DEVELOPING AN ACCESS CONTROL SYSTEM FOR STUDENTS' IDENTIFICATION IN HIGHER INSTITUTIONS OF LEARNING USING BIOMETRIC TECHNIQUE

BY

AUWALU SUNUSI

REG.NO.1161-04156-05028

BEING A DISSERTATION SUBMITTED TO THE COLLEGE OF HIGHER DEGREES AND RESEARCH IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF SCIENCE IN COMPUTER SCIENCE KAMPALA INTERNATIONAL UNIVERSITY

SEPTEMBER, 2019

DECLARATION

This dissertation is the original work and has not been presented for any degree or other academic award in any university or institution.

---------- ----------

Name and Signature of candidate Date

APPROVAL

I affirm that the work presented in this dissertation was carried out by the candidate under my supervision.

Name and Signature of Supervisor

Date

ACKNOWLEDGMENT

All thanks are to Almighty Allah, the maker and the sustainer of the universe, who in his infinite mercy guided me through the completion of this research. My profound gratitude goes to my supervisor, Dr. Adeleke Raheem Ajiboye, for his numerous efforts and guidance towards successful completion of this research, may almighty Allah reward you.

I would like to appreciate all my lecturers in the School of Computing and Information Technology (SCIT), Kampala International University, in particular Doctoral Committee Members, chaired by Prof Gonzalez Armando and the Dean, School of Computing and Information Technology, Dr. Margaret Kareyo, as well as my HOD, Dr. Olutola Fagbolu. They have all contributed immensely to the successful completion of this research.

I am grateful to my family members for their support and prayers throughout my studies and greatly indebted to my late father for his exceptional support given to me during his life time, may almighty Allah forgive him and grant him Aljannatul Firdausi.

Also, I wish to extend my deep appreciation to my colleagues for the supports and encouragement throughout my studies, thank you so much, may Allah bless you all.

LIST OF TABLES

Table 4.1: Admin login 47
Table 4.2: Structure of Lecturer Login Information. 47
Table 4.3: Structure of Student Login Information. 48
Table 4.4: Structure for Bio data of Lecturer and Records Storage.....48
Table 4.5: Structure of Bio data of Student and Record Storage.....49
Table 4.6: Structure of Course Registration 50
Table 4.7: Structure of Student Record.....50
Table 5.1 Comparison of the Old and New System.....65
The table 5.1 below shows the details of student biometric attendance system evaluation. 67
Table 5.2: To compute the usability of the application developed in this study based on system usability scale (SUS).....68
Table 5.3: Computation of User Response for Usability Testing.....69

LIST OF FIGURES

Figure 2.1: Scanners.....13
Figure 2.2: Fingerprint Characteristics. Adapted from .Afolalu, *et al.* (2016). 14
Figure 2.5: The Abstract Transition Model of the BESAMS Behaviours. 30
Figure 2.6: The Transition Model of the BESAMS Behaviours 31
Figure 3.1 Arduino microcontroller.....35
Figure 3.2 the scanner sensor.....35
Figure 3.3 Circuit board diagrams 36
Figure 4.1: Diagram of the biometric finger print of student attendance 43
Figure 4.2 : Class Diagram for staff and student biometric attendance system. 44
Figure 4.3: Fingerprint procedures by the Administrator. 45
Figure 4.4: Sequence Diagram showing Logging Procedures for Students. 46
Figure 4.5: Biometric Device capturing Student Fingerprint 54
Figure 5.1: Main Menu 55
Figure 5.2: The Interface showing Biometric Enrollment System 56
Figure 5.3: An Interface of Administrator Login. 56
Figure 5.4: An Interface of Lecturer Login. 57
Figure 5.5: An Interface for Lecturer Enrollment. 58
Figure 5.6: An Interface of Student Login. 59
Figure 5.7: An Interface for Students Enrollment (first login). 60
Figure 5.8: Capturing of Lecturer Image. 61
Figure 5.9: An Interface of Register Students Photograph. 62
Figure 5.10: Interface for adding Courses. 63
Figure 5.11: showing Comparison of the manual attendance system with the fingerprint-based attendance system. 65

LIST OF ABBREVIATIONS

AFIS	Automated Fingerprint identification system
BESAMS	Biometric Examination Screening and Attendance Monitoring System
DNA	Deoxyribonucleic Acid
FBI	Federal Bureau of Investigation
HTML	Hypertext Mark-up Language
ICT	Information Center for Technology
ID	Identity card
IDE	Integrated Development
IT	Information Technology
NFC	Near Field Communication
RFID	Radio Frequency Identification
SES	School of Environmental Studies
SGS	School of General Studies
SMS	School of Management Studies
SOT	School of Technology
SRES	School of Rural Entrepreneurship
SUS	System Usability Scale
WAP	Wireless Access Protocol

TABLE OF CONTENTS

DECLARATION i
APPROVAL ii
ACKNOWLEDGMENT iii
LIST OF TABLES iv
LIST OF FIGURES v
LIST OF ABBREVIATIONS vi
ABSTRACT xi
CHAPTER ONE 1
INTRODUCTION 1
1.1 BACKGROUND TO THE STUDY 1
1.1.1 Historical Perspectives. 3
1.1.2 Conceptual Perspectives. 4
1.1.3 Contextual Perspectives. 5
1.2 PROBLEM STATEMENT 6
1.3MAIN OBJECTIVE OF THE STUDY 7
1.3.1 Specific Objectives of the Study 8
1.4 RESEARCH QUESTION 8
1.5 SCOPE OF THE STUDY 8
1.5.1 Geographical Scope 8
1.5.2 Content Scope 9
1.5.3 Time Scope 9
1.6 SIGNIFICANCE OF THE STUDY 9
1.7 DISSERTATION STRUCTURE 10
CHAPTER TWO 11
LITERATURE REVIEW 11
2.0 INTRODUCTION 11
2.1 BIOMETRIC SYSTEM 11
2.2 FINGERPRINT SCANNER 12
2.2.1 Fingerprint Recognition 13

2.2.2 Types of Biometrics 15
2.2.3 How Biometric Fingerprint Works 18
2.3 APPLICATION OF BIOMETRIC TECHNIQUES. 19
2.4 CHALLENGES OF USING BIOMETRICS. 20
2.5 BENEFITS OF USING BIOMETRICS FOR STUDENT ATTENDANCE MONITORING... 22
2.6 RELATED WORKS 23
2.7 GAPS THAT NEED TO BE FILLED. 26
2.8 THEORETICAL FRAMEWORK OF THE MODEL 27
2.9 THE USE OF SYSTEM USABILITY SCALE 32
2.10 REVIEW OF THE EXISTING METHODS OF STUDENT ATTENDANCE REGISTRATION. 32
CHAPTER THREE 34
METHODOLOGY 34
3.0 INTRODUCTION 34
3.1 RESEARCH DESIGN 34
3.3 DATA COLLECTION 36
3.4 RESEARCH INSTRUMENT 37
3.5 TARGET POPULATION 37
3.6 SAMPLE SIZE 37
3.7 SAMPLING TECHNIQUE 37
3.8 DATA ANALYSIS TECHNIQUE 37
3.9 DATA COLLECTION PROCEDURE 37
3.10 SYSTEM MODELLING 38
3.11 ETHICAL CONSIDERATIONS 38
CHAPTER FOUR 39
ANALYSIS, DESIGN AND IMPLEMENTATION 39
4.0 INTRODUCTION 39
4.1 DATA PRESENTATION AND ANALYSIS FROM THE RESPONSES ON THE SPECIFIC OBJECTIVES. 39
4.1.1 Analysis of the Existing System of Identifying Students at Kano State Polytechnic, Nigeria. 39

4.2 DESIGN AND DEVELOPMENT OF A BIOMETRIC SYSTEM FOR IMMEDIATE IDENTIFICATION OF THE STUDENT FINGER PRINT. 41
4.2.1 System modeling using UML 41
4.2.2 Software 41
4.2.3 Hardware 42
4.2.4 Block Diagram of the System 42
4.2.5 Diagram 43
4.2.6 Sequence Diagram for Administrator 44
4.2.7 Sequence Diagram for Student 46
4.3 IMPLEMENTATION OF DATABASE STRUCTURE 47
4.3.1 Database Structure 47
4.4 FINGER PRINT CAPTURING PROCEDURE OF SELECTED REGISTERED STUDENTS. 51
CHAPTER FIVE 55
RESULT, DISCUSSION, EVALUATION, AND TESTING 55
5.1 The System Main Menu implementation. 55
5.2 RESPONSE FROM THE SPECIFIC OBJECTIVE ONE 64
5.2.1 To analyze the existing system being used in Kano State Polytechnic. 64
5.2.2 To design and develop a biometric system for immediate identification of the students fingerprint. 65
5.2.3 To capture the finger print of registered students at Kano State Polytechnic using a biometric device. 66
5.3 Evaluating the performance of the developed biometric System using registered and unregistered student. 67
5.4 Testing of the Prototype System 70
5.4.2 Steps: Software is tested from two different views: 71
5.5 UNIT TESTING: 71
5.5.1 System Testing 71
5.5.2 Performance Testing 71
5.6 TEST CASES 72

CHAPTER SIX 73
CONCLUSION AND RECOMMENDATIONS. 73
6.1 CONCLUSION....73
6.2 RECOMMENDATIONS.....75
6.3 FUTURE WORK.....75
6.4 CONTRIBUTION TO KNOWLEDGE.....75
6.5 LIMITATIONS OF THE STUDY....76
6.6 SUMMARY....76
REFERENCE....78
APPENDICES 87
Appendix A: Interview Guide....87
APPENDIX B: INTERVIEW TRANSCRIPT 88
APPENDIX C: QUESTIONNAIRE....92
APPENDIX D: HARDWARE AND SOFTWARE CODES 93
APPENDIX E: BUDGET....105

ABSTRACT

Biometric technology is a technique that is capable of uniquely identifying a person through his/her characteristics features. The use of this approach is gaining ground in recent times, particularly in higher institution of learning where impersonation is currently at alarming rate. The technology offers a reliable solution for solving recognition problem through features such as: fingerprint, faces, iris, palm print etc. The main objective of this study is to implement a system that uses fingerprint to identify registered students of Kano State Polytechnic and further track their attendance during lectures and examinations. This study developed a system, configure the system and ensure proper synchronization with a biometric device. The system was developed using dot net framework. Specifically, visual basic.net is used for coding all the interactive interfaces, while SQL server 2008 was used as the back-end. In order to establish the efficiency of the developed system in terms of usability, its usability was determined using the approach of System Usability Scale (SUS). A total of 60 students participated in the study by navigating through the system and based on their interactions, they responded to the structured questionnaire designed to test the system's usability. The result of evaluating the usability of the system based on the SUS approach gave 82.7%. Hence, the system was found to be very accurate, reliable and secured for keeping students bio data and it restricts access to intruders that is unregistered person. Thus, it was concluded that, this system is an indispensable tool for curtailing impersonation by students and for keeping authentic records of students. Hence, the relevance and academic importance of this system cannot be over emphasizing. Thus, in order to bring an end to the rampant cases of impersonations during lectures and examinations in the institutions of higher learning. Kano State Polytechnic in particular can adopt the system developed in this study for total eradication of such menace.

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND TO THE STUDY

Biometric Identification Systems has found its application in different domain and industries such as workforce management and are quickly becoming more useful in the education sector for accurate Student Identification and Tracking of students. This is due to the limitations and inaccuracies of traditional student attendance tracking methods like roll calling (Alia& Al-Allaf, 2013). The need for biometric student tracking systems in educational institutions is rising because these systems are more accurate, faster and convenient besides being a more effective tool to protect student identities and privacy, Alia *et al.* (2013). According to Cruz, Paglinawan, Bonifacio, Flores & Hurna (2015), traditional student identification and attendance methods such as roll calling or paper based attendance are outdated and often lead to unnecessary time spent by lecturers and administrators to register student track. Moreover, with large groups of students, manual supervision is difficult to execute. Therefore, these traditional student tracking methods have loopholes which cannot prevent proxy attendance, ID card theft, impersonation and attendance tracking errors which has serious problems with direct effect on education quality. Cruz, *et al.* (2015).

(Manoharan, Reddy & Akash,2016), argue that biometric access and identification systems are automated and provide a convenient way to quickly record student check-in and check-out. Biometric technology uses human physical and biometric characteristics (which are unique for every individual) to ensure identification accuracy, prevent errors, and eliminate proxy attendance even in case of identical twins. Biometric technology also protects students from identity theft because it uses sophisticated encryption to secure and protect user identity privacy. According to Thomas, *et al*, (2013), biometric attendance system has brought more precise accuracy in recording and measuring student attendance. This is done when biometric attendance machine captures a unique biological/physical feature such as hand or finger print, iris pattern and sometimes even voice as a record for identity verification so as to permit an authenticated person to perform a task as authorized. Biometric attendance machines also count employees' work schedule, like which employee did what, and at what time did he do it, etc. Biometric attendance system is a foolproof technology to ensure the accuracy of attendance and useful to

the ones who deal with large number of employees or students and further uses the biometric feature of finger print to authenticate the claim of any enrolled employee or students. It also provides an efficient way for administrators to manage either employee attendance record or students' attendance record.

Biometrics technologies verify identity through characteristics such as fingerprints, faces, irises, retinal patterns, palm prints, voice, hand-written signatures, and so on. These techniques, which use physical data, are receiving attention as a personal authentication method that is more convenient than conventional methods such as a password or ID cards because it uses data taken from measurements and such data is unique to the individual and remains so throughout one's lifetime (Kadry & Smaili, 2010).(According to Rufai, Adigun & Yekini 2012). Examination is an instrument for testing, assessment evaluation and accreditation. But in most institution before any student is allowed to sit for examination such student needs to meet specified percentage of class attendance but due to stress of manual attendance taking and record keeping the percentage required before sitting for an examination has not been adhered to in many institution of developing nation. Pen and paper are used to keep record of class attendance in most higher institution in the developing country, and this has been prove to be very stressful, time consuming, unreliable, inaccurate and inefficient (Adetiba, Lortim, Olajide & Awoseyin,2013).

Similarly, biometric system will uniquely identify a student and will be authenticated to take part in an examination. In this case a unique characteristic like fingerprint of each student is used to prevent unauthorized access to take part in an examination by checking the behavior characteristics. Jaiswa *et al.* (2011), reviewed that Biometric system is commonly used today in the authentication of a person by analyzing physical characteristics, such as fingerprints, or behavioral characteristics such as signatures. (Akaranga & Ongong 2013) proposed that, examination is the most common instrument around in which the entire system of education revolves. There is hardly any educational system which does not include one form or another of assessment as an indicator of the said system of education. It is the instrument used to decide who is permitted to go to the next academic level. In fact, it is the results of examinations and lecturer judgments which form the grading system in which all the students are classified annually or more frequently.

1.1.1 Historical Perspectives.

According to (Asha & Chellappan 2012). Biometrics is not a new concept; it is the oldest form of identification and the use of non-automated biometrics dates back to the beginning of human civilization, when individuals first began identifying other individuals based on certain physical or behavioral characteristics. (Woodward, Orlans &Higgins;2003), (Aisha & Chellapan, 2012).It is emphatic note that biometrics as an organized system of authentication dates back to more than one thousand years in East Asia, when potters placed their fingerprints on their wares as an early form of brand identity. Anderson (2001), the use of handwritten signatures (chops) in classical China as an example of an early biometric.

Bertillon Systems in 1882 took subject's photography, height, the length of one-foot, an arm and index finger. One of the first institutionalized use of biometric data (in this case fingerprints) was their usage in crime registers. In 1903, New York state prisons adopted fingerprint identification to verify the identity of criminals. This solution spread like wildfire among the various penal institutes and police forces. This process culminated in the founding of the fingerprint analysis department of FBI in the 1st July, 1921.

In the year 1924, Federal Bureau of Investigation (FBI) setup a fingerprint identification division. By 1926, law enforcement officials in several U.S. cities had begun submitting fingerprint cards to the FBI in an effort to create a database of fingerprints from known criminals. In the early 1960‘s the FBI invested a large amount of time and effort into the development of automated fingerprint identification systems. This automation of biometric identification for law enforcement purposes coincided with the development of automated systems for non-forensic applications, such as high-security access control. AFIS installed in 1965 with a database of 810,000 fingerprints. During the 1970‘s a biometric product based on measuring the geometry of the hand was introduced in a number of access control applications. Goldstein. *et al*. (2008).

The development of contemporary biometric systems can be viewed as an outgrowth of the efforts of forensic scientists and law enforcement agencies to identify and classify criminals in the late 19^{th} and early 20^{th} centuries. Fully automated biometric systems including (AFIS) automated fingerprint identification system used by law enforcement agencies and commercial

biometric systems (typically relying on hand geometry) designed for use to physically access buildings and emerged in the 1960s and 1970s.

The computer industry began using biometrics few years ago. Which are created for a specific function, and they lacked the adaptability required to integrate into a variety of environments. This resulted in costly solutions that few were able or willing to incorporate. However, over time, as technology advanced, biometric solutions evolved to be widely recognized as viable options to security solutions such as control of fraud and security breaches, and human administrative error are helping to drive the expansion of biometric technology (Nunavut & Thieme, 2002).

In the same vein, emergence of biometrics has addressed the problems that plague traditional verification methods. By using biometrics it is possible to establish an identity based on `who you are', rather than by `what you possess' (e.g., an ID card) or `what you remember' (e.g., a password). Current biometric systems make use of fingerprints, hand geometry, iris, retina, face, facial thermo grams, signature, palm print and voiceprint to establish a person's identity. Biometric systems have an edge over traditional security methods in that they cannot be easily stolen or shared. Besides strengthening security, biometric systems also enhance user convenience by alleviating the need to design and remember passwords (Asha & Chellappan, 2012).

1.1.2 Conceptual Perspectives.

Biometrics is generally used as a noun to refer to the automatic recognition of individuals based on their physical and behaviuoral characteristics. The term biometric can be used as a noun in reference to a single technology (e.g., finger scan is a commonly used biometric) or as an adjective as in a biometric system uses integrated hardware and software to conduct identification or verification (Nunavut& Nanavati, 2002).

Biometric characteristics are considered to be unique on a particular individual hence, use it provides a good platform against impersonation. Which ensures users to authenticate a person’s distinctiveness based on who he/she is rather than confirming via what he/she possesses such as ID card or by what he/she recalls a password? Adeyemo, *et al.* (2014). Similarly (Jain, *et al.* (2004). Biometric recognition system signifies design recognition system that is capable of recognizing individuals based on their physiological or behaviuoral traits. These characters are

considered to be unique to each individual and unlike knowledge or token-based security mechanisms; it cannot be forgotten, lost or stolen. The most common individualities used for biometric recognition are: fingerprint, Faces, palm-print, speech, and iris.

Jain, *et al.* (2008).The process of Biometric authentication is done to access some identifying biological or traits can be specifically recognized in an individual. These unique identifiers are retina, earlobe geometry, iris patterns, fingerprints, hand geometry, voice waves, earlobe geometry DNA and signatures. Law enforcement has implemented Facial-recognition technology to fish out people in gathering with significant firm quality and reliability. Generally industries utilize hand geometry for providing physical access to buildings, for people who try to impersonate another individual, earlobe geometry is utilized to detect their identity In Computer Science, biometric identification or biometric authentication is utilized as a mode of identification and access control which are being implemented to detect individuals in groups that are being watch or under surveillance.

1.1.3 Contextual Perspectives.

Kano State Polytechnic is an institution of higher learning located in Kano city of Kano state, North-Western Nigeria. It was established in the year 1968, which five hundred and fifty (550), staff as well as total number of student fifteen thousand two hundred (15,200).students.

It offers both part time and full time programmed. The polytechnic has five schools namely: School of Technology (SOT), School of Management Studies (SMS), School of Environmental Studies (SES), School of Rural and Entrepreneur Studies (SRES) and School of General Studies (SGS). The Central Administration is the heart of the school where administrative issues are carried out.

Similarly, the research was conducted in the School of Technology, Kano State Polytechnic, and Nigeria. School of Technology was founded 42 years ago which the ability as to offer relevant educational.Competance in Science and Technological courses. However, the aim of the School of Technology is to provide a focus and framework for its constituent departments to formulate and express views pertinent to technology, methods and processes, both within and outside the Polytechnic

1.2 PROBLEM STATEMENT

Obviously, the existing methods of student attendance identification in most institutions of higher learning are mostly manual which involves the use of paper, pencil and other archaic means where students write or sign against their names. This method is not only time consuming but is also inefficient in the sense that updating students' records, storage and management of such records as well as calculating percentages of attendance for examination purposes tend to be quite difficult and mostly unachievable. The method of student attendance identification lacks the capability to track time on individual attendance records. Saheed, *et al.* (2016). Besides, most of the times, data from these records turn out to be fake, unreliable and not authentic because of the manner in which the required data for these records are obtained as such, the motive behind keeping the students' attendance records becomes defeated.

Consequently, inefficiencies of the current methods used in taking and keeping students' attendance records makes it very easy for false attendance and impersonation whereby students find it very easy to write their friends names on the attendance list without being detected by the teacher or any other officer in charge. Most of the time, lecturers face the problems of having an empty classroom and yet the attendance list is full. This arises from the fact that most of the time, some truant students tend to attend classes during the first few weeks after which they stop attending and request their punctual friends to sign the attendance on their behalf. Since lecturers are always busy teaching in the classes they tend to be oblivious of what happens with the attendance register and have no time to check the attendance list one-by-one. Olaniyi, *et al.* (2015).

Clearly, the consequences of lack of authentic attendance list as well as that of fake attendance lists are enormous. As a result of the ineffectiveness of the present manner of recording students' attendance in the polytechnic, teachers find it very difficult to ascertain true lecture attendants or produce authentic statistics of students' attendance for record keeping. Moreover, impersonations during examinations are also very difficult to detect with these ineffective students' attendance taking methods. Stripling, *et al.* (2013), reported that, the effects of non-attendance not only impacts the overall students' performance but also affects the entire community of a classroom. Non-attendance negatively influences class success as well as faculty morale as learning declines

and academic standards are compromise. Furthermore, as the academic semester progresses and on particular days of the week like Friday as weekend approaches class attendance reduces.

In many instances, when students fail to present their examinations cards during semester examinations due to loss or being forgotten at home, both the students and the school authorities tend to lack any tangible evidence to prove that such students had the required percentage of attendance to be allowed to sit for the examination. Consequently, many students have ended up missing examinations because of such simple problems that could be effectively solved had there been a fingerprint biometric identification system. This was confirmed by .Salako, (2018).

The increasing rate of examination impersonation among candidates in institutions of higher learning reduces their self-developing skills and self-confidence towards reading and writing an examination. It negatively affected the growth of educational system in Nigeria despite various strategies deployed by stakeholders to ensure candidates obeyed the rules governing an examination. Awojide, *et al.* (2018). Nowadays in Nigeria, having a certificate is much more important than getting individual skills and these have prompted students to engage in various illegal activities such as non-attendance of lectures and boycott in other to get what they want.

Furthermore, despite concerted efforts by authorities of the polytechnic to bring an end to issue of lack of effective students' attendance records as well as impersonations by students by providing attendance register for roll calls among others, the menace still prevails with dire consequences on the students, the polytechnic as well as the larger society.

Thus, it is against this background that this study was conducted with the sole aim of designing an effective biometric finger print for efficient attendance records of students across all faculties of the polytechnic so that the production of fake students' attendance records as well as impersonations during examinations can be curtailed.

1.3 MAIN OBJECTIVE OF THE STUDY

The main objective of this study was to develop a means of identifying students and staff using biometric fingerprint system. To achieve this central objective, the following specific objectives have been formulated:

1.3.1 Specific Objectives of the Study

i). To analyze the existing system of students' identification at the Kano State Polytechnic, Nigeria.

ii). To develop a biometric system that can work with a biometric device for immediate identification of students' fingerprints.

iii). To use the system developed in (ii) for the capturing of students' finger prints at the Kano State Polytechnic.

iv). To evaluate the performance of the developed biometric system using the data that comprised of registered and unregistered students.

v). To compute the usability of the application developed for use with biometric device based on system usability scale (SUS).

1.4 RESEARCH QUESTION

In the course of this study the implementation of the proposed system answer the following research questions:

i. What is the existing system of students' identification at Kano State Polytechnic?
ii. How can a biometric system be developed for immediate identification of the students fingerprint?
iii. How can the developed system used for capturing of students finger print at Kano State Polytechnic using a biometric device?
iv. How can the performance of the developed biometric system be evaluated using the data that comprised of registered and unregistered students?
v. How can usability of the application developed be computed for use with biometric device based on system usability scale (SUS)?

1.5 SCOPE OF THE STUDY

1.5.1 Geographical Scope

Kano State Polytechnic is a State owned tertiary institution located in the city of Kano, Kano state, Nigeria Founded in 1968.

1.5.2 Content Scope

There are many types of Biometric techniques. The choice made for this study is fingerprint. Specifically, this study focused on the student's bio data of School of Technology of Kano State Polytechnic, Nigeria, in order to produce a biometric fingerprint identification system.

1.5.3 Time Scope

The study covers a period of August 2018 – September 2019.

1.6 SIGNIFICANCE OF THE STUDY.

The proposed system provides a more accurate and efficient record of student attendance for proper identification of both absentee and impersonated. Furthermore, the system process faster and simpler information compared to current paper based student attendance register. Other than that, this system will assist lecturers in taking the student attendance more effectively without worrying about losing or damaging their attendance sheets while passing it among the students around the whole class.

Besides, the system will also allow the institution management to track students' class attendance in a particular course having poor attendance, thereby enabling the management to rectify the situation by providing the necessary interventions. The system provide high level of security whereby making it impossible for imposters and impersonators to make their ways to examination halls. The system using fingerprint biometric will keep historical data making it easy for lecturers to access. Furthermore, the authentication system is not only useful to the institutions and lecturers alone, even the students benefit a great deal by reducing the stress encountered in queuing up which often result in delay and at times damage the attendance sheet. It also prevents mistakes and anomalies that is associated with manual signing in which student that attend a class are marked as not present thereby losing the mark accorded to the particular attendance due to multiple attendance sheet.

Fingerprint Based Student Attendance Monitoring System is extremely useful in institutions especially during classes and examination in which heavy security are normally use to validate student's identity in order to cob imposters, through the use of Verification System the number of security personnel will be greatly reduce.

Also, the proposed system addresses the challenge of missing attendance register for the examinations, since information about students can be automatically generated on the spot with the help of the designed system.

1.7 DISSERTATION STRUCTURE

This Dissertation is divided into five chapters as follows:

CHAPTER 1: This chapter introduces the dissertation and discusses some key sections as regards the problem statement, research questions, specific objectives and others.

CHAPTER 2: The review of literatures and some related are shown here.

CHAPTER 3: The proposed method procedures design and implementations are shown here.

CHAPTER 4: The chapter shows the result and the discussion of these results and the evaluation approach.

CHAPTER 5: This dissertation is concluded here.

CHAPTER TWO

LITERATURE REVIEW

2.0 INTRODUCTION

This chapter reviews literature as regard the research work from different scholars and publications to understand the concept and the context clearly and to apply it in the proposed research work.

2.1 BIOMETRIC SYSTEM

Biometrics refers to the automatic identification of a person based on his or her physiological or behaviuoral characteristics. It includes fingerprint, iris, facial and retina. Biometrics technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Today, biometric is being spotlighted as the authentication method because of the need for reliable security. Cappelli *et al.* (2007). Fingerprint authentication is one of the most well-known and publicized biometrics technologies, because of their uniqueness and consistency over time, fingerprints have been in use for identification for over a century, more recently becoming automated due to advancements in computing capabilities.

Fingerprint is popular because of the inherent ease of acquisition, the numerous sources for instance ten fingers available for collection, and their established use and collections by law enforcement and immigration. According to (Oloyede, Adedoyin & Adewole, 2013), many industries are experiencing technological advancement and changes in the mode in which they carry out their business processes. With the rise of globalization, it is becoming essential to find an easier and more effective system to help an organization or company improve their employee's productivity. In spite of this matter, there are still business establishments that use the old-fashioned method of manual process of recording employee's attendance .Yuihotakaishi, (2011).

Staff attendance management system is an effective way to keep track of attendance of staff within an organization. It covers the requirements of the personnel department in terms of day to day monitoring of staff, calculation of overtime and transfer of relevant information to the payroll system and manpower analysis. Hence, staff attendance is an important issue every organization must take into consideration in order to be productive (Kadry & Smaili, 2010).

(Naik & Patil 2016). Pointed out that biometric system is the most authentic method for authenticating a user based on his/her thumb impression. The scope of biometric authentication is used for staff attendance as well as student attendance system. The biometric contains the vast data generated by biometric device which are used by system developer to design and implement automated students' attendance.

Mohit *et al.* (2016), revealed some importance of the biometric system. The system is useful for the student attendance and staff attendance registering. The approach involves the collection of the student information and ensuring proper maintenance of the record captured.

(Saumyarup, 2016), further stated that finger verification technique to display the match found otherwise no equal found. It checks the fingerprint of the person's. Mohd *et al.* (2016), it is cost effective and portable system. The finger print is unique to each and every person in the world.

2.2 FINGERPRINT SCANNER

(Akinola, Abayoma & Adeniyi, 2015), identification device has been commercialized from the late 19th century. The device is the most popular among all the identification devices because of its ease in acquisition, and also the number of sources that are available for its data collection. Sir Francis Galton, in 1892, developed a classification of system for fingerprints using minutiae characteristics that is being used by researchers and educationalists even today.

A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The image captured from the sensor is referred to as a live scan, which in turn is processed digitally to develop an accumulation of extracted features (Biometric Template). This template is stored in a database and utilized for matching. Figure 2.1 presented some fingerprint sensor.

Figure 2.1: Scanners

Source: https://www.lifewire.com/scanner

Fingerprint scanner enrolls and verifies the identity of every person based on the marks on his or her fingers and these marks have a pattern that cannot be changed or removed except through physical injury. The print is made up of ridges and furrows as well as characteristics that occur at minutiae points. Standard systems are comprised of a sensor for scanning a fingerprint and a processor which stores the fingerprint data and software which compares and matches on the fingerprint to the stored data in the database. Within the database, a fingerprint is usually matched to a reference number or Pin number which is then matched to a person's name. In use of security, the match is generally used to allow or disallow access. Thornton, (2000).

2.2.1 Fingerprint Recognition

Basically, biometric technology uniquely recognizes individual even a twin brother will not have the same fingerprint. Thus, the individual fingerprint is capable of storing a unique identifiable

piece of information. The uniqueness in each fingerprint is due to the peculiar generic code of DNA in each person. Peter, (2005).This code causes the formation of a different pattern of our fingerprint.

Figure 2.2 shows all the characteristics of a fingerprint. These characteristics are helpful during the process of minutiae extraction. (Afolalu, Tope-Oke & Atsadu, 2016).

Figure 2.2: Fingerprint Characteristics. Adapted from .Afolalu, *et al.* (2016).

Fingerprints are considered to be the best and fastest method for biometric identification, they are secure to use, unique for every person and do not change in one's life time. A fingerprint recognition system operates either in verification mode or in identification mode (Sarker, Hossain, & Jamil, 2016). Automated fingerprint identification is the process of automatically matching one or many unknown fingerprints against stored records in the database. Automated fingerprint verification is closely related technique used in applications such as attendance and access control systems. On a technical level, verification systems verifies a claimed identity (a user might claim to be John by presenting his PIN or ID card and verify his identity using his fingerprint), whereas identification systems determine the identity based solely on fingerprints.
Matching algorithm plays a key role in fingerprint recognition system matching algorithms are used to compare previously stored templates of fingerprints against candidate fingerprints for authentication purposes .Onaolamipo, (2014).

Fingerprint is the pattern of ridges and valleys on the tip of a finger and is used for personal verification of people. This is based on recognition method because of its relatively outstanding features of universality, permanence, uniqueness, accuracy and low cost. These features have made fingerprint the most popular and reliable technique and is currently the leading biometric technology .Jain *et al.* (2004).

Similarly, fingerprint has certain natural traits that make them ideal for use in biometric systems. Fingerprints are developed between the first and second trimester and remain unchanged (barring any damage or scarring) until death. Fingerprints are unique. No two people on record have been found to have the same. Fingerprint scanning can be done in several different ways. Some systems scan the distinct marks on the finger called minutiae points (similar to the traditionally used police method). The positioning of pores and straight pattern matching may also be used. More recent developments include the use of moiré fringe patterns (superimposing of lines and grids to capture three dimensional surface shapes) as well as ultrasound. Fingerprint systems should be kept clean as smudges or dirt and grime may cause problems for the reader (Griaule 2007; Gorman 2001).

According to Ezeman *et al, (*2015).Two of the first smartphone manufactures to integrate fingerprint recognition into their phones were Motorola with Atirx 4G in 2011 and apple with the IPhone 5S in September 10, 2013. The fingerprint authentication has many merits such as high accuracy easier access through PC. It is one of the safest biometric authentication methods

2.2.2 Types of Biometrics

Biometric technology differs from technique to technique. Kalyani, (2017), identifies the following as some of the popular biometric technologies:-

Fingerprints: The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available, users no longer need to type passwords –instead, only a touch provides instant access. Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names .Robert *et al.* (2005).

Similarly, they are several benefits of using fingerprint recognition systems. This system is easy to use and install. It requires cheap equipment which generally has low power consumption. However, there are some disadvantages in this system. If the apparent of the finger gets damaged and has one or more marks on it, identification becomes increasingly hard. Furthermore, the system requires the users' finger surface to have a point of minutiae or pattern in order to have matching images. This will be a limitation factor for the security of the algorithm. Fingerprint security system is used widely in different applications such as: cell phones, laptops, USB flash drives and others devices. It is also used in judicial systems in order to record users' information and verify one person's identity. Biometrics New Portal. (2011).

Hand geometry: Hand geometry involves the analysis and measuring of the hand and fingers. Alotaibi, (2010), the user places their hand on the reader with their fingers in designated positions. A camera is then used to capture both a top view, which gives the length and width, as well as a side view, which gives the thickness. Hand geometry is one of the most established uses of biometrics today which is accurate and fast.

Signature Verification: This technology uses the dynamic analysis of signature to authenticate a person; this Technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.Salil. (2001).

Voice Recognition: There are two main influences which makes a person's voice unique. Firstly, it is the physiological component which is known as the voice tract. Secondly, it is a behavioral component which is known as the voice accent. By combining both of these factors, it is almost impossible to imitate another person's voice exactly. Taking advantages of these characteristics, biometrics technology created voice recognition systems in order to verify each person's identification using only their voice. Mostly, voice recognition will emphasis on the vocal area because it is a unique characteristic of a physiological trait. It works perfectly in physical access control for users (Peter, Anne, Shaun & Lucy, 2011).

Iris Recognition: This recognition method uses the iris of the eye which is the coloured area that surrounds the pupil. Iris patterns are unique; the iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Methods based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities. Salil, (2001).

Face Recognition: The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image, by using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Key benefits of facial recognition it is non-intrusive, hands-free, and continuous and accepted by most users (George & Rajesh, 2009)

Attendance Management falls into two categories namely; Conventional and Automated methods. Conventional methods include time sheet, attendance register and time clock. (Ononiwu & Okorafor, 2012). Time sheets are documents, automated or else that record what time was spent by the employee on what tasks. Attendance register is an official list of people who are present at an institution or organization. Time clock which is a mechanical (or

electronic) time piece used to assist in tracking the hour worked by an employee of a company. Automated methods include Barcode system attendance system, magnetic stripe attendance system, Radio Frequency Identification (RFID) and the biometric attendance system. (Ononiwu & Okorafor, 2012).

2.2.3 How Biometric Fingerprint Works

Raymond, *et al*, (2015), stated that Fingerprint identification is the oldest method that has been successfully used in various applications. Each of our ten fingerprints is different from one person to another. Even identical twins have unique fingerprints. That makes them ideal for personal identification. A fingerprint is made of a sequence of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint is determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur when a ridge splits apart or a ridge ends. Finger scanning uses flat images of only two fingers to create templates. Flat images reveal the center of the finger and require only a minimum of unique identifying points in order to make a match. The purpose is to recognize a person already being enrolled in particular software.

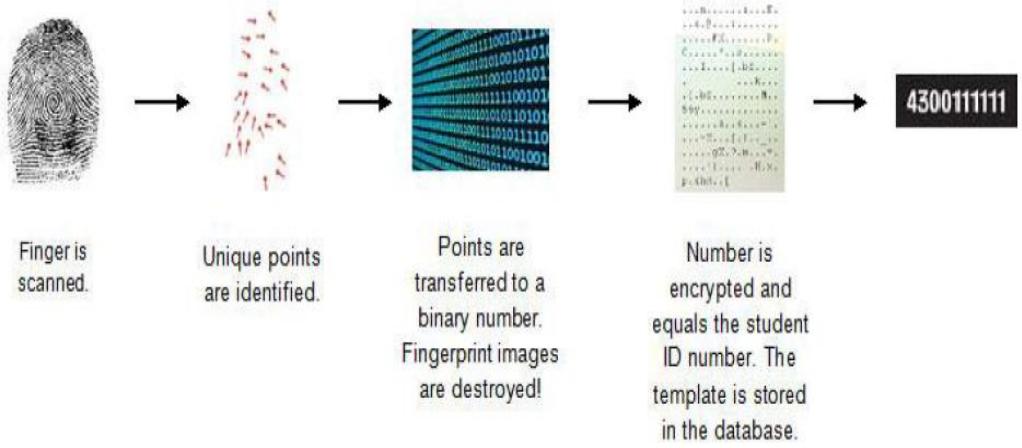


Figure 2.3: How Finger Scanning Works.

When the student returns to be authenticated, the finger scanner again scans the finger. The computer software now compares the new template with the other templates in the database. When a matching template is found, the student is authenticated. This authentication and matching process takes about one second to complete.

(According & Edmund 2002), the study reviewed that fingerprint scanning is the acquisition and recognition of a person's fingerprint characteristics for identification purposes. This allows the recognition of a person through quantifiable physiological characteristics that verify the identity of an individual. There are mainly two types of finger-scanning technology that make this possible.

2.3 APPLICATION OF BIOMETRIC TECHNIQUES.

(Raymond, *et al*, 2015), identifies that the following as the application of biometrics system:-

School Access: A controlled environment is critical to a school's success. Access to the school must be permitted only to authorized persons. Students, teachers, staff and frequent visitors can be accurately time-stamped and identified using biometric finger scanning technology and attendance applications. Administrators will have a certain record of the date and time of each person's entry into the building. Biometric finger scanning systems can assure administrators that those entering their schools actually belong there.

Attendance: School administrators are being held responsible by federal and state governmental funding sources for accurate attendance records since certain money is provided based on the number of students who attend the school each day. Schools that have made faults in attendance reporting have been required to pay back hundreds of thousands of cash to the governmental funding sources. Biometric finger scanning technology provides administrators with irrefutable proof of student attendance for accurate and auditable reporting. In addition, administrators can be provided with period-by-period attendance records in real-time, quickly identifying students who are not in the appropriate classrooms. Also, teachers of large classes, such as band, group, chorus, and physical education can use the entire classroom period for training instead of using respected time to take attendance.

Cafeteria: Most cafeteria debt systems use swipe cards or PINs. Schools are now using finger scanning to eliminate the expenditure and problems associated with these methods and to ensure accurate reporting. Biometrics is also being used in retailing machines to increase reimbursements and decrease costs. In addition, by integrating a biometric finger scanning system with the cafeteria application, accurate lunch reporting for students entitled to the free or reduced lunch program is provided anonymously, with the important result of increasing participation by eliminating embarrassment.

Library: School libraries store thousands of millions at schools' assets such as books, periodicals, recordings and pieces of art. Librarians can use finger scanning to substitute library cards eliminating the distribution of library cards with students who have overdue materials.

Transportation: School students get lost at wrong schools and bus stops each day, especially young students. New buses drivers are hired throughout the school year due to their paths are frequently changed. This makes it difficult for them to get to know the students well enough to visually identify them and where they fit. School areas have implemented finger scanning on buses in order to help the driver know if the student is on the correct bus goes to the correct school and gets off at the precise stop.

Nurses: Nurses are charged with dispensing medication to students every day. In many schools, nurses change duties and substitutes dispense medication when the school nurse is unavailable. Finger scanning provides an irrefutable record, and prevents any potential life threatening errors.

Other Applications*:* Wireless applications now being developed can assist large schools in hallway monitoring. This technology can also be applied to off-site student identification for field trips and outdoor events. Emergency identification as a result of a fire or other disaster is a critical use of this technology.

2.4 CHALLENGES OF USING BIOMETRICS.

Public acceptance is the main reason hindering the Development of biometrics, there is fear among people that usage of biometrics may lead to annexation of their privacy (freedom from observation). Different organizations store the information about different biometric identifiers of people in their database, they are afraid that some organizations might use this information to track their activities and performance and also share this information with other organizations for various reason in that their knowledge. People also think that the government uses this information to track their daily actions and control them completely in the name of fighting crimes and terrorism, Lee. (2002).

Similarly, kind of misuse of personal information violates the user's privacy and civil liberty (El-Abed, Mohammad, Romain, Baptiste & Christophe, 2010). It is exposed through media that biometrics are complex and are used only in military organizations requiring high level security.

They feel that this level of security is avoidable in their everyday life due to its complexity. Recognition of biometrics may also depend greatly on the culture, in order for biometrics to gain public acceptance, the hurdles of privacy and its perception are to be conquered .Mark, (2014). However, it is difficult to false biometric identifiers but not impossible, behaviuoral biometrics like signature and voice can easily be stolen compared to physiological biometrics. Although signature is infrequently used for security, a person's voice is commonly used. Voice can be mimicked. Fingerprint scanners can be misled with a silicone finger. A mold of hand can be used to fake hand biometrics. An image of the face and iris can be used to deceive the biometric scanning systems. Iris can be faked using a contact lens also. All these techniques of replicating biometrics should be eliminated. Biometric identification consists of two stages – Enrollment and Verification .Soutar *et al.* (1998). The Biometric is converted to a template using an algorithm and then stored. In the verification stage, a person presents his identity during the enrollment stage, a person can provide false documents as identifiers and once the new forged identity has been accepted by the system, a person can engage in a lot of illegal activities. Chinchilla, (2012).

Despite the biometric attendance system its protecting meaningless, reframe are slighter with chances of alleviating the information stores and influence of prejudice is less. However, the performance of the biometric devices in tandem with biometric attendance system need to be monitored for errors and issues which may pitch in from time to time and the authorities have to ensure timely fixation of the issues related to biometric attendance system. The operative aspect of the biometric attendance system makes it very inspiring and to address these challenges is an important task that administrative authorities have to take care of some of the institutions find it difficult to manage resources to acquire Information Technology (IT) infrastructure and other ICT tools to enable proper connectivity of biometric attendance system with biometric devices. Uninterrupted electricity supply at different educational institutions in isolated location within the state is an issue of concern. There is fewer recognition of the biometric attendance system by the stakeholders of an educational institution. Mudasir, (2017). The study further stated additional challenges which include the following:

i). ***Technology is not foolproof***—Interest probably will not start growing until biometrics systems overcome technical problems related to the reliability of the biometrics application.

ii). ***Cost of deployment***—deploying biometric readers on every door leading into a building or every PC on a network can be an expensive proposition. Hardware and software costs may not be the only consideration the organization must bear in mind the associated complexity involved in enrolling new users and administering usage training.

iii). ***Accuracy***—Verification and positive identification systems may allow unauthorized users to access facilities or resources as a result of incorrect matches. In a negative identification system, the result of a false match may be to deny access.

iv). ***Resistance to change***—as with many technologies, some users would rather not change the way they do things. Some users have the perception that using a username and password to log onto a system is faster than using a fingerprint scanner. This perception may arise from frustration related to the finger rejected rate, a performance measure that tracks the percentage of times an individual who should be positively accepted is rejected. (Michel & Richard, 2004).

2.5 BENEFITS OF USING BIOMETRICS FOR STUDENT ATTENDANCE MONITORING.

There are many benefits of integrating biometrics with Student Attendance Management Systems in educational institutions .Cruz, *et al*, (2015). Ezema, (2015), reveal that biometric attendance systems do not require complex technical knowledge so students can easily use the system with minimal training and can check-in or out through this system by simply placing their fingers on a biometric hardware device. Biometrics systems also provide a faster process to track student attendance as well as protect their identity and privacy.

Furthermore, Li. (2017), relates the main benefits of using biometrics for student attendance tracking to the accuracy it delivers. In educational institutions can centrally and precisely monitor student attendance to prevent proxy attendance and errors which are common problems when using traditional check-in and check-out methods. Li. (2017), also adds that biometric student attendance systems provide a convenient way to check-in and check-out into the system by simply scanning their fingerprints.

Similarly, Ikuomola, (2014), suggests that biometric student attendance management systems reduced time consuming in recording class attendance. These systems can track student attendance in mere seconds which saves lecturers a lot of time correcting attendance data errors from manual methods. Ikuomola, (2014), reveal that biometric systems not only reduce errors related to tracking attendance data but also speed up data verification which reduces administration time and increases productivity.

(Rukshana & Haleem, 2017), opined that in the process of enrollment, biometric systems convert scanned biometric templates to computer code and store the information in a database. This is later used for matching and verification, making it almost impossible to duplicate the original image for spoofing or fraud purposes. Biometric student attendance systems use strong encryption methods to protect a database from being compromised. This helps to increase security and protect student privacy.

2.6 RELATED WORKS

Most of the attendance systems reviewed uses paper based methods for taking and calculating attendance and this manual method requires paper sheets and a lot of stationery material. Previously, very few works have been done relating to the academic attendance monitoring problems. Biometrics has been used in biological studies including forestry for the collection, synthesis, analysis as well as management of quantitative data on biological communities such as forests. Biometrics in reference to biological sciences has been studied and applied for several generations and is somewhat simply viewed as "*biological statistics*" (Smart Cart Alliance Identity Council, 2007).

Development of Biometric techniques in students' attendance system

Oloyede *et al.* (2013), carried out extensive research on applicability of biometric technology to solve the problem of staff attendance. However, the researchers did not propose any software to address the difficulties of attendance.

According to, Shoewu *et al, (*2011), which proposed an Embedded Computer-Based Lecture Attendance Management System, the system is a single- chip computer based subsystems which is made up of electronic card and card reader. The electronic card includes the student identity, such as ID, name, matriculation number as well as five encrypted code. The student ID is

authenticated by matching the entrance code with the encrypted code on the card ‘swiped through the card reader. The student is granted or denial lecture attendance base on the comparison. The systems however provide a sampled, low cost embedded computer based system solution is the management. The drawback of the system is that it does not eliminate the risk of impersonation also the system is device-base where by the student have to carry their Radio Frequency Identification (RFID) card and also the Radio Frequency Identification (RFID) detectors need to be installed.

Furthermore, (Shehu & Dika, 2011), proposed the real time computer vision algorithms in automatic attendance management systems. The systems used computer vision, face recognition algorithms and both are integrated into the process of attendance management. The system eradicates classical student identification such as calling student names or checking respective identification card. However, the system lacks to identify each student present in class, this provide a lower recognition rate because facial images are subject to change between the time of enrollment as well as the time of verification. It also poses a bigger financial liability during installation and does not offer privacy protections.

Also, (Kadry & Smaili, 2010), proposed a wireless attendance management based on iris recognition using Daugman’s algorithm. The system uses an offline iris recognition management system which can finish all the process including; capturing the image of iris recognition, extracting minutiae, storing as well as matching.

Adeyemo *et al.* (2014), developed Attendance Management System using Biometrics System. The system took attendance of students via a fingerprint module and the records were stored in a database. There was no false identification of students as success rate was over 90%. However, the drawback there were no security methods adopted in the database to protect students’ data.

The study reported in, (Eze, Joe-Uzuegbu, Laz & Opara, 2013), shows the design of student/ staff biometric attendance system. The system monitors attendance through online Internet interfaces. It is a good work but the research fails to show how to allow students' guardians monitors their students on the website. (Shoewu & Idowu, 2012), proposed the use of fingerprint to take attendance in a class. The recommendation made was highly worthy in terms of

packaging for easy use and flexibility. However, nothing is reported on students' attendance monitoring.

According to, Geetha, (2010), an embedded use of fingerprint verification system which is widely explored in the areas of fingerprint was proposed. The researcher implemented this plan on the ZF Microsystems GX based on a single board computer with Cyrix Media GX based on processor and coprocessor with a bus speed of 180MHz. The board has only provision of Windows 3.11, 95/98, and Red Hat Linux 4.0 .Survey investigation and analysis of the current method of paper-based examination authorization in some higher institutions was also encounter of the impersonation of another user with genuine card. Due to the inadequacy of outdated methods of clearance, a more secured and accurate biometric based classical is needed to be formulated and executed.

In addition, Kokumo, (2010), proposed the use of electronic fingerprint scanner to solve student attendance monitoring difficulty in Bells University of Technology, Ota, Nigeria. The suggested solution ensures that only valid students are allowed access into lecture venues by capturing student fingerprint and comparing it with a database of stored fingerprint templates. The system ensured that only students registered for a particular course are allowed access into lecture venues. The drawback of system failed to cater for the recording of student attendance and thus could not provide a means of authenticating students for examination based on lecture attendance.

Elmehdi, (2008), developed a mobile system for maintaining time and attendance in schools. The author seeks to ensure effective monitoring of student attendance records by making such records available via the mobile phone. A system based on WAP (Wireless Access Protocol) was developed for monitoring student attendance. While the developed system enjoyed the portability of the mobile phone, and was noted to provide ease of navigation between modules and provision for feedback, thereby making the end-user great. The developed solution still depend on the lecturer to mark the attendance of each student from his/her mobile phone. Use of this system is therefore time consuming and stressful to the instructors.

(Patel & Priya, 2014), proposed the use of FRID for attendance taking and facial scanner used for verification. The Radio Frequency Identification (RFID) has long read range and facial recognition, also has long distance reading. The students are giving identity cards with RFID tag

mounted where they read the student data and pass it on to the server. Database logs are maintained that contains RFID tag id, and image captured by camera. If the student id from RFID tag and captured image matches presence is marked, otherwise it is mark absent. The disadvantage with this system is that it can be expensive since you need several devices i.e. an RFID reader, a camera and a bigger database also required to record the facial images which also lead to increase cost.

Somasundaram, *et al.* (2016), developed an android mobile base authentication system for students' attendance tracking using VB.NET and SQL server. It involves registration of administrators who register and update or delete user records, new users' registration login module and SMS module which is used to send an SMS to the parents notifying them of student presence or absence .The android module is used to receive text messages from students notifying about their leave.

For this system to function effectively, it requires additional resource from students, staff and parents where each must have an android phone to communicate student's attendance status to both parent and students.

2.7 GAPS THAT NEED TO BE FILLED.

In a research by Oloyede *et al.*, (2013), on the applicability of biometric technology, the researcher failed to develop any software which is inevitable for taking attendance.

Furthermore, Shoewu *et al.*(2011), proposed an embedded computer based lecture management system. The system does not eliminate the problem of impersonation and the student has to carry the radio frequency identification card with them which may be lost at any time.

Similarly, (Shehu & Daku, 2011), proposed a real time computer vision algorithms in automated attendance management system. The researcher fails to identify student present in the class, this provide a lower recognition, because facial images are subject to change between time of enrollment as well as time of the verification.

Adeyemo *et al.* (2014), Develop attendance management system using biometric system which captured attendance of student via fingerprint module and records were stored in a database. The system failed to provide security method accepted in the database to protect student's data.

In addition, Kokuma, (2010), proposed an electronic fingerprint scanner to solve student's attendance monitoring challenges of Bells University of Technology, Ota, Nigeria. The study did not deliver the students record attendance and also could not provide a means of authenticating students for examination based on lecture attendance.

(Patel & Priya, 2014), Reviewed RFID used for attendance taking and facial scanner used for verification. The reason was that radio frequency identification (RFID) has long read variety and facial recognition, also has long distance reading. The students are giving identity cards with RFID tag mounted where they read the student data and pass it on to the server. Database logs are maintained that contains RFID tag id, and image captured by camera. The disadvantage with this system is that it can be expensive since you need several devices i.e. an RFID reader, a camera and database is required to keep the facial images which in variable to increase cost.

Somasundaram, *et al.* (2016). Developed an android mobile base authentication system student attendance tracking using VB.NET and SQL server. It involves registration of administrators who register and update or delete user records, new user's registration login module and SMS module which is used to send an SMS to the parents notifying them of student presence or absence. The researcher is unsuccessful for additional resource from students, staff and parents where each must have an android phone to communicate student's attendance status to both parent and students.

2.8 THEORETICAL FRAMEWORK OF THE MODEL

The Biometric Examination Screening and Attendance Monitoring System (BESAMS), developed by .Rufai *et al.,* (2015), underpinned some of the basic feature of biometric system. The process in line with the general features and procedures of a biometric system has two parts which are:

Enrollment:

i). A student registers at the beginning of a session by filling an online student and course registration form.

ii). The biometric identity of the student(e.g. fingerprint) is also captured

iii). The data is preserved in a database

iv). The data is updated on regular interval (e.g. at the beginning of every semester)

Verification:

Verification takes place before the commencement of the examination. It is repeated two or three times during and at the end of the examination

i. The student append his fingerprint on the biometric device for data capture
ii. The captured data is compared with the template in the database for a match. The existence of match confirms the studentship of the candidate
iii. The system checks for the registration and payment status of the student. If this is confirmed the student access to examination room is granted.
iv. At the end of the exam process (ii) is repeated which serve as one sign out
v. The matric no, name, time of operation and class of the student is extracted as attendance

The formal model of the Biometric Examination Screening and Attendance Monitoring System as a Finite State Machine BESAMS is defined as a five tupple relationship

$BESAMS \mid\mid (S, \Sigma, s, F, \delta)$ (1)

Where

S is a set of valid states that forms the domain of the BESAMS, S = {s0, s1…, s8} where the states are:

s0 –System,
s1 – Welcome,
s2 – Biometric ID Capture,
s3 - Register,
s4 – Identity Verification,
s5 – Registration and Payment Status checked
s6 - Attendance is taken
s7 - Entry is granted,
s8 – Entry denied
s9 – Exit

Σ is a set of events that the (ATM) automated teller machine may accept and process, Σ = {e0, e1… e12} where:

e0 - Start,

e1- Append Fingerprint,

e2 – Supply Registration and Payment Data,

e3 – Check for Fingerprint Match,

e4 – Match Found,

e5 – Match not found,

e6 –Status confirmed,

e7 – status not confirmed,

e8 – Sit allocated,

S is the start state of the ATM, s = s1 (Welcome);

F is a set of ending states, F = {s1};

δ is the transition function of the ATM that determines the next state of the FSM, si+1, on the basis of the current state si and a specific incoming event ei, i.e., si+1 = δ (si, ei), where δ = f: S × Σ → S (2

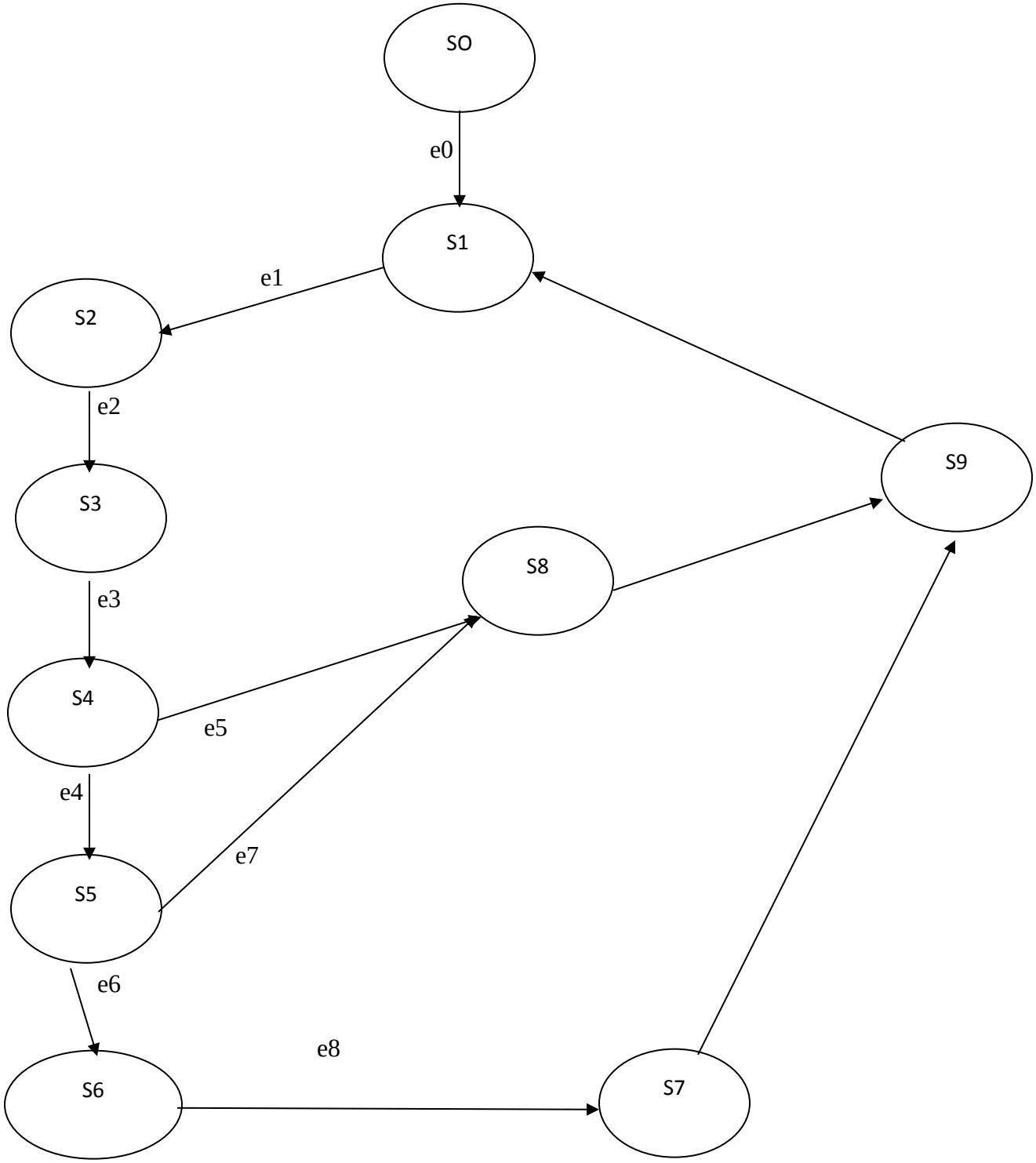


Figure 2.5: The Abstract Transition Model of the BESAMS Behaviours.

Source: Adapted from .Rufai *et al*, (2015)

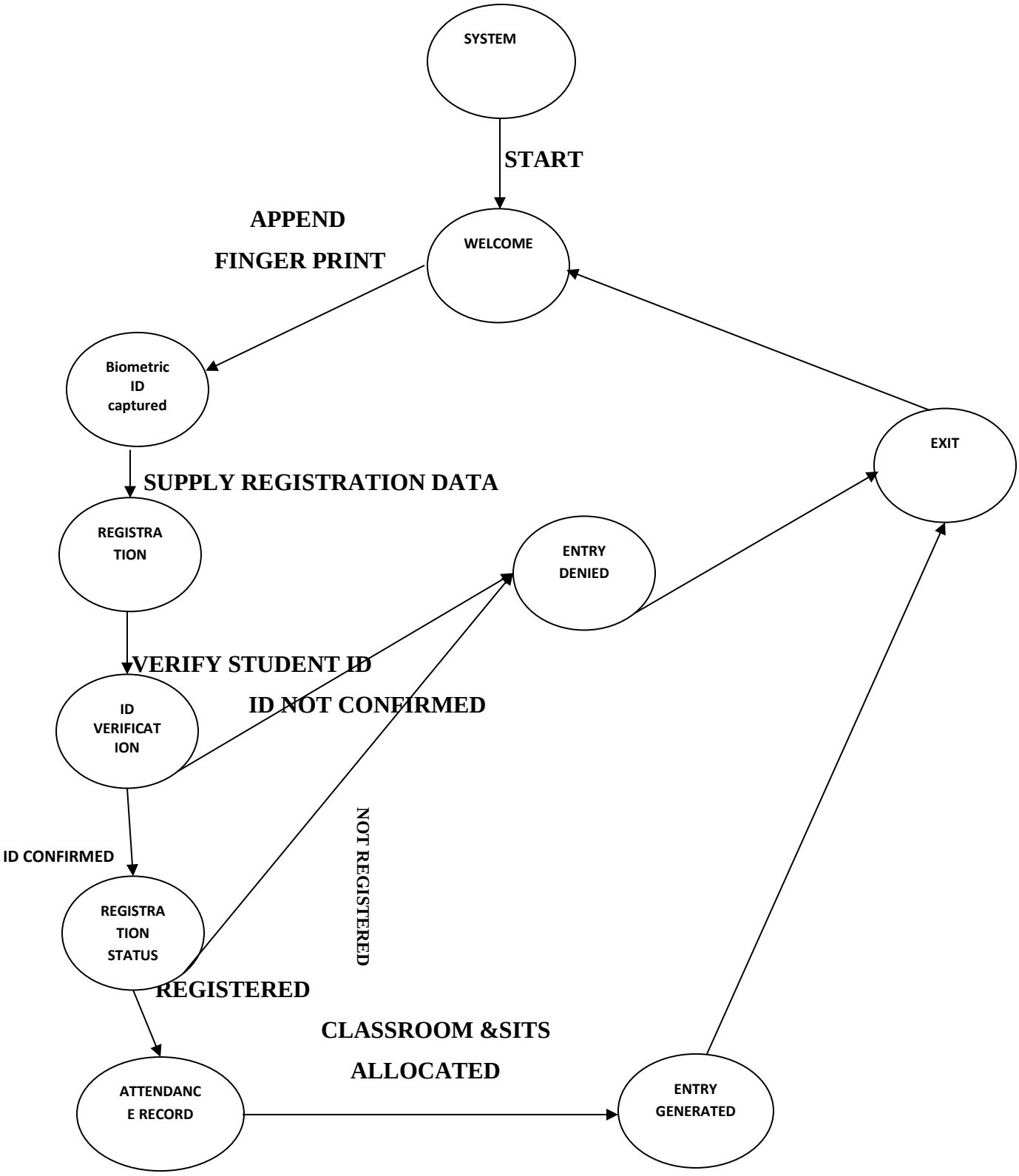


Figure 2.6: The Transition Model of the BESAMS Behaviours

Source: Adapted from .Rufai *et al.* (2015).

2.9 THE USE OF SYSTEM USABILITY SCALE.

In 1996, the System Usability Scale (SUS) was introduced by John Brooke with the object of developing a quick, reliable and inexpensive method for evaluating the usability of technologies. John, (1996). The System Usability Scale (SUS) is a survey that consists of only 10 statements (table), and participants strongly disagree or strongly agree with the statement based on 5-point Likerts scale. A System Usability Scale can be within range of 0 and 100 for each participant. The score indicates the usability level of the technology from the respondents without providing any explanation for the respondent's perception. Kastsanos *et al.*(2012).

Similarly, many system were developed for evaluating the usability systems, SUS has some distinguishing features. Bonger *et al.* (2008). The SUS is simple and inexpensive compared to many other methods of system usability evaluation. Moreover, the questionnaire can be completed quickly because it is short and contains only 10 important questions. The SUS is between 0 and 100, which makes it understandable by experts and non-experts alike.

Also, Bargor *et al.* (2008). Created a scale for an acceptable SUS score. A system usability scale SUS score between 85 and 100 indicate that the system is highly usable. The usability of the system is excellent when the SUS score is between 70 to about 85, but SUS score from 50 to about 70, is acceptable.

2.10 REVIEW OF THE EXISTING METHODS OF STUDENT ATTENDANCE REGISTRATION.

The conventional methods of student attendance registration in most higher learning institutions are manual where attendance is written by hand in register, Saheed *et al.*(2016). Some of the challenges with the method were when it comes to the retrieval of the data. Students put their information that is Name and registration number on a piece of paper or the lecturer provides a list of an enrolled student and their registration details to the students and the students have to sign against their Names. They also further mention more other challenges which are the followings:

> Manual work involved, transfer of the registered information to other systems for analysis is very tedious and time consuming. Furthermore, the collected data is not used

to help the improved courses and classrooms. While using the current system it is hard to tell at what point students come in i.e. whether early during the lesson or later just sign in.

The process is error prone since students have found to sign for their colleagues, therefore accuracy was lost.

Since the attendance is made on paper sheets the same is likely to get lost and students are requested to sign in again. This will allow the students who had not attended the lesson earlier to sign in as well.

CHAPTER THREE

METHODOLOGY

3.0 INTRODUCTION

This Chapter describes the research design, population of the study, sample size, sampling procedure, research instrument, data collection procedures, data analysis, system modeling approaches, ethical consideration and limitation of the study.

3.1 RESEARCH DESIGN

Research design is the plan on how the researcher goes about finding accurate answers. The research design plan contain clear objectives, derived from research objective(s), specify the sources from which data are to be collected, and consider the constraints that may arise, such as access to data, time, location and money as well as discussing ethical issues (Saunders & Thornhill, 2007).Thus, this study employed the Experimental Research Design which involve the development of Biometric Finger print for students attendance which was finally tested and found. In addition the biometric fingerprint for students' attendance was configuring using hardware and software component. The software components include Asp.Net, C# programming language, My-Sql server 2008, Microsoft Visual studio 2013 while Hardware include fingerprint scanner, Microcontroller, laptop, Lcd and Buzzer.

The students and staff fingerprints were captured and stored in the database. During attendance taking, the system prompts the students to place his/her fingerprint on the sensor which is then captured and compared with the one stored in the database. If there is a match, the attendance of that student is marked (valid) and the whole process is viewed through the Liquid Crystal Display (LCD). Besides, if the fingerprint does not match, the fingerprint would be rejected and mark (invalid) would be displayed on the LCD. The system was evaluated using the System Usability Scale (SUS) to measure its effectiveness and efficiency.

THE HARDWARE

Hardware components of the developed device consisted of fingerprint scanner, Arduino, laptop, LCD and Buzzer.

The Arduino

Arduino is a microcontroller board based on the ATmega328. It has 14 digital input/output pins (of which 6 can be used as PWM outputs),6 analog inputs, a 16MHZ crystal oscillator, a USB connection, a power card, an ICSP header, and a reset button. It contains all things needed to support the microcontroller. It can be simply connected to a computer with a USB cable as well as a power cable an AC-to-DC adapter or battery to get started. The Arduino differs from all proceeding boards in that it does not use the FTDI USB-to-serial driver chip. Instead, it features the Atmega8U2 programmed as a USB-to-serial convertor.

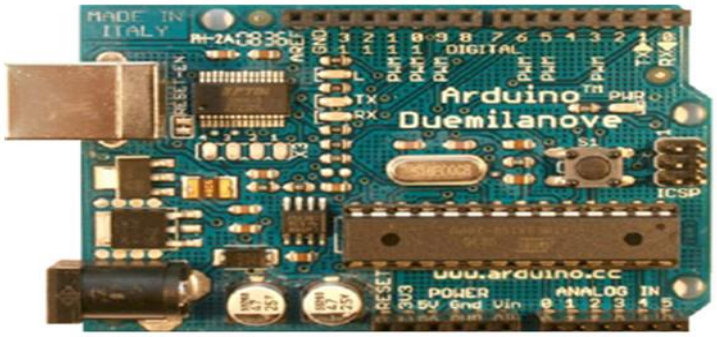


Figure 3.1 Arduino microcontroller

THE SCANNER

This is a fingerprint sensor scanner with a ticket time limit (TTL) UART interface for direct connection to microcontroller UART trough MAX232/USB-Serial adapted. This can store the fingerprint data in the module and can be configured in 1:1 or 1: N mode for identifying the person. The fingerprint scanner can directly interface with 3v or 5v Microcontroller. A level convert (like MAX 232) is required for interfacing with PC serial port.

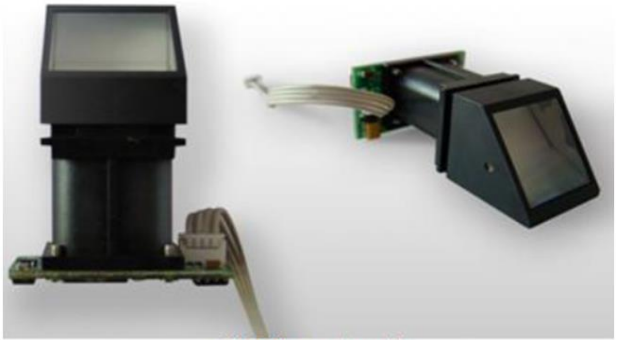


Figure 3.2 the scanner sensor

Circuit Diagram and Description for Fingerprint Attendance System Project

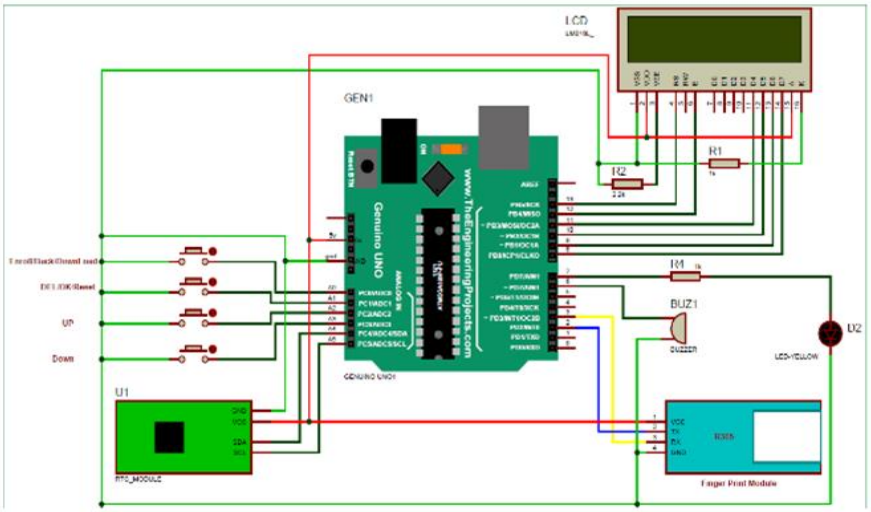


Figure 3.3 Circuit board diagrams

As shown in the circuit diagram above, wire directly connected to pin A0(ENROL), A1(DEL), A2(UP), A3(DOWN) of Arduino with respect to the ground and Yellow LED is connected at Digital pin D7 of Arduino with respect to ground through a 1k resistor. Fingerprint module's Rx and Tx directly connected at Serial pin D2 and D3 (Software Serial) of Arduino. 5v supply is used for powering finger print module taken from Arduino board. A buzzer is also connected at pin A5. A 16x2 LCD is configured in 4-bit mode and its RS, EN, D4, D5, D6, and D7 are directly connected at Digital pin D13, D12, D11, D10, D9, and D8 of Arduino.

3.3 DATA COLLECTION

The major purpose of collecting data in this study was to test the application software developed to work with the biometric device; and to know the challenges being faced with the existing system. Therefore, huge data was not required. Apart from the interview conducted, the data necessary for use in this study were collected at two different stages. First, data capturing which involves the finger print images collected from both staff and students (from 52 students and 5 staff members). Documents in form of forms were used to collect bio data information. Secondly, at the time to determine the usability of the system developed, questionnaire was designed and distributed to some stake holders and their responses were analyzed using SUS strategies.

3.4 RESEARCH INSTRUMENT

Data collection instruments in this study were Structured Interview Guide using Key Informant Interview (KII) and Closed ended questionnaire. The interview guide was used to gather information for the analysis of the existing system used in registering students' attendance in the polytechnic while the questionnaire was used to collect information for the evaluation of the developed system using the System Usability Scale (SUS). The questionnaire had the Likert scale, ranging from 1=Strongly Disagree and 5= Strongly Agree.

3.5 TARGET POPULATION

The study targeted a population 60 students of the Department of Computer Science of the Kano state Polytechnic.

3.6 SAMPLE SIZE

The sample size was determined using Krejcie and Morgan (1970) sample table. For a population of 70 the computed sample size is 60. Hence the sample size for this study was 60 students' respondents.

3.7 SAMPLING TECHNIQUE

The amount of data needed to be collected by acquiring data from only a subgroup rather than an entire population is made possible by the use of sampling techniques that provides a range of methods to achieve this (Saunders, Lewis & Thornhill, 2007). Thus, in order to obtain the sample size of the study, the purposive sampling techniques were employed.

3.8 DATA ANALYSIS TECHNIQUE

System Usability Scale was the data analysis technique used to analyse data obtained from the quantitative while Content Analysis method was used to analyse qualitative data obtained from the interviews conducted.

3.9 DATA COLLECTION PROCEDURE

All data collection procedures were self-administered while the construction of the model was self-done. Construction of the model, testing and evaluation as well as all data collection procedure lasted 7 months from September, 2018 – March, 2019.

3.10 SYSTEM MODELLING

The following modeling approaches were used in modeling both the system data and information.

i). Block Diagram of the Proposed System

ii). Sequence Diagram for Administration

iii). Sequence Diagram for Student

iv). Class Diagram

The designed modeling approaches were used to interpret the requirements needed then the anticipated system functionalities were expected. It also guided the coding of the developed system. (Howard & Bookboon.com, 2015), observed that modeling approach is needed when designing a database system so that information gatherings can check that the design will satisfy the requirements.

3.11 ETHICAL CONSIDERATIONS

In conformance with the ethical standards, the letter of introduction collected from the university was presented at every place necessary while respondents' consent was also sought and the research's motive was fully explained. In order to avoid plagiarism, all quoted works were properly cited and referenced. To top it all, all data collected were used only for the purpose of the study.

CHAPTER FOUR

ANALYSIS, DESIGN AND IMPLEMENTATION

4.0 INTRODUCTION

In this chapter, present the analysis, design and implementation of biometric fingerprint for students' attendance are presented.

4.1 DATA PRESENTATION AND ANALYSIS FROM THE RESPONSES ON THE SPECIFIC OBJECTIVES.

4.1.1 Analysis of the Existing System of Identifying Students at Kano State Polytechnic, Nigeria.

To find answers to the first objective of the study which aimed at analyzing the existing system of identifying students at Kano State polytechnic, Nigeria, two key interview informants participated in the interview. Their responses are discussed as follows:

The findings of both the key interview informants revealed that, the current student attendance system in use is the manual system (students sign in attendance).

The whole student attendance registration, storage and retrieval are done manual by (students sign in attendance) (Interviewee1).

The whole of the process of current student registration is purely done on paper recording, storing which entails retrieval in Kano State Polytechnic (Interviewee2).

Based on the challenges encountered in the current attendance records, the finding shows that, the challenges encountered include the following: time consuming, prone to error, easily get lost as there will be only one saved copy of it. The findings further identified additional challenges to include: impersonation among student by signing for others as well as misplacement of student attendance by lecturer and student representatives.

The challenges encountered with the current attendance system are::Attendance recording is prone to error when , easier to misplace or lost as there will be only one copy, time consuming as well as bias among lecturer and student representative (Interviewee1).

Paper-based Record Keeping System is cheaper and the process is simplified, but challenges associated with it outweigh its benefits when compared with the biometric fingerprint. For instance issue of misplacement of student's records resulting from putting the folder in wrong place is extremely challenging and its retrieval takes a lot of time. In such circumstances, security of the stored folders cannot be guaranteed. Besides, there are also issues with regards to student's privacy which do arise as a result of the manual mode of transmitting students' records (Interviewee2).

The finding also revealed that, the student attendance generate reports which include: student course enrollment, examination attendance as well as class attendance.

The report generated by student attendance in Kano State Polytechnic which include the following: student examination attendance, student course enrollment, continuous assessment and student eligibility for examination (75% attendance) (Interviewee1.)

The types of report generated by student attendance in Kano State Polytechnic comprises of test attendance, exams attendance, students enrollment, active and inactive students, frequency of students and lecturers attendance (Interviewee2).

Based on the need to improve the current student attendance system , the finding reveal that there is need to improve the current student attendance thereby eliminating time consuming, dishonesty among student signing the attendance for others as well as misplacement of attendance by lecturer and student representative.

There is need to improve these, the current student attendance system so that it can eliminate the problem of time consuming, dishonesty among student signing for others, Misplacement of student attendance by lecturer and student representative (Interviewee1).

Yes it is importance to improve the current attendance system so as to eradicate the dishonesty among student and misplacement of attendance by student representation as well as bias among lecturer and improve the current system of the Polytechnic (Interviewwe2).

The respondents also revealed the following benefits of biometric fingerprint records system and implementation which include: save time for student attendance, security purpose both for the

student and lecturer within or outside the school, digital records is maintained for future use and provide effective and efficient report generation.

The major benefit of biometric fingerprint records system and implementation include: accurate student attendance, save time for student attendance and it provide effective and efficient report generation (Interviewee1).
The introduction of biometric fingerprint records will increase the overall satisfaction of student and help the school authority to take good decision within a specific time (Interviewee2).

4.2 DESIGN AND DEVELOPMENT OF A BIOMETRIC SYSTEM FOR IMMEDIATE IDENTIFICATION OF THE STUDENT FINGER PRINT.

4.2.1 System modeling using UML

According to, Nithya Venkatachalma *et al. (*2016), a detailed design is a blue print of a computer system solution to a given problem having the same components and inter-relationships among the same components the original problem. At this stage, database, inputs, forms, outputs, processing, specifications and codes are outline in detailed. Furthermore, it is during the design stage that the hardware and software as well as the programming language on which the new system shall run on are selected.

4.2.2 Software

The list of software development tools which will be used in designing this project are.

WAMP Server version 3.0.6 an integrated development tool was selected for the implementation of the system.

- Asp.Net
- C# programmed language
- SQL Server 2008
- Microsoft Visual Studio 2013
- CSS
- PHP
- HTML

At the front end, HTML and CSS are the most important technologies used in implementing the system for developing web pages while MySQL was used for implementing the system at the back end for the design of various tables into MySQL WAMP Server.

4.2.3 Hardware

Set of hardware, which are needed in designing biometric fingerprint attendance system are:

- Fingerprint scanner
- Microcontroller
- laptop
- LCD
- Buzzer

4.2.4 Block Diagram of the System

According to Vikas *et al.*(2017). Block diagram of system represents the attendance system which can be implemented anywhere in the institution, colleges or office. Also it can be used for security purpose. For the implementation of fingerprint based attendance system Microcontroller ATMEGA32A is used. It has several advantages over other microcontroller such as, low power consumption, high speed of operation, low price, and wide range of peripherals. The microcontroller is interfaced with fingerprint module. Fingerprint module scan users fingerprint and send data to microcontroller for further process. A person put his/her finger on fingerprint scanner if it matches with previous database the LCD shows person “verified” otherwise show “not verified”.

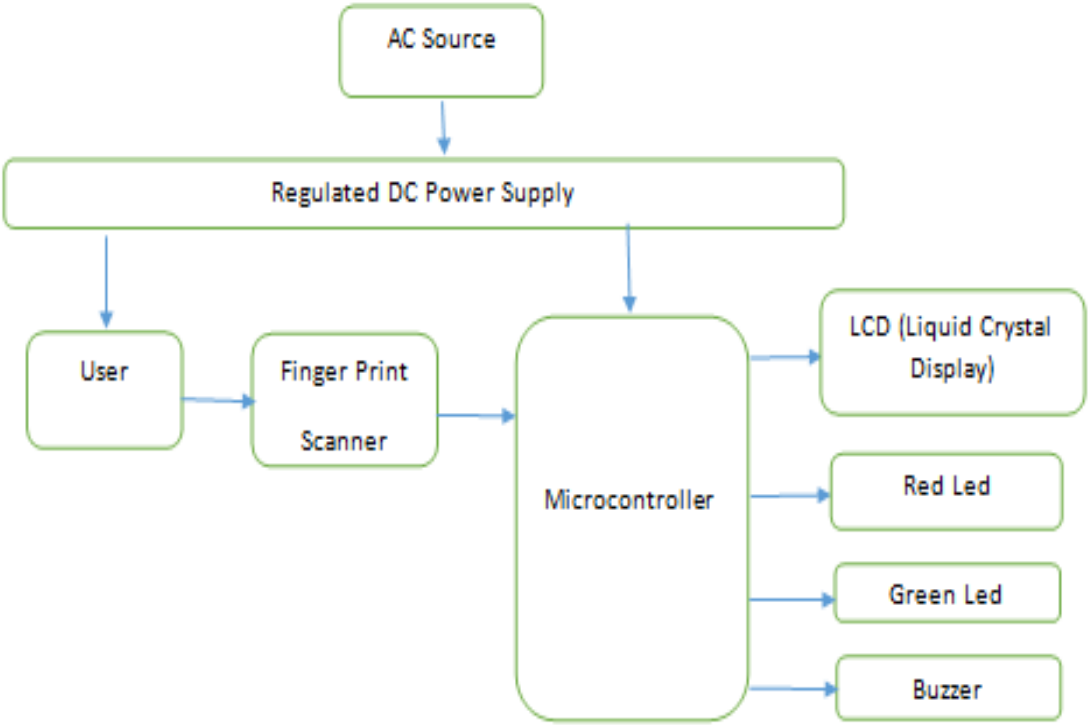


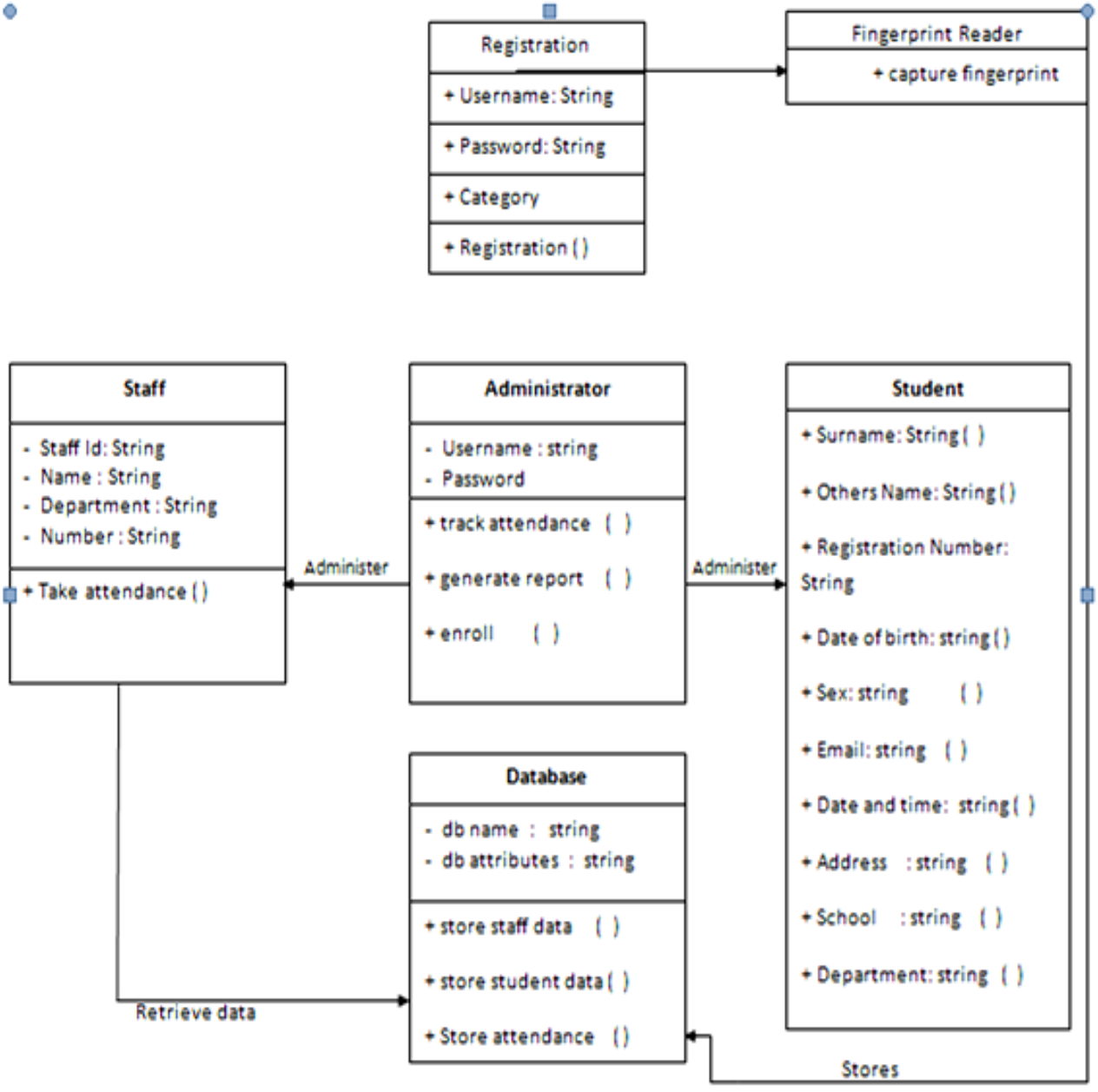
Figure 4.1: Diagram of the biometric finger print of student attendance

4.2.5 Diagram

According to. Hoffer, *et al,* (2002). Class diagrams are the most popular UML diagrams used by the object oriented community. It describes the objects in a system and their relationships. Class diagram consists of attributes and functions. A single class diagram describes a specific aspect of the system and the collection of class diagrams represents the whole system. Basically the class diagram represents the fixed view of a system.

Similarly. Adewole, *et al,* (2014). Moreover, Class diagram was not only used for visualizing describing and documenting different aspects of a system but also for constructing executable code of the software application. Other uses include describe the attributes, operations and also the constraints imposed on the system. The classes diagrams are widely employed in the software modeling of object oriented systems because they are the only UML diagrams which can be mapped directly with object oriented languages .The class diagram shows a collection of

classes, interfaces, associations, collaborations and constraints. That is referred to as a structural diagram.



4.2.6 Sequence Diagram for Administrator

Sequence diagrams describe intersections among classes in terms of exchanging messages actively. They are also called event diagrams, a sequence diagram is a good way to pictured and

authenticate various runtime scenarios. These can help to predict how a system will behave and to determine tasks a class may need to complete in process of modeling a new system.

The sequence diagram is a unified modeling language (UML) diagram that depicts the behaviuoral features of a system in conjunction with the class diagram or use case. (Dobing & Parsons, 2006). It shows that the sequence diagram is more commonly used in practice than teamwork defect diagram.

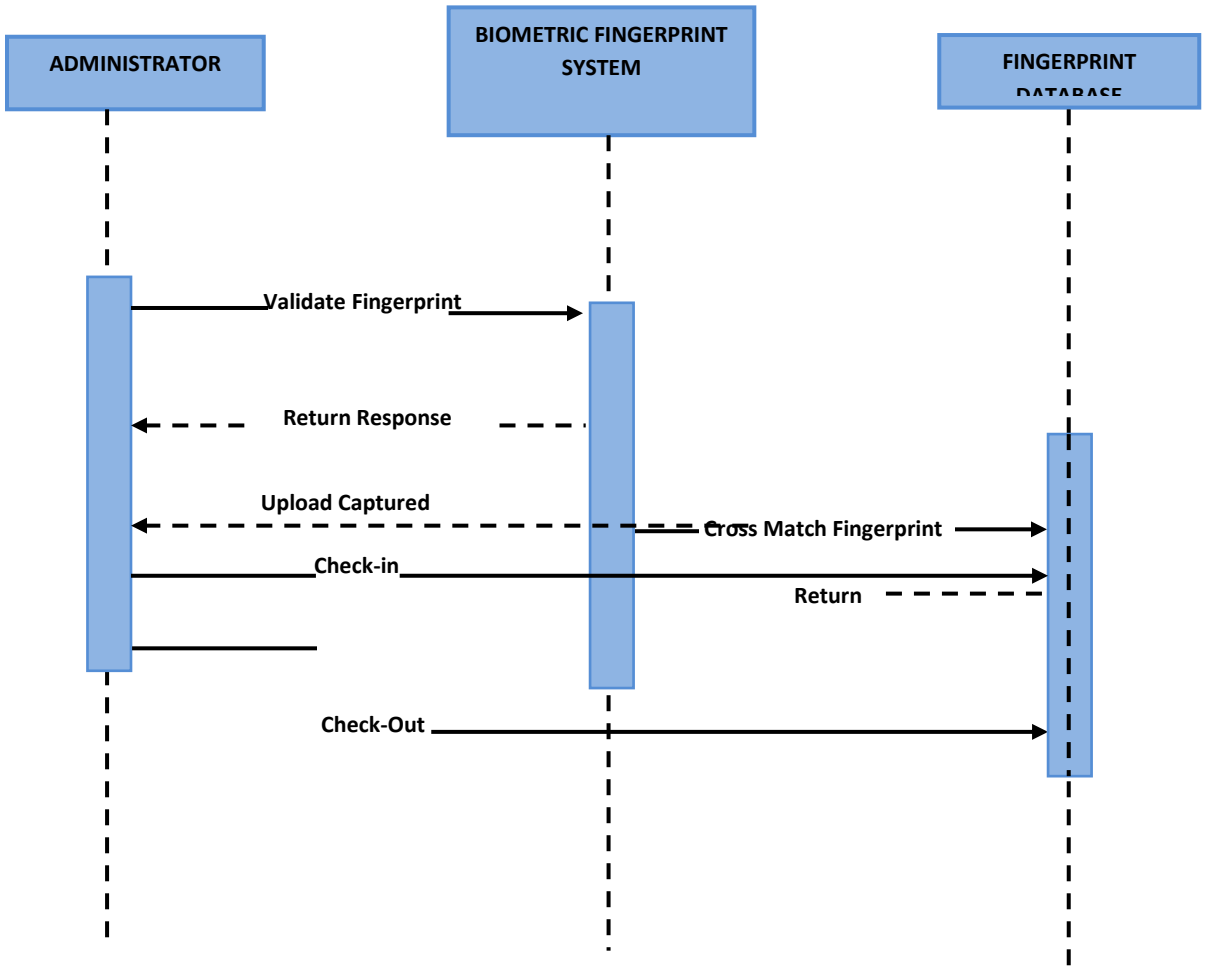


Figure 4.3: Fingerprint procedures by the Administrator.

4.2.7 Sequence Diagram for Student

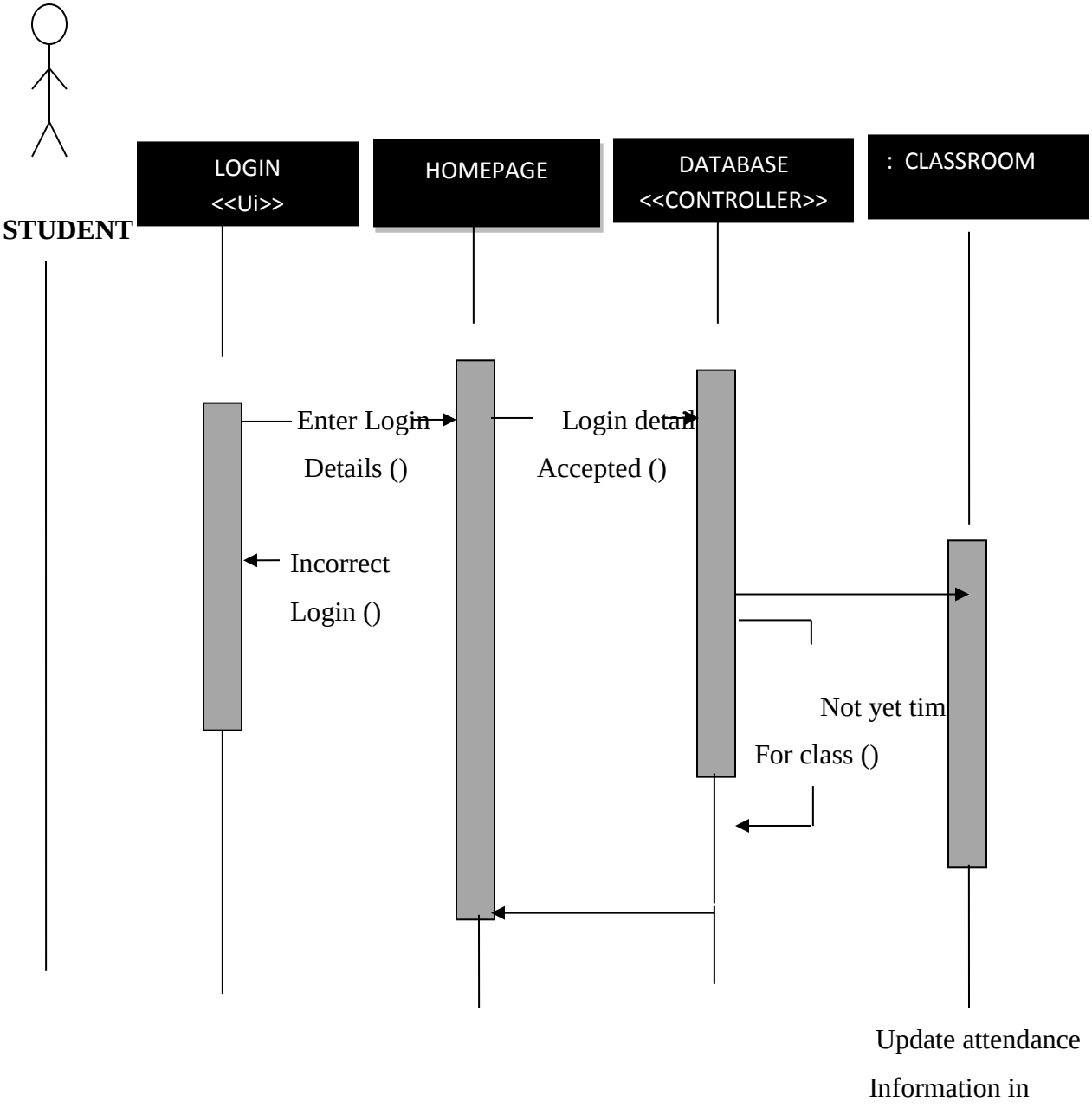


Figure 4.4: Sequence Diagram showing Logging Procedures for Students.

4.3 IMPLEMENTATION OF DATABASE STRUCTURE

4.3.1 Database Structure

Table 4.1: Admin login

DESKTOP-F8C5O7H...dbo.admin_login

Column Name	Data Type	Allow Nulls
Id	int	☐
username	varchar(50)	☑
pass	varchar(50)	☑
image	image	☑
		☐

Table 4.1 administrator table in SQL.

They are four attribute Namely, ID, username, password and image, the data type is written against attribute, while the attribute that does not allowed empty value is indicated (as uncheck box only two).

Table 4.2: Structure of Lecturer Login Information.

DESKTOP-F8C5O7H...o.lecturer_login | DESKTOP-F8C5O7H

Column Name	Data Type	Allow Nulls
Id	int	☐
l_surname	varchar(50)	☑
l_othername	varchar(50)	☑
l_phone	varchar(50)	☑
l_image	varchar(50)	☑
		☐

Lecturer Table: Maintains five attribute Namely, ID, surname, other name, phone no. and image**,** the data type is written against attribute, while the attribute that does not allowed empty value is indicated (as uncheck box only two).

Table 4.3: Structure of Student Login Information.

DESKTOP-F8C5O7H...o.student_login | DESKTOP-F8C5O7H

Column Name	Data Type	Allow Nulls
Id	int	☐
s_name	varchar(50)	☑
s_regno	varchar(50)	☑
s_date	varchar(50)	☑
image	image	☑
		☐

Table Stores five attribute consists of ID, first name, reg, no. date and time. The data type is written against attribute, while the attribute that does not allow empty value is indicated (as uncheck box only two).

Table 4.4: Structure for Bio data of Lecturer and Records Storage.

DESKTOP-F8C5O7H\...egister_lecturer | DESKTOP-F8C5O7

Column Name	Data Type	Allow Nulls
Id	int	☐
l_startno	varchar(50)	☑
l_surname	varchar(50)	☑
l_othername	varchar(50)	☑
l_sex	varchar(50)	☑
l_dob	varchar(50)	☑
l_address	varchar(500)	☑
l_phone	varchar(50)	☑
l_email	varchar(500)	☑
l_faculty	varchar(50)	☑
l_department	varchar(50)	☑
l_image	image	☑
f_image	image	☑
		☐

These table stores twelve attribute Namely, ID, staff no, surname, other name address, dob.etc. The data type is written against attribute, while the attribute that does not allow empty value is indicated (as uncheck box only two).

Table 4.5: Structure of Bio data of Student and Record Storage

DESKTOP-F8C5O7H...register_student | DESKTOP-F8C5(

Column Name	Data Type	Allow Nulls
Id	int	☐
s_regno	varchar(50)	☑
s_surname	varchar(50)	☑
s_othername	varchar(50)	☑
s_sex	varchar(50)	☑
s_dob	varchar(50)	☑
s_adress	varchar(500)	☑
s_phone	varchar(50)	☑
s_email	varchar(500)	☑
s_faculty	varchar(50)	☑
s_department	varchar(50)	☑
s_year	varchar(50)	☑
s_image	image	☑
f_image	image	☑
s_part	varchar(50)	☑

These tables contain fourteen attribute namely. ID, reg.no. surname, other name, sex, dob, address, phone,email,facaulty,etc The data type is written against attribute, while the attribute that does not allow empty value is indicated (as uncheck box only one).

Table 4.6: Structure of Course Registration

DESKTOP-F8C5O7H\...nt - dbo.courses | DESKTOP-F8C5O7

Column Name	Data Type	Allow Nulls
Id	int	☐
courses_name	varchar(50)	☑
course_code	varchar(50)	☑
course_room	varchar(50)	☑
year_of_course	varchar(50)	☑
		☐

They are five attribute namely, tables contain eleven attribute namely. ID, course name, course code, course room, year of course. The data type is written against attribute, while the attribute that does not allow empty value is indicated (as uncheck box only two).

Table 4.7: Structure of Student Record

DESKTOP-F8C5O7H...o.student_record | DESKTOP-F8C5O7

Column Name	Data Type	Allow Nulls
Id	int	☐
s_name	varchar(50)	☑
s_regno	varchar(50)	☑
s_datetime	varchar(50)	☑
s_image	image	☑
s_coursecode	varchar(50)	☑
s_course	varchar(50)	☑
		☐

They are seven attribute namely, tables contain eleven attribute namely. ID, name, reg, no, date and time, image, course code, and course. The data type is written against attribute, while the attribute that does not allow empty value is indicated (as uncheck box only two).

4.4 FINGER PRINT CAPTURING PROCEDURE OF SELECTED REGISTERED STUDENTS.

The fingerprints of each student and members of staff were captured during the registration exercise using a fingerprint reader in the form of digital personal fingerprint scanner. The required unique features were extracted and stored in the database as a template for the subject along with the ID. Those features formed a template that is used to determine the identity of the student as well as for formulating process of authentication. The registration/authentication process is carried out by an administrator (researcher). Students' data are collected and stored during the registration process where students' names, sex, date of birth, address, school, department, registration number, phone number and e-mails are provided same data was also collected and registered for the members of staff except that the staff provided their staff Identity numbers instead of registration numbers. After the registration process, verification process was also conducted with the sole purpose of comparing the students' finger prints with the data already stored in the data base during the registration exercise. For the verification exercise, the extracted features for each and every student are compared with the stored features in the database to determine a match.

In situations where a student failed to be verified, it was the responsibility of the administrator to confirm whether the student was actually registered in the first place such students were expected to clear with the administrator in case of any inaccuracies or abnormalities in the registration process. The lecturers were registered on the device so that records of attendance by lecturers teaching courses could be taken by the device. This could curtail cases where lecturers fill in fake information to show that they attend lectures promptly while they do not. Biometric fingerprint for student attendance system is recorded digitally by scanning the fingerprint. The process of capturing student/staff fingerprints include: enrollment of students, verification of students as well as deleting of students from the database. The pseudo code below shows the detailed in capturing students finger prints.

PSEUDO CODE FOR STUDENTS' ENROLMENT:

Step 1: fingerprint scanner from serial port.

Step 2: Get sensor information

Step 3: Start service to read a finger

Step 4: Wait that finger is read

Step 5: Checks if finger is not enrolled go to 8

Step 6: Display ID number

Step 7: Go to step 16

Step 8: Convert read image to characteristics and store it in the database….1

Step 9: Wait that finger is read again

Step 10: Compare the fingerprint with the enrolled fingerprint store in the database

Step 11: If the finger is match it will show successful

Step 12: Generate a template and store it to fingerprint scanner device.

Step 13: Get ID and save in the database.

Step 14: Show successful

Step 15: Print success message

Step 16: Stop

PSEUDO CODE FOR STUDENTS' VERIFICATION:

Step 1: Initialize fingerprint scanner from serial port

Step 2: Start service to read the fingerprint

Step 3: Wait that finger is read

Step 4: If finger match go to step 7

Step 5: show “finger print not fund”

Step 6: Go to step 3

Step 7: Match position with database and get id

Step 8: Show successful or unsuccessful

Step 9: Print report of student attendance

Step 10: Stop

PSEUDO CODE TO DELETE STUDENTS’ RECORD FROM THE SYSTEM:

Step 1: Get student id

Step 2: Check student in database

Step 3: If student found go to step 6

Step 4: Print “student not found”

Step 5: got to step 12

Step 6: Initialize Fingerprint Scanner from Serial Port

Step 7: Get sensor information

Step 8: Start service to read a finger

Step 9: Wait that templates are read

Step 10: Delete from database

Step 11: Delete from device

Step 12: Stop

Fingerprint sensor module captures finger print images and then converts it into the equivalent template and saves them into its memory as per selected ID by Arduino. All the processes like taking images of fingerprints, changing it into templates and storing as ID are ordered by Arduino. Figure 4.12 below shows how the fingerprint is captured.

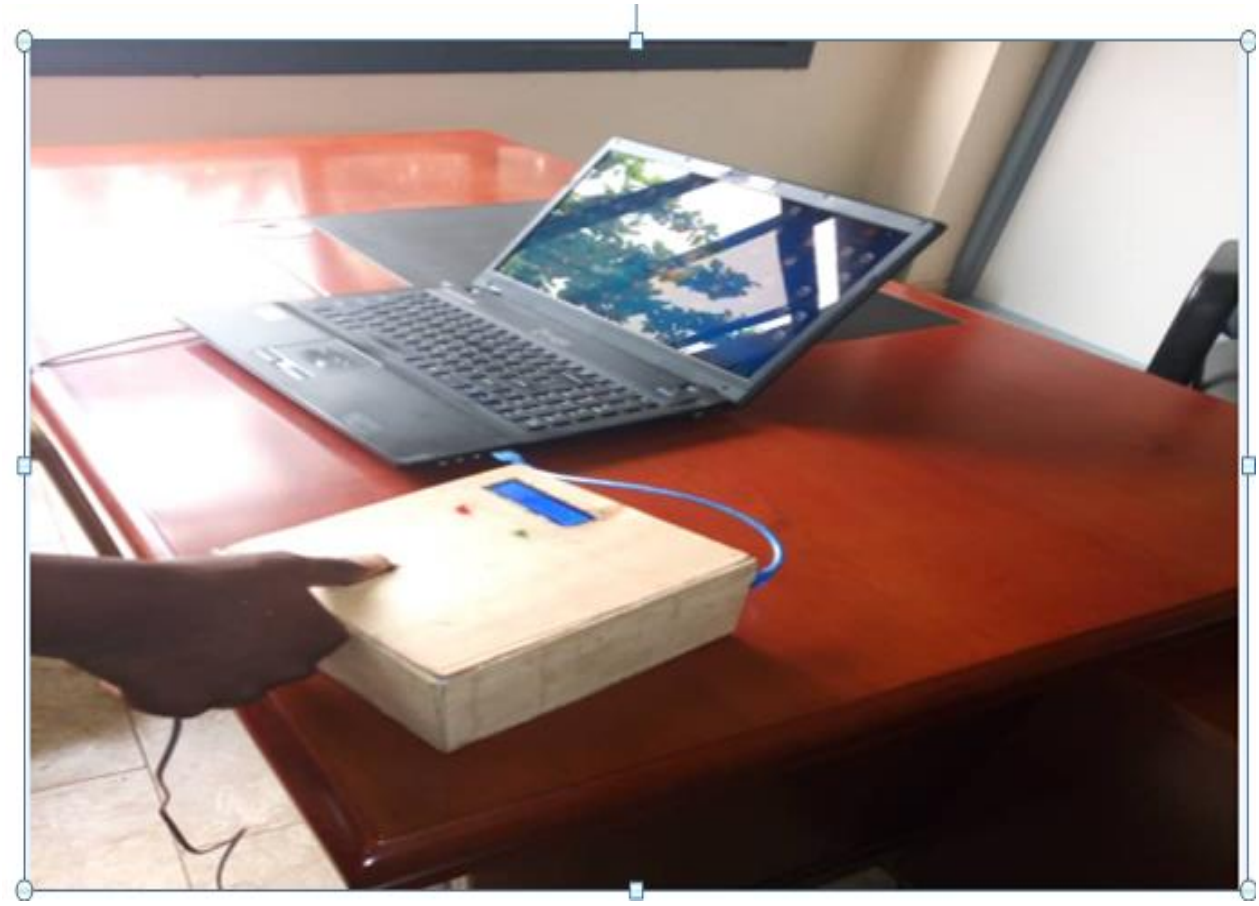


Figure 4.5: Biometric Device capturing Student Fingerprint

CHAPTER FIVE

RESULT, DISCUSSION, EVALUATION, AND TESTING

This developed system will reduce the manual work and avoid redundant data, efficient reports which cannot be generated and are difficult to maintain in manual attendance registration are achievable with the automated approved however, and with this system data can be safeguarded and can be easily retrieved whenever needed.

5.1 The System Main Menu implementation.

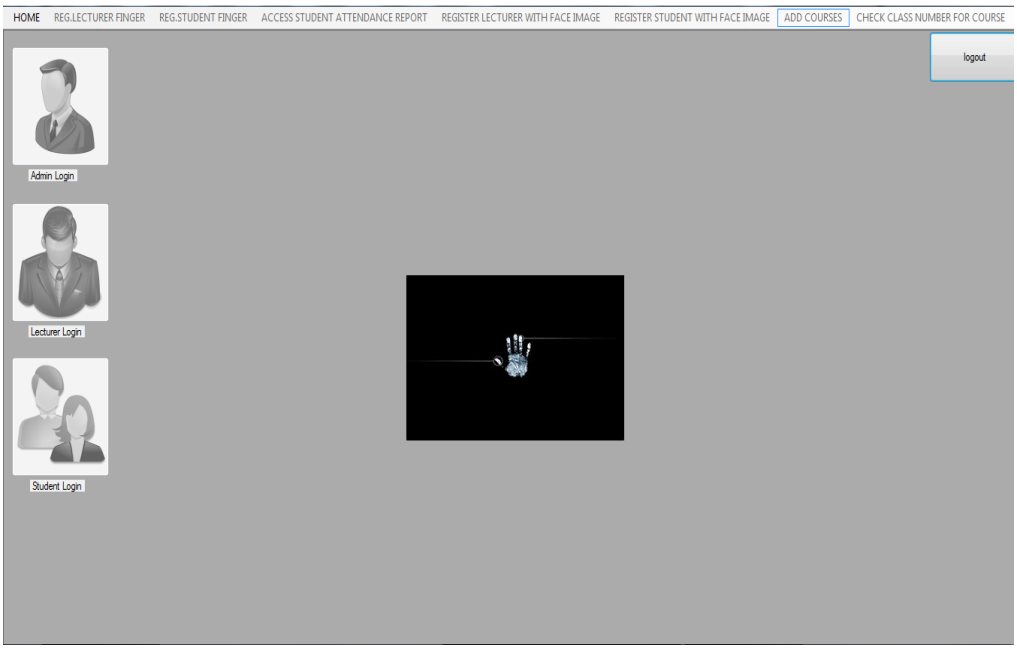


Figure 5.1: Main Menu

Figure 5.1 shows the administrator login phase where students and lecturers are registered. Here the administrator can log in by clicking on the home login and then proceeds to other locations. So also lecturers and students can proceed to other actions by clicking on the various options on the main menu.

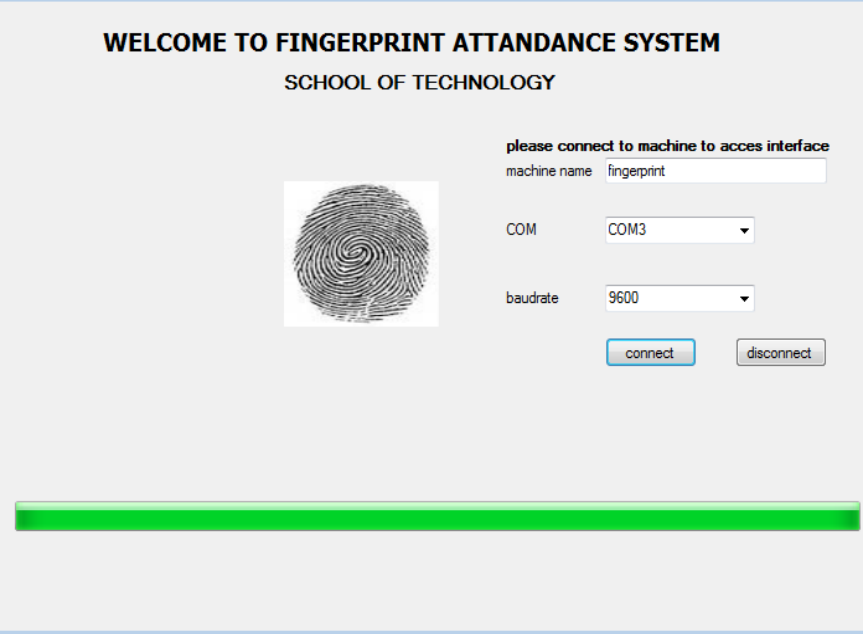


Figure 5.2: The Interface showing Biometric Enrollment System

Figure 5.2 shows the biometric introduction page. A drop down button where one chooses to enroll the fingerprint, enrollment has to be done first after which one is allowed to attend classes. This serves as security measure in order to ensure that only authorized users get access.

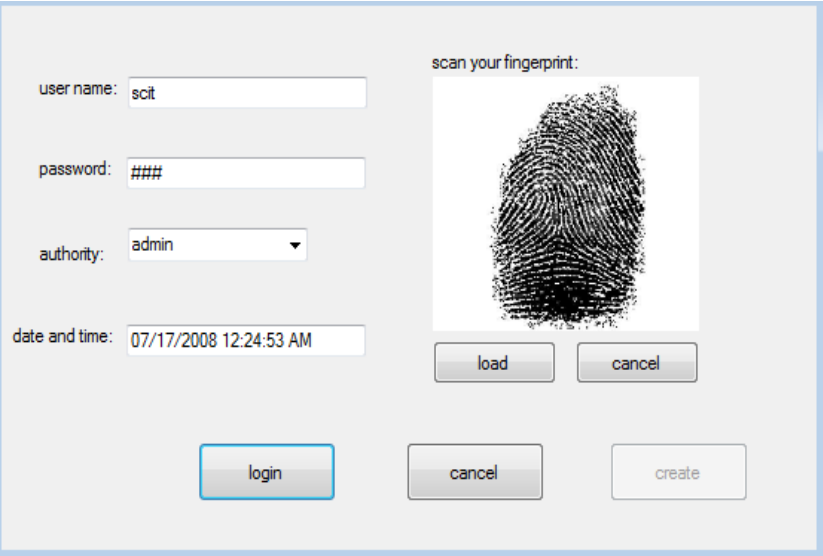


Figure 5.3: An Interface of Administrator Login.

Figure 5.3 shows the login page of administrator. The administrator types in his/her user name, password and fingerprint in order to navigate to the main page to perform enrollment.

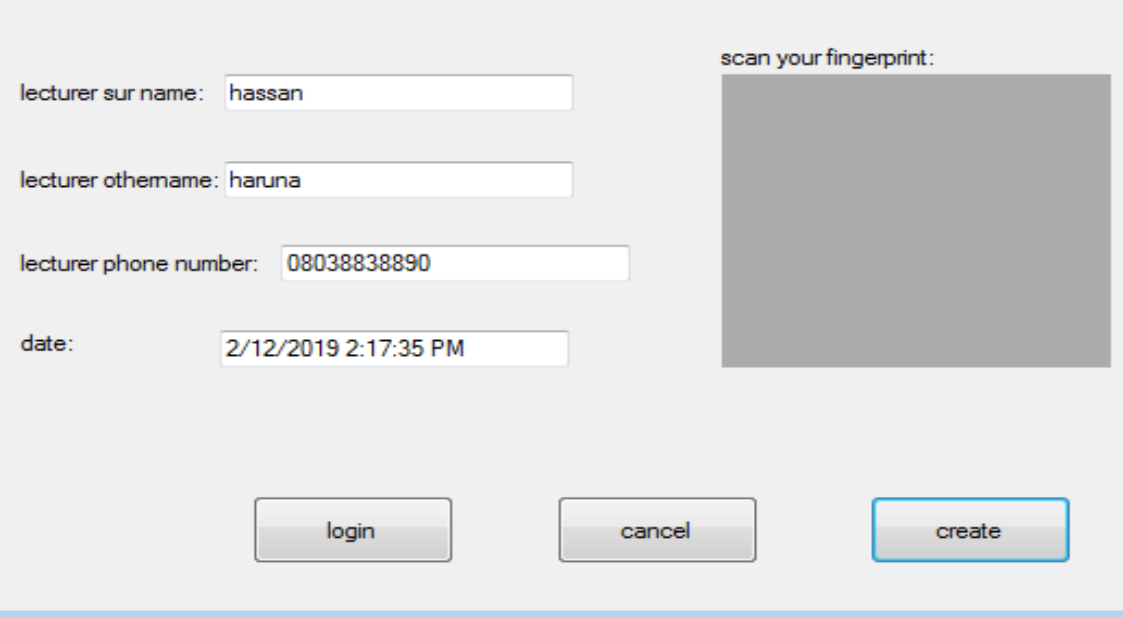


Figure 5.4: An Interface of Lecturer Login.

Figure 5.4: shows the attendance activator for lecturers giving lectures in any particular class. The lecturer will have to log in, inputs his/her fingerprint for verification and then activates a particular session of class, date and time. Students cannot register their attendance unless with the lecturer's notice.

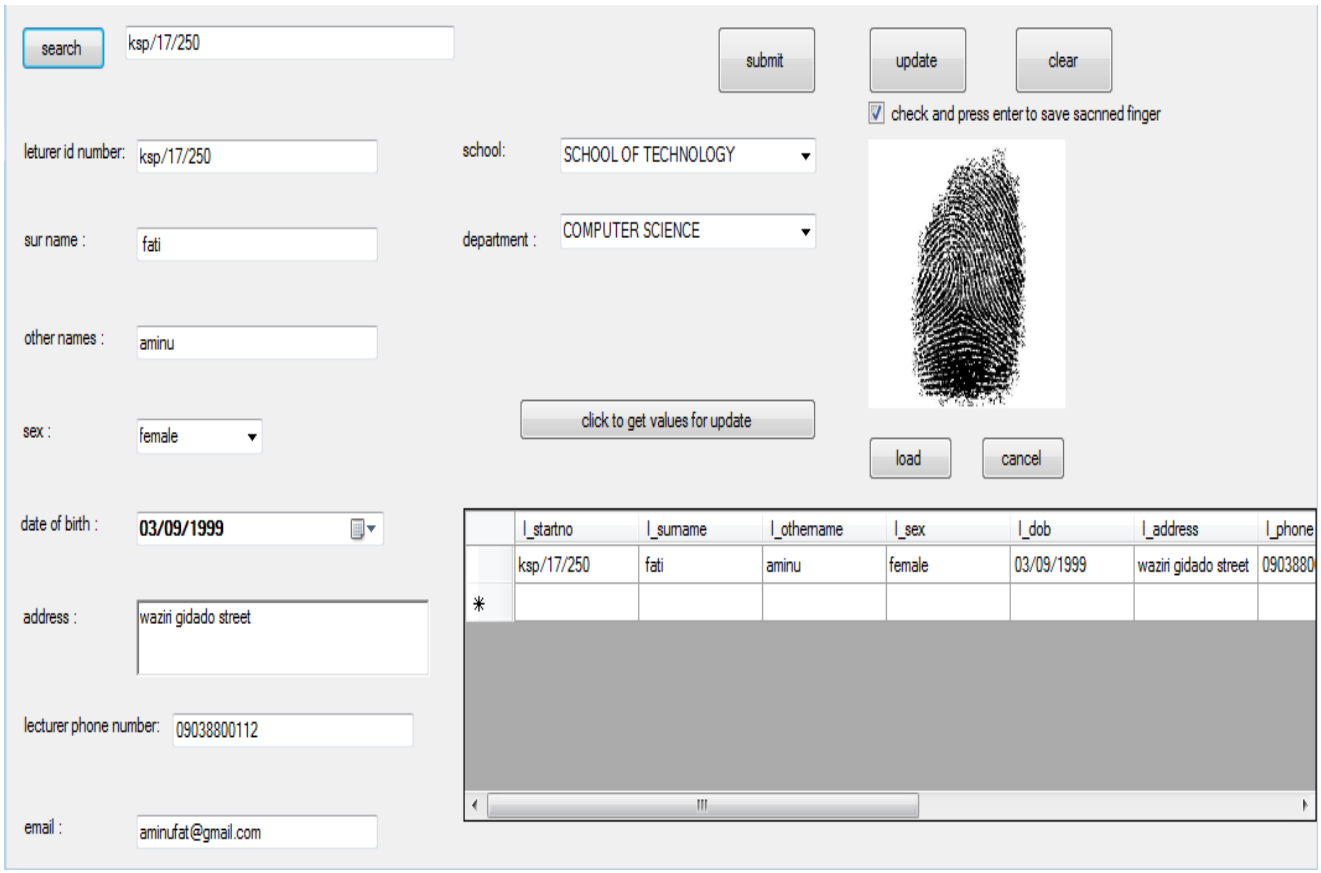


Figure 5.5: An Interface for Lecturer Enrollment.

Figure 5.5 shows where lecturers' bio data including fingerprints are captured. Personal data captured here are lecturer's ID number, surname; others name sex, date of birth, address, phone number, email, school, and department. After putting all the necessary data, each user (lecturer) was verified for matching with the data already stored in the database.

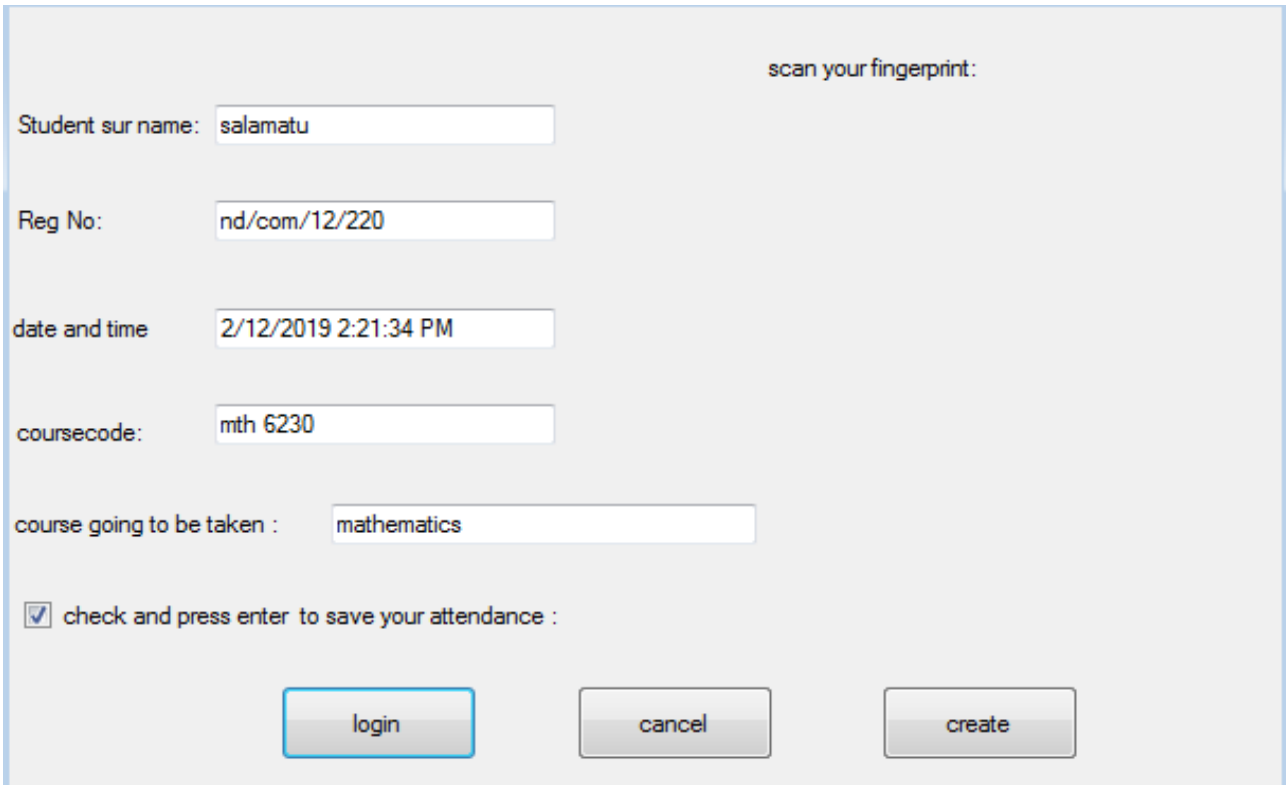


Figure 5.6: An Interface of Student Login.

Figure 5.6 shows an interface where students can log in to the biometric fingerprint platform to perform the required activities after which they could be allowed to attend lectures.

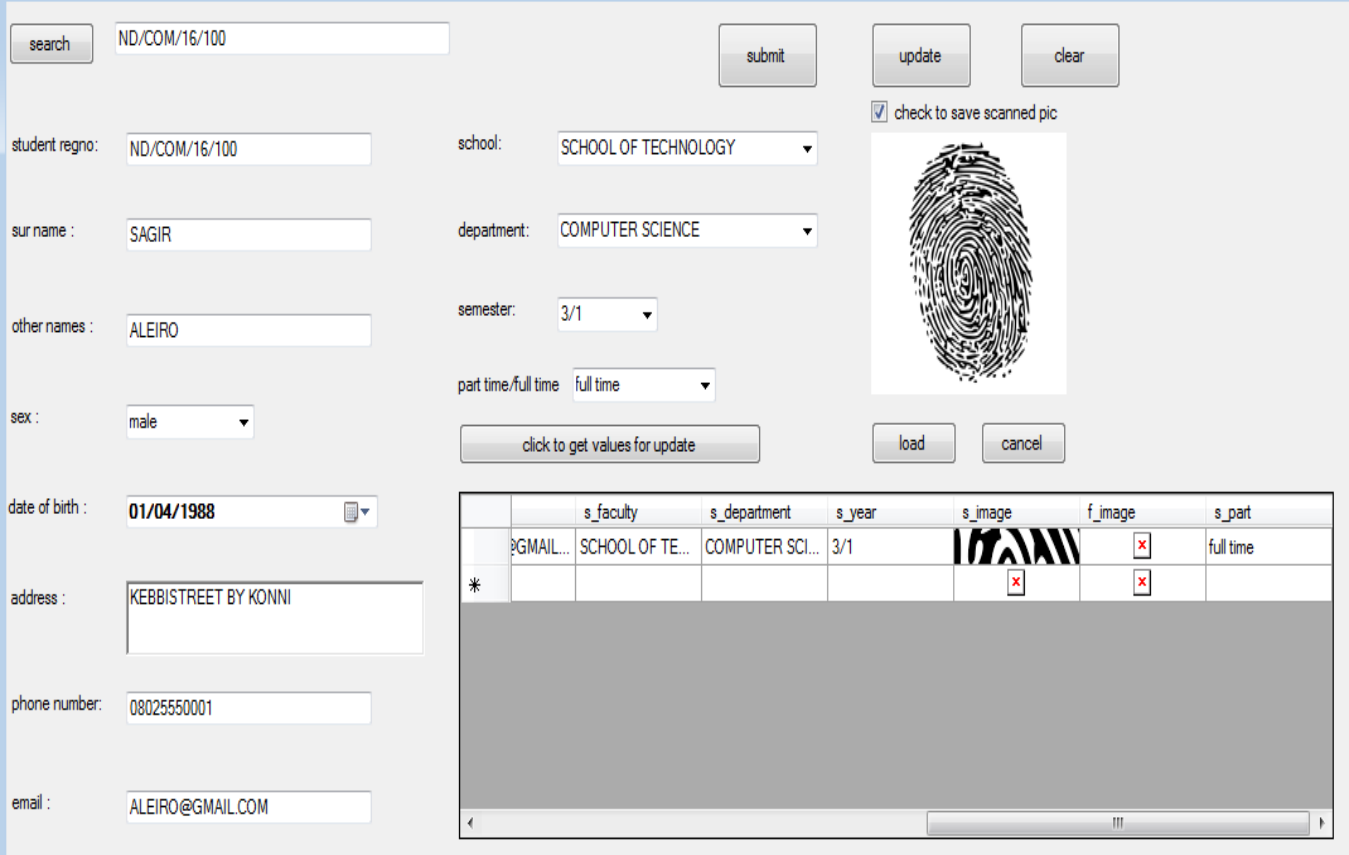


Figure 5.7: An Interface for Students Enrollment (first login).

Figure 5.7 shows a page where the administrator confirms whether a student was duly registered or not. After putting the students' registration number, data in respect of the student that was initially stored in the database is displayed automatically this proves that, the student was really registered.

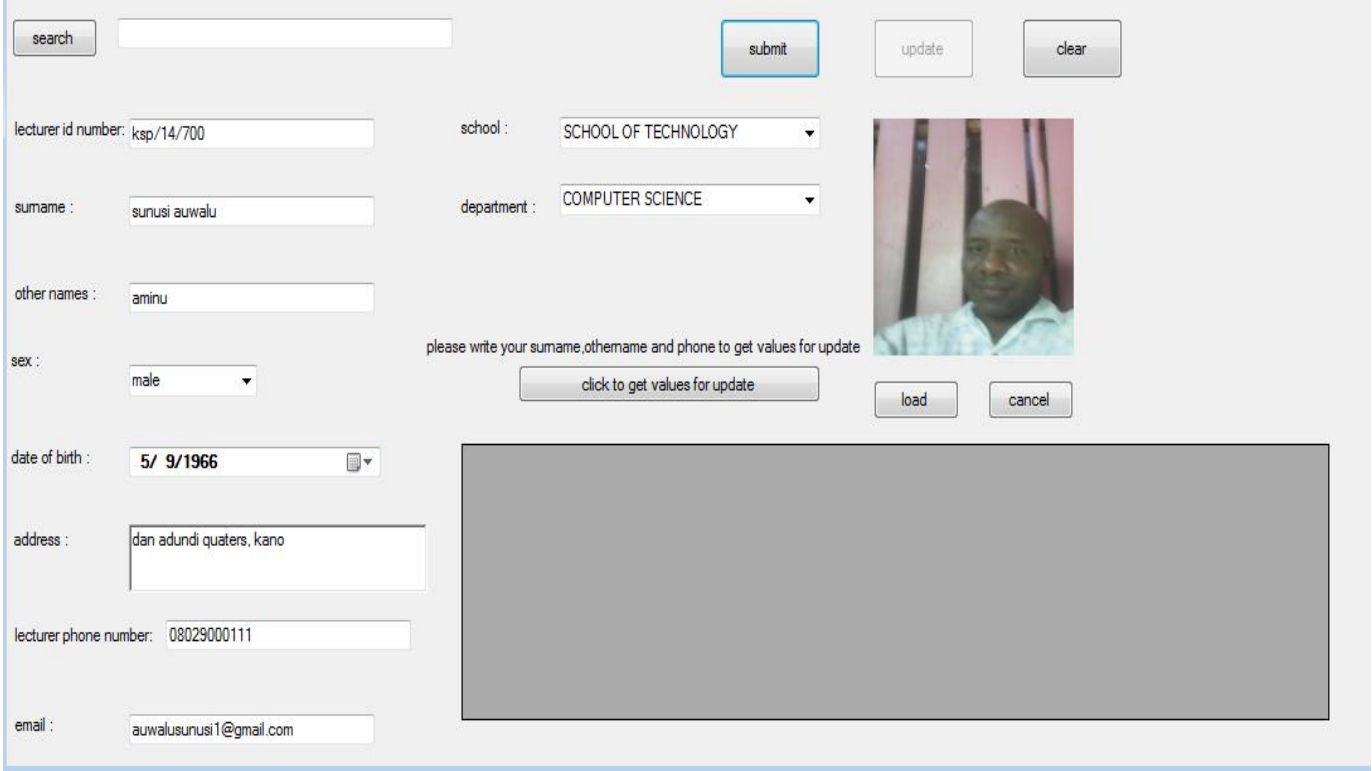


Figure 5.8: Capturing of Lecturer Image.

Figure 5.8 shows lecturers' facial images to ascertain whether there is a match with template in the database for the facial image of each lecturer.

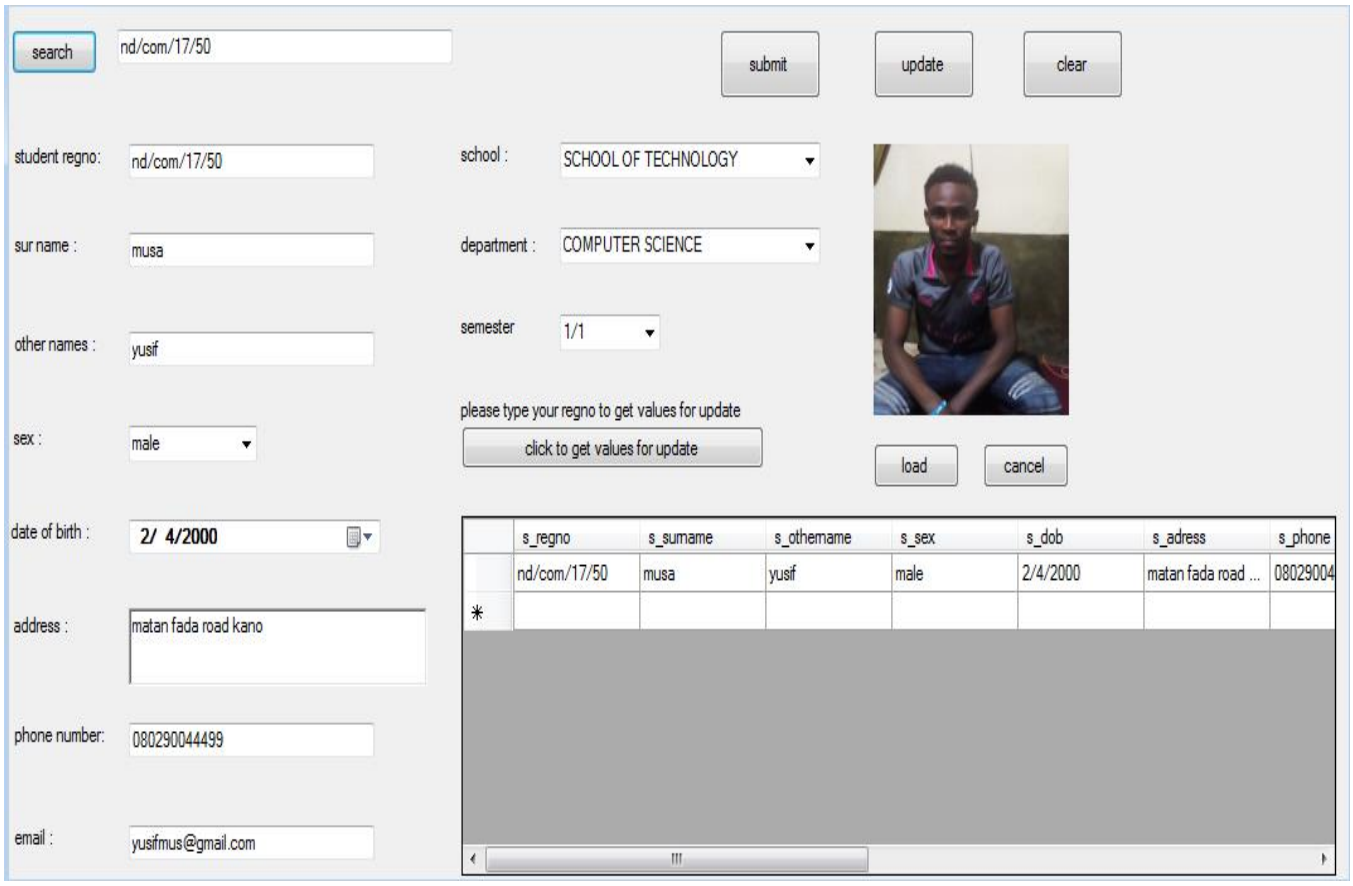


Figure 5.9: An Interface of Register Students Photograph.

Figure 5.9 above shows where students' facial images are taken to determine whether they match with the templates stored in the database for the facial image of each student in the classroom.

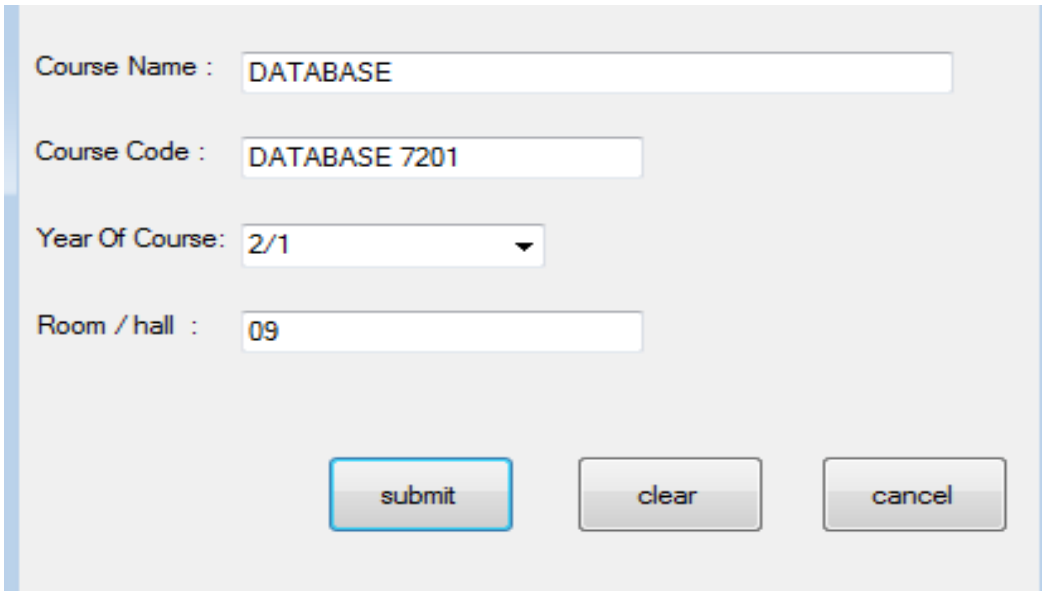


Figure 5.10: Interface for adding Courses.

Figure 5.10 shows where the administrator uses to add the various courses for the semester in the database, for instance, in the page displayed above, year two semester one course titled "database" is displayed here.

5.2 RESPONSE FROM THE SPECIFIC OBJECTIVE ONE

5.2.1 To analyze the existing system being used in Kano State Polytechnic.

Findings from the Key Informant Interview conducted revealed that Kano State Polytechnic has been using a manual system keeping in students' attendance records. This finding was in line with the findings of (Walia & Jain, 2016), which revealed that most educational institutions in the developing countries still use paper based attendance method for maintaining the attendance records. There is a need to replace these manual methods of attendance recording with biometric attendance system.

The findings also showed that the challenges encountered in the current attendance records include: time consuming, prone to error, easily get lost as there will be only one saved copy of it, dishonesty among student signing for others as well as misplacement of student attendance by lecturer and student representative. This outcome also agreed with that of (Shrilakshmi & Arpitha, 2018), where it was revealed that schools and colleges monitor their students' attendance using paper and pen registers which takes long time for the lecturer to call out each student and mark attendance.

In line with this, it was also discovered that in Kano State Polytechnic, reports on students' attendance are generated including information on the students' course enrollment, examination attendance as well as class attendance records. Agreeing with this was the finding made by Gunjan *et al.*(2015), that developed a palm vein pattern-based biometric recognition system whereby the student places his/ her finger over the fingerprint device and the student's matriculation number is sent to the database as having attended that particular lecture. At the end of the semester, reports are generated to enlist the name of students that are eligible for examination and number of times the student attended lecture.

COMPARISON

The proposed system and the old system are compared based on a number of metrics as shown in the following table:

Table 5.1 Comparison of the Old and New System

METRIC	OLD (MANUAL)	NEW (BIOMETRIC)
Possibility of impersonation	Possible	Impossible
Security	Not Secured	Secured
Timing	Slow	Fast
Report Generated	Prone to Error	Accurate & Reliable

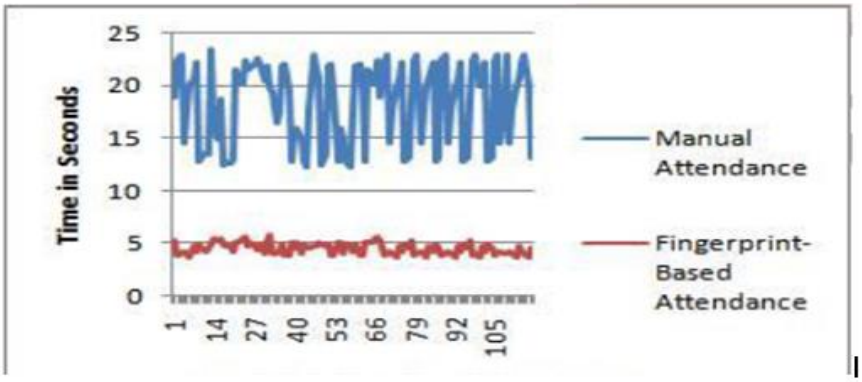


Figure 5.11: showing Comparison of the manual attendance system with the fingerprint-based attendance system.

Based on the figure the attendance system using manual method may take 10 to 25 second which is time consuming and prone to errors. While the student attendance system using fingerprint based may take less time not like the manual method, may take 0 to 5 second which shows that is more efficient, effectiveness and accurate.

5.2.2 To design and develop a biometric system for immediate identification of the students fingerprint.

The Biometric Fingerprint for students was designed using software and hardware components including Microsoft Visual Studio 2013, Sql Server 2008, C# programming language, Asp.Net

(HTML) and CSS. Hardware component are; fingerprint sensor, Microcontroller, LCD and Buzzer. SQL Server was used for the implementation of the developed system at the back-end for the design of various tables into SQL Server. SQL database management system is popular for many reasons; it is fast and easy to set up, use and administer. In addition, it runs on many operating system platforms such as Windows and UNIX, and SQL based programs can be written in many languages. At the front-end, HTML and CSS are the technologies used in implementing the system and the most important technologies used for developing web pages. Most of the front-end framework uses Hypertexts Markup Language (HTML), whereas CSS allows the user to separate the content of the website from its style.

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop computer programs as well as websites, web app, web services and mobile apps. Visual Studio uses Microsoft software development platforms such as window API and Asp.Net. The Asp.Net is an open- source server-side web app framework designed for web development to produce dynamic pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web app and web services. C# is an object-oriented programming language used with XML-based web services on the .NET platform and designed for improving productivity in the development of web application whereas fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern while a Microcontroller is the circuit that contains the fingerprint sensor. A graphic LCD displays information of registered students as an output.

5.2.3 To capture the finger print of registered students at Kano State Polytechnic using a biometric device.

Students' finger prints were captured using a finger print sensor which has two modules including enrollment module and authentication module. The enrollment module was used to the enroll users and their fingerprint into the system database. During enrollment, the fingerprint and other bio-data of the user is captured and the unique features are extracted from the fingerprint image and stored in a database as a template for the subject along with the user's ID. Besides, staff bio data captured included staff number, surname, other names, sex, position, staff type, phone number, email, department and passport photograph. For students, bio data captured

included matriculation number, surname, other-names, sex, department, level, phone number and passport photograph.

The authentication module was used to validate identity of the persons intending to access the system. The person to be authenticated indicates his/her identity and places his/her finger on the fingerprint scanner. The fingerprint images captured is enhanced and thinned at the image processing stage, and at feature extraction stage after which the biometric template is extracted. It is then fed to a matching algorithm which matches it with the person's biometric template stored in the system database to establish the identity.

5.3 Evaluating the performance of the developed biometric System using registered and unregistered student.

Biometric system will never generate error-free recognition results. However, with appropriate instruction and direction on the way to position the fingerprint when capturing the users, the rate of errors can be reduced. In order to ascertain the performance of any system, evaluation should be conducted. Hence, to evaluate performance of the developed biometric system, sixty (60) students of the School of Technology were used. The fingerprint captured for all registered students were found as valid inputs while the fingerprint of unregistered students not yet captured were found as in valid inputs by the system.

The table 5.1 below shows the details of student biometric attendance system evaluation.

CATEGORY	SUCCESS RATE%	FAILURE RATE%
Student Enrollment Process	60%	0%
Student Verification process	55%	5%

OBJECTIVE FIVE

The SUS system usability scale is generally used after the respondent partaken an opportunity to use the system being evaluated, but before any debriefing or discussion takes place. Respondents should be asked to record their immediate response to each item.

To calculate the SUS score, first sum the score contributions from each item. Each item's score contribution will range from 0 to 4. For items 1, 3, 5, 7, and 9 the score contribution is the scale position minus 1. For items 2,4,6,8 and 10, the contribution is 5 minus the scale position. Multiply the sum of the scores by 2.5 to obtain the overall value of SUS.

Table 5.2: To compute the usability of the application developed in this study based on system usability scale (SUS)

		Strongly dis agree 1	2	3	4	Strongly agree 5	
1	The system consistently accept the already captured fingerprints					✓	4
2	It can be inferred from the system that special knowledge is required to use biometric system	✓					4
3	The system is found to be more advantageous than using manual method of identifying students					✓	4
4	I believe this is perfect techniques to get rid of impersonation during the examinations	✓					4
5	The Biometric fingerprint is found to be well integrated					✓	4
6	It is a good approach if all lectures and examination can introduce the use of this system	✓					4
7	I am satisfied with how easy it is to use this system					✓	4
8	I feel so frustrated using this system		✓				3
9	The system shows that biometric is capable of curbing impersonation					✓	4
0	The proposed system appears to be secured and accurate		✓				3

Total score = 38

SUS Score = 38×2.5 = 95%.

In order to calculate the SUS, one filled questionnaire by the students was taken as a sample based on which the system usability scale (SUS) was calculated as shown in the table below.

Table 5.3: Computation of User Response for Usability Testing.

No. of respondent	Total score	SUS score	No. of respondent	Total score	SUS score	No. of respondent	Total score	SUS score	No. of respondent	Total score	SUS score
1	40×2.5	100	16	31×2.5	77.5	31	29×2.5	72.5	46	36×2.5	90
2	30×2.5	75	17	38×2.5	95	32	28×2.5	70	47	27×2.5	67.5
3	37×2.5	92.5	18	36×2.5	90	33	29×2.5	72.5	48	35×2.5	87.5
4	40×2.5	100	19	40×2.5	100	34	28×2.5	70	49	26×2.5	65
5	31×2.5	77.5	20	36×2.5	90	35	29×2.5	72.5	50	36×2.5	90
6	36×2.5	90	21	33×2.5	82.5	36	29×2.5	72.5	51	32×2.5	80
7	34×2.5	85	22	36×2.5	90	37	29×2.5	72.5	52	36×2.5	90
8	30×2.5	75	23	31×2.5	77.5	38	29×2.5	72.5	53	40×2.5	100
9	37×2.5	92.5	24	37×2.5	92.5	39	36×2.5	90	54	30×2.5	75
10	38×2.5	95	25	32×2.5	80	40	29×2.5	72.5	55	33×2.5	82.5
11	36×2.5	90	26	31×2.5	77.5	41	27×2.5	67.5	56	30×2.5	75
12	30×2.5	75	27	31×2.5	77.5	42	35×2.5	87.5	57	31×2.5	77.5
13	38×2.5	95	28	30×2.5	75	43	29×2.5	72.5	58	34×2.5	85
14	31×2.5	77.5	29	36×2.5	90	44	34×2.5	85	59	32×2.5	80

15	**34×2.5**	**85**	**30**	**31×2.5**	**77.5**	**45**	**36×2.5**	**90**	**60**	**29×2.5**	**72.5**

$$Mean = \bar{x} = \frac{\sum fx}{\sum F}$$

$$= \frac{4900.5}{60} = 81.7\%$$

Based on the findings made from the calculation of the SUS table as shown, the system indicated that the overall percentage of SUS score was 81.7%. This means that, the respondents agreed that the system was usable to them and appears to be more secured and accurate as well as capable of curbing impersonation. These results have shown that a revolutionary and systematic system is indeed needed in the higher institution for efficient process of recording and reporting the students' attendances. Same findings were made by .Bargor *et al.* (2008), which created a scale for an acceptable System Usability Scale (SUS) score. A SUS score between 85 and 100 indicate that the system is highly usable. The usability of the system is excellent when the SUS score is between 70 to about 85.With an SUS score from 50 to about 70, the acceptability is good.

5.4 Testing of the Prototype System

Both unit and system testing (system as a whole) were carried out using some sample data from the filled questionnaire in order to ensure that the proposed system conforms to the needs and characteristics of the polytechnic. In this case, all the system's logical and run – time errors as well as debug were detected and corrected before the system was integrated as a whole.

Once a source code has been generated, the software must be tested to detect and correct possible errors before delivery to a client. A series of test cases with high chance of finding errors are available for use. To detect errors, software techniques are used. These techniques provide systematic guidance for designing test that

(1) Exercise the internal logic of software components, and

(2) Exercise the input and output fields of the program to uncover errors in program function, behavior and performance.

5.4.2 Steps: Software is tested from two different views:

(1) Internal program aim is exercised using: white box‖ test case design techniques.

(2) Software requirements are exercised using: block box‖ test case design techniques.

In both cases, the intent is to find the maximum number of errors with the minimum amount of effort and time.

5.5 UNIT TESTING:

Unit testing focuses on verification efforts on the smallest unit of software design and software component. The unit test is white-box oriented. The unit testing is implemented in every component of student attendance system. By giving correct manual input to the system, the data is stored in the database and retrieved. If one wants a module to access input or get output from the end user, any error will accumulated the time will provide supervisor to show what type of error will accrued.

White box technique was employed in conducting unit testing which was utilized as a part of testing solitary unit of source code. According to. Johan, (2013), unit testing tests a small function which is testing a single unit of source code, for example, individual units of code, function/class level.

5.5.1 System Testing

Johan, (2013), commented that, system testing is geared towards testing the validity of the result. Shiva, (2012), reported that, System Testing is geared towards functional requirements of an application in order to verify that the system components perform a control function, to perform the inter-system test and demonstrate that the system does both functionally and operationally as specified. Moreover, (Jeff & Paul, 2015), contended that system testing is targeted towards eliminating faults as early as possible, improve quality, reduce cost and preserve customer satisfaction.

5.5.2 Performance Testing

Performance testing is designed to test the run-time performance of software within the context of an integrated system. Performance testing occurs throughout all steps in the testing process. Even at the unit level, the performance of an individual module may be assessed as white-box tests are conducted.

5.6 TEST CASES

A test case is an object for executing other modules in the design that does not represent any interaction by itself. A test case is a set of sequential steps to execute a test operating on a set of predefined inputs to produce certain expected outputs. There are two types of test cases:-manual and automated. A manual test case is executed manually while an automated test case is executed using automation.

In system testing, test data should cover the possible values of each parameter based on the requirements. Since testing of every value is impossible, a few values should be chosen from each equivalence class. An equivalence class is a set of values that should all be treated the same. Ideally, test cases that check error conditions are written separately from the functional test cases and should have steps to verify the error messages and logs. Realistically, if functional test cases are not yet written, it is ok for testers to check for error conditions when performing normal functional test cases. It should be clear which test data, if any is expected to trigger errors.

CHAPTER SIX

CONCLUSION AND RECOMMENDATIONS

6.1 CONCLUSION

Biometric techniques remain the most secure and safe means of authenticating, since tokens can be stolen and presented by another person. Passwords and username can be shared, but as for biometric, the users has to appear in person to be authenticated. A biometric technology is also becoming the foundation of an extensive display of higher secure identification and personal verification solution. As the matter fraud raises and the level of security infringes, the requirement for higher secure identification and personal verification technology are becoming apparent.

Based on the findings made by this study, it can be concluded that the existing methods of student registration in use at the Polytechnic was purely manual which is more time wasting, laborious and insecure. Thus, by continuing to use that method, the authenticity of records especially those of students attendance could not be guaranteed and cases of impersonation by students during lectures and examinations cannot be curtailed as such the quality of education can be comprised.

Secondly, evaluation of the Biometric Fingerprint for students' attendance developed in this study indicated the accuracy and effectiveness of the system hence; it can be concluded that the system was reliable and recommendable for use in institutions of higher learning in order to ensure that records of students' identification and attendance are reliable and authentic. The devise could also address the problem of identifying students during taking of lectures or writing examination. The study have shown that the develop system was reliable and capable enough to curb impersonations in examinations.

The third objective of the study was to capture the fingerprints of some students using the biometric device. This was successfully achieved as a total of 60 students were registered using the developed system. Obviously, fingerprint is one of the best and effective means of identifying people as no two persons have same fingerprints thus, it can be concluded that once used accordingly, this system will surely serve the purpose of students' identification that is

necessary for credible record keeping that can help in solving sensitive issues such as impersonations. The fingerprint based students' attendance system is very effective as it requires students to physically present themselves for the identification process. The fingerprint technique came up with high acceptability, collectability, circumvention, performance, permanence, uniqueness and medium universality. Also, in terms of economy of scale this method is cost effective and does not need a complex hardware and software. Using this system will overwhelm the hitches of the current system within the study domain.

Evaluation of the developed system which was one of the specific objectives of the study was also successfully done because during the testing process, fingerprints of all students who were not duly registered on the system during the authentication process were rejected and tagged as 'invalid". Thus, conclusively, the system can be said to be very effective for the purpose it was meant. The developed system has proved to be more successfully when compared with manual systems. The genuineness in the use of fingerprint makes it reliable access control technique. The fact that a user no longer needs to carry identity card and other documents for identification explain the ease to use. Student verification system redefines the manual verification system, hence forestalls academic fake and illegal studentship certificate.

Finally, computation of the usability of the developed system which was done using the SUS gave 81.7% hence; the system was found to be very useful. Therefore, it can be concluded that a reliable, secure, fast and an efficient system has been developed replacing a manual and unreliable system. Results have shown that this system can be implemented in academic institutes everywhere for better results regarding the management of attendance. This system will save time, reduce the amount of work the administration has to do and will replace the stationery material with electronic apparatus.

Generally, based on findings made on the developed students' identification system, it can be concluded that the numerous problems being faced in schools and universities pertaining students attendance in lectures and during examinations especially cases of impersonations can be brought to an end by the adoption of this system. Thus, quality of education can also be guaranteed through ensuring that students attend lectures physically and write examinations by themselves against what is obtained with the use of manual attendance taking using registers

where students fill in attendance forms for their friends who are physically absent in the class or go to the extent of writing examinations for their friends.

6.2 RECOMMENDATIONS.

- The biometric system should be made available in every lecture room or hall for proper identification of students.
- Necessary support should be given to the Electronic Engineering Department for subsequent maintenance of these devices.
- Since the biometric attendance system is faster, more accurate and secured, academic institutions should adopt it in lieu of the manual approach.

6.3 FUTURE WORK.

This study can be extended through several ways:-

- More security may be provided to interface by ensuring that introduced information will be inserted through authorized operators.
- The study can further be improved upon to automatically calculate attendance percentage of students and intimate the lecturers if a student's attendance is below an acceptable percentage.
- The system can be further implemented using a wireless network for the transmitting student record directly to the database of the application software rather than SD card.
- Using multi-model biometric system (using two or more biometric feature) to identify staff or student. The present system identifies student and staff with only fingerprint biometric features, incorporating other biometric features such as face, voice iris or retina will definitely enhance the performance and security of the system.

6.4 CONTRIBUTION TO KNOWLEDGE.

i). This study has demonstrated how part of human body can be used to uniquely identify students and staff, a system has been developed which is capable of running online and therefore can be used regardless of location.

ii). With the use of Visual basic and other supporting software, this study establishes secured communication between the biometric device and the application developed that guarantee smooth capturing of finger print images.

iii). This study also demonstrates how biometric technique can be implemented to achieve an interactive system in dot net environment.

6.5 LIMITATIONS OF THE STUDY

Although not many limitations were faced in the conduct of this study, some constraints especially with regards to finances were experienced. A number of measures were taken to ensure that effectiveness of the outcome of the study was not affected. Besides, construction of the system was also very hectic, difficult and time consuming. However, this was overcome as enough time was allocated for the study by suspending all other schedules; this ensures a very accurate and a reliable system.

6.6 SUMMARY

This project focused on the protection of student manual attendance system using fingerprint biometric. The fingerprint Biometrics is one of the most successful applications of biometric technology. The use of fingerprint for student attendance monitoring System serves as a good alternative for traditional manual signing processes that was previously been used in class attendance and examination attendance. Reviewing and assessing the authentication system for student class attendance follows a hierarchical flow from policies down through the specific actions taken to enforce them.

In the old system, attendance is usually noted using paper sheets and the old file system, this approach has been in use for a long time. It becomes difficult and obsolete for the management to regularly update the record. For any growing institution, tracing and checking student attendance could be tedious, time consuming and more prone to errors. Keeping up with security threats and countermeasures requires a continuous education and understanding.

The programming languages that was chosen were Microsoft Visual Basic.net 2013 and MSSQL Server 2008 those languages was discussed briefly. The implementation of all the components were tested and integrated for proper performance and evaluation of the system. This verifies that the system elements have been properly integrated.

Students Attendance summary functions are the most important and more convenient function in the system. It will provide valuable details which can access whole information of the students with historical data. Supervisor can refer student's history in few second. This is vast improvement produced by the system. Therefore user no need to waste time to check the all personal files. Therefore it minimizes the stress involved in manual computation of attendance and the system is easy to deploy and operate but the system does not eliminate the risk of impersonation.

REFERENCE

Alia, M. A., Tamimi, A. A., & Al-Allaf, O. N. (2013). Integrated system for monitoring and recognizing students during class session. *The International Journal of Multimedia & Its Applications*, *5*(6), 45.

Akaranga, S. I., &Ongong, J. J., (2013). The Phenomenon of Examination Malpractice: An Example of Nairobi and Kenyatta Universities, *Journal of Education and Practice,* 4 (18).

Anderson, R. J., (2001). *Security engineering: A guide to building dependable distributed systems.* New York: John Wiley & Sons.

Alotaibi, S. (2010). "Using biometrics authentication via fingerprint recognition in e -exams in e-learning environment", *The 4th Saudi International Conference,* The University of Manchester, UK.

Adetiba, E., Iortim, O., Olajide, A.T. & Awoseyin, R. (2013). An online Biometrics – based class Attendance management system. *African Journal of Computing & ICT*, 6 (3), 25 – 38.

Akinola, O .A., Abayomi Alli, A., &. Aeniyi, A., (2015) Development of a Microcontroller Based Fingerprint Examination Access Control System, *African journal of computing & ICT,* 8(2), 145-152.

Asha, S. & Chellappan C., (2012). Biometrics. An Overview of the Technology, Issues and Applications, *International Journal of Computer Applications*, 39(10), 35–52.

Adewole, K. S., Adewole, S. O., Abdulsalam, R. S., Babatunde, Shittu. M., & Oloyede, M. O., (2014). "Development of Fingerprint Biometric Attendance System for Non-Academic Staff in a Tertiary Institution,"5(2), 62–70.

Adeyemo, Z., Oyeyemi, O., & Akanbi, I. A. (2014.).Development of hybrid radio frequency and biometric security attendance system, *International Journal of Applied Science and Technology*, 4(5), 190-197.

Awojide, Simon, Awe, O., S & Babatope, T., S. (2018). Biometric Fingerprint System Using an Online Based Pattern Recognition for Candidate Authentication in Nigerian Institution Examinations. *The design perspective International Journal of Scientific & Engineering Research.* 9(5).

Afolalu, C. A., Tope-Oke, A & Atsadu, S. (2016). Toward an efficient biometric employee attendance system. Impact: *International journal of research business management* (IMPACT: IJRBM), 4(2), 65-78.

Biometricsnewportal (2011). "Biometrics new portal." Retrieve from http://www.biometricnewsportal.com/.

Bangor, A., Miller T. T., & Kortum, P. T. (2008) .An empherical evaluation of the system usability scale, *international journal of human-computer interaction*, 24(6), 574-594.

Brooke, J., (1996) .Sus-A quick and Dirty usability scale usability evaluation in industry, 189(194), 4-7.

Cappelli, R., Lumini, A., Maio, D. & Maltoni, D. (2007). Fingerprint Image Reconstruction from Standard Templates, *IEEE Transactions*, 29, 1489-1503.

Cruz, J. C. D., Paglinawan, A. C., Bonifacio, M. I. R., Flores, A. J. D., & Hurna, E. V. B. (2015). Biometrics based attendance checking using Principal Component Analysis. In Humanitarian Technology Conference (R10-HTC), *IEEE Region 10,* 1-5.

Chinchilla, R., (2012) "Ethical and Social Consequences of Biometric Technologies". American Society for Engineering Education.

Dobing, B., & Parsons, J.(2006). How UML is used, communications of the ACM, 49(5), 109-113.

Eze Peter U., Joe-Uzuegbu C. K. A, Laz Uzoechi & Opara F.K (2013). Biometric-based Attendance System with Remote Real-time Monitoring for Tertiary Institutions in developing Countries. IEEE International Conference on Emerging & Sustainable Technologies for Power & ICT in a Developing Society (NIGERCON).

Ezema, L.S., Joe-Uzuegbu, C.K.A., Eneh, J. N. &I. Amanze(2015). Fingerprint Based Attendance Management System. *International Journal of Science & Engineering Research*, 6(7).

Elmehdi, A., A., A. (2008.).Mobile system for student attendance in school. BSc. dissertation: University Utara Malaysia.

Edmund, S., (2002).Biometric Scanning Technologies: Finger, Facial and Retinal Scanning, (SANS) institute, San Francisco.

El-Abed, M, Romain, G., Baptiste, H., & Christophe R. (2010). A study of users' acceptance and satisfaction of biometric systems. In *Security Technology (ICCST), IEEE International Carnahan Conference*, 170-178.

Gaddan, J., Kola Sridhar, R., Ramakrishna R., Gujjale, R. & Raveena, K. (2016). Attendance Checking Framework for Online Understudies in Classroom Utilizing Radio Frequency Identification Technology. *International Journal of Innovative Technology and Research*, 66-69.

George, C., Chandran, J. & Rajesh, R. S. (2009). Performance Analysis of Multimodal Biometric System Authentication. *IJCSNS International Journal of Computer Science and Network Security*, 9 (3).

Geetha, M. R. (2010). ZF Microsystem Based Embedded system Application for Fingerprint Verification. California: Department of Electrical and Electronic Engineering, California: State University, Sacramento.

Goldstein, J. R., Angeletti, M. Holzbach, D. Konrad, & Snijder, M. (2008). Large-scale Biometrics Deployment in Europe: Identifying Challenges and Threats, in: J.R.C., European Commission, Sevilla.

Griaule Biometrics LTDA (2007). *Fingerprint SDK. Developer's Manual*. Retrieved from

http://www.griaulebiometrics.com

Gorman, L. O. (2001). *"Fingerprint Verification" in Biometrics personal Identification in*

Education sector. Kluwer academic Publishers. 45-66.

George, Chellin Chandran. J, & Rajesh, R., S., (2009). Performance Analysis of Multimodal Biometric System Authentication. (IJCSNS), *International Journal of Computer Science and Network Security*, 9 (3).

Hoffer, J. A., George J. F., & Valacich, J., S. (2002). Object- Oriented Analysis and Design, Modern Systems Analysis and Design Third Edition. Prentice- Hall, Inc., 20(1), 20-34.

Howard, G., & Bookboon.com (2015). *Database Design and Implementation: A Practical Introduction Using Oracle SQL*. Accessed on January 3rd 2017 from https://www.bookboo.com

Ibrahim, A. (2016). History of Kano state polytechnic. Retrieved from: http// kanopoly.edu.ng/.

Ikuomola, A. J. (2014). Fingerprint-Based Authentication System for Time and Attendance

Management. *BJMCS, 5*(6), 735-747.

Jain, a. k., nandakumar k., lu x., & park u. (2004). Integrating Faces, Fingerprints, and Soft Biometric Traits for User Recognition. *Proceedings of Biometric Authentication Workshop,* 259-269.

Jain, A., Nandakumar, K. & Nagar, A., (2008). Biometric Template Security. *EURASIP urnal on Advances in Signal Processing,* 1-17.

Jain, A. B., Ross, A. & Pankanti, S., (1999). "A Prototype Hand Geometry- Based Verification System", 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication. Washington D.C. 166-171.

Jaiswa, S., Bhadauria, S., S, & Jadon, R., S. (2011). Biometric: Case Study, *Journal of Global Research in Computer Science,* (JGRCS), 2(10).

Jain, A., Nandakumar, K. & Nagar, A., (2008). Biometric Template Security. *EURASIP urnal on Advances in Signal Processing,* 1-17.

Johan, S., (2013). *Introduction to Software Testing*. Accessed on February 13th, 2017 from http://www. Sintef.no/globalassets/project/evitameeting/2013/winterschooltdd.pdf

Jeff, O., & Paul, A. (2015). *Software Testing.* Accessed on August 21st, 2017 from www.cs.gmu.edu/~offutt/softwaretest/pwerpoint

Kadry S. & Smaili M. (2010). Wireless Attendance Management System based on Iris Recognition. *Scientific Research and Essays*, 5(12), 1428-1435.

Kokumo, B. (2010.). Lecture attendance system using fingerprint. B Tech Dissertation: Bells University of Technology, Ota, Nigeria.

Kastsanos, C., Tselios, N. & Xenosa, M. (2012), perceived evaluation of learning management system: A first step towards standardization of the system usability scale Greek, *in 16th panhellenic conference on information (PCI).*

Kalyani, C., H. (2017) Various Biometric Authentication Techniques: A Review. J Biom Biostat, 8(371).

Lee Eng Chuah, (2002). The Future Challenges of Biometrics, GSEC Practical Assignment Version. Retrieved from http://www.giac.org/paper/gsec/2145/future-challenges-biometrics/103654.(accessed on 9/19/2014).

Li, T. (2017). *Fingerprint Identification by Improved Method of Minutiae Matching.* Doctoral dissertation, Miami University.

Mohit Bais, Deeksha Rawat & Gunjeet Kaur (2016). "biometric attendance system circuit", *International Journal of Engineering Applied Science and Technology*, 1(6), 19-199.

Manoharan, P. A., Reddy, P. M. & Akash, S. (2016). Bio-Metric Attendance System using Mobile Wi-Fi Hotspot. Retrieved from http://www.djeee.org/files/publish/10.18831djeee.org2016021003.pdf.

Mudasir, K. (2017).Impact of Biometric Attendance System on Secondary and Higher Secondary Educational Institutions .*Orient journal computer science and Technology*, 10(2), 291-297.

Michel P. Down. OCNP & Richard J. Sands CISS. OCNP. (2004). Biometric: An Overview of the Technology, Challenges and Control Considerations. *Information system control journal* (4).

Mohd Ahmed, Qureshi Sualaheen Mohd Amin, Ansari Suhail Mohd Saeed & Shaikh Zind Parvaiz (2016).Cost Effective and Portable Wireless Fingerprint Device for Classroom Attendance Using ZigBee Technology. *Imperial Journal of Disciplinary Research*, 2(4),431-434.

Mark, W., W. (2014).“Stronger Authentication Methods: Biometrics and Public Acceptance”, GSEC Practical Assignment (Version 1.2b), http://www.giac.org/paper/gsec/628/stronger-authentication-methods-biometrics-public-acceptance/101398.

Naik, P. G. & Patil, M. B. (2016). biometric data analysis of student attendance system at csiber,*International Journal of Current Research,*8(2), 26751-26762.

Nunavut, S., Thieme, M., & Nanavati, R. (2002). *Biometrics: Identity verification in a networked world*. New York: John Wiley & Sons, Inc.

Olaniyi, M., Omotosho, A., Oluwatosin, E., Adegoke, M., &Akinmukomi, T. (2015). Students Exeat Monitoring System Using Fingerprint Biometric Authentication and Mobile Short Message Service. *Ar Xiv preprint arXiv: 1506.03237*.

Oloyede, M. O., Adedoyin, A. O. & Adewole, K. S. (2013). Fingerprint Biometric Authentication for Enhancing Staff Attendance System, *International Journal of Applied Information Systems (IJAIS)*, Foundation of Computer Science, 5(3), 19-24.

Onaolamipo, A. T. (2014). Development of a Computerized Biometric Control Examination Screening and Attendance Monitoring System with Fees Management. *Development*, *4*(6), 76-81.

Ononiwu G. C & Okorafor G. N (2012). Radio Frequency Identification (RFID) Based Attendance System with Automatic Door Unit, *Academic Research International,* 2(2).

Orfanou, K., Tselios, N. & Kastanos, C (2015), perceived usability evaluation of leaning management systems: Empherical evaluation of the system usability scale, *the international Review of Research in open and Distributed learning,* 16(2), 227-246.

Patel, A& Priya, R., S. (2014). 'Development of a student attendance management system using RFID and face recognition: *A Review', International journal of Advance….,* 109-119.

Peter, K. (2005). Automated fingerprint identification system (AFIS), academic press.

Raymond, J., Fry, Ed.D. & Anne Marie Dunphy (2015) Biometric student's identification: Practical solutions for Accountability and security in schools. Retrieve from https: // www. Identimetrics. Net/images/identiMetrics-White-paper-2015pdf.

Rebort, L., L. (2007). Class Attendance .1(9).

Rouse, M. (2008). Developing inclusive practice. A role for teachers and teacher education.

Robert, C., Ron, M., & Dan, M. (2005) "Automated fingerprint identification systems", Technical Report by Computer world honors case study.

Education in North. 16(1),1-20.Retrieve January 10, 2017from www: https:www.abdn.ac.uk/etin/documents/issue16/ETTN-Rousepdf.

Rukshana, S. L., & Haleem, S. L. (2017). *The design of efficient and synergetic attendance system using fingerprint techniques.* Retrieved August 9, 2018 from http://192.248.66.13/handle/123456789/3005.

Rufai, M. M. Adigun, J.O. & Yekini, N. A (2015). A biometric model for examination screening & attendance monitoring in Yaba College of technology. *World of Computer Science & Information Technology Journal,* pp. 120 – 124.

Shoewu, O., Olaniyi, O. & Lawson, A. (2011).Embedded computer-based lecture attendance management system, *African Journal of Computing and ICT*, 4(3), 27– 36.

Shoewu O. & Idowu O.A. (2012). Development of attendance management system using Biometrics. *The Pacific Journal of Science & Technology,* 13(1), 300 – 307.

Salako, E. A. (2018). A Secured Fingerprint Biometric Technique for Curbing Problem of Examination Impersonation. Retrieved August 18, 2018 from https://www.researchgate.net/

Sarker, D. K., Hossain, N. I., & Jamil, I. A. (2016). Design and implementation of smart attendance management system using multiple step authentications. In *Computational Intelligence (IWCI), International Workshop on*, 91-95).

Salil, P., (2001.).Fingerprint classification and matching with filter bank. University of Michigan.

Shehu V. & Dika A. (2011). Using Real Time Computer Vision Algorithms in Automatic Attendance Management Systems. Proceedings of the ITI 2010 32nd *Int. Conf. on Information Technology Interfaces*.

Saumyarup, R. (2016). attendance monitoring using biometric sensor *American Journal of Electronics & Communication*, 1, 26-29.

Soutar, C., Danny R., Alex S., Rene, G, & Bhagavatula, V., K. (1998). Biometric Encryption: enrollment and verification procedures." In *Aerospace/Defense Sensing and Controls*, 24-35.

Saunders, M., Lewis, P., & Thornhill, A. (2007). Research methods for Business Students (4th ed.), Pitman publishing, ISBN: 978–0–273–7168670.

Somasundaram, V., Kannan, M., & Sriram, V. (2016). Mobile based attendance management system', *Indian journal of science and technology,* 9(35).

Saheed, Y. K. et al., (2016) 'Attendance Managements System Using Barcode Identification on Student, Identity Card.', (17)2, 224-230.

Stripling, C.., Roberts, T. & Israel, G. D., (2013) Class Attendance: An Investigation of Why Undergraduates Choose to Not Attend Class, 57(3), 47-59.

Stake, R., E. (2010). Qualitative Research, Studying how things work. Retrieved 24/6/ 2012 from http://books.google.co.uk/books?hl=en&lr=&id=wwwVp.

Thomas, Y., Ing E Opoku-Mensah, & Christopher, A. A, (2013). Automatic Biometric Student Attendance System. A Case Study Christian Service University College, *Journal of Engineering, Computers & Applied Sciences,* 2(6).

Shivkumar, H.T. (2012). Software Testing Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering, 2(10), 433-438.*

Thornton, J. (2000). Latent Fingerprints, Setting Standards in the Comparison and Identification. 84thAnnual Training Conference of the California State Division of IAI. Retrieved from http://www.latentprints.com/Thornton.htm.

Tullis, T., T. & Stetson, J., N. (2004), Comparison of questionnaire for accessing website usability, in usability professionals Association (UPA) conference.

Vikas, R., S., M., Avadhesh, S., M., G, Tahir, Hassan., M., K., & Shahrukh, M., M. (2017). Fingerprint based attendance system imperial journal of interdisplinary research (IJIR) 3(2).

Woodward, J.D., Orlans, N.M., & Higgins, P.T. (2003). *Biometrics*. New York: McGraw-Hill/Osborne.

Yuihotakaishi, (2011). Attendance Monitoring System Using Biometrics for Security Staff, study Mode Inspiring. Retrieved Date: 9/6/ / 2012 from http://www.studymode.com/essays/Attendance Monitoring-System-Using-Biometrics-For- 732262.html.

APPENDICES

Appendix A: Interview Guide

1. What is the current student attendance system in use in Kano State Polytechnic?

……

……

2 What are the challenges you encountered with the current student attendance system in use in Kano State Polytechnic?

……

……

3 What type of report do you generate for student's attendance in Kano State Polytechnic?

……

……

4 Is there need to improve on the current student's system used in Kano State Polytechnic?

……

……

5 What are the major benefits of biometric fingerprint records system implementation?

……

……

6 Thank you very much for your input. Are there any other comments on biometric finger record system which we didn't ask but that you think is essential?

……

……

APPENDIX B: INTERVIEW TRANSCRIPT

Participant's code:

Interviewee 1

Interviewee 2

---------- **********----------

Interviewer

The first interview was conducted with the Head of Department for Computer Science of School of Technology, Matan Fada Road**,** what is the current student attendance system in use in Kano State Polytechnic?

Interviewee 1

The current student attendance system in use is the manual system (students sign in attendance). Based on my experience, the current system in Kano State Polytechnic is a manual system which is use in keeping records of student attendance.

Interviewer

What are the challenges you encountered with the current student attendance system in use in Kano State Polytechnic?

Interviewee 1

The challenges encountered in the current attendance system used in Kano State Polytechnic include: prone to error when recording attendance, time consuming as well as bias among lecturer and student representative.

The challenges associated with the current attendance system comprises of time consuming, dishonesty among student signing for others, Misplacement of student attendance by lecturer and student representative.

Interviewer

What type of report do you generate for student's attendance in Kano State Polytechnic?

Interviewee 1

The report we generated in Kano State Polytechnic include the following: student examination attendance, student course enrollment and student eligibility for examination (75% attendance).

Based on my knowledge, the Kano State Polytechnic student attendance report generates continuous assessment, practical attendance as well as exam attendance.

Interviewer

Is there need to improve on the current student's attendance used in Kano State Polytechnic?

Interviewee1

Yes, there is need to improve the current student attendance system so that it can eliminate the problem of time consuming, dishonesty among student signing for others, Misplacement of student attendance by lecturer and student representative.

Yes it is importance to improve the current attendance system so as to eradicate the dishonesty among student and misplacement of attendance by student representation.

Interviewer

What are the major benefits of biometric fingerprint records system implementation?

Interviewee 1

The major benefit of biometric fingerprint records system implementation include: accurate student attendance, save time of student attendance and it provide effective and efficient report generation.

The biometric fingerprint record implementation will provide us with security purpose both to the student and lecturer within or outside the school as well as digital records is maintained for future use.

The second interview was conducted with staff of computer science department in order to assess how current system records recorded, stored and retrieved within the organization.

Interviewer

What type of report do you generate for student's attendance in Kano State Polytechnic?

Interviewee 2

The Kano State Polytechnic use manual record system to keep student record which is based on pen and paper register.

Interviewer

What are the challenges you encountered with the current student attendance system in use in Kano State Polytechnic?

Interviewee 2

Based on my experience, the current challenges encountered in manual system include the following: dishonesty among students (student signing for other), misplacement by student representative as well as security and privacy among student.

Interviewer

What type of report do you generate for student's attendance in Kano State Polytechnic?

Interviewee 2

The types of report we generated for student attendance in Kano State Polytechnic comprises of test attendance, exams attendance and class attendance.

Interviewer

Is there need to improve on the current student's used in Kano State Polytechnic?

Interviewee 2

there is need to improve the current student attendance by eliminating time consuming in taking attendance as well as bias among lecturer and student representative.

Interviewer

What are the major benefits of biometric fingerprint records system implementation?

Interviewee 2

The introduction of biometric fingerprint records implementation will increase the overall satisfaction of student and help the school authority to take good decision making within a specific time about the student.

APPENDIX C: QUESTIONNAIRE

Dear Sir/ Madam

Iam Auwalu Sunusi a student of Kampala International University Uganda, undertaking a research thesis in partial fulfillment of the requirement for the award of a Master Degree in Computer science. This questionnaire has been designed for the sole purpose of collecting data on system quality as part of the evaluation of a ***"developing an access control system for students' identification using biometric finger print techniques".***

I humbly request your participation is voluntary and the result of this study will be used for academic purpose only. And answering this questionnaire according to your true and sincere opinion. Be assured that the data collected will be treated with a very high degree of confidentiality; the identity of respondents will be kept anonymously.

		Strongly dis agree				**Strongly agree**
		1	**2**	**3**	**4**	**5**
1	The system consistently accept the already captured fingerprints	○	○	○	○	○
2	It can be inferred from the system that special knowledge is required to use biometric system	o	o	o	o	o
3	The system is found to be more advantageous than using manual method of identifying students	o	o	o	o	o
4	I believe this is perfect techniques to get rid of impersonation during the examinations	o	o	o	o	o
5	The Biometric fingerprint is found to be well integrated	o	o	o	o	o
6	It is a good approach if all lectures and examination can introduce the use of this system	o	o	o	o	o
7	I am satisfied with how easy it is to use this system	o	o	o	o	o
8	I feel so frustrated using this system	o	o	o	o	o
9	The system shows that biometric is capable of curbing impersonation	o	o	o	o	o
10	The proposed system appears to the secured and accurate	o	o	o	o	o

APPENDIX D: HARDWARE AND SOFTWARE CODES

The following code has been used to allow connection between fingerprint reader and visual studio interface.

FOR ENROLLING USERS

```
#include<Wire.h>

#include<LiquidCrystal_I2C.h>

#include <Adafruit_Fingerprint.h>

#include <SoftwareSerial.h>

SoftwareSerial mySerial(2, 3);

LiquidCrystal_I2C lcd(0x3F,2,1,0,4,5,6,7,3,POSITIVE);

Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);

int ledgreen=7;int ledred=5;int buzzer=6;void setup()  {

  pinMode(ledgreen,OUTPUT);  pinMode(ledred,OUTPUT);  pinMode(buzzer,OUTPUT);

  digitalWrite(buzzer,HIGH);  Serial.begin(9600);  while (!Serial);  delay(100);
Serial.println("finger detect test");  finger.begin(57600); lcd.begin(16,2);  lcd.backlight();
lcd.setCursor(0,0);

  if (finger.verifyPassword()) {     Serial.println("Found fingerprint sensor!");  } else {
Serial.println("Did not find fingerprint sensor :(");     while (1) { delay(1); } }
finger.getTemplateCount();

  Serial.print("Sensor contains "); Serial.print(finger.templateCount); Serial.println(" templates");

  Serial.println("Waiting for valid finger...");

  lcd.clear();  lcd.setCursor(0,0);  lcd.print("put right thumb");  lcd.setCursor(0,1);

  lcd.print("for verification");  delay(1000);}void loop(){  getFingerprintIDez();  delay(50);}
```

uint8_t getFingerprintID() { uint8_t p = finger.getImage(); switch (p) { case FINGERPRINT_OK:

Serial.println("Image taken"); lcd.clear(); lcd.setCursor(0,0); lcd.print("image taken");

break;

CASE FINGERPRINT_NO FINGER:

Serial.println ("No finger detected"); lcd.clear(); lcd.setCursor(0,0); lcd.print("No Finger detected"); return p; case FINGERPRINT_PACKETRECIEVEERR: Serial.println("Communication error"); lcd.clear(); lcd.setCursor(0,0); lcd.print("communication"); lcd.setCursor(0,1); lcd.print("error"); return p; case FINGERPRINT_IMAGEFAIL: Serial.println("Imaging error");

lcd.clear(); lcd.setCursor(0,0); lcd.print("Imaging error"); return p; default:

Serial.println("Unknown error");

lcd.clear(); lcd.setCursor(0,0); lcd.print("Unknown error"); return p; } case

// found a match!

SerMNNial.print("Found ID "); Serial.print(finger.fingerID);

lcd.clear(); lcd.setCursor(0,0); lcd.print("match"); digitalWrite(ledgreen,HIGH); delay(1000);

digitalWrite(ledgreen,LOW); lcd.setCursor(0,1); lcd.print("success"); delay(1000); lcd.clear();

lcd.setCursor(0,0); lcd.print("put right thumb"); lcd.setCursor(0,1); lcd.print("for verification");

delay(1000); p = finger.image2Tz(); return finger.fingerID;

void loop()

```
{  getFingerprintIDez();  delay(50);}

uint8_t getFingerprintID() {  uint8_t p = finger.getImage(); switch (p) {

case FINGERPRINT_OK:

    Serial.println ("Image taken");     lcd.clear();     lcd.setCursor(0,0);     lcd.print("image
taken");

    break;    case FINGERPRINT_NOFINGER:     Serial.println("No finger detected");
lcd.clear();

    lcd.setCursor(0,0);     lcd.print("No Finger detected");     return p;}

// returns -1 if failed, otherwise returns ID #

int getFingerprintIDez() {

  uint8_t p = finger.getImage();

if (p != FINGERPRINT_OK)  return -1;lcd.clear();lcd.setCursor(0,0);lcd.print("thank
you");lcd.setCursor(0,1);lcd.print("try2
again");digitalWrite(ledred,HIGH);digitalWrite(buzzer,LOW);delay(1000);digitalWrite(ledred,L
OW);digitalWrite(buzzer,HIGH);  }
```

SOFTWARE CODES

(REGISTER STUDENT)

```
namespace final_fingerprint_interface
{public partial class register_student : Form
   {string CNSTR = @"SERVER=ZINOX-
PC\SQLEXPRESS;DATABASE=final_project_fingerprint;USEr
ID=sa;PASSWORD=1234567";
       SqlCommand cmd;
       string imgloc = "";
       SpeechSynthesizer jarvis = new SpeechSynthesizer();
       PromptBuilder pb = new PromptBuilder();
```

```
SpeechRecognitionEngine recog = new SpeechRecognitionEngine();
public register_student()     {    InitializeComponent();   }
private void btn_submit_Click(object sender, EventArgs e)
{  SqlConnection con = new SqlConnection(CNSTR);
   con.Open();     try     { byte[] img = null;
      FileStream fs = new FileStream(imgloc, FileMode.Open, FileAccess.Read);
      BinaryReader br = new BinaryReader(fs);
      img = br.ReadBytes((int)fs.Length);
      string isql = "insert into
register_student(s_regno,s_surname,s_othername,s_sex,s_dob,s_address,s_phone,s_email,s_facu
lty,s_department,s_year,s_part,s_image) values ('" + textBox1.Text + "','" + textBox2.Text + "','"
+ textBox3.Text + "','" + comboBox1.Text + "','" + dateTimePicker1.Text + "','" +
richTextBox1.Text + "','" + textBox4.Text + "','" + textBox5.Text + "','" + comboBox2.Text +
"','" + comboBox3.Text + "','" + comboBox4.Text + "','" + comboBox5.Text + "',@img)";
      cmd = new SqlCommand(isql, con);
      cmd.Parameters.Add(new SqlParameter("@img", img));
      int x = cmd.ExecuteNonQuery();
      jarvis.Speak("success");
      MessageBox.Show(x.ToString(), "sucess");
         catch (Exception ex)
   {MessageBox.Show(ex.Message);}
   finally { con.Close();} }
private void btn_load_Click(object sender, EventArgs e)
{ OpenFileDialog open = new OpenFileDialog();
   open.Filter = "image(*png,*jpg)|*png; *jpg";
   open.InitialDirectory = @"c:\";
   if (open.ShowDialog() == DialogResult.OK)
   {    imgloc = open.FileName.ToString();
      pictureBox1.ImageLocation = imgloc;    }  }
private void btn_search_Click(object sender, EventArgs e)
{SqlConnection con = new SqlConnection(CNSTR);
```

```
        con.Open();
            try          {  string ssql = "select * from register_student where s_regno = ('" +
textBox6.Text + "') or s_surname = ('" + textBox6.Text + "') or s_othername = ('" +
textBox6.Text + "')";
            SqlDataAdapter sda = new SqlDataAdapter(ssql,con);
            DataSet ds = new DataSet();
            sda.Fill(ds);
            dg_student.DataSource = ds.Tables[0];
            dg_student.Columns[0].Visible = false;       }
        catch (Exception ex)   {   MessageBox.Show(ex.Message);    }  finally    { con.Close();
}    }
      private void btn_update_Click(object sender, EventArgs e)
      {  if (textBox1.Text != "" && textBox2.Text != "" && textBox3.Text != "" &&
comboBox1.Text != "" && dateTimePicker1.Text != "" && richTextBox1.Text != "" &&
textBox4.Text != "" && textBox5.Text != "" && comboBox2.Text != "" && comboBox3.Text
!= "" && comboBox4.Text != "")
        {       SqlConnection con = new SqlConnection(CNSTR);              con.Open();
try             {
            string usql = "update register_student set [s_surname]=('" + textBox2.Text +
"'),[s_othername]=('" + textBox3.Text + "'),[s_sex]=('" + comboBox1.Text + "'),[s_dob]=('" +
dateTimePicker1.Text + "'),[s_address]=('" + richTextBox1.Text + "'),[s_phone]=('" +
textBox4.Text + "'),[s_email]=('" + textBox5.Text + "'),[s_faculty]=('" + comboBox2.Text +
"'),[s_department]=('" + comboBox3.Text + "'),[s_year]=('" + comboBox4.Text +
"'),[s_part]=('"+comboBox5.Text+"') where s_regno =('" + textBox1.Text + "')";
            cmd = new SqlCommand(usql, con);
            cmd.ExecuteNonQuery();
            MessageBox.Show("succesfully updated");              }
          catch (Exception ex)
          {   MessageBox.Show(ex.Message);      }
          finally {     con.Close();    }}}
      private void button1_Click_1(object sender, EventArgs e)
```

```
{       try     {
        SqlConnection con = new SqlConnection(CNSTR);
        con.Open();
        string bsql = "select
s_surname,s_othername,s_sex,s_dob,s_adress,s_phone,s_email,s_faculty,s_department,s_year,s_
part,s_image from register_student where s_regno = ('" + textBox1.Text + "') ";
        cmd = new SqlCommand(bsql, con);
        SqlDataReader dr = cmd.ExecuteReader();
        dr.Read();          if (dr.HasRows)
        {       textBox2.Text = dr[0].ToString();
          textBox3.Text = dr[1].ToString();
          comboBox1.Text = dr[2].ToString();
          dateTimePicker1.Text = dr[3].ToString();
          richTextBox1.Text = dr[4].ToString();
          textBox4.Text = dr[5].ToString();
          textBox5.Text = dr[6].ToString();
          comboBox2.Text = dr[7].ToString();
          comboBox3.Text = dr[8].ToString();
          comboBox4.Text = dr[9].ToString();
          comboBox5.Text = dr[10].ToString();
          byte[] img = (byte[])(dr[11]);
          if (img == null)
            pictureBox1.Image = null;
          else          {
            MemoryStream ms = new MemoryStream(img);
            pictureBox1.Image = Image.FromStream(ms);          }
          btn_update.Enabled = true;    }
        con.Close();        }
      catch (Exception ex)      {       MessageBox.Show(ex.Message);     }     }
    private void register_student_Load(object sender, EventArgs e)
    {       btn_update.Enabled = false;
```

```
    btn_load.Enabled = false;       }
  private void checkBox1_KeyDown(object sender, KeyEventArgs e)
  {    pb.ClearContent();
    jarvis.SelectVoiceByHints(VoiceGender.Female, VoiceAge.Senior);
        if (checkBox1.Checked)      {
            if (e.KeyCode == Keys.Enter)            {
        jarvis.Speak("your pic has been successfully scanned and saved into folder scanned pics as image(2).jpg ");
        MessageBox.Show("your scanned picture has been saved into c-pictures-scanned pictures as image(2).jpg ");
        btn_load.Enabled = true;       }
      else { if (e.KeyCode == Keys.F2)
        {     jarvis.Speak("your pic has been successfully scanned and saved into folder scanned pics as image(3).jpg ");
          MessageBox.Show("your scanned picture has been saved into c-pictures-scannedpictures as image(3).jpg ");
          btn_load.Enabled = true;   } }}
  private void btn_delete_Click(object sender, EventArgs e)
  {
    if (textBox1.Text != "" || textBox2.Text != "" || textBox3.Text != "" || textBox4.Text != "" || textBox5.Text != "" || textBox6.Text != "" || comboBox1.Text != "" || comboBox2.Text != "" || comboBox3.Text != "" || comboBox4.Text != "" || dateTimePicker1.Text != "" || richTextBox1.Text != "" || comboBox5.Text != "")
      {  textBox1.Text = "";
        textBox2.Text = "";
        textBox3.Text = "";
        textBox4.Text = "";
        textBox5.Text = "";
        textBox6.Text = "";
        comboBox1.Text = "";
        comboBox2.Text = "";
```

```
            comboBox3.Text = "";
            comboBox4.Text = "";
            dateTimePicker1.Text = "";
            richTextBox1.Text = "";
            comboBox5.Text = "";      }       }
        private void btn_cancel_Click(object sender, EventArgs e)
        {     if (pictureBox1.Image != null)    {
            pictureBox1.Image = null;   }        }
```

(**REGISTER LECTURER)**

```
l_startno,l_sex,l_dob,l_address,l_phone,l_email,l_faculty,l_department,l_image from
register_lecturer where l_surname = ('" + textBox2.Text + "') and l_othername=('" +
textBox3.Text + "') ";
            cmd = new SqlCommand(bsql, con);
            SqlDataReader dr = cmd.ExecuteReader();
            dr.Read();
            if (dr.HasRows)               {
               textBox1.Text = dr[0].ToString();
               comboBox1.Text = dr[1].ToString();
               dateTimePicker1.Text = dr[2].ToString();
               richTextBox1.Text = dr[3].ToString();
               textBox4.Text = dr[4].ToString();
               textBox5.Text = dr[5].ToString();
               comboBox2.Text = dr[6].ToString();
               comboBox3.Text = dr[7].ToString();
               byte[] img = (byte[])(dr[8]);
               if (img == null)
                  pictureBox1.Image = null;
               else                  {
                  MemoryStream ms = new MemoryStream(img);
                  pictureBox1.Image = Image.FromStream(ms);  }
```

```
            btn_update.Enabled = true;      }
            con.Close();          }
        catch (Exception ex)          {          MessageBox.Show(ex.Message);          }       }
    private void btn_update_Click(object sender, EventArgs e)
    {
        if (textBox1.Text != "" && textBox2.Text != "" && textBox3.Text != "" &&
comboBox1.Text != "" && dateTimePicker1.Text != "" && richTextBox1.Text != "" &&
textBox4.Text != "" && textBox5.Text != "" && comboBox2.Text != "" && comboBox3.Text
!= "")
        {              SqlConnection con = new SqlConnection(CNSTR);
            con.Open();              try              {
                string usql = "update register_lecturer set [l_surname]=('" + textBox2.Text +
"'),[l_othername]=('" + textBox3.Text + "'),[l_sex]=('" + comboBox1.Text + "'),[l_dob]=('" +
dateTimePicker1.Text + "'),[l_address]=('" + richTextBox1.Text + "'),[l_phone]=('" +
textBox4.Text + "'),[l_email]=('" + textBox5.Text + "'),[l_faculty]=('" + comboBox2.Text +
"'),[l_department]=('" + comboBox3.Text + "') where l_startno =('" + textBox1.Text + "')";
                cmd = new SqlCommand(usql, con);
                cmd.ExecuteNonQuery();              MessageBox.Show("succesfully updated");
}
            catch (Exception ex)              {
                MessageBox.Show(ex.Message);              }
            finally              {              con.Close();              }          }       }
    private void btn_search_Click(object sender, EventArgs e)
    {          SqlConnection con = new SqlConnection(CNSTR);
        con.Open();          try          {
            string ssql = "select * from register_lecturer where l_startno = ('" + textBox6.Text + "')
or l_surname = ('" + textBox6.Text + "') or l_othername = ('" + textBox6.Text + "')";
            SqlDataAdapter sda = new SqlDataAdapter(ssql, con);
            DataSet ds = new DataSet();
            sda.Fill(ds);
            dg_lecturer.DataSource = ds.Tables[0];
```

```
            dg_lecturer.Columns[0].Visible = false;          }
        catch (Exception ex)          {             MessageBox.Show(ex.Message);          }
finally          {
            con.Close();          }       }

    private void checkBox1_KeyDown(object sender, KeyEventArgs e)
    {          pb.ClearContent();
        jarvis.SelectVoiceByHints(VoiceGender.Female, VoiceAge.Senior);
        if (checkBox1.Checked)          {             if (e.KeyCode == Keys.Enter)             {
            jarvis.Speak("your scnned pic has been saved into c:-pictures-scannedpic2 as
image(4).jpg");
            MessageBox.Show("your scnned pic has been saved into c:-pictures-scannedpic2 as
image(4).jpg");
            btn_load.Enabled = true;             }             else             {                 if
(e.KeyCode == Keys.F1)
            {                 jarvis.Speak("your scnned pic has been saved into c:-pictures-
scannedpic2 as image(5).jpg");
                MessageBox.Show("your scnned pic has been saved into c:-pictures-scannedpic2
as image(5).jpg");
                btn_load.Enabled = true;                 }             }          }       }
    private void btn_cancel_Click(object sender, EventArgs e)
    {
        if (pictureBox1.Image != null)
        {             pictureBox1.Image = null;          }       }
    private void btn_delete_Click(object sender, EventArgs e)
    {
        if (textBox1.Text != "" || textBox2.Text != "" || textBox3.Text != "" || textBox4.Text != ""
|| textBox5.Text != "" || textBox6.Text != "" || comboBox1.Text != "" || comboBox2.Text != "" ||
comboBox3.Text != ""  || dateTimePicker1.Text != "" || richTextBox1.Text != "")
        {             textBox1.Text = "";
            textBox2.Text = "";
```

```
            textBox3.Text = "";
            textBox4.Text = "";
            textBox5.Text = "";
            textBox6.Text = "";
            comboBox1.Text = "";
            comboBox2.Text = "";
            comboBox3.Text = "";
                        dateTimePicker1.Text = ""; richTextBox1.Text = "";          }       }  }}
```

(ADMIN LOGIN)

```
      private void button4_Click(object sender, EventArgs e)
      {           SqlConnection con = new SqlConnection(CNSTR);
         con.Open();          try   {      byte[] img = null;
         FileStream fs = new FileStream(imgloc, FileMode.Open, FileAccess.Read);
         BinaryReader br = new BinaryReader(fs);
         img = br.ReadBytes((int)fs.Length);
         string isql = "insert into admin_login(username,pass,image)values('" + textBox1.Text +
'','" + textBox2.Text + "',@img)";
         cmd = new SqlCommand(isql, con);
         cmd.Parameters.Add(new SqlParameter("@img", img));
         int x = cmd.ExecuteNonQuery();
         MessageBox.Show(x.ToString(), "success");          }
         catch(Exception ex){MessageBox.Show(ex.Message);}
         finally{con.Close();}       }
      private void button3_Click(object sender, EventArgs e)
      {    OpenFileDialog open = new OpenFileDialog();
         open.Filter = "image(*jpg,*png)|*jpg;*png";
         open.InitialDirectory = @"c:\";
         if (open.ShowDialog() == DialogResult.OK)
         {              imgloc = open.FileName.ToString();
            pictureBox1.ImageLocation = imgloc;          }       }
```

(STUDENT LOGIN)

```
            catch (Exception ex) { MessageBox.Show(ex.Message); }
            MessageBox.Show("you have successfully logged in");   }          else
        {  button5.Enabled = true;          }        }
    catch (Exception ex)
    {    MessageBox.Show(ex.Message);    } finally {     con.Close();    } }

  private void button5_Click(object sender, EventArgs e)
  {   register_student rs = new register_student();
    rs.Show();          }   }}
```

(LECTURER LOGIN)

```
    MessageBox.Show("please check your login details");          }          }
      catch (Exception ex)       {          MessageBox.Show(ex.Message);       }
finally       {
        con.Close();   }
    private void textBox4_TextChanged(object sender, EventArgs e)
    {       textBox4.Text = dateTimePicker1.Value.ToString();      }      } }
```

APPENDIX E: BUDGET

Activity	Requirement	Amount (UGX)	Amount (NGN)
Internet connection	Night bundle data subscription	150,000	15,500
Proposal correction from the Supervisor	Typing and Printing	8,000	8,000
Field data collection	Printing of Questionnaire	30,000	3,000
Prototype design and develop	Tools and Consultation	200,000	20,000
Final thesis copies	Typing, photocopy, and binding	50,000	5,000
Hardware cost		750,000	75,000
Local runs		500,000	50,000
Total		**168,800.00**	**175,500**