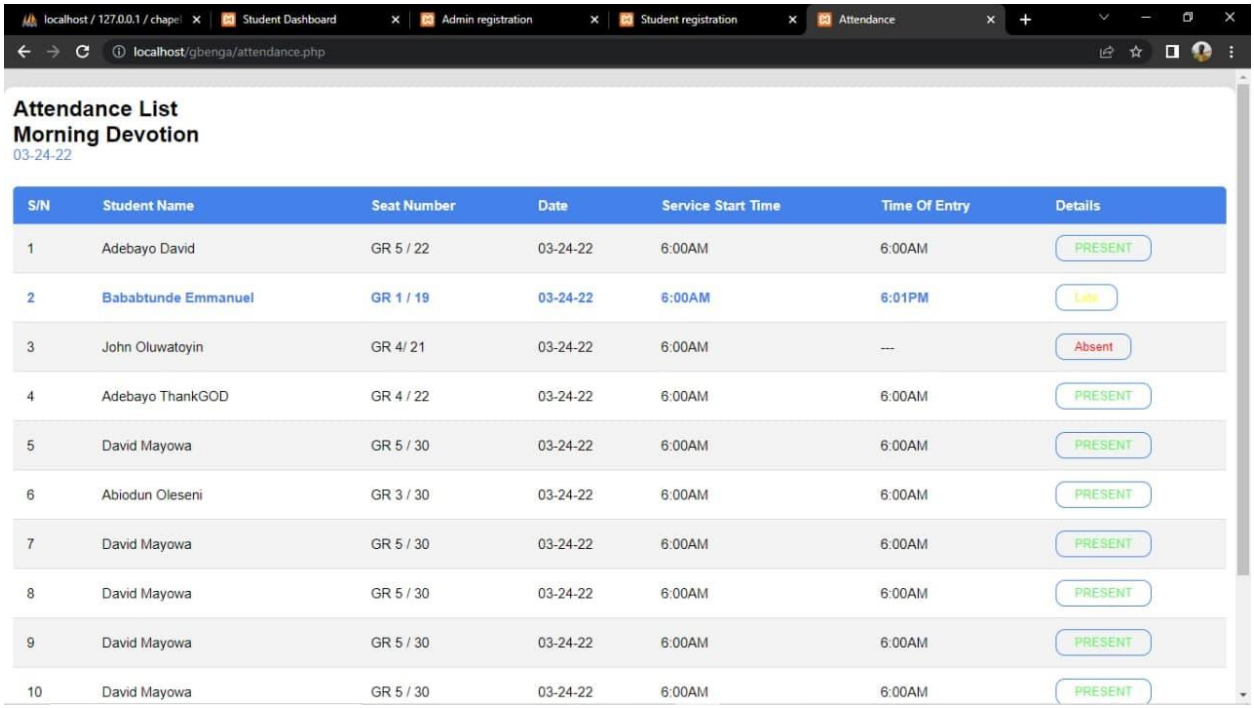

Figure 22:Attendance list

4.6 System testing:

Software testing is required to check for the presence of flaws in the software and make improvements to eradicate the flaws. Testing is required to avoid system failure. The major testing done include:

i. **Unit testing:** splits the software down into components and tests the functionality of each independently inside the programming environment It also examines if each component works as, it should, why it receives the needed input and delivers the required output.

ii. **Integration Testing:** This was done once each software module had been tested satisfactorily. Testing is carried out by developing interfaces between components and ensuring that they interact effectively and that essential input and output is exchanged for the overall efficient operation of the system.

iii. **Acceptance Testing:** Following the system's implementation, acceptance testing was carried out. Acceptance testing will determine if the system operates successfully in the user environment and whether all user-specified features are available. It also determines if the system follows the regulations and quality standards.

4.7 Chapter summary

This chapter describes how the system should be configured in order for it to perform efficiently, as well as the procedures that all system users should take. It provides customers with concise documentation as well as information on testing techniques conducted on the project.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATIONS

5.1. Summary

Using Mountain Top University Chapel as a case study, this project aimed to create a system for collecting attendance. With issues of trust, credibility, and user apathy recurring in the traditional manual method of taking attendance with the university chapel community, the development of this attendance system with fingerprint biometrics authentication - specifically the use of student fingerprints - will be a welcome innovation to the attendance process in general.

This project implements a biometric attendance system for Mountain Top University Chapel in order to reduce, if not eliminate, the issues of eligibility, erroneous user (student) information, and the centralized and stressful human attendance routine.

5.2. Conclusion

Traditionally, student attendance is recorded manually using pen and paper registers. The introduction of a biometric-based technique of attendance management system would considerably aid institutions or any company and therefore eliminate time-consuming operations. The biometric attendance system allows administrators to easily obtain student attendance statistics as well as monitor weekly or monthly attendance summaries. This will increase the net productivity of institutions or any organization. The suggested system is dependable, secure, and efficient, and it is capable of replacing the existing manual and unreliable way of attendance management. This approach maintains the security of student records, eliminates phony attendance records, saves time, and reduces the amount of effort done by the administrator in acquiring student attendance records. The suggested

system may be enhanced by using multimodal biometric technologies to increase the security of the student attendance management system.

5.3. Recommendation

The following recommendations of this system implementation may simplify and ease the burden for the administrators as reporting and analyzing of data will be improved. Several improvements can be done for further development as follow:

i. **Upgrade to mobile application:** Mobile application will be more practical since the emergence of mobile application technology has become a bridge to communication and expand profit in more business industries.

ii. **Integrate with existing system:** Student attendance system using fingerprint can be integrated with existing Campus Management System (CMS) in providing existing database of admins (chaplaincy unit workers) and students.

iii. **Reporting:** More related reports should be produced to see more information about the users (students).

References

Adesua, O. (21 November 2016.). *ONLINE VOTING SYSTEM WITH BIOMETRIC AUTHENTICATION FOR UI.* University of Ibadan.

Admin, B. (2021, December 8). *https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/#:~:text=While%20the%20earliest%20accounts%20of,classification%20and%20comparison%20of%20criminals.* Retrieved from www.bioconnect.com: https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/#:~:text=While%20the%20earliest%20accounts%20of,classification%20and%20comparison%20of%20criminals.

Akinduyite C.O, A. A. (2017, August 12). *http://pubs.sciepub.com/jcsa/1/5/4/index.html*. Retrieved from http://pubs.sciepub.com/jcsa/1/5/4/index.html: http://pubs.sciepub.com/jcsa/1/5/4/index.html

Anil K. Jain, A. R. (2004, August 9). *ipl.org/essay/Literature.* Retrieved July 8, 2022, from ipl.org: ipl.org

Asare, J. (2021, May 17). *https://www.academia.edu/33092069/Biometric_Attendance_System_pdf.* Retrieved from www.academia.edu: https://www.academia.edu/33092069/Biometric_Attendance_System_pdf

B.M., M. (1993). Fingerprint image analysis for automatic identification. *Machine Vision and Applications*, 124-139.

Edgar, H. J. (n.d.). *https://www.britannica.com/topic/fingerprint*. Retrieved from https://www.britannica.com/.

El-Abed, M. G. (2012). Evaluation of Biometric Systems: A study of users'. *Halal Open Science*, 27. Retrieved from www.academia.edu.

Gangotri, S. (2018, Novermber 27). *https://shodhgangotri.inflibnet.ac.in/bitstream/123456789/3370/4/04_objectives.pdf.* Retrieved from www.shodhgangotri.inflibnet.ac.in: https://shodhgangotri.inflibnet.ac.in/bitstream/123456789/3370/4/04_objectives.pdf

INTERPOL. (n.d.). *https://www.interpol.int/en/How-we-work/Forensics/Fingerprints*. Retrieved from www.interpol.int: https://www.interpol.int/en/How-we-work/Forensics/Fingerprints

John, T. (2015, July 30). *https://www.m2sys.com/blog/education/the-value-of-biometrics-for-student-attendance-management-systems/#:~:text=Accurate%20Attendance%3A%20The%20main%20benefits,in%20and%20check%2Dout%20methods.* Retrieved from www.m2sys.com: https://www.m2sys.com/blog/education/the-value-of-biometrics-for-student-attendance-management-systems/#:~:text=Accurate%20Attendance%3A%20The%20main%20benefits,in%20and%20check%2Dout%20methods.

Lebi, D. A. (2021). FINGERPRINT BASED BIOMETRIC STUDENT ATTENDANCE SYSTEMA CASE STUDY OF DATA LINK INSTITUTE. *Global Scientific Journals*, 9.

Mensah, J. (2014, MAY 29). *www.academia.com.* Retrieved from www.academia.com: www.academia.com

Pushpaveni, S. T. (2019). Survey on Development of Fingerprint Biometric Attendance. *International Research Journal of Engineering and Technology (IRJET)*, 7.

Samuel, O. (2015, july 17). *https://projectregards.com/computer-science/fingerprint-based-student-attendance-monitoring-system/undergraduate-research-project-topics-and-materials-students-in-nigeria*. Retrieved from https://projectregards.com/: https://projectregards.com/computer-science/fingerprint-based-student-attendance-monitoring-system/undergraduate-research-project-topics-and-materials-students-in-nigeria

Shoewu O., O. O. (2011, March). Embedded Computer-Based Lecture Attendance Systems with Automatic Door Unit. *Academic Research International, 2*.

Uniproject, A. (2021, May 15). *https://uniprojectmaterials.com/computer-science/fingerprint-based-student-attendance-monitoring-system/project-topics-materials-for-final-year-students#:~:text=Fingerprint%20Based%20Student%20Attendance%20monitoring%20System%20is%20extremely%20useful%20i.* Retrieved from uniprojectmaterials.com: https://uniprojectmaterials.com/computer-science/fingerprint-based-student-attendance-monitoring-system/project-topics-materials-for-final-year-students#:~:text=Fingerprint%20Based%20Student%20Attendance%20monitoring%20System%20is%20extremely%20useful%20i

V., S., & A, D. (2010). Using Real Time Computer Vision Algorithms in Automatic Attendance Management Systems. *Proceedings of the ITI 2010 32nd Int. Conf. on Information Technology Interfaces*, 21-24.

Williams, J. (2019). *www.attorneyatlawmagazine.com*. Retrieved July 8, 2022, from www.attorneyatlawmagazine.com/various-types-fingerprints/amp: www.attorneyatlawmagazine.com/various-types-fingerprints/amp

Yashin, K. (2022, JANUARY 21). *https://how2electronics.com/fingerprint-biometric-attendance-system-arduino/*. Retrieved from https://how2electronics.com: https://how2electronics.com/fingerprint-biometric-attendance-system-arduino/