DESIGN AND IMPLEMENTATION OF AUTOMATED EXAMINATION ATTENDANCE SYSTEM BASED ON FINGERPRINT RECOGNITION

BY

ALFRED OLAOLUWA BARNABAS	**ICT/225200067**
OSAGIE MONEY OGIE	**ICT/225200136**
OKUN AUGUSTINE OBOZUWA	**ICT/2252030180**
ALABI OBOZEMOGIE VICTORY	**ICT/2252070253**

BEING A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY, AUCHI POLYTECHNIC, AUCHI, EDO STATE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN COMPUTER SCIENCE, AUCHI POLYTECHNIC, AUCHI, EDO STATE.

SUPERVISED BY:

DR. IGBAPE E. M.

NOVEMBER, 2022

CERTIFICATION

We, the undersigned hereby certify that this project was carried out by;

ALFRED OLAOLUWA BARNABAS **ICT/225200067**

OSAGIE MONEY OGIE	**ICT/225200136**
OKUN AUGUSTINE OBOZUWA	**ICT/2252030180**
ALABI OBOZEMOGIE VICTORY	**ICT/2252070253**

in the department of Computer Science, School of Information and Communication Technology.

We also, certify that the work is adequate in scope and quality in partial fulfillment of the requirements for the award of Higher National Diploma (HND) in Computer Science.

_____ _____

DR. IGBAPE E.M. **DATE**

(Project Supervisor)

_____ _____

MR. SYLVESTER AKHETUAMEN **DATE**

(Head, Department of Computer Science)

DEDICATION

This project work is dedicated to God almighty for his mercies and strength throughout our educational pursuit.

ACKNOWLEDGEMENT

Firstly, our profound gratitude goes to the Almighty God, the Father of wisdom whose wisdom has been our guide. This project would not have been completed without the valuable contribution of our supervisor, colleagues, friends and family.

We owe our deep appreciation to our supervisor; **DR. IGBAPE E.M.** for his encouragement, assistance and thorough supervision during the course of our research. We appreciate his devotion for helping us achieved our goal. Thank you for the attention you gave to us even with your busy schedule.

We would like to also express our sincere gratitude to the Head of department of computer science, **MR. SYLVESTER AKHETUAMEN** for his support and invaluable advice.

We would like to express our deepest gratitude and respect to our parents and siblings for their financial support, moral teaching, love, care and motivation.

Others in the trend are the departmental lecturers and a lot of friends in the computer science field; we say a very big thank you for all your support.

God bless you all.

TABLE OF CONTENTS

ABSTRACT

This project focuses on the design and implementation Automated Examination Attendance System Based on Fingerprint Recognition that can be used to monitor attendance of the student and can assist in curtailing examination impersonation. The research methodology adopted in this work is design science approach. Initial investigation was carried out through interaction and enquiries with technology users and domain experts to establish the existence of real problems that require technical solutions by way of deploying available I.T appliances. It will eliminate the problems of manual method. Up till now, the Federal Polytechnic, Auchi is not using fingerprint as mode of identification during examination, this has resulted in people sitting for examinations for others. With the adoption of the new system, the problem of examination impersonation will be eliminated. The new system utilizes

a portable fingerprint scanner as the input to acquire fingerprint images and notebook personal computer as the mobile terminal for the processing of the images and records attendance. It also includes database to store student's information and attendance records. To achieve more reliable verification or identification we should use something that really characterizes the given person. Main objective is to eliminate any form impersonation during exam by employing a more secured means of fingerprint biometrics. Automated biometrics in general, and fingerprint technology in particular, can provide a much more accurate and reliable user authentication method. More importantly, this system should be used in various tertiary institutions to curb examination impersonation.

Keywords: Biometrics, Authentication, Technology Exam Impersonation, Fingerprint Recognition, Attendance.

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

In era of Information technology (IT), biometrics refers to technology for measuring and analyzing human physiological traits along with fingerprints, eye retinas and irises, voice patterns, facial styles, and hand measurements, specially for authentication functions (Olaniyi, Omotosho, Oluwatosin, Adegoke, and Akinmukomi, 2012).

Biometrics is the science of measuring physical and/or behavioural characteristics that are specific to each character and they verify that a person is who she or he claims to be (Pankaj 2014).

Reliable user authentication is becoming an increasingly important task in the Web- enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer enhanced security.

The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations. The relevance of biometrics in modern society has been reinforced by the need for large-scale identity management systems whose functionality relies on the accurate determination of an individual's identity in the context of several different applications. Biometric method has come to be a prominent alternative and secured means of authentication able to sustaining the emerging popular computing.

All academic institutions have certain criteria for admitting students into examination hall; that is why preserving the correct file of attendance and fees payments are very critical. In nearly all institutions in the growing countries, clearance is generally finished manually using paper sheets and antique report gadget method, but this method is prone to impersonation. Biometric identity of a person is fast, easy-to-use, specific, truthful and cost effective over traditional understanding-based totally and manual techniques. A biometric gadget includes mainly a photograph taking pictures module, a feature extraction module and a sample matching module. A photograph shooting module acquires the raw biometric facts of a person using a sensor, making use of appropriate set of rules characteristic extraction module that improves the exceptional of the captured picture. Database module shops the biometric template information of enrolled folks. Sample matching module compares the extracted features with the saved templates, which in-flip generates fit score. This technique discourages fraud, impersonation at some stage in the examination in contrast to the paper clearance strategies which inspire fraud, impersonation etc.

The rate of problems encountered in conducting higher institutions examination is too high and the approach used is too poor. Some of these problems include: student impersonation, unsecured authentication of students, manual verification of students, time consumption etc. Hence, this research study focuses on the design and implementation of

automated examination attendance system based on fingerprint recognition to curb impersonation in examination conduct in higher institutions.

1.2 Statement of the problem

Attendance systems in various educational institutions are taken manually by using an attendance sheet. The problems which are encountered in the manual system are student impersonation, unsecured authentication of students, stress and time-consuming (because the student has to go through a long process so as to just obtain an examination slip which is used to prove that he or she is eligible to sit for an exam. This leaves a gap and a desire to come up with new and improved ways of capturing attendance information and verifying if a student is eligible to sit for an examination. Hence, propositions have been made that fingerprint recognition will help in dealing with these problems.

1.3 Aim and Objectives of the study

The main aim of this study is to develop a biometric attendance system based on fingerprint recognition that can be used in exam halls to verify or differentiate between an authentic student and an imposter before entering the examination hall.

The study seeks to achieve the following objectives;

- To create a system that is capable of tracking impersonators in the examination system using the methodology of fingerprint biometrics.
- To reduce stress, time-consumption and rate of corruption in the educational sector and increase the rate of self-confidence in students.
- To demonstrate the possibility of computer technology in the satisfaction of human needs and also enforce strict security measures that ensure unregistered students do not write exams for other registered students.

1.4 Significance of the study

With the increasing rate of examination malpractices in the educational sectors the school management deserves to inculcate tight security means to ensure that these activities of exam impersonators stop. The system uses fingerprint biometrics; this would help ensure that only registered students during registration with their fingerprints are allowed into the examination hall. The system would contribute in the area of stopping any activity of corruption in the educational sector among students, and students to invigilators. Hard work would be encouraged as every registered student knows he/she is going to write the exam by himself or herself. The impersonation which has eaten the educational system thereby encouraging laziness among students would be eliminated and the standard of student educational performance would be increased.

1.5 Scope of the study

The main scope of this project is to replace the manual current attendance system by an Automated Examination Attendance System (AEAS) based on fingerprint recognition which will be more accurate, easier and faster.

1.6 Research Methodology

Good systems engineering begins with a clear understanding of the context, the world view and then progressively narrows until technical detail is achieve (Pressman, 2005).

The research methodology adopted in this work is design science approach (Hevner et. al, 2005; March and Smith, 1995). In this approach, the first step is to identify the existence of a problem that requires viable solution.

- Initial investigation was carried out through interaction and enquiries with technology users and domain experts to establish the existence of real problems that require technical solutions by way of deploying available I.T appliances.

- A review of related literature was carried out on the established research domain of interest such as research journals, product manuals, books and related technical materials.
- Key concepts were identified, defined, and research objectives written
- Thereafter, a case study was selected using Examination Centre to establish the technical feasibility of the deployment of biometric attendance system based on fingerprint recognition to provide solution to the established real-life problem.

1.7 Definition of Terms

Biometrics: This refers to technology for measuring and analyzing human physiological traits along with fingerprints, eye retinas and irises, voice patterns, facial styles, and hand measurements, especially for authentication functions.

Examination: is a set of questions or exercises evaluating skill or knowledge

Examination malpractice: unethical or misconduct in an Examination Hall

Examination Impersonation: Examination impersonation is act by which an individual who is not registered as a candidate for a particular examination takes the place of one that is registered

Software: Written programs or procedures or rules and associated documentation pertaining to the operation of a computer system and that are stored in read/write memory.

Fingerprint Scanner: A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern

Fingerprint: Analyzing fingertip patterns.

Facial Recognition: Facial recognition is a way of identifying or confirming an individual's identity using their face. Facial recognition systems can be used to identify people in photos, videos, or in real-time.

CHAPTER TWO

LITERATURE REVIEW

According to Kinoti, Sylvester and Henry, (2015), the most commonly used biometrics for authentication are the fingerprints, a special device which might be a portable fingerprint scanner with USB connector is required to scan users imprints and compare with the fingerprint pattern already on the database as captured during registration of candidate. Some laptops and some personal computers already have inbuilt fingerprint scanners. Employing knowledge factors such as biometrics is surest way to address Type B impersonation threat but the scheme may be susceptible to Type C impersonation threat in which the right candidate is correctly authenticated but leaves another person to complete the examination. To address Type C impersonation threat, continuous re-scan of the candidate's biometrics throughout the test session is required.

The drawback of normal identification methods that only based on credentials lead means username, password, personal identification number (PIN). To the introduction of user authentication and verification techniques that are based on behavioural and physiological biometrics which are assumed to be unique to each other and hard to steal (Sachin et al., 2015).

In Jaiswa et al. (2011), Biometric authentication can be used to control the security of computer networks, electronic commerce and banking transactions, and restricted areas in office buildings and factories. It can help prevent fraud by verifying identities of voters and holders of driver's license or visas. In authentication, a sensor captures a digital image of the characteristic being used to verify the user's identity. A computer program extracts a pattern of distinguishing features from the digital image. Another program compares this pattern with the one representing the user that was recorded earlier and stored in the system database. If

the patterns match well enough, the biometric system will conclude that the person is who he or she claims to be.

2.1 Examination Impersonation

(According to ***arcjournal.com***) Examination impersonation is act by which an individual who is not registered as a candidate for a particular examination takes the place of one that is registered. Usually this involves collusion between the chief examiner and the examination supervisor. It frequently involves tertiary institutions students taking the test for monetary reward or a favour for a girl friend or boyfriend.

(According to a research work carried out by Eneh I.B, 2013, published on academia.edu) reviewed that the Board of Intermediate & Secondary Education (BISE) Lahore‘s inspection team caught two fake candidates appearing in chemistry paper of the ongoing Secondary School Certificate (Supplementary) Examination, 2012. Interestingly, one of the candidates had already done his graduation while the other was caught impersonating for a genuine candidate. Sources in BISE say the candidate who had done graduation might have appeared in the ongoing exam to help some other candidate in solving paper as under the rules such candidates cannot appear in the exam.

This is not for the first time that the BISE examination staff caught fake candidates or impersonators. Each year during examinations, whether of matriculation, intermediate, graduation and even MA/MSc, candidates are caught committing academic crimes like these. However, what can be learnt from such unfortunate but

illegal acts is the growing tendency of negativity and cheating, in the broader sense, among educated youth and the same need to be addressed immediately. Every technology implementation has got a particular fulfillment to achieve the fingerprint biometrics is aimed at granting security access to individuals base on what you are. This technology can be

applied to examination system to grant access to only registered individuals. The process of misconduct in the exam which can also include impersonation is called malpractices.

2.2 The Concept Of Biometric

2.2.1 History

There are evidences of biometric uses on human history as early as prehistorical age. Estimated 31000 years old caves are adorned with prehistorical pictures apparently signed by fingerprints stamps of authors. Another evidence is the use of fingerprints by Babylonian at 500 B.C. They used to record business transactions on clay tables in which were found fingerprint stamps.

The first reported use of biometrics was related by Portuguese explorer João de Barros in the 14th century. He described the practice of Chinese merchants of stamp children´s palmprints and footprint to distinguish from one another.

The first real biometric system was created in 1870 by French anthropologist Alphonse Bertillon and turned biometrics a distinguished field of study. He developed an identification system (Bertillonage) based on detailed records of body measurement, physical description and photographs. Despite their imprecise measures and difficulty to apply methodology, the Bertillonage was an important advance on criminal and people identification. It began to fail when it was discovered that many people share the same anthropologic measures.

The first classification method for fingerprints was developed in 1892 by Sir. Francis Galton. The features used by Galton´s method were the minutiae that are still used nowadays.

Some years later in 1896, Sir Edward Henry General Inspector of the Bengal police, began to use Galton´s method to replace the anthropometrics system for identification of criminals. Henry created a method to classify and store fingerprint that lets a quick searching

of records. Later, that method was introduced by Henry in London for the first British fingerprint file***. (https://studymafia.org/biometrics-seminar-and-ppt-with-pdf-report-2/)***

2.2.2 What Is Biometric Security?

Biometric security is a security mechanism that identifies people by verifying their physical or behavioural characteristics. It is currently the strongest and most accurate physical security technique that is used for identity verification. Biometrics are mainly used in security systems of environments that are subject to theft or that have critical physical security requirements. Such systems store characteristics that remain constant over time; for instance, fingerprints, voice, retinal patterns, facial recognition, and hand patterns. These characteristics are stored as "templates" in the system. When somebody tries to access the system, the biometric security system scans them, evaluates the characteristics, and attempts to match them with stored records. Then, if a match is found, the person is given access to the facility or device (Recfaces, 2021).

2.2.3 What Are Biometric Identification and Authentication?

Biometric security systems can combine identification and authentication, the two functions are not the same. With biometric identification, a person's features are compared to an entire database. With biometric authentication, on the other hand, the system is checking to see if the person is who they say they are – so their attributes are compared against one particular profile from the database. For example, facial recognition security systems might use video surveillance to identify known shoplifters when they enter the premises of a store. The store might also have a separate fingerprint system that authenticates an employee and gives them access to a restricted room upon scanning their fingerprint – the scanned data is compared to the stored, approved template.

2.2.4 Types of Biometrics

There are two types of biometrics:

- **Physical biometrics:** Physical biometrics analyses facial features, eye structure, hand

shape, and other things involving your body's physical form. It is used for verification.

- **Behavioural biometrics:** With behavioural biometrics, the system analyses any pattern of behavior that is associated with the individual. It is used for either identification or verification.

2.2.4.1 Physical biometrics:

- ***Fingerprint-*** Analyzing fingertip patterns.
- ***Facial Recognition-*** Measuring facial characteristics.
- ***Hand Geometry-*** Measuring the shape of the hand.
- ***Iris recognition-*** Analyzing features of colored ring of the eye.
- ***Vascular Patterns-*** Analyzing vein patterns.
- ***Retinal Scan-*** Analyzing blood vessels in the eye.
- ***Bertillonage-*** Measuring body lengths (no longer used).

2.2.4.2 Behavioural biometrics:

- ***Speaker Recognition-*** Analyzing vocal behavior.
- ***Signature-*** Analyzing signature dynamics.
- ***Keystroke-*** Measuring the time spacing of typed words.

2.2.5 Characteristics of Biometric

Biometric characteristics can be divided in two main classes:

- Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, palm print, hand geometry, iris recognition (which has largely replaced retina recognition), and odor/scent.
- Behavioural are related to the behavior of a person. Examples include, but are not limited to typing rhythm, gait, and voice. Some researchers have coined the term

"behaviometrics" for this class of biometrics.

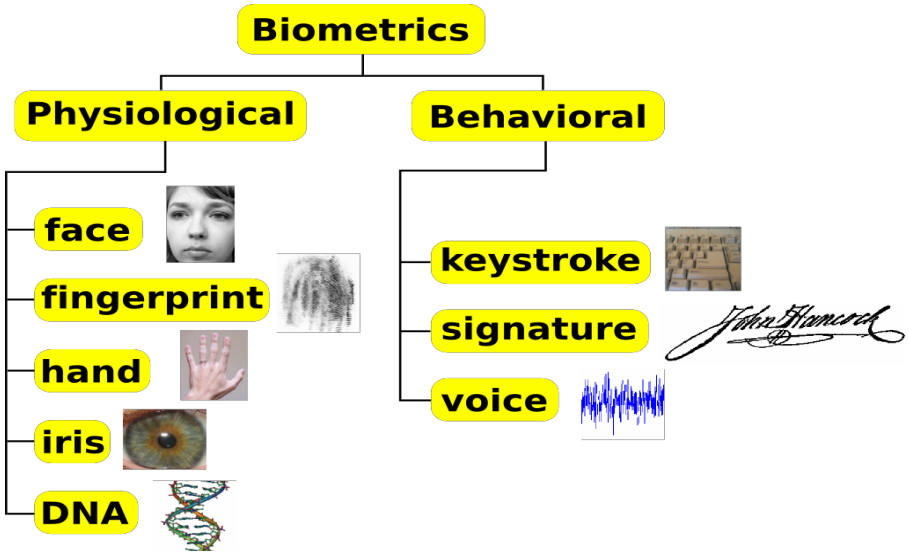

Figure 2.1: characteristics of biometrics (https://studymafia.org/biometrics)

2.3 Applications

In the last years has considerably increased the area of application of biometrics and it's expected that in the near future, we will use biometry many times in our daily activities such as getting in the car, opening the door of our house, accessing to our bank account, shopping by internet, accessing to our PDA, mobile phones, laptops, etc. Depending of where the biometrics is deployed, the applications can be categorized in the following five main groups: forensic, government, commercial, health-care and traveling and immigration. However, some applications are common to these groups such as physical access, PC/network access, time and attendance, etc.

2.3.1 Forensic

The use of biometric in the law enforcement and forensic is more known and from long date, it is used mainly for identification of criminals. In particular, the AFIS (automatic fingerprint identification system) has been used for this purpose.

Lately the facial-scan technology (mug shots) is being also used for identification of suspects. Another possible application is the verification of persons of home arrest, a voice-scan is an attractive solution for this problem. The typical applications are:

- Identification of criminals
- Surveillance
- Corrections
- Probation and home arrest

2.3.2 Government

There are many applications of the biometry in the government sector. An AFIS is the primary system used for locating duplicates enroll in benefits systems, electronic voting for local or national elections, driver's license emission, etc. The typical applications are:

- National Identification Cards
- Voter ID and Elections
- Driver's licenses
- Benefits Distribution (social service)
- Employee authentication
- Military programs

2.3.3 Commercial

Banking and financial services represent enormous growth areas for biometric technology, with many deployments currently functioning and pilot project announced frequently. Some applications in this sector are:

- Account control

- ATMS
- Expanded service kiosks
- Online banking
- Telephony transaction
- PC/Network access
- Physical access
- E-commerce
- Time and attendance monitoring

2.3.4 Health Care

The applications in this sector includes the use of biometrics to identify or verify the identity of individuals interacting with a health-care entity or acting in the capacity of health-care employee or professional. The main aim of biometrics is to prevent fraud, protect the patient information and control the sale of pharmaceutical products. Some typical applications are:

- PC/Network Access
- Access to personal information
- Patient identification

2.3.5 Travel and Immigration

The application in this sector includes the use of biometrics to identify or verify the identity of individual interacting during the course of travel, with a travel or immigration entity or acting in the capacity of travel or immigration employee. Typical applications are:

- Air
- Border
- Employee
- Passports

2.4 Biometric Modality

There is no single biometric modality that is best for all implementations. Commonly implemented or studied biometric modalities include: Fingerprint, face, iris, voice, signature and hand geometry. Many other modalities are in various stages of development and assessment. Many factors must be taken into account when implementing a biometric system, including but not limited to: physical location, security risks, task (identification or verification), expected number of end users, user circumstances. Each biometric modality has its own strengths and weaknesses that must be evaluated in relation to the application before implementation. The effectiveness of a particular implementation of biometric technology is dependent on how and where the technology is used.

Key decision factors for selecting a particular biometric technology for a specific application includes but is not limited to:

- The environment
- Throughput needs (the required speed of the transaction)
- Costs associated with obtaining and storing templates and conducting biometric recognition
- Population size and demographics
- Ergonomics
- Interoperability with existing systems
- Other user considerations — for instance, an access control system to a coal mine, where individuals might have very worn and/or dirty fingerprints, will not be a suitable environment for a fingerprint reader.

2.5 Biometric Devices

2.5.1 Iris Scanner

Iris cameras perform recognition detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines

computer vision, pattern recognition, statistical inference and optics. Of all the biometric devices and scanners available today, it is generally conceded that iris recognition is the most accurate. The automated method of iris recognition is relatively young, existing in patent since only 1994.

Figure 2.2: Iris scanner (https://studymafia.org/biometrics)

Iris cameras, in general, take a digital photo of the iris pattern and recreating an encrypted digital template of that pattern. That encrypted template cannot be re-engineered or reproduced in any sort of visual image. Iris recognition therefore affords the highest-level defense against identity theft, the most rapidly growing crime.

The imaging process involves no lasers or bright lights and authentication is essentially non-contact. Today's commercial iris cameras use infrared light to illuminate the iris without causing harm or discomfort to the subject.

The iris is the coloured ring around the pupil of every human being and like a snowflake, no two are alike. Each are unique in their own way, exhibiting a distinctive pattern that forms randomly in utero. The iris is a muscle that regulates the size of the pupil, controlling the amount of light that enters the eye.

2.5.2 Fingerprint Scanner

A fingerprint scanner is an electronic device used to capture a digital image of the fingerprint pattern. This scan is digitally processed to create a biometric template which is stored and used for matching.

Figure 2.3: Finger scanner (https://studymafia.org/biometrics)

2.5.3 Face Camera

Face detection is used in biometrics, often as a part of (or together with) a facial recognition system. It is also used in video surveillance, human computer interface and image database management. A face model can contain the appearance, shape, and motion of faces. There are several shapes of faces. Some common ones are oval, rectangle, round, square, heart, and triangle. The models are passed over the image to find faces, however this technique works better with face tracking. Once the face is detected, the model is laid over the face and the system is able to track face movements.

Figure 2.4: Face camera (https://studymafia.org/biometrics)

2.6 Advantages Of Biometric Security

- Increase security - Provide a convenient and low-cost additional tier of security.
- Reduce fraud by employing hard-to-forge technologies and materials. e.g. minimize

the opportunity for ID fraud, buddy punching.

- Eliminate problems caused by lost IDs or forgotten passwords by using physiological attributes. For e.g. prevent unauthorized use of lost, stolen or "borrowed" ID cards.
- Reduce password administration costs.
- Replace hard-to-remember passwords which may be shared or observed.
- Integrate a wide range of biometric solutions and technologies, customer applications and databases into a robust and scalable control solution for facility and network access.
- Make it possible, automatically, to know WHO did WHAT, WHERE and WHEN!
- Offer significant cost savings or increasing ROI in areas such as Loss Prevention or Time & Attendance.
- Unequivocally link an individual to a transaction or event.

CHAPTER THREE

SYSTEM DESIGN AND ANALYSIS

3.1 System Study

We went through literature on biometrics, and also, we visited different schools such as the School of Engineering, School of art and design, School of Information and Communication Technology etc. of the Federal Polytechnic Auchi to investigate the way examination authentication is carried out. We discovered that the way of capturing attendance information and verifying if a student is eligible to sit for an examination is taken manually by using an attendance sheet. Problems such as student impersonation, stress (because the student has to go through a long process so as to just obtain an examination slip which he or she can use to prove that he or she is eligible to sit for an exam), and unsecured authentication of students are encountered in the manual authentication system. Hence, it is time-consuming.

3.2 System Analysis

In the manual examination authentication system, student will first of all register their courses which they will take in a semester. After the registration process, when examination is approaching, students are grouped, and every student is given an examination permit (ID card) which is brought to the examination hall, and students are verified with the permit. But this is still not a strong measure or security because the eyes are used in this case to check for the occurred passport and the physically occurring human. When it is time of exams student are expected to arrive at the examination hall with their exam permit (photo card or id card), this exam permit serves as an authorization for them to gain access to the exam hall and participate fully in the examination. Since the process use is what you have and not what you are, impersonator can simply make black and white photocopy of the photo card making his picture to be dark so when check during the exam or even swap the photo on the exam permit to his own photo. Certain student who is not capable of writing the proposed course due to

laziness in studies might pay people to come and write the courses for him. Using the eye, a physical matching is now taken between the passport that has been printed and the physically present human to check if the student that has register is actually the one writing the exam and if not, he/she is apprehended. But this has proven to be very inefficient. Several problems tend to exist within the use of the system and as such include:

- Inefficient in its usage and comprehend the act of exam impersonation
- The process of authorization is based on a concept of what you have; which can be manipulated at anytime.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present with recognition.

3.2.1 Flow Chart of the Current System

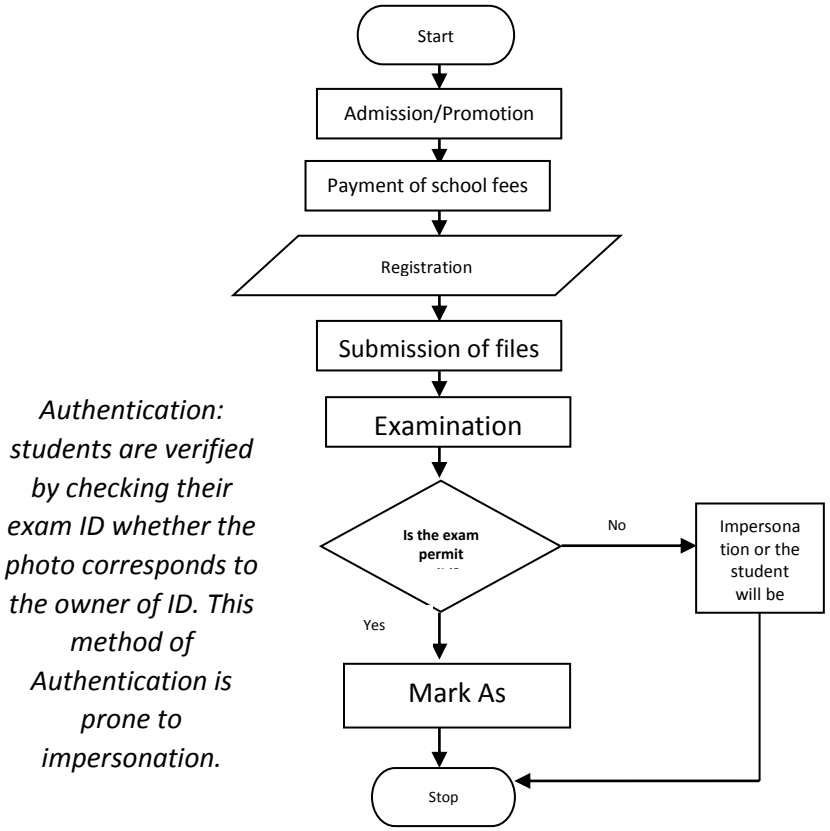

Figure 3.1: Existing System Flowchart

The Admission/Promotion:

At the stage, the student is admitted into the institution or promoted from one level to another.

Payment of school fees:

The school fees payment made by the student is processed and acknowledged at this stage.

Registration:

At this stage, the student login to the school portal and carries out all the steps required for the registration and prints out the necessary documents.

Submission of files:

The printed documents are filed and submitted to the departmental administrator by the student.

Examination attendance (Authentication):

When it is time for examination, the student is expected to arrive at the examination hall with his/her exam permit (photo card or id card), this exam permit serves as an authorization for them to gain access to the exam hall and participate fully in the examination. The student is verified with the permit. But this is still not a strong measure or security because the eyes are used in this case to check for the occurred passport and the physically occurring human. Several problems tend to exist within the use of the system and as such include:

- Inefficient in its usage and comprehend the act of exam impersonation
- The process of authorization is based on a concept of what you have; which can be manipulated at anytime.
- Matching to establish security measures occurs through the physical eye and this is a very big problem and requires great power of recognition, hence an impersonator can be present with recognition.

Hence this system needs to be corrected by deploying a biometric attendance system based on fingerprint recognition.

3.3 Design of the proposed system

The proposed system provides solution to examination impersonation problems through the use of interacting software that is interfaced to a fingerprint device. The student bio-data (Matriculation number, Name, Gender and Date of Birth) and the fingerprint are enrolled first into the database. The fingerprint is captured using a fingerprint device. For examination, the student places his/ her finger over the fingerprint device and the attendance is taken by comparing a single fingerprint image with the fingerprint images previously stored in a database during the registration process. During the exam the school management is expected to come with system containing the student's database of information for those exams and each student is expected to thumb print before entering for the exams. During the process of thumb printing, if a student that has not registered for the exams wants to impersonates, a matching template will fail and the student will be apprehended as impersonator. The system is meant to permit only users verified by their fingerprint scan and doesn't allow non verified users. This system will add more security measures to the examination processes using finger print biometrics and eliminates the possibility of an imposter appearing in an exam.

3.3.1 Flowchart Of The Proposed System

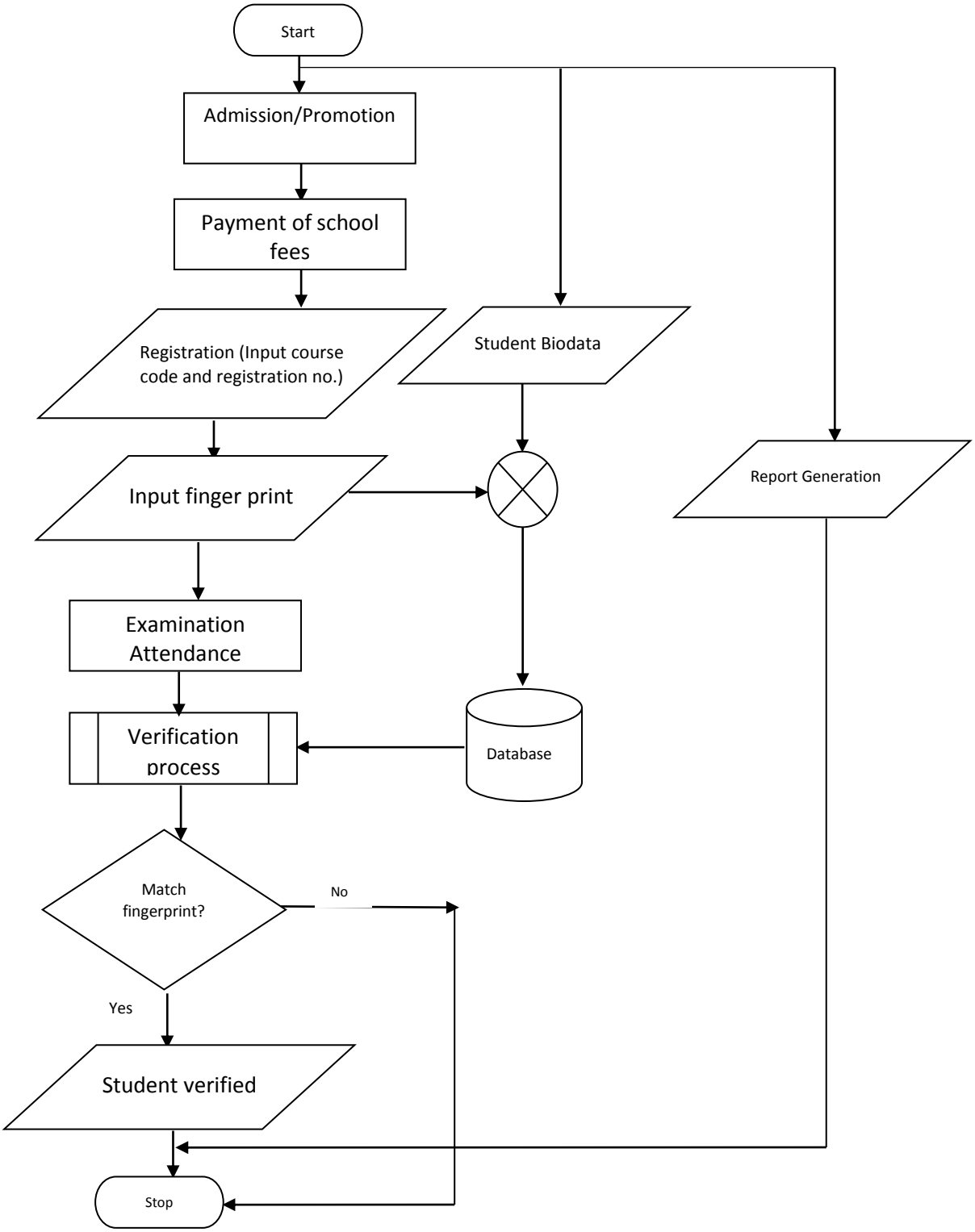

Figure 3.2: Flowchart of the proposed system

3.4 PROGRAM FLOWCHART

3.4.1 Admin Login

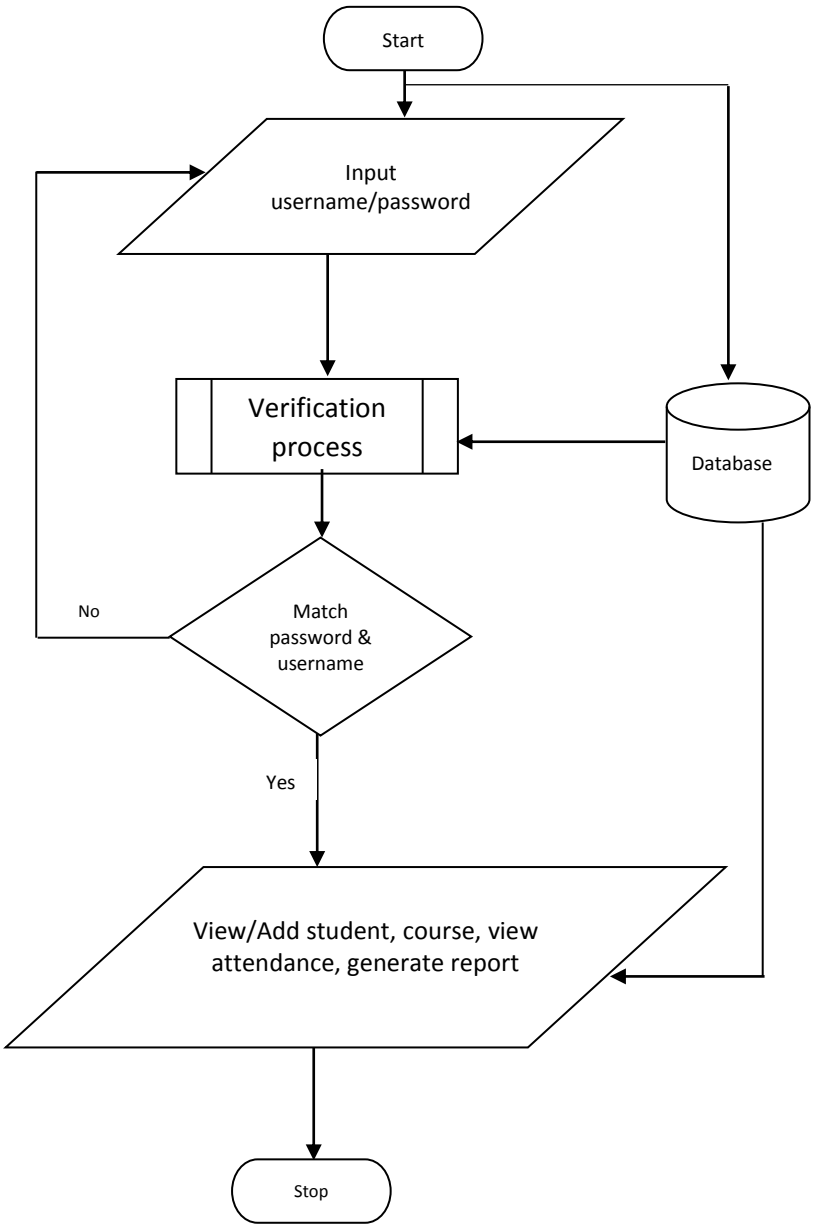

Figure 3.3: Admin login flowchart

3.4.2 Student Fingerprint verification (Time-In/Time-out) flowchart

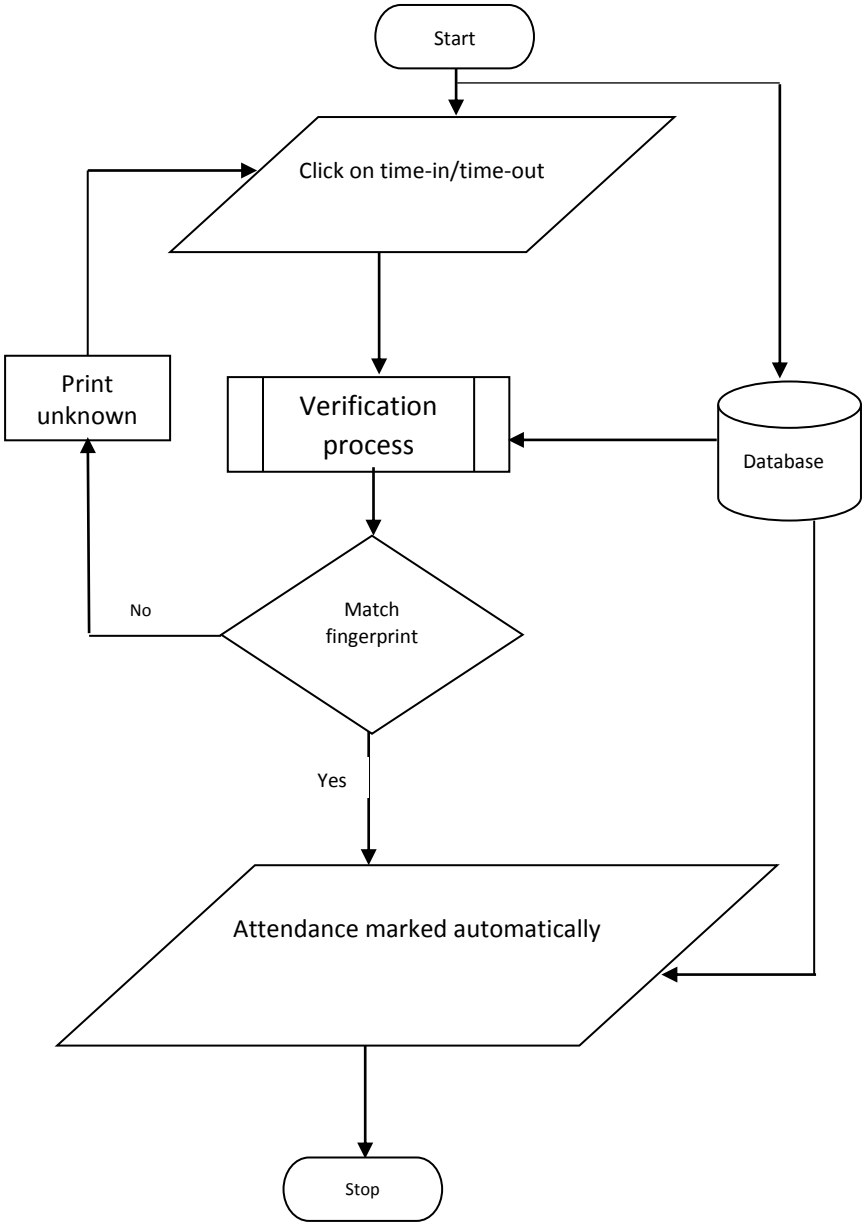

Figure 3.4: Student Time-in/Time-out Flowchart

CHAPTER FOUR

IMPLEMENTATION AND TESTING

This chapter describes and shows how this standalone system is implemented, developed and tested, using the appropriate necessary programming languages, tools and technology.

4.1 IMPLEMENTATION

System or Software Implementation is the conversion of the System Requirements into an executable and working system.

4.1.1 Implementation Choices

The Automated Examination Attendance System based on Fingerprint Recognition works as web-based and offline application system. It was implemented using PHP, C# and MySQL was used for the database and the Integrated Development Environment (IDE) used was Bracket text editor, Visual Studio 2017 and XAMPP was used as the offline local server.

4.1.1.1 PHP

PHP is a general-purpose programming language originally designed for web development. It was originally created by Rasmus Lerdorf in 1994; the PHP reference implementation is now produced by The PHP Group. PHP originally stood for Personal Home Page, but it now stands for the recursive initialism PHP: Hypertext Preprocessor.

PHP code may be executed with a command line interface (CLI), embedded into HTML code, or it can be used in combination with various web template systems, web content management systems, and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in a web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and

executed PHP code, which may be any type of data, including images, with the generated web page. PHP can be used for many programming tasks outside of the web context, such as standalone graphical applications and robotic drone control.

4.1.1.2 MySQL

MySQL is an Oracle-backed open-source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX and Windows. Although it can be used in a wide range of applications. MySQL is most often associated with web applications and online publishing.

4.1.1.3 XAMPP

XAMPP is a software distribution which provides the Apache web server, MySQL database (actually MariaDB), Php and Perl (as command-line executables and Apache modules) all in one package. It is available for Windows, MAC and Linux systems. No configuration is necessary to integrate PHP with MySQL. It is a great fit for this course and provides a relatively stress-free installation and way to manage the configuration changes. Also provided is PhpMyAdmin which gives a graphical user interface (GUI) tool for managing MySQL databases.

4.1.1.4 C#

C# (pronounced "See Sharp") is a modern, object-oriented, component-oriented and type-safe programming language. C# enables developers to build many types of secure and robust applications that run in .NET. C# has its roots in the C family of languages and will be immediately familiar to C, C++, Java, and JavaScript programmers. C# provides language constructs to directly support these concepts, making C# a natural language in which to create and use software components. Several C# features help create robust and durable applications.

4.1.1.5 Visual Studio

Visual Studio is a complete set of development tool for windows application, web applications and mobile applications. Visual Basic, Visual C#, Visual C++, Visual F# and many other languages are supported in Visual Studio. Programmers or developers like to develop software using Visual Studio. It is very user friendly.

4.2 System Requirements

The system requirements are the software and hardware requirements. The software requires a set of instructions that controls a computer's action. It is a computer program that accomplishes some specific applications or tasks. This software can be purchased or a user can develop the software from software developers.

The hardware requirements unlike the software refer to the physical components of the computer i.e. the peripherals in this design. The hardware and software requirements for this system are listed below.

Software Requirements

- Operating System — Windows 2007/2010/later versions\
- Browser — Chrome
- Web/Application Server — XAMPP
- Database Server — MySQL
- Database Connectivity — PHP
- IDE — Visual Studio 2017, Bracket

Hardware Requirements

- Computer — Desktop/laptop
- Intel Core i3 and above — 1.6 GHZ or above
- RAM Capacity — 4GB or above
- Hard Disk — 120GB or above

- Fingerprint scanner Digital Persona U and U 4500

4.3 SAMPLE INTERFACES

4.3.1 Admin Panel

Login: The admin will insert his/her username and password in the provided spaces and click on the LOGIN button to access the admin panel.

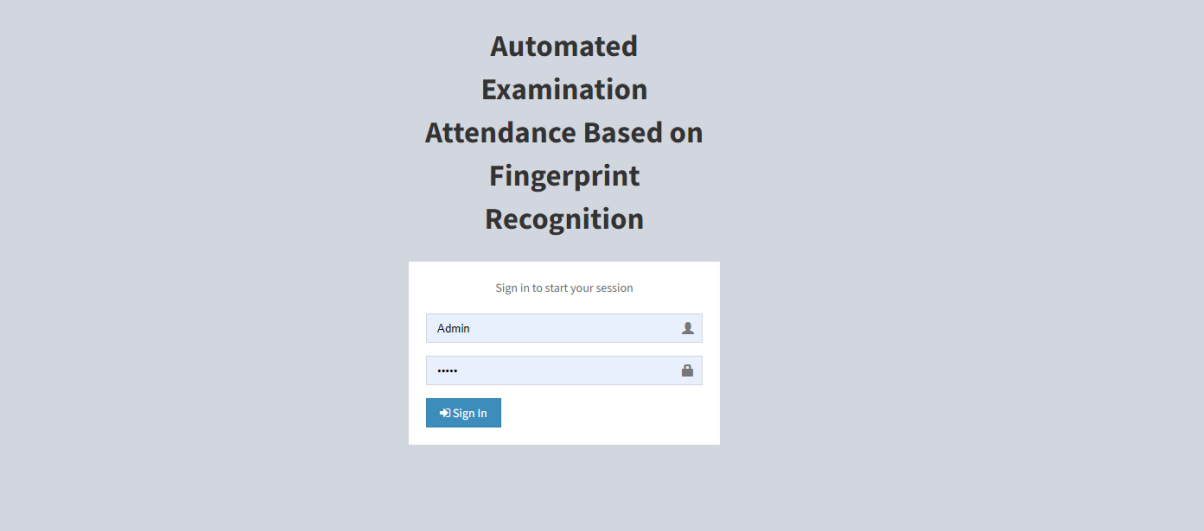

Figure 4.1: Admin Login Page

Home Page: After Login, the admin homepage will open which will allow admin to navigate to his/her dashboard.

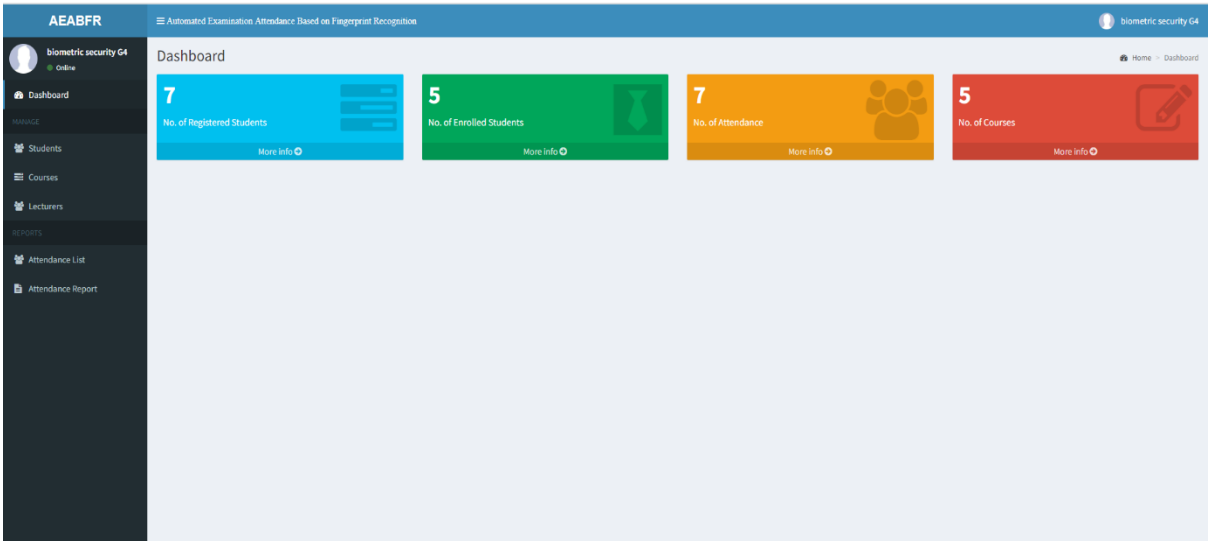

Figure 4.2: Admin Home Page

Dashboard: The window that allows admin to

- Add Student
- Add Lecturers
- Add Courses
- View Attendance list
- View Attendance Report
- View Number of registered students
- View Number of Courses etc.

Add Student: The window that allow admin to add student, view student or edit his profile if needed.

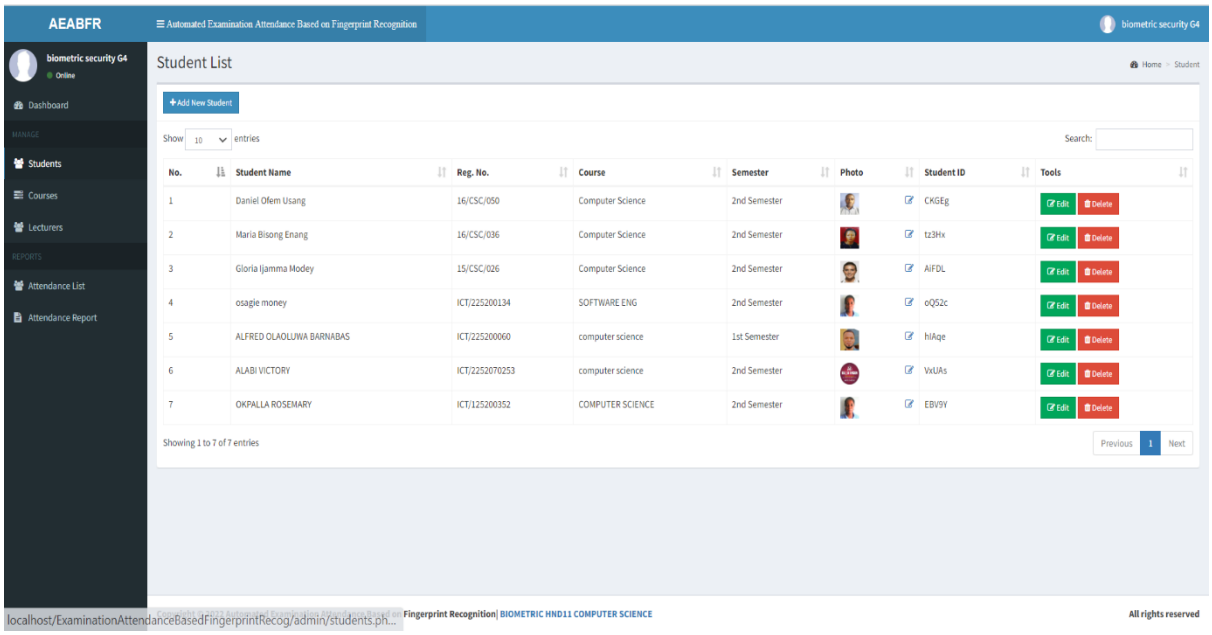

Figure 4.2.1: Admin Dashboard – Add/Delete/Edit Student Detail

Add Lecturers: The window enables the admin to add lecturers, view or edit lecturer profile if necessary.

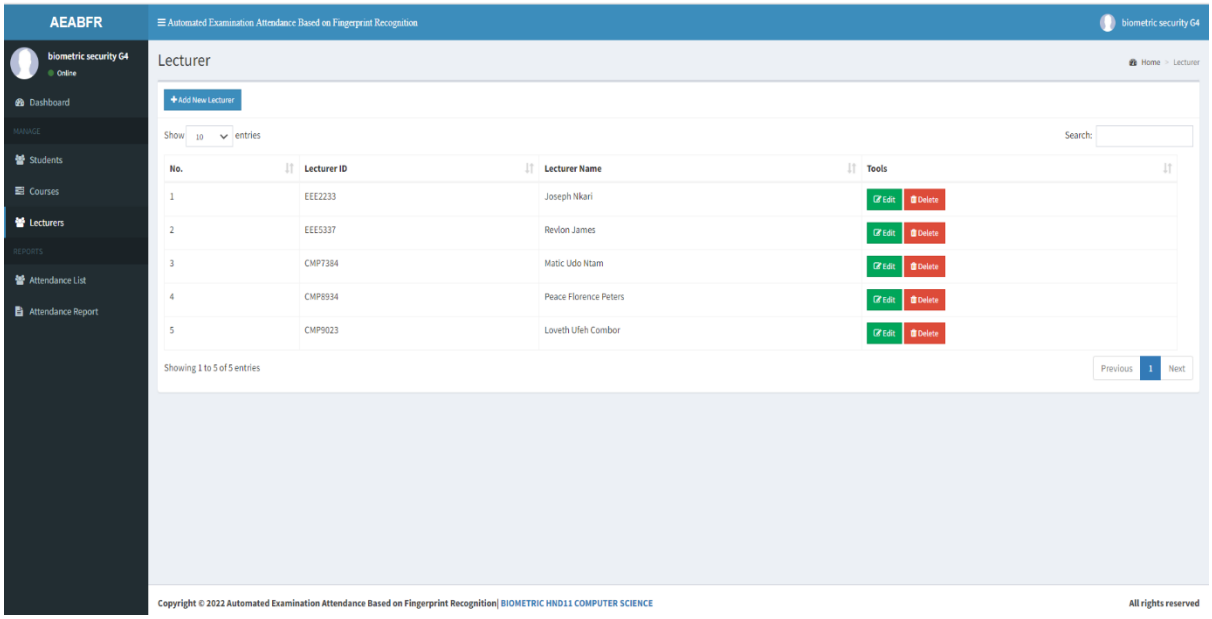

Figure 4.2.2: Admin Dashboard – Add/Delete/Edit Lecturer Detail

Add Courses: This window allows admin to add/remove courses.

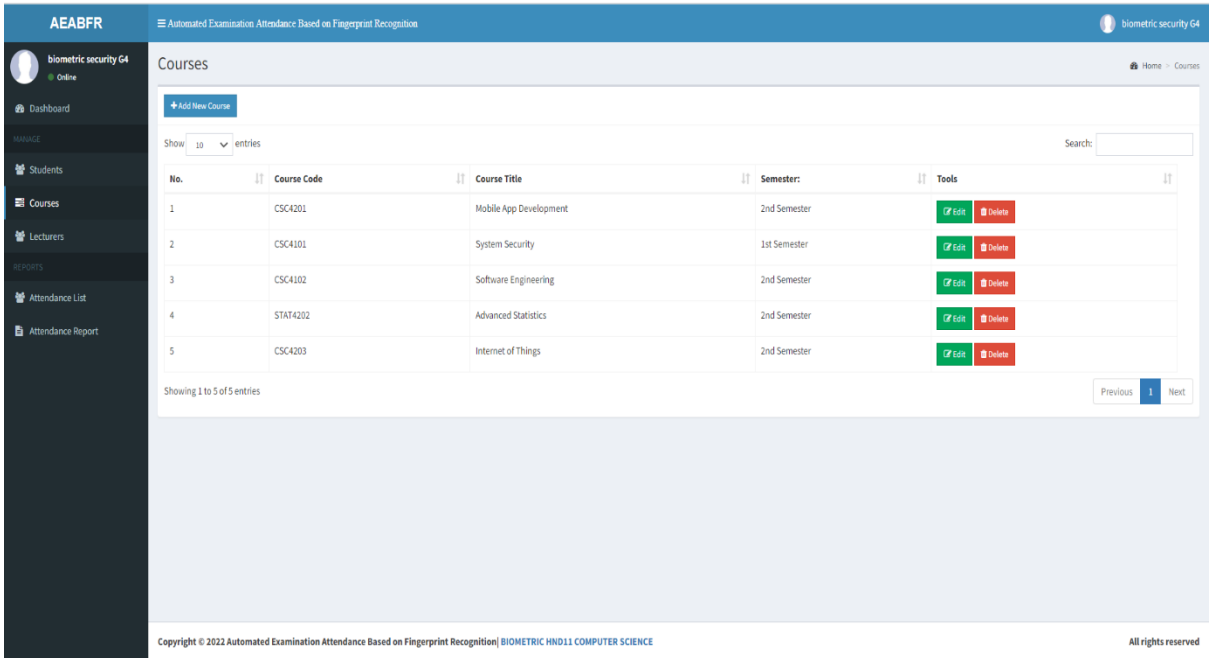

Figure 4.2.3: Admin Dashboard – Add/Delete/Edit Course Detail

View Attendance list: this enables the admin to view attendance list of students that participated in the examination.

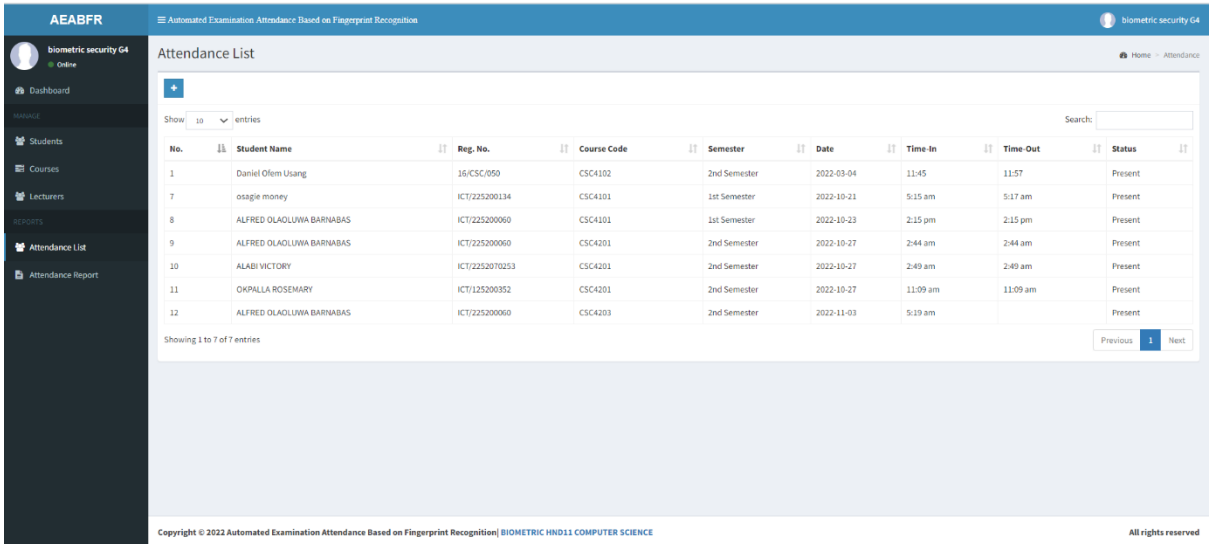

Figure 4.2.4: Admin Dashboard – View Attendance List

View Number of registered students: Enables the admin to view the total number of registered students to participate in the examination.

View Number of Courses: Enables the admin to view the total number of student courses.

View Attendance Report: This enables the admin to generate both old and recent attendance reports.

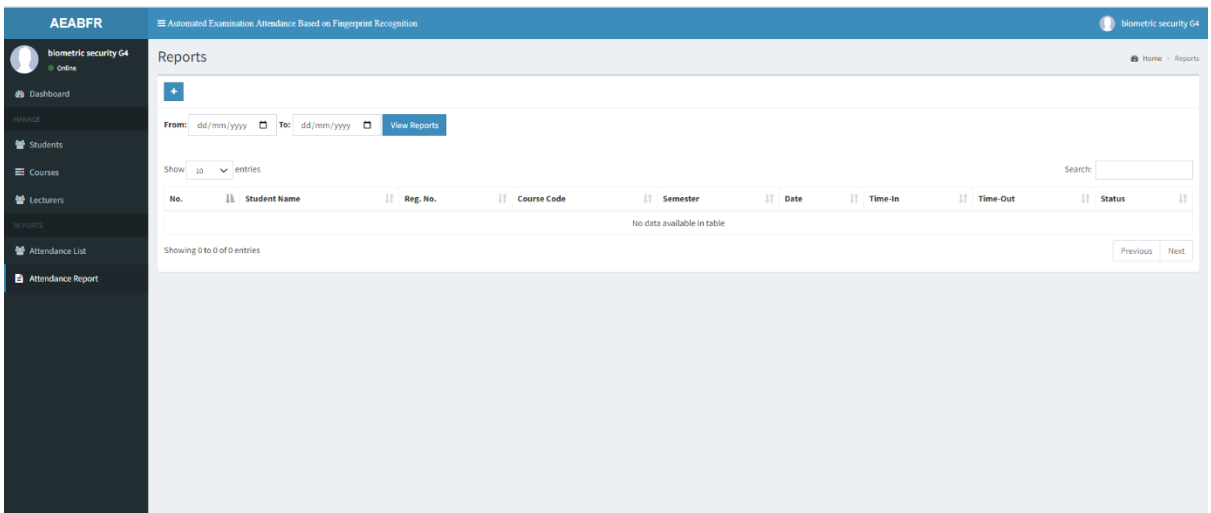

Figure 4.2.5: Admin Dashboard – View Attendance Report

4.3.2 User Interface

This interface consists of the following:

Capture Fingerprint: This captures the student fingerprint.

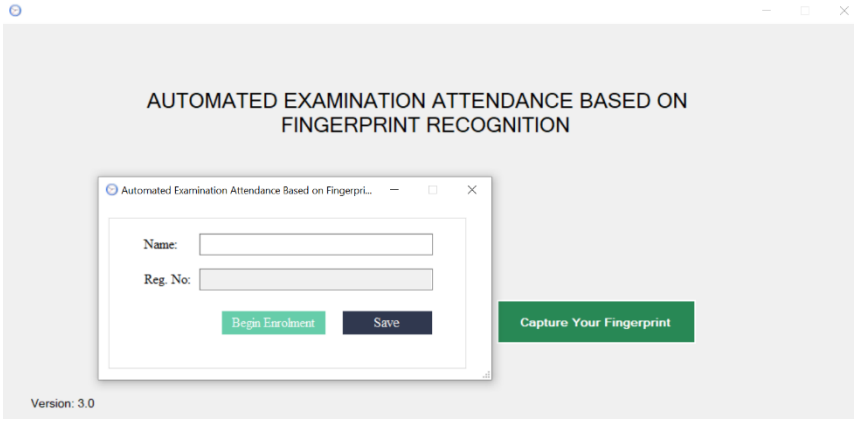

Figure 4.3: User Interface – Capture Student Fingerprint

Time-In: This enables the student to sign in and also verify the student eligibility to sit for the examination.

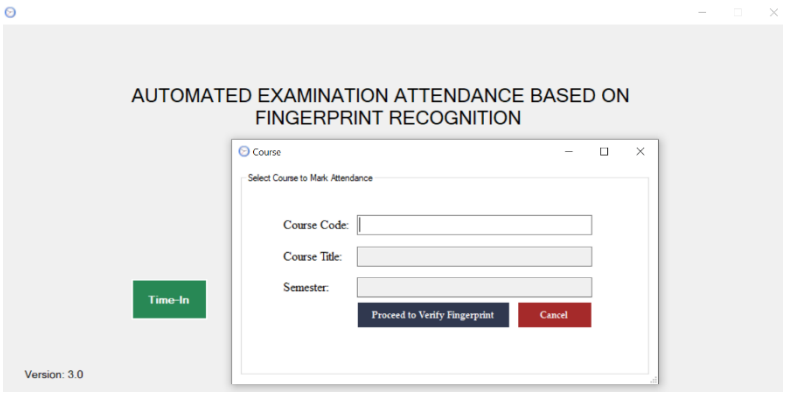

Figure 4.3.1: User Interface – Time-In

Time-Out: This verify that the student participated in the exam.

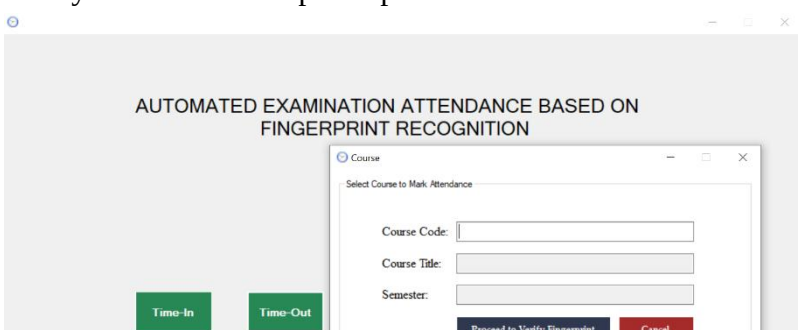

Figure 4.3.2: User Interface – Time-Out

4.4 System Maintenance

The process of modifying an information system to meet changing needs is known as system maintenance. System maintenance is a primary task or obligation any computerized organization must take up in order to ensure efficiency and continuity of the developed system. It is a routine activity, which is to say that the maintenance of the system is very essential to the smooth running of the system.

The following practices and measure must be taken to ensure that the new system does not breakdown and achieve its proposed aim and objectives:

i. Information Management: Each student is required to provide all the necessary and accurate information during registration; this enhances this integrity of the data in the database. For maximum security, each Admin must protect their password.

ii. Regular Database Backup: This involves the creating duplicates of data which acts as an insurance copy should in case the active copy is damaged or destroyed. The backup is usually stored in an external storage device. Recovery involves the use of specialized utility programs to rebuild or replace damaged files. The best way to recover a file or program is to restore it from a backup copy.

iii. Virus Protection: A virus is a program that infects a computer and could damage a system depending on its nature. Because new viruses must be analyzed as they appear, the antivirus must be updated regularly to be effective.

iv. Training End Users: In order for the new system to work properly, proper training has to be provided by the institution on the use of the new system. Training the users is

necessary so as to acquaint them with the working of the system before it is fully developed.

v. Proper use of the system: These include starting (booting) and shutting down the system in the right manner to prevent the system from hanging or data corruption and file loss.

vi. Regular servicing of the computer hardware and peripherals when due to prevent unforeseen breakdown.

4.5 Documentation

Documentation involves all the function performed by the system and how the system is to be used. Documentation describes how the program is used and it also clarifies any obscurities in the design. Documentation usually shows how to use the system, how to install and operate the system, system implementation and test procedure so that it may be maintained.

To initiate the program execution, we launch xampp, create a database and import the sql file to enable the application runs on local server. Then launch the browser (Google Chrome or Mozilla Firefox) then browse the file index. At this point, the content displays the admin login interface. On entering all the necessary detail, the browser takes him/her to corresponding web page. With the way the site is organized, one browses through all the available links without any hitch. And in order to capture and verify students, the admin has to launch the window-based version which was designed with C#.

To capture student fingerprint, the admin will enter the student's name, the system automatically searches the database to know if the student's name is valid. Then, the student will return the name and matriculation number of the student if name is found and then student fingerprint will be enrolled by placing his or her finger on the fingerprint scanner.

To verify and take student attendance, the admin will launch the windows-based version, then click on Time-in to verify and takes the student attendance while entering into the examination hall. The same procedure is applicable to Time-out.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATION

5.1 Summary

This project; a software for Examination Attendance is developed after reviewing and analyzing the existing manual system at the investigation stage. The design is implemented using PHP, C# and MySQL was used for the database and the Integrated Development Environment (IDE) used was Bracket text editor, Visual Studio 2017 and XAMPP was used as the offline local server. The web application starts with login which contains Admin login, then the Home Page where Admin can click to view the various menus on the Dashboard.

5.2 Conclusion

The Automated Examination Attendance System based on fingerprint recognition is developed and tested using the appropriate necessary programming languages, tools and technology that fully meets the objectives of the system which has been developed. The system has reached a steady state where all bugs have been eliminated. The system is operated at a high level of efficiency, the admin and students associated with the system understands its advantage. The system solves the problem it was intended to solve as requirement specification.

5.3 Recommendations

As a result of the findings made during the analysis and design stages of this research work, in order to improve the effectiveness of the system to its greater height and full potential, it is recommended that the following features should be added for future expansion of this project.

- E- Learning (Virtual Classes)
- A website for student forums
- Online Tutorial Classes
- Online Quiz/Exams

For the effective usage of this system and to have good management of it, it is necessary to provide computer to the various registration/examination centers and staff should be trained to acquire knowledge on how to use the computer and new system to meet global standard and modern challenges of information technology. More importantly, this system should be used in various tertiary institutions to curb examination impersonation.

REFERENCE

Hevner, A. R. (2005). A three-cycle view of design science research. *Scandinavian journal of information systems*, *19*(2), 4.

https://*arcjournal.com (October, 2022)*

https://studymafia.org/biometrics-seminar-and-ppt-with-pdf-report-2/ (July 13, 2022)

Jaiswa S., Bhadauria S.S, Jadon R.S (2011). Biometric: Case Study, *Journal of Global Research in Computer Science, (JGRCS) ISSN -2229-371X, Volume 2, No. 10.*

Kinoti P, Sylvester O. M and Henry O. O (2015). Addressing Impersonation Threats in Online Assessment Environment Using Temporal Information and System. *Interactions Merit Research Journal of Education and Review, Vol. 3(6), pp.215-220.*

March S. T. and Smith, G. F. (1995). Design and natural science research on information technology. *Decision support systems*, *15*(4), 251-266.

Olaniyi, O.M, Omotosho. A, Oluwatosin E. A, Adegoke M. A, and Akinmukomi, T (2012). Students Exeat Monitoring System Using Fingerprint Biometric Authentication and Mobile Short Message Service, *The Don International Journal of ICT and Youth Development, Vol 2 pp76 – 85.*

Pankaj S. (2014). Biometrics – Introduction, Characteristics, Basic technique, its Types and Various Performance Measures, *International Journal of Emerging Research in Management &Technology ISSN: 2278-9359 (Volume-3, Issue-4).*

Pressman R. S. (2005). Software Engineering: A Practitioner's Approach, 7th Edition. Published by McGraw-Hill.

Recfaces W. (2021). What Is Biometric Security and Why Does It Matter Today? https://recfaces.com/articles/biometric-security

Sachin T, Miss. Pranjali B, Miss. Pooja G, Miss. Priyanka S, Miss. Rutuja W. (2015). Direct Indirect Human Computer Interaction Based Biometrics. *International Journal of Emerging Engineering Research and Technology Volume 3, Issue 3, March 2015.*

APPENDIX I: BACKEND SOURCE CODE

```
<?php include 'includes/session.php'; ?>
<?php include 'includes/slugify.php'; ?>
<?php include 'includes/header.php'; ?>
<body class="hold-transition skin-blue sidebar-mini">
<div class="wrapper">

  <?php include 'includes/navbar.php'; ?>
  <?php include 'includes/menubar.php'; ?>

  <!-- Content Wrapper. Contains page content -->
  <div class="content-wrapper">
    <!-- Content Header (Page header) -->
    <section class="content-header">
      <h1>
        Dashboard
      </h1>
      <ol class="breadcrumb">
        <li><a href="#"><i class="fa fa-dashboard"></i> Home</a></li>
        <li class="active">Dashboard</li>
      </ol>
    </section>

    <!-- Main content -->
    <section class="content">
      <?php
        if(isset($_SESSION['error'])){
          echo "
            <div class='alert alert-danger alert-dismissible'>
              <button type='button' class='close' data-dismiss='alert' aria-
hidden='true'>&times;</button>
              <h4><i class='icon fa fa-warning'></i> Error!</h4>
              ".$_SESSION['error']."
```

```
          </div>
         ";
         unset($_SESSION['error']);
        }
        if(isset($_SESSION['success'])){
         echo "
          <div class='alert alert-success alert-dismissible'>
           <button type='button' class='close' data-dismiss='alert' aria-
hidden='true'>&times;</button>
           <h4><i class='icon fa fa-check'></i> Success!</h4>
           ".$_SESSION['success']."
          </div>
         ";
         unset($_SESSION['success']);
        }
      ?>
      <!-- Small boxes (Stat box) -->
      <div class="row">
        <div class="col-lg-3 col-xs-6">
         <!-- small box -->
         <div class="small-box bg-aqua">
          <div class="inner">
            <?php
             $sql = "SELECT * FROM students";
             $query = $conn->query($sql);

             echo "<h3>".$query->num_rows."</h3>";
            ?>

            <p>No. of Registered Students</p>
          </div>
          <div class="icon">
           <i class="fa fa-tasks"></i>
          </div>
          <a href="students.php" class="small-box-footer">More info <i class="fa fa-arrow-
circle-right"></i></a>
         </div>
        </div>
        <!-- ./col -->
        <div class="col-lg-3 col-xs-6">
         <!-- small box -->
         <div class="small-box bg-green">
          <div class="inner">
           <?php
             $sql = "SELECT DISTINCT EmpCNIC FROM finger";
             $query = $conn->query($sql);

             echo "<h3>".$query->num_rows."</h3>";
            ?>
```

APPENDIX II: USER INTERFACE SOURCE CODE

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using MySql.Data.MySqlClient;
using System.IO;

namespace ExamAttenBasedFingerprintRecog
{
   public partial class Clock_In : Form
   {
      //MySqlDataReader rdr = null;
      DataTable dtable = new DataTable();
      //MySqlConnection con = null;
      //MySqlCommand cmd = null;
      DataTable dt = new DataTable();
      MySqlConnection con = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
      MySqlConnection con3 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
      MySqlConnection con2 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
      MySqlConnection con4 = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");

      public Clock_In()
      {
         InitializeComponent();
      }

      //private void Clock_In_Shown(object sender, EventArgs e)
      //{
      //    ClockIn();
      //    gridView();
      //}

      #region fill to Datagrid view
      //public void gridView()
      //{
```

```
      //    MySqlCommand cmd = new MySqlCommand("select StudentName as'Student Name', CourseCode as'Course
Code', Semester as'Semester',Date,TimeIn,TimeOut,Status From Attendance", con4);
      //    try
      //    {
      //       con4.Open();
      //       MySqlDataAdapter da = new MySqlDataAdapter();
      //       da.SelectCommand = cmd;
      //       DataTable dt = new DataTable();
      //       da.Fill(dt);
      //       BindingSource bs = new BindingSource();
      //       bs.DataSource = dt;
      //       dataGridAttendance.DataSource = dt;
      //       da.Update(dt);
      //       con4.Close();
      //    }
      //    catch (Exception ex)
      //    {
      //       MessageBox.Show(ex.Message);
      //    }
      //}
      #endregion

      private void Clock_In_Load(object sender, EventArgs e)
      {
         //Get Data from GetCourse form
         txtCourseCode.Text = GetCourse.GetCourseCode;
         txtCourseTitle.Text = GetCourse.GetCourseTitle;
         txtSemester.Text = GetCourse.GetSemester;

         try
         {

            if (!(txtStaff_ID.Text.Equals("")))
            {
               MySqlConnection con = new MySqlConnection("SERVER=localhost; DATABASE=biostudent_attendance;
userid=root; PASSWORD=; PORT=3306;");
               con.Open();

               string strcom = "select name, photo from students where regno='" + txtStaff_ID.Text + "'";
               MySqlDataAdapter daDetails = new MySqlDataAdapter(strcom, con);
               DataSet dsDetails = new DataSet();
               daDetails.Fill(dsDetails);

               if (dsDetails.Tables[0].Rows.Count > 0)
               {
                  txtStaff_Name.Text = dsDetails.Tables[0].Rows[0][0].ToString();
                  //txtJobTitle.Text = dsDetails.Tables[0].Rows[0][1].ToString();


                  //MemoryStream ms = new MemoryStream((byte[])dsDetails.Tables[0].Rows[0]["Picture"]);
                  //pix.Image = new Bitmap(ms);

               }

               MySqlDataAdapter dpt = new MySqlDataAdapter(strcom, con);
               DataSet ds = new DataSet();
               dpt.Fill(ds);
               if (ds.Tables[0].Rows.Count > 0)
               {
                  string imagePath = @"C:\xampp\htdocs\ExaminationAttendanceBasedFingerprintRecog\images\" +
dsDetails.Tables[0].Rows[0]["photo"].ToString();

                  txtImg.Text = imagePath;

                  pix.Image = new Bitmap(txtImg.Text);

               }
```

```
                con.Close();

            }
            else
            {

                MessageBox.Show("ID can't be Empty!", "Fingerprint Enrollment", MessageBoxButtons.OK,
MessageBoxIcon.Warning);
            }

            ClockIn();
            //gridView();
        }
        catch (Exception ex)
        {
            MessageBox.Show(ex.Message);

        }


    }
```