



**UNIVERSITY OF NAIROBI  
SCHOOL OF COMPUTING AND INFORMATICS**

**BIOMETRICS CLASS ATTENDANCE MANAGEMENT SYSTEM**

**BY**

**WACHIRA SALOME NJOKI  
P53/73284/2014**

**Supervisor: Dr. Christopher Chepken**

**A Research Project Proposal Submitted In Partial Fulfillment Of The  
Requirements Of The Degree Of Master Of Science In Distributed Computing  
Technology At The University Of Nairobi.**

**DECLARATION**

I declare that this research proposal report is my original work and has not been submitted for examination in any university.

**Salome Wachira**

Signature.....

Date.....

This research project has been submitted for examination with our approval as university supervisors.

**Supervisor: Dr. Chepken**

School of Computing and Informatics

University of Nairobi

Po Box 30197 Nairobi

Signature.....

Date.....

## **ACKNOWLEDGEMENT**

I take this opportunity to thank the almighty God for enabling me and for his provision throughout this course. I would also like to pass my sincere appreciation to my Supervisor Dr. Chepen for his invaluable guidance, counsel and support ensuring this project was completed.

Much appreciation to my immediate and extended family for their support, inspiration and encouragement. Am forever grateful.

## **ABSTRACT**

Transfer of knowledge in most institutions of higher learning is done through lecturing where students are expected to attend classes and a lecturer dictates notes and share the contents of the lesson with the students. Overtime, class non-attendance has been frequent in most institutions and has become a concern since a negative relationship exists between attendance and the overall performance. Non-attendance makes a boring lecture environment, affects class success as well as faculty morale as learning declines and academic standards are compromised. Current methods used to manage class attendance which are mostly use of sign sheets have been abused by students signing for their counterparts. Further, they are known to be misplaced and represented later and therefore not presenting the actual status. Data analyses using the current method is cumbersome due to their manual nature and linking with timetable and classroom is also a big issue. This study proposes use of fingerprint biometric identification for class attendance. The students undertaking a given course are registered first then their fingerprints are captured and saved in a database. This is later used to identify students during class attendance for a given lesson. The developed system allows only registered students and it also helps to shows a student percentage attendance for a lesson thus helps easier manage and monitor the attendance policy. An experiment was conducted on the system accuracy, performance and effectiveness which showed the system is very accurate since the Weighted Error Rate from the sample was zero, the True Acceptance Rate was one and the Crossover Error Rate was at zero percent. Performance accuracy was achieved from the False Acceptance Rate and False Rejection Rate being at 0. The system was also able to allow all the users from the sample taken hence it is highly inclusive.

## TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>ii</b>
<b>ACKNOWLEDGEMENT.....</b>	<b>iii</b>
<b>ABSTRACT.....</b>	<b>iv</b>
<b>LIST OF FIGURES AND TABLES.....</b>	<b>vii</b>
<b>CHAPTER ONE .....</b>	<b>1</b>
<b>INTRODUCTION.....</b>	<b>1</b>
1.0 Background.....	1
1.1 Problem Statement.....	2
1.2 Justification.....	3
1.3 Objectives .....	3
1.4 Research Questions.....	3
1.5 Scope of study.....	4
<b>CHAPTER TWO .....</b>	<b>5</b>
<b>LITERATURE REVIEW .....</b>	<b>5</b>
2.0 Introduction.....	5
2.1 Characteristics of biometrics.....	6
2.2 Classification of biometric.....	6
2.3 Stages in Biometric registration and Identification .....	7
2.4 Existing methods of student attendance registration.....	8
2.5 Related Work .....	9
2.6 Conceptual Architecture .....	11
<b>CHAPTER THREE .....</b>	<b>13</b>
<b>RESEARCH METHODOLOGY .....</b>	<b>13</b>
3.0 Introduction.....	13
3.1 Research Design.....	13
3.1.1 Process Flow .....	15
3.1.2 User Interaction with the System.....	16

3.1.3 Database Design .....	19
3.1.4 Biometric System Design .....	20
3.1.5 Integration Approach.....	21
3.1.6 Experimental Design.....	23
3.1.7 Development tools.....	24
3.2 Target Population.....	24
3.3 Sampling Procedure .....	25
3.4 Sample size .....	25
3.5 Data Collection .....	26
<b>CHAPTER FOUR.....</b>	<b>28</b>
<b>RESULTS AND DISCUSSION .....</b>	<b>28</b>
4.0 Introduction.....	28
4.1 Experiment.....	36
4.2 Discussion .....	38
<b>CHAPTER FIVE .....</b>	<b>39</b>
<b>CONCLUSION AND RECOMMENDATIONS.....</b>	<b>39</b>
5.0 Introduction.....	39
5.1 Achievement of objectives.....	39
5.2 Challenges.....	42
5.3 Recommendation .....	43
<b>REFERENCES.....</b>	<b>44</b>

## LIST OF FIGURES AND TABLES

Figure 1 Biometric Registration Process .....	8
Figure 2 Conceptual Architecture .....	11
Figure 3 Prototype Development Method.....	15
Figure 4 Process Flow of the biometric class registration System. ....	16
Figure 5 Staff Use Case .....	17
Figure 6 Administrator Use case diagram .....	18
Figure 7 Student Use Case .....	18
Figure 8 Database Structure.....	19
Figure 9 Fingerprints Capturing and Verification .....	20
Figure 10 Biometric System registration and Integration Design .....	21
Figure 11 Home Page for Biometric System attendance .....	28
Figure 12 Signup page for administrators.....	29
Figure 13 Login page after Registration .....	30
Figure 14 Adding Student.....	31
Figure 15 Adding Unit .....	32
Figure 16 Biometric Enrollment .....	32
Figure 17 Biometric Login Page.....	33
Figure 18 Fingerprint Enrollment .....	34
Figure 19 Class Attendance .....	35
Figure 20 Check in.....	35
Figure 21 Attendance Policy Confirmation .....	36
Table 1 Experiment Results .....	37

# CHAPTER ONE

## INTRODUCTION

### 1.0 Background

Lecturing remains the most widely used method of sharing education content in institutions of higher learning since it has been shown to be the most economical and the highly productive way of transmitting knowledge. A tutor /lecturer stands in front of a class and share or read out content as students take notes. Through lecturing as while sharing a story, the listeners will show interest in what is being said and will grasp a lot and even use the same to educate others. Lecturers or tutors in a class facilitate and guide the learning process by analyzing and synthesizing complex materials simplifying it and making it clear in order to ensure that the learners grasp the contents of the said course or unit. They can also give different points of view creating independent thinking with the said topic. Other than listening to the tutor, the students also interact with their peers while attending classes (Bati *et al.*, 2013, Schmidt *et al.*, 2015).

Class attendance is therefore essential upon every student in order to receive information and get content of the said course or unit. Through class attendance, student's engagement and assimilation of what is being taught is measured and it has been shown that those who attend classes without fail are likely to perform better than their counterparts during final examinations. According to Foldnes, 2017, a clear and positive relationship exists between class attendance and course grades obtained by the students and can be used as the most accurate known predictor of final outcomes.

At the same time, class absenteeism has been a major concern in many institutions of higher learning and since lack thereof implies poor performance on the final exam. Larger classes especially are notorious for lack of attendance because of the inability of being noticed and smaller classes having higher attendance. Introductory courses as well poses high chances of non-attendance compared to upper level specialized courses. The scientific and mathematical courses have lower levels of non-attendance. Other than leading to lower performance in final exam, nonattendance leads to boring lectures and an overall feeling of dead classroom environment (Robert, 2007).

Class attendance can be used to reflect students' motivation with the course. Students cite various reasons for missing classes some which are institution related and others as personal. Some of the factors are availability of campus accommodation implying less travel time, scheduling of lectures



with lectures in early morning, Mondays and Fridays recording low attendance. On personal reasons, student participation during the lecture, social activities engagement, bad weather conditions, engagement with other assignments such as part time work, health, non-liking of the subject and having alternatives such as technology were some of the reason cited by Stripling, Roberts and Israel, 2013 and Kelly, 2012 for lack of attendance.

## **1.1 Problem Statement**

Stripling, Roberts and Israel, 2013 quoting Westrick et al. on class non-attendance explained 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 compromised. Further he explains as the academic term progresses and on particular days of the week like Friday as weekend approaches, class attendance reduces.

Existing methods of students attendance identification are mostly manual (i.e. use of paper sheets where students write and/or sign against their names) which are not only time consuming but also inefficient in that updating of student records and calculating percentage attendance for examination purposes is quite difficult. The system also lacks time on individual attendance records. (Saheed *et al.*, 2016). Other proposed automatic authentication methods have shown their downside including higher cost of implementation and additional resources for the faculty, students, staff and even the parents. The said automatic systems are also prone to abuse as students can share the Bluetooth tags, smartcards, phones with their peers to be marked 'present' for the lesson without having to attend class. Use of facial recognition technology has been known to be spoofed using photos to authenticate and hence grant access (Behara and Raghunadh (2013), Lodha *et al.*, 2015)

Even with compulsory student attendance policies that have been introduced in institutions of higher learning, the vice continues to be experienced and most institutions agree that non-attendance is the leading cause of academic failure (Guleker and Keci, 2014). Students have found a way of going round the existing implemented policies of ensuring a given percentage attendance is achieved by having other students stand in for them. Students not registered for particular

courses have also been found to attend the courses since the existing identification methods for registered students can be circumvented (Saheed *et al.*, 2017).

This study proposed a fingerprint biometric authentication mechanism of students registered for a given course that is less time consuming, is more accurate and ensures that the registered student attends at least two thirds of the course. The system also helps to get rid of impostors who would want to freely enjoy a course not registered for.

## **1.2 Justification**

It is paramount for every institution or faculty to ensure that students attend classes for registered courses because as argued by St. Clair, 1999, if students do not attend courses but pass their courses and obtain degrees, the institution's reputation is at stake. At the same time, if they do not attend which consequently leads to failure as shown by most researchers, it negatively affects the institution including decreased enrollment. In a white paper by Blackboard transact, 2015, lack of automated system for supporting attendance policies poses a risk to the institution on academic success, student retention as well as financial sustainability. For the general well-being of an institution and for its growth, it is important to monitor who and how course attendance is done.

## **1.3 Objectives**

The main objective of the study was to design and develop a system for class attendance that uses biometric for identification. The specific objectives were;

- i. To identify existing methods of identifying student's attendance and their challenges.
- ii. To develop a biometric system of student authentication during class attendance.
- iii. To test the developed system and understand its challenges.

## **1.4 Research Questions**

The research tried to answer the following questions;

- i. What are the existing methods of identifying student attendance and what are their challenges?

- ii. What authentication method is effective to ensure challenges in the existing methods are countered?
- iii. Can the system be applied in a classroom environment to ensure set minimum attendance is achieved and is there any challenge in its implementation?

### **1.5 Scope of study**

The study was conducted within a university set-up. The study was considered for one of the main courses and population was limited to around twenty students.

## **CHAPTER TWO**

### **LITERATURE REVIEW**

#### **2.0 Introduction**

When attending a lesson/course, students are identified to ensure that only the registered students are allowed in the classroom as well as ensuring the set policy for attendance is met. It is also important to have attendance register to ensure that the minimum stipulated period of course attendance by student is met. Identification acts a mean of protecting and maintaining integrity of systems world over. Identification as defined by Zarina and Abdel, 2015, is non-private information provided by the user to identify him or her and can be known by other system users. Common means of identification are names, user ID, E-mail address. To increase security, authentication mechanisms are used which contains both public and private information. Common authentication methods as outlined by Zarina and Abdel, 2015 are;

- a) Knowledge Based Authentication (KBA): they are commonly used form of identification especially while accessing online content. This requires knowledge of private information of an individual to access the content. Knowledge based authentication are advantageous in that they are inexpensive, simple to use and attractive to users. The cons of KBA is that it is susceptible to compromise through sharing as it relies on ‘what the user knows’ mechanism. Examples of KBA is user ID, password and challenge questions
- b) Possession based authentication: Employs ‘what a user has’ mechanism. It is mostly convenient in a well monitored environment such a school lab because the token used for identification may not be a true prove of ownership as it may have been stolen or duplicated examples are smart cards, memory cards and keys. Currently, smart cards are the most used form of student identification and more so during exams where attendance is also used to tell whether one should sit for exam or not. Smart cards are prone to compromise as stated above.
- c) Biometrics based authentication: Uses ‘what a user is’ mechanism. Users are identified using physiological and behavioral characteristics. These characteristics includes fingerprints, face, iris and retina (also known as hard biometrics) and soft biometric characteristics such as voice, signature and keystroke.

Biometrics remains the most secure and safe means of authentication since tokens can be stolen and presented by another person while passwords and usernames can be shared as a sign of good gesture or 'friendship'. For biometrics, the user has to appear in person to be authenticated. (Tiwari, Tiwari and Tiwari, 2015)

## **2.1 Characteristics of biometrics**

According to Tinyari et.al. 2015, all biometric schemes should possess characteristics that are widely accepted such as

- Universality where each person should possess the characteristics.
- Distinctiveness; different individuals can be differentiated based on the feature.
- Permanence: the feature should remain throughout as a way of identifying the individual. The properties thereof should be constant over a given period of time regardless of age.
- Reducibility: Data should be reduced to a file easy to handle and/or store.
- Tamper-resistance: the captured data should not be manipulated.
- Privacy: The biometric process should not violate the privacy of the individual

Biometrics can be used as a way of identifying an individual without knowledge or consent of the individual and on the other hand to verify a person with full knowledge of the party in question. Students' attendance identification will be done with knowledge since the first step will be registration of fingerprints then identification.

## **2.2 Classification of biometric**

According to Kant & Dr. Nath, 2006 and Tiwari et al., 2015 biometrics system can be classified as follows;

- Unibiometric where it uses only a single biometric identifier,
- Unimodal biometric that uses a single instance, single representation and a single matcher for a recognition decision.

- Multibiometric system; uses more than one physiological or behavioral characteristic of a biometric identifier of the same individual for enrollment, verification and identification.
- Multimodal Biometric: uses more than one correlated biometric measurement such as multiple facial images, multiple impressions of a finger to provide foolproof identification thereby reducing false ejection and false acceptance rates.

### **2.3 Stages in Biometric registration and Identification**

A biometric device with a sensor collects the data for an individual i.e fingerprint, retina, voice and others depending on the choice. This data is compressed and transmitted to a storage location and is later used for identifying the individuals. A decision is later made from the stored information on whether the access is granted or not depending on the information stored in the database. It is important that the information collected by the sensor/the biometric device is of high quality to reduce instances of False rejection and false acceptance thereby compromising what was being secured (Tiwari et al. (2015), Kant & Dr. Nath (2006))

The two stages of biometric registration

- i. Enrollment/ Identification: The user initial sample is taken using the biometric registering device for future processing. The sample is compressed and stored in a database of users.
- ii. Verification/authentication: the identified users are authenticated against the database of existing samples to certify whether they are genuine users or not. If the degree of similarity is high, access is granted otherwise the user is rejected.

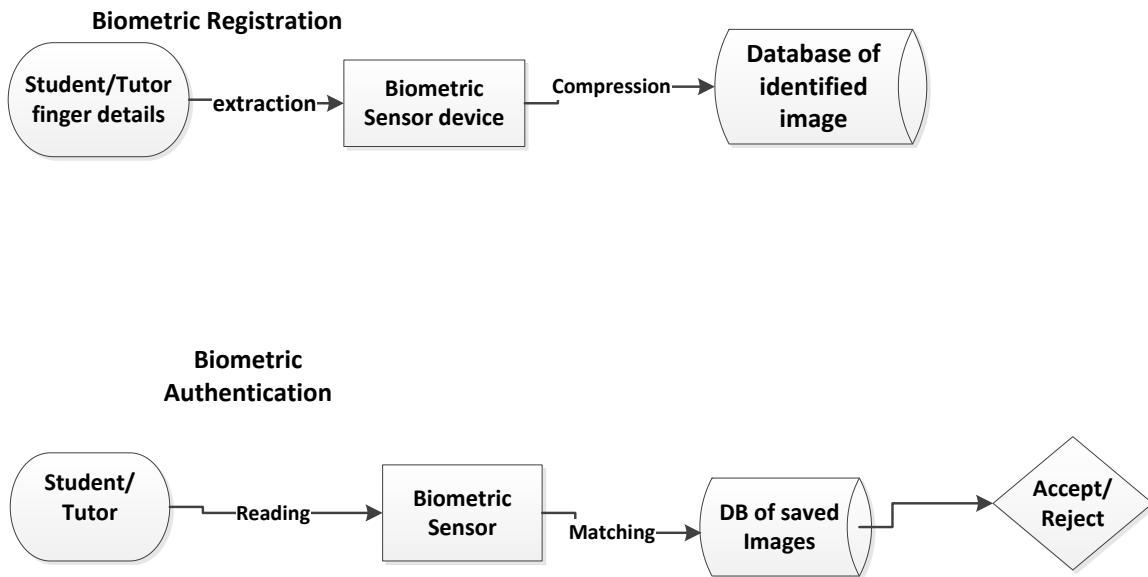


Figure 1 Biometric Registration Process

## 2.4 Existing methods of student attendance registration.

The existing student attendance registration methods in most higher learning institutions are manual where attendance is recorded in hand written registers. Saheed *et al.*, 2016 cites some of the challenges with the method is when it comes to the retrieval of the information. Students put their information i.e name and registration number on a piece of paper or the lecturer provides a list of enrolled student and their registration details to the students and the students have to sign against their names.

### Challenges

- Because of the manual work involved, transfer of the registered information to other systems for analyses is very tedious and time consuming. Further, the collected information is not used to help improve course timetables and classroom bookings. While using the current system, it is hard to tell at what point students came in i.e. whether early during the lesson or later just to sign.
- The process is error prone since students have been found to sign for their peers therefore accuracy is 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.

Another method used to identify student attendance is by use of smart student cards. Where class attendance is in a controlled area, students are issued with smart chip card which they can use to get access to the class room. While this method is easier in that the students details are captured and saved in a system including the time the student came in for the class, it is still has the challenges of students sharing the card or having another student clock in for you even while one is away. This method is highly employed in organization to clock in working hours for employees (Bhalla *et al.*, 2013).

Student attendance has also been considered by having lecturers call out students name and the student confirm their presence. This is only suitable where the class size is small. Where the class size is large as is common with most common or elementary courses, it is not only a hassle for the lecturer to call out all the names of the students but it is also time consuming and would end up eating most of the time meant for the lesson (Awedh and Mueen, 2015).

## **2.5 Related Work**

Bhalla *et al.* (2013) developed an electronic system for student registration using Near Field Communication (NFC) technology. The developed application is required to be installed on a student phone. The students register on to the system by providing their ID number which later takes them to a screen showing their university number. The phone is required to be slide next to the NFC tag where information regarding location of the student is displayed and later show if registration is successful or not. The drawback with this method is that all students must have a smartphone for registration to take place. On the other hand, one can just share a phone and their ID number with their peers in order to undertake attendance for them.

Another system, Bluetooth Based Attendance Management System, was proposed by Lodha *et al.*, 2015 that makes use of Bluetooth wireless technology to authenticate students. A Bluetooth smart chip is programmed and configured to work with android application via Bluetooth. Students are



issued with unique tags that can be detected by the application using Bluetooth. Once they attend the lessons, a serial number of the tag is registered in the student database with a timestamp. The lecturer moves around the class with the application detecting the tags and registering in the database along every student record. This system is also prone to abuse since student can give out their tags for them to be detected even when not attending class. Since it depends with movement of the lecturers as Bluetooth is range based, very large classes can be cumbersome for the teacher.

An attendance system that incorporates RFID and facial recognition was proposed by Patel and Priya (2014). The RFID was used for attendance taking and facial scanner used for verification. The reason is that RFID has long read range and facial recognition also has long distance reading. The students are given identity cards with RFID tags 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 marked absent. The disadvantage with this system is that it can be expensive since you need several devices i.e. an RFID reader and a camera. A bigger database also required to record the facial images which also lead to increased costs.

Behara and Raghunadh, 2013, proposed a facial recognition time and attendance system that uses Viola-Jones face detection algorithm for face detection and simple PCA/LDA algorithm for feature extraction and recognition. The system records the individual after facial recognition in an excel sheet. This also includes the time and date of arrival. The system is likely to be spoofed where one can represent a photograph of a user instead of a real person and the system allows or mark the presence of the individual. The computational complexity of this system is also high.

Somasundaram, Kannan and Sriram (2016) developed an android mobile based 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 users' registration, login module and SMS module which is used to send an SMS to the parents notifying them of students' presence or absence. The airdroid module is used to receive text messages from students notifying about their leave. For this system to work effectively, it requires additional resources from both students, staff and parents where each must have an android phone to communicate students' attendance status to both parents and students.

## 2.6 Conceptual Architecture

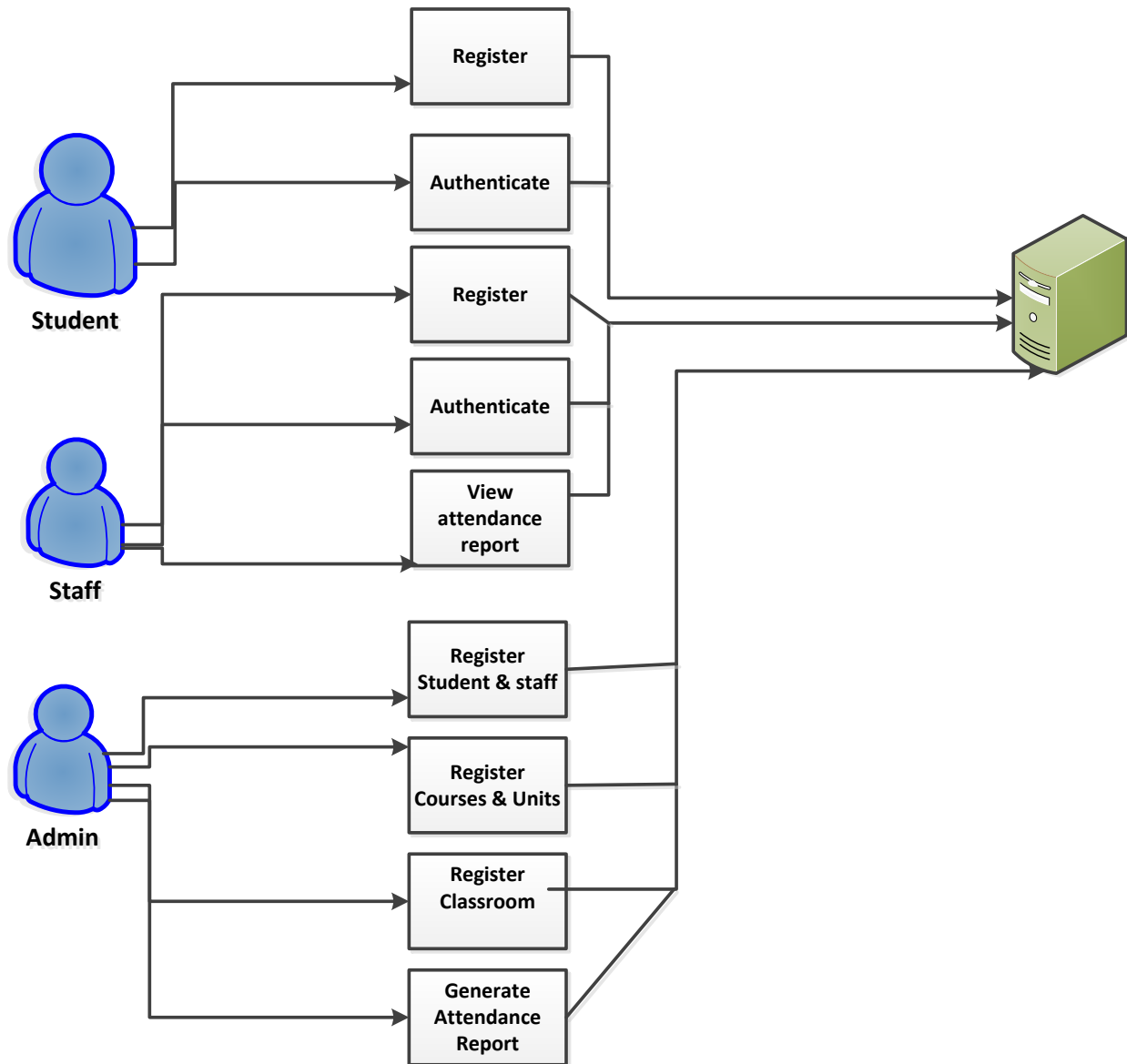


Figure 2 Conceptual Architecture

The student and staff fingerprint details were captured using the biometric device by the course administrator. The image were saved in a database with the name, student Identification number

or staff number. The administrator also registered courses, units in the course, lessons and where the lessons were conducted i.e. classroom. During class attendance, the staff and students were required to authenticate with the biometric kit. If the fingerprint matched, the lecturer was allowed to conduct the lesson and the students were allowed to attend the lesson. Otherwise, they are required to clear with the administrator. The administrator could also view the taken lessons and print a report in order to analyze the percentage attendance by the staff and students.

## **CHAPTER THREE**

### **RESEARCH METHODOLOGY**

#### **3.0 Introduction**

This section gives details on procedures used to conduct the study. Issues outlined here includes research design, sample size, sample procedure, methods of data collection, validity and reliability of research instruments as well as the data analysis procedure.

#### **3.1 Research Design**

According to Tobergte & Curtis (2013), a research design is “the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with the research. The design selected in this case was quantitative research design. The type of research employed is applied or action research which aims at finding a solution to an immediate problem facing a society or an organization. This type of research aims at solutions facing a social or business problem, identify social or economic trends that may affect a particular institution (C R Kothari, 2015). In this case, the research helped to solve the problem of class non-attendance or unregistered attendance through impostors in institutions of higher learning. This type of research was also descriptive in nature in that it had specific predictions with narrations of facts and characteristics concerning an individual i.e. students and lecturers taking or conducting a given course respectively.

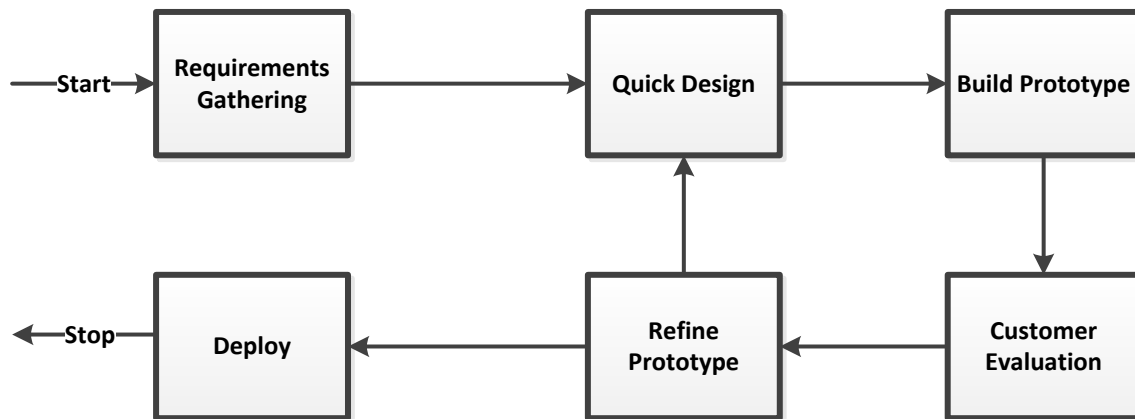
In this descriptive study, the researcher identified individual characteristics of students registered for a particular course or unit using their fingerprint i.e. “what an individual is” mechanism other than “what an individual has” and “what an individual knows” which have been prone to compromise through sharing and thus affecting the integrity of the process. This mechanism was adopted because it is not prone to abuse (Tiwari, Tiwari and Tiwari, 2015).

The system was developed using incremental prototype method where development was done using the known requirements and refined with time through continuous involvement of the users of the system i.e. administrators, staff and student to better understand their needs. User feedback was acquired as several modules were created. The stages involved were;

- Requirements gathering : This involved interaction with the stakeholders of the system mostly administrators to get to understand much on the registration of the course, units and classroom allocations. The researcher established the various roles undertaken by each user in order to effectively capture them in the system. This also helped to get a perspective of the number of students to be used for the study. The scope set to 20 students since only one biometric device was available. The course administrator was advised on their role of registration and provision of student and staff data for BSC IT course for year one semester one. The tutor role of viewing the various courses, unit, and students' and the attendance policy was also taken in to consideration. The students played a passive role where their details needed to be captured in the system.
- User design: This involved initial setup of the system database with the main table which is the users table and the various fields involved. Other tables were setuo and the various fields linking them with the main table. An entity relationship diagram was constructed showing how various components of the table relate with each other. After database design, quick design of the web-based system to be used by the administrator for registration process was done. The design of the biometric registration was also done. The modules involved were considered as well and the inter-relation of the several modules.
- Construction (Prototype): development of the said biometric and web based system was done module by module i.e. iteratively. The module were interlinked and interconnected through the database. Construction was done using PHP language for the web system and java for the biometric system. MySQL was used for the database. As development progressed, module testing was done for the components to ensure the expected results were achieved and if user requirements were met as well.
- Customer Evaluation: The constructed system was delivered to the stakeholders mainly the administrator to see if the requirements had been met. Each constructed module was evaluated to see if the user were satisfied with the deliverable and if requirements had been met. Any concern and non-functionality was noted. New ideas were embraced after re-engagement with better understanding
- Prototype Refining: Continuous refining was done after re-engaging the users and understanding the requirements more. a redesign was done to fit with the newer requirements. The various modules were redone with the concerns addressed. The

administrator was engaged to know if the requirement were satisfactory. and the after satisfying the requirement and testing each module

- **Deployment:** The constructed system was later user to perform the experiment with twenty students in BSC IT. The administrator performed users (student and staff) registration as well as courses, units and classroom. The administrator also performed the fingerprint capture for the students where later they would be allowed to attend lessons.



*Figure 3 Prototype Development Method*

### **3.1.1 Process Flow**

This specifies the steps taken in the system in order to achieve the objectives.

- i. Administrator registered as a user on the web based system after which they logged on to the system.
- ii. Administrator captured other users of the system who were students and tutors undertaking or teaching BSC information Technology.
- iii. The administrator captured the units.
- iv. The administrator log to the biometric system.
- v. The registered students had their fingerprints enrolled in the biometric system by the administrator using the registration or staff number as the reference.
- vi. In the biometric system, the users were verified if their fingerprints had been captured using the staff number or the student registration number.
- vii. The users' fingerprints were identified with the biometric device for class attendance.

- viii. The student access the attendance system and select the course which showed the lessons of the course that were ongoing at that time and the venue.
- ix. The student checked in to the system to attend the lesson that was ongoing at that particular time.
- x. An attendance report was generated by the system and the administrator log to the web based system to view the attendance report and the policy.

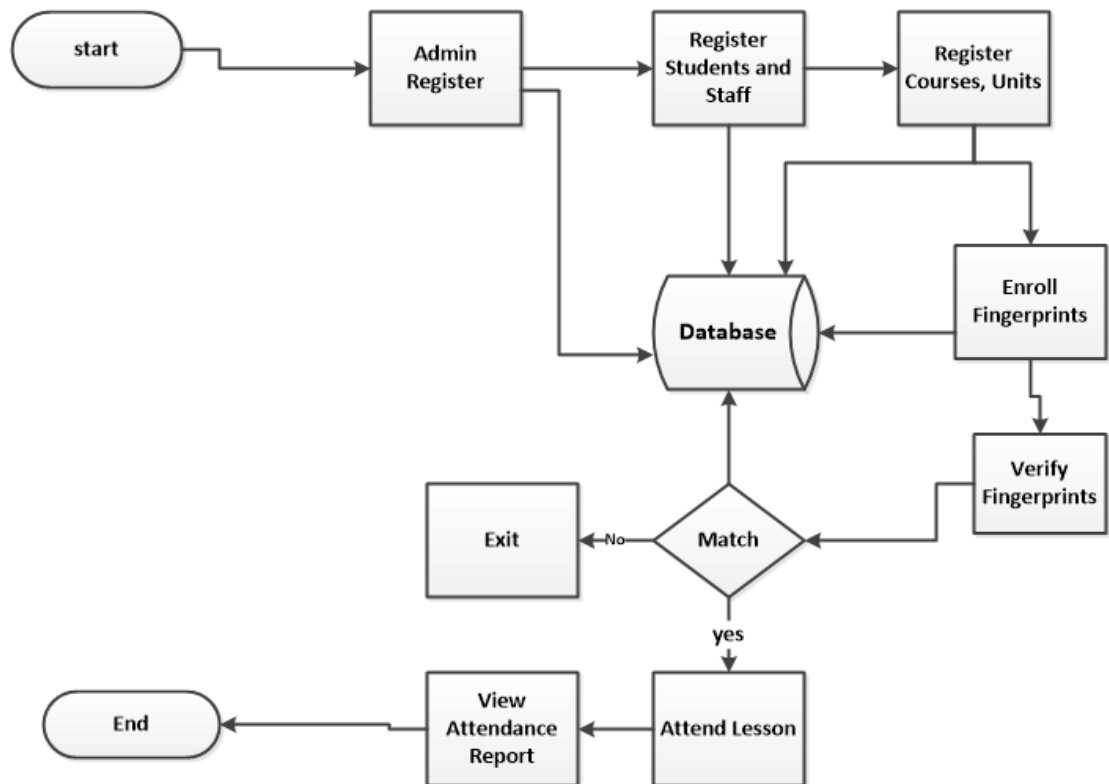


Figure 4 Process Flow of the biometric class registration System.

### 3.1.2 User Interaction with the System

This shows the functional overview of the system in a use-case diagram

The different actors of the system are;

- a) Administrators: the role of the administrators is to add students and staff, courses, units to the system. They can also update the records in the database. They can also view system reports.
- b) Students: these will be registered to the system by the administrators and will be required to perform class attendance.
- c) Staff (Lecturers): these are the people who conduct the lessons. They can also view reports on class attendance to ensure that the stipulated attendance policy is maintained.

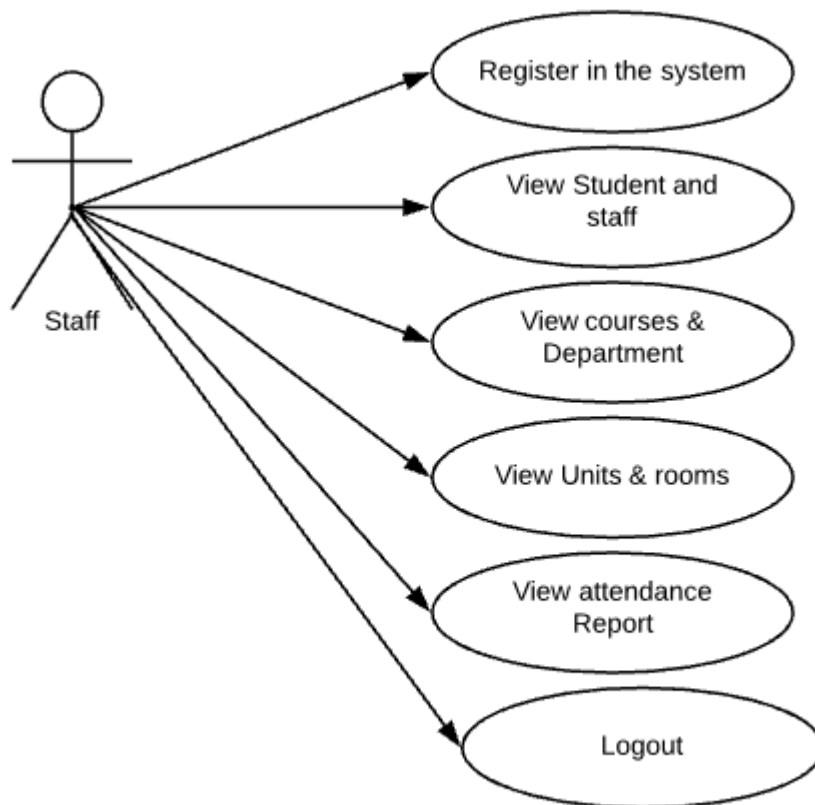


Figure 5 Staff Use Case

After registering in the biometric system and logging in, a lecturer or tutor is able to view the students taking the course as well as fellow colleagues teaching within the department. The lecturer would also be able to view courses, units, rooms where the lesson is taking place and the attendance report of each student in order to know if they have met the required policy or not and hence if they qualify to sit for the exam for that unit.



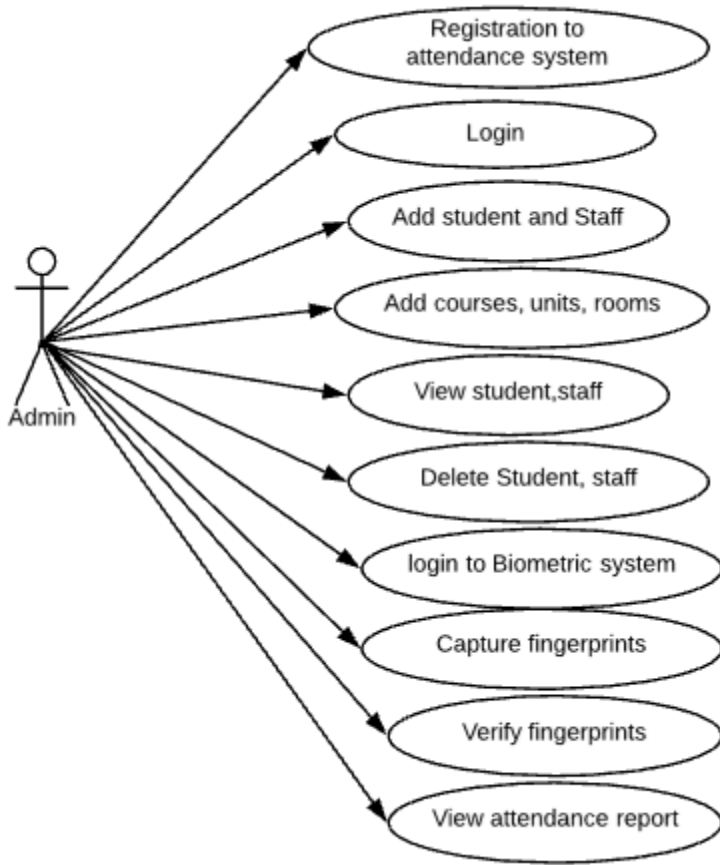


Figure 6 Administrator Use case diagram

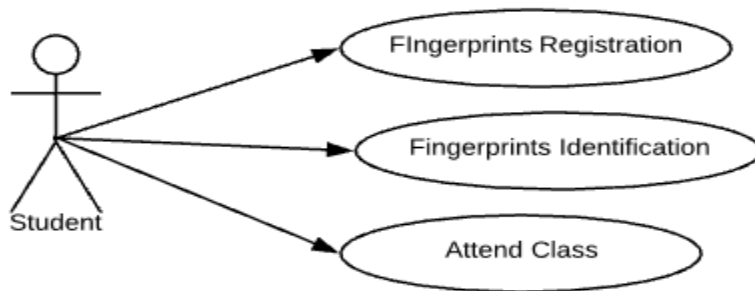


Figure 7 Student Use Case

### 3.1.3 Database Design

The database was designed using MySQL database. The main table of users was linked with other tables on a one-one or one-to-many relationship.

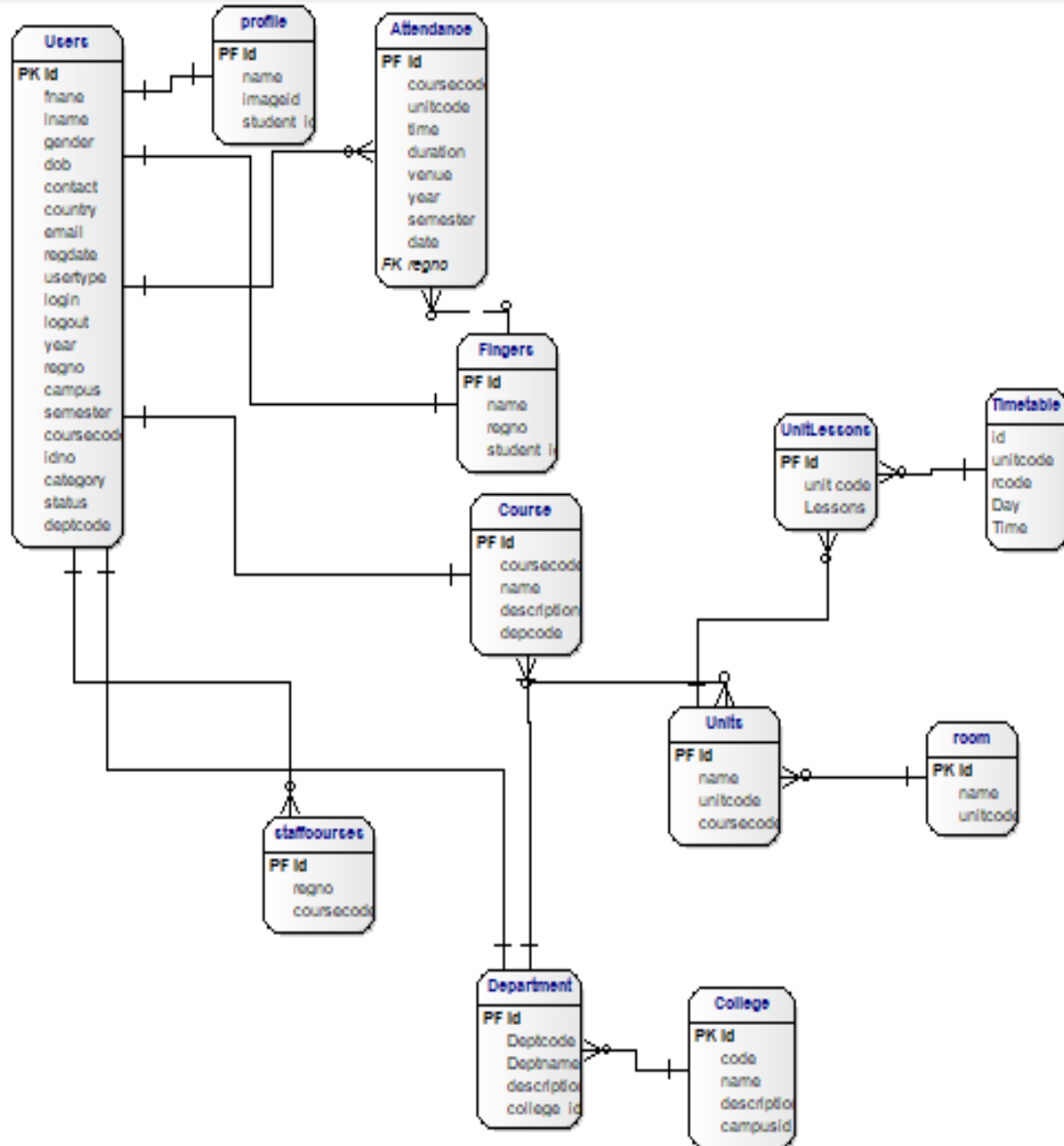


Figure 8 Database Structure

### 3.1.4 Biometric System Design

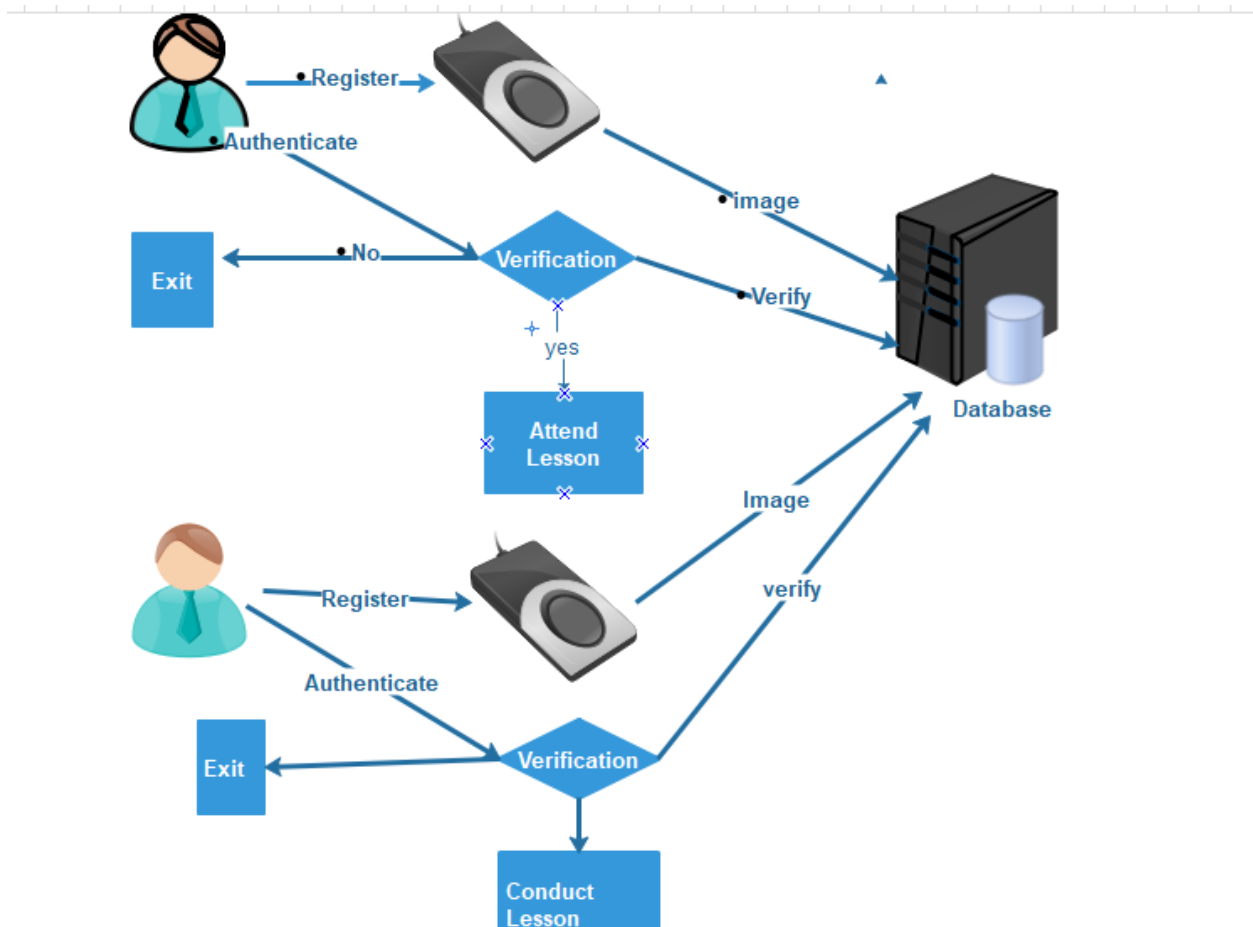


Figure 9 Fingerprints Capturing and Verification

A biometric device was used to register students information by the administrator i.e. fingerprint details of the students who have registered to sit for a particular course or unit and their information will be saved in a database. Information of the tutors who teaches a given unit was also registered using the biometric device. Before being allowed in a class, the registered students were identified using the biometric device. If the details of the students were available in the server database of the registered students, they were allowed to attend the lesson. If the student details were not found, the device would give an alert to the verifier through a beep sound that the student is not authenticated. The student not verified would be expected to clear with the administrator in case of any inaccuracies or unregistered user. The lecturers were also registered with the device so that only those authorized to conduct a particular course are allowed in the classroom.

The course administrator registered staff and students, added units, courses, lessons as well location where the class was conducted. The lecturer would view lessons courses, students, room, campus, department and view attendance report.

### 3.1.5 Integration Approach

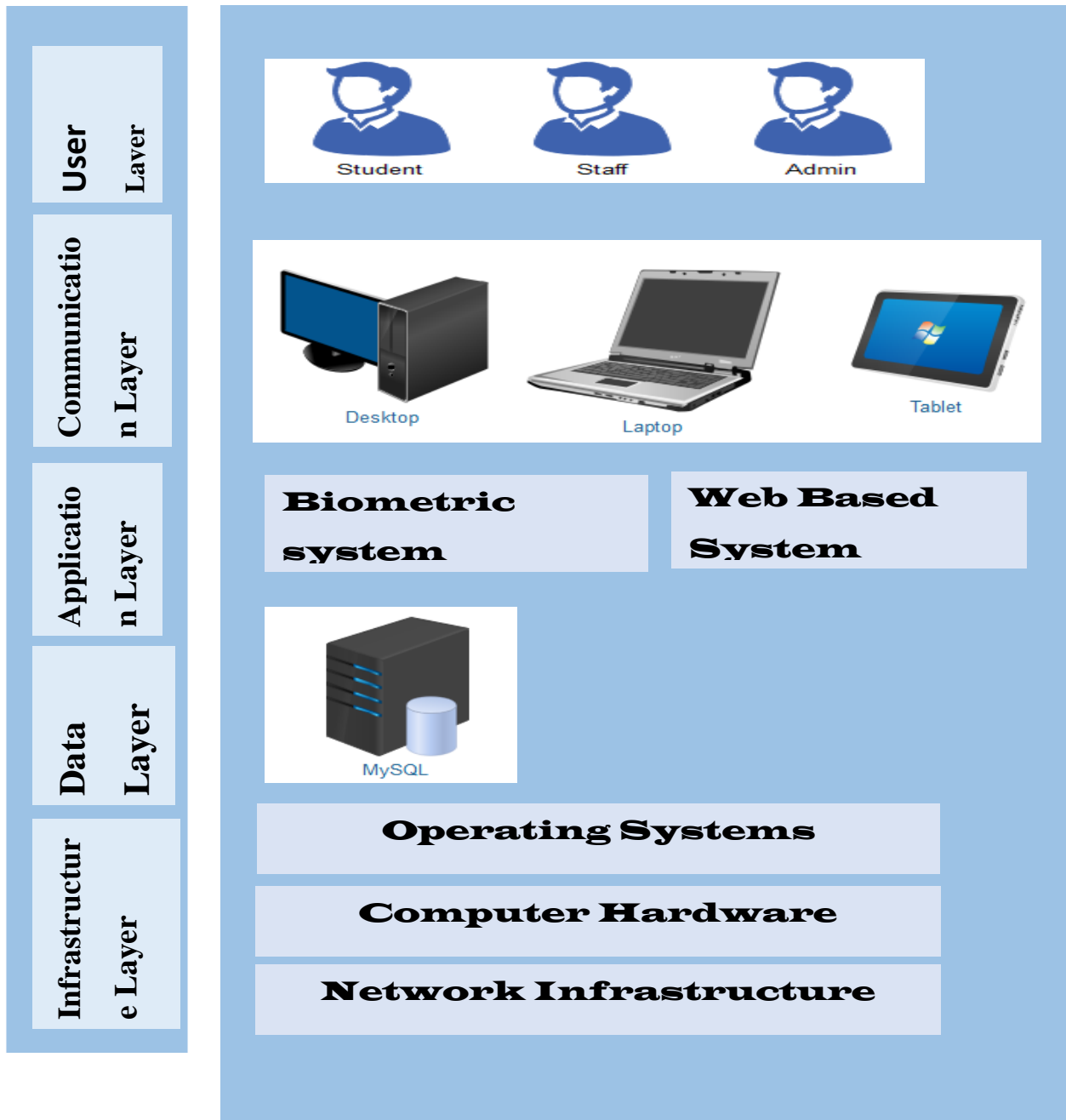


Figure 10 Biometric System registration and Integration Design

The integration process has got several layers which includes user layer, communication layer, application layer, data layer and the infrastructure layer.

Form the user layer, the administrator used either a desktop, a laptop or a tablet to capture student or staff details including names, registration number, course, or unit. The same was used for registration of units and courses. The biometric device was attached to the computer or laptop through a USB cable and the administrator captured biometric images which were recorded in MySQL database. The database also recorded the captured student and staff details, courses and units available as well as the room assigned to a particular course or unit. The database used was a local database. In the school environment, we need to do data transfer to the database in the data center using wireless or Ethernet medium. If Ethernet is to be used for connection, a cat6e UTP cable is required plus a port where the administrator is required to plug in the cable. If wireless medium is to be used for connectivity, the administrator is required to have credentials to allow access to the wireless network. The network structure is expected to be in place and in stable working conditions. The computer is expected to have an operating system windows or linux in place. The OS used in the project in a virtual environment was windows 7 professional, 32 bit.

In the application layer, a web based attendance management system was put in place that acted as an interface for adding student and staff details by the administrator. The administrator first registered as a user after which they could login to be able to capture the details. The administrator added units, courses, rooms and departments from the same place. The administrator was also able to check-in student class attendance through this web application as well as viewing the attendance report. The captured details were transferred to MySQL database. The biometric fingerprints system was used to capture the student and staff biometric images which were saved in the same database. MySQL connector for java was used to link the system with the database. SDK pro for java was used in connecting the biometric system with the fingerprint device. The fingerprint image captured was the thumb and index fingers. In the biometric system, the captured images were identified and verified in the database.

Other network infrastructures required are switches and servers in a network system which would assist in relaying and housing the captured data. The data can then be retrieved when or as required.

Security of the system was catered for from the operating system, and the application level where only the authorized users were given access to the system. The server housing the database requires authentication and is to be stored in a secure data center. Physical security is also considered for the biometric device and the PC or laptop where the administrator is required to take good care of the devices. The biometric registration is also to be undertaken in a secure environment like a classroom set-up.

### ***3.1.6 Experimental Design***

While verifying the biometric images, the system was tested for its accuracy on positively identified users or lack thereof.

The experiment was measured using the following performance metrics;

- **The false positives or False Acceptance Rate (FAR):** This is where an impostor is incorrectly matched to a genuine user template stored within the biometric system. This reflects the ability of non-authorized users i.e. student or lecturers to access the biometric system through no effort or using spoofing methods. (Academy and Point, 2012)
- **The False Reject Rate (FRR)/False Negatives:** this is where a genuine user is incorrectly rejected from a biometric system. This may occur as a result of user presentation error or corruption of previously enrolled authentication templates. (Academy and Point, 2012)
- **Weighted Error Rate (WER):** Weighted Error Rate is the sum between the False Acceptance Rate and the False Rejection Rate. (Poh *et al.*, 2012) In equation form, Weight Error Rate is expressed as follows;

$$WER = FAR + FRR$$

- **True Acceptance Rate (TAR):** Probability that the system correctly matches a genuine user. A measure of accuracy defined as follows

$$TAR = 1 - FRR$$

- **Failure to capture rate:** Within automatic systems, the probability that the system fails to detect a biometric input when presented correctly (Academy and Point, 2012).
- **Crossover Error Rate (CER):** Percentage rating of FRR versus FAR. A lower CER indicates better matching accuracy.
- The non-cooperative users were those from the population but refused to participate in the exercise for one reason or another.
- The unidentifiable users are those whose fingerprints cannot be captured because they are not present or the fingers are not in a good state.

### ***3.1.7 Development tools***

The project was developed using open source tools. The system was developed on a windows platform whose operating system was windows 10 pro with 64-bit OS, Intel core i3 processor and 4GB Ram. XAMPP version 5.6.12 was used on the server side integration which contained MySQL version 5.6.26. For the web based system, the language used was PHP version 5.6.12. On the biometric side, java programming language was used with java development kit (JDK) version 8 and NetBeans IDE 8.2. For the fingerprint device FDX SDK pro for java was used. Secugen Hamster Plus Fingerprint Reader was used as the biometric device.

The web based system was run and tested on a standard web browser environment while the biometric system was run on and tested on a Java runtime Environment.

## **3.2 Target Population**

A population is defined as a complete set of individual cases or objects with some common observable characteristics, it is the population to which the researcher wants to generalize the results of the study (Mugenda and Mugenda, 2003).

The target population was students from Jomo-Kenyatta university of Agriculture and Technology (JKUAT) in the school of Computing and Information Technology undertaking BSC in IT, year one semester one undertaking a unit Introduction to Computers. The population also targeted were

the lecturers that are responsible for training BSC Information Technology. Course administrator for BSC IT were also a target as they were concerned with registration of both students and lecturers on the biometric toolkit, course and unit registrations as well as classroom allocation.

### **3.3 Sampling Procedure**

**Sampling** is the process of selecting a few (a sample) from a bigger group (the **sampling population**) to become the basis for estimating or predicting the prevalence of an unknown piece of information, situation or outcome regarding the bigger group. A sample is a subgroup of the population the researcher is interested in (Kumar, 2015) .

A sample design is a definite plan for obtaining a sample from a given population. It refers to the technique or the procedure the researcher would adopt in selecting items for the sample. Sample design may as well lay down the number of items to be included in the sample i.e. the size of the sample. Probability sampling and purposive sampling were employed. Probability sampling is the type of sampling where every item within the sample has equal chances of inclusion in the sample and has no chance of appearing again in the sample once selected whereas purposive sampling where items are selected deliberately by the researcher (C R Kothari, 2015).

From the group of students undertaking BSC IT in first year first semester, a random number of students were selected from the student nominal roll to participate in the study where they were registered and authenticated using the biometric device. On the other hand, the tutors were chosen on purpose i.e. those that teaches BSC IT.

### **3.4 Sample size**

Sample size refers to the number of items to be selected from the universe to constitute a sample. The sample size should be optimum in that it should fulfills the requirements of efficiency, representativeness, reliability and flexibility (C R Kothari, 2015). A sample of up to twenty students was considered for the study depending on the size of the class. For effective working with the biometric device, the sample size of the class was limited to twenty to ensure that registration and authentication was taken using the least time possible. In real environment and



where the class size is large especially the common courses, one would require several biometric devices/scanner to identify the students. All the tutors teaching the BSC IT were considered when selecting the sample

The sample size was calculated using the following formula;

$$n = N/(1 + Ne^2)$$

- n is the sample size
- N is the population size
- e is the confidence interval

The entire class comprised of 87 students undertaking BSC Information Technology year 1. Since the population size is known, we don't need the standard deviation. The confidence interval used was 95%. Thus the sample size was calculated as;

$$\begin{aligned} n &= 87 / (1 + 87 * 0.05) \\ &= 87 / 5.35 = 16.26 \end{aligned}$$

The sample size settled for was twenty students. Since the nature of the universe was homogenous the sample size required was not large. The other factor that influenced the selection of the sample size was the nature of study and this being a technical study, a sample size of twenty students was sufficient.

### **3.5 Data Collection**

Secondary data was used to get the list of students that are in the nominal roll. The BSC IT course administrator was responsible for registering students and considered the students that had signed the nominal roll for registration with the toolkit. The administrator also considered the lecturers that have been authorized to train BSC Information Technology. From this data, primary data was collected through direct interaction with the respondents. Student and tutor information i.e. fingerprints were captured using Hamster Plus Fingerprint scanner and saved in MySQL database. While taking and conducting the lesson, the students and lecturer details were verified against what was saved in the database.

The researcher observed whether the student was authenticated and in case the data was not in the database, an error was displayed showing their details had not been registered. This allowed students to clear with the course administrator where they could either be registered after confirmation that they were in the nominal roll, otherwise they left. The same was done for the lecturers.

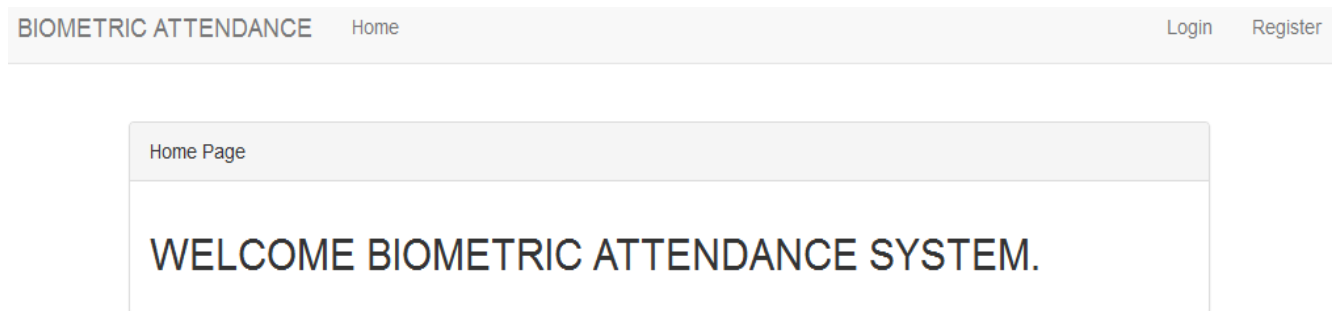
## CHAPTER FOUR

### RESULTS AND DISCUSSION

#### 4.0 Introduction

This chapter describes the results of the prototype development which is the web and biometric system as well as the experiment results.

a) Home page



*Figure 11 Home Page for Biometric System attendance*

At the home page, the users has the option of either registering or logging in to the system. A first time user was required to first register in the system i.e. sign up. If not a new user, one was just required to login to the system. Only administrators and staff would be allowed to use this section.

b) Administrator Registration

The administrator creates own account after which they login using their Pf number.

The image shows a web form titled "Create Account" for administrator registration. The form contains the following fields and values:

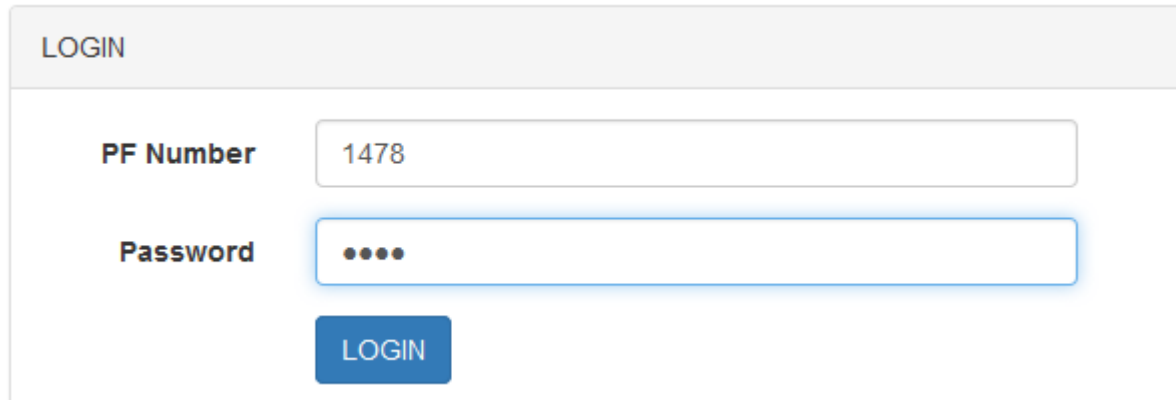
- First name:** Ann
- Last Name:** Mukeha
- PF Number:** 1478
- Jkuat Email:** Ann@jkuat.ac.ke
- Phone Number:** Enter contact Number
- Id Number:** idno
- Campus:** Jkuat Main juja
- usertype:** Admin
- Password:** Masked with four dots

A blue button labeled "REGISTER" is positioned below the password field.

Figure 12 Signup page for administrators

During registration, the user specifies if they are administrators of the system or staff (Lecturers) since the operations are different for staff and administrators. After filling in all the details, the users who are members of staff (lecturers or administrators) in the IT department click the registration button which allows the details to be saved in the database of users in the user table. They can then login using the form below.

c) Login Page



The image shows a login form with a light gray header containing the word "LOGIN". Below the header, there are two input fields. The first is labeled "PF Number" and contains the text "1478". The second is labeled "Password" and contains four black dots. Below the password field is a blue button with the text "LOGIN" in white capital letters.

*Figure 13 Login page after Registration*

The login page is used by either the lecturers or the administrators who are members of staff in the IT department. Depending on the user profile, the staff can perform various roles after logging in. For the lecturers, they are able to view students, courses, units, rooms, campus and the departments. The lecturers are also able to view attendance of students.

The administrators profile has got more role since you not only view the various functions but also are allowed to do addition or deletion from the various fields. In addition to the fields that the lecturers can add, the can also add the timetable of the various units using the unit code and the day and time where each is being conducted and this is saved in the database on the timetable table. There is also a section for the recommended lessons for each lesson/unit which the administrator uses to add or update the lesson and/or the lesson hours of the unit and saving the results in the lessons table in the database.

d) Student Registration

ADD STUDENT	
<b>First name</b>	<input type="text" value="Enter First Name"/>
<b>Last Name</b>	<input type="text" value="Enter Last Name"/>
<b>Registration Number</b>	<input type="text" value="sct211-1234/2017"/>
<b>Jkuat Email</b>	<input type="text" value="Enter Your Email"/>
<b>Phone Number</b>	<input type="text" value="Enter contact Number"/>
<b>Id Number</b>	<input type="text" value="idno"/>
<b>Campus</b>	<input type="text" value="Jkuat Main juja"/>
<b>Course</b>	<input type="text" value="BSc. Information Technology"/>
<b>Department</b>	<input type="text" value="Department of Information Technology"/>
<b>Category</b>	<input type="text" value="student"/>

Figure 14 Adding Student

This adds a new student and save the records on the user table in the database. All the fields are captured including the year of study and the semester. I.e. year one and semester one for this particular study.

The same is used for adding a staff only that the category changes where the administrator selects the staff category from the drop down box.

e) Add Unit

Unit

**Course Name** BSc. Information Technology

**Unit name** Unit Course name

**Unit Code** Enter Unit Code

Add Unit

Figure 15 Adding Unit

The administrator used this page to add the various units for year one semester one in the BSC information Technology course. The unit name used for the study was Introduction to Computers and the Unit code was Bit221. The units were saved in the database under the units table.

f) Biometric Intro Page

Welcome!

Go To Enroll

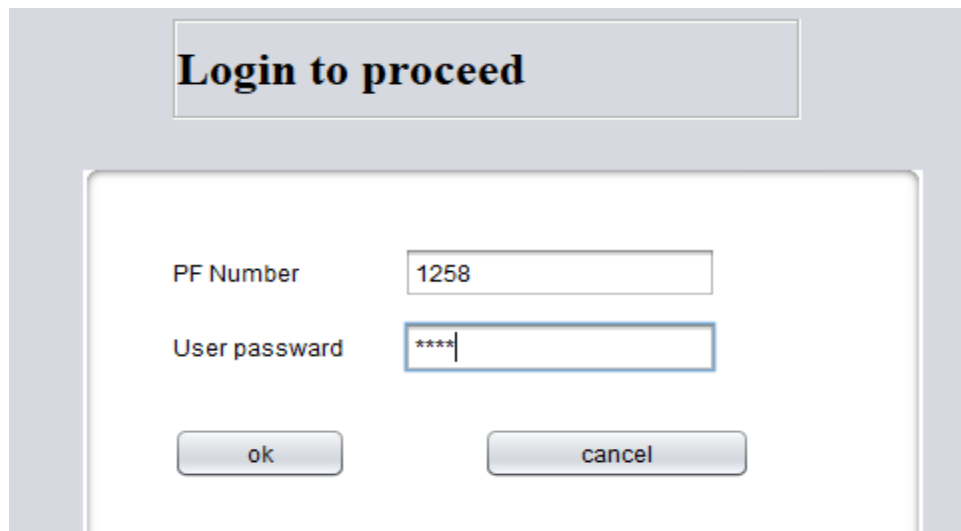
Go

Figure 16 Biometric Enrollment Welcome Page

For the biometric introduction page, a drop down button where one chooses to either enroll the fingerprints or attend class. Enrollment has to be done before after which, one is allowed to attend the class. The teachers and administrators also enroll their fingerprints. After clicking the enroll

button, the system asks for the login credentials so that not anyone is allowed to do the enrollment or capturing of the fingerprints. This is a security measure in order to ensure that only the authorized users (Administrator) can capture the fingerprint records of either the students or the staff. The fingerprint login page is shown below.

g) Login Page



The image shows a login dialog box with a title bar that says "Login to proceed". Inside the dialog, there are two text input fields. The first is labeled "PF Number" and contains the text "1258". The second is labeled "User password" and contains four asterisks "\*\*\*\*". Below these fields are two buttons: "ok" on the left and "cancel" on the right.

*Figure 17 Biometric Login Page*

For the administrator to be allowed to register users, their details must already have been captured in the database during the sign-up process. These details are retrieved from the database on the user table. The system allows access only if the PFNo given and the password corresponds with what is in the database. Once the details match, the administrator does the fingerprint scanning using the form below.



## h) Fingerprint scanning

The screenshot shows a web interface titled "Enroll Page". At the top right, there is a button labeled "Go to Attendance". The main form area includes a "Verify" button next to an input field for "ENTER REGISTRATION NUMBER/ID". Below this is a dropdown menu for "FINGER NAME" with "LEFT THUMB" selected. Two large rectangular boxes are provided for fingerprint scans, labeled "SCAN 1" and "SCAN 2". At the bottom center, there is a "SAVE" button.

Figure 18 Fingerprint Enrollment

The registered users enrolled their fingerprints using the staff number for staff or registration number for the students. After putting the registration number, the users were verified whether they were in the system. If the registration number or staff number is not in the user database, it means their details had not been captured as students/tutor in that class and an error is displayed to enter a valid pf/registration number. Scanning of fingerprints cannot happen since the fields are inactive. Only when a genuine registration number is entered are the scanning fields activated. If they were in the system as genuine users, they were allowed to enroll their fingerprints. The finger being scanned is selected from the dropdown button. Up to ten fingers could be scanned for one individual and the image template was saved in the fingers table in the database. Any finger scanned had to be confirmed by scanning the second time and if there was a match, the image was saved in the database and the user is alerted of success. After successful enrollment of the fingers, the administrator would then click on the “Go to Attendance” button above the page where they are taken to the class attendance page below.

i) Class Attendance

JKUAT CLASS ATTENDANCE SYSTEM

SELECT COURSE: Bsc Information Technology

SELECT ROOM: LEC HALL 1

Proceed

Figure 19 Class Attendance

The student is expected to select the course they are undertaking from the drop down box and the room where the class is being conducted. Once a room is selected, the system chooses the unit that is being conducted in that room. The student is then allowed to proceed to the check-in page where they are authenticated to attend the lesson.

j) Check-in

CURRENT UNIT NAME: Introduction to computers

CURRENT UNIT CODE: bit221

CHECK IN

Classmates in class

sNo	RegNO	First Name	Last Name	Time In
1	sct211-0006/2017	Willis	Gitangu	14:12
2	sct211-0004/2017	Joseph	Waweru	14:12
3	sct211-0003/2017	Brian	Maina	14:13
4	sct211-0002/2017	Ann	Waithira	14:13
5	sct211-0001/2017	Frank	Makori	14:13

Figure 20 Check in page for Class Attendance

The check-in page shows the unit name that is taking place at that time and the unit code as from the timetable. These details are retrieved from the timetable table in the database. During the given time, there is already a unit that has been allocated for the class at the timetable. The students were checked into the classroom to attend the lesson after their fingerprints were correctly identified in the system. The time of attendance when the student clocked in was also displayed.

k) Attendance policy

Enter A Student Reg No.  Enter Year.  Enter Semester.

view attendance				
S/No	Unit Code	Unit Name	Attendance (%)	Attendance score
1	bit225	Communication Skills	20	failed
2	bit221	Introduction to computers	100	passed

Figure 21 Attendance Policy Confirmation

After class attendance, the system calculates the number of times you have attended class versus the total number of lessons recommended for the unit. The student enters their registration number and the year and semester of study. The system displays the records of the student for the attended lessons. If the times attended exceeds two thirds, the system will give an attendance score of pass otherwise if it is less it will show a fail.

### 4.1 Experiment

The experiment was conducted from a group of twenty users whose fingerprints were enrolled using the fingerprint reader after which they were verified and considered to be undertaking a course in BSC Information Technology first year, first semester. The unit that was considered was Introduction to Computers. The experiment results were as follows;

	False Positives (FAR)	False Negatives (FRR)	Weighted Error Rate (WER)	True Acceptance Rate(TAR)	Failure to Capture	Cross Over Error Rate	Non Cooperative	Unidentifiable	Registration Delays	Other Challenges
<b>No. from Sample</b>	0	0	0	1	None	0	2	0	yes	Yes

Table 1 Experiment Results

From the experiment of the twenty students, no users was allowed to check in for class attendance and they had not been previously identified by the system. At the same time, no user was denied an opportunity to check-in for lesson attendance and were genuine users.

$$WER = FAR + FRR$$

$$WER = 0$$

$$\text{True Acceptance Rate (TAR)} = 1 - FRR$$

$$TAR = 1$$

$$\text{Crossover Error Rate} = FRR / FAR * 100 = 0 / 0 * 100 = 0$$

Two of the approached users refused to participate in the experiment arguing they did not understand how their data was going to be used.

There was no user who failed to be registered as a result of not having thumbprints. From the population considered, everyone had thumbprints and therefore they could participate in the experiment. Registration delays were experienced and the biometric device could take time to register. Intervention was by one wiping the biometric device as well as requesting users to wipe the fingerprints with a piece of cloth.

Other challenges that were experienced was one of the biometric device that had been used previously malfunctioned as a result of loose USB cable connection and it had to be replaced.

## **4.2 Discussion**

From the results of the experiment, the system is quite accurate as it did not accept any non-authorized users neither did it deny access to any genuine user. The total error rate which is the total sum of users accepted and those rejected was also zero from the sample. This shows that the system is 100% effective and can comfortably be used within the university set-up as a means of identifying users for class attendance. Further, the True acceptance rate was also 100% which confirms the accuracy of the system.

The Crossover Error Rate which measures the accuracy of the system was zero. The low crossover error rate shows that the system accuracy is very high. From the results, the performance of the system in curbing impostors is without any doubt and at the same time, only genuine users are allowed. The issue of students responding for their peers is completely done away with and this helps with the objective of ensuring that the students attends lessons as stipulated without failure and hence transfer of knowledge is achieved in institutions of higher learning.

With regular usage and interaction with the biometric device, the USB cable connection with the fingerprints loosens and it cannot be detected by the end user computer. Care should therefore be taken not to move the device so much. Where possible, have the fingerprint reader stationed in a permanent place where users can come in and their details are captured and registered other than constant movement which interferes with its effective operation.

## **CHAPTER FIVE**

### **CONCLUSION AND RECOMMENDATIONS**

#### **5.0 Introduction**

In line with the general objective of the study, this chapter describes the conclusion and recommendations which were arrived at after system development and experiment. It also gives suggestions for further research. The conclusion of the project has been made in accordance to the objectives established at the beginning of the study. Further the chapter has offered possible recommendation and a suggestion for further development.

#### **5.1 Achievement of objectives**

In regards to objective number one on identification of existing methods of students identification during class attendance and their challenges, the existing methods of students' registration were identified from the literature review to be mostly paper based and manual presenting the challenges of inaccuracies since they could not only be circumvented by students signing for their colleagues but in case of loss, the paper could be presented again for signing while the actual lecture is not in progress making those that had not attended the lesson the first time to also sign. Further, the information collected could not easily be transferred to other system for analyses as well as classroom or timetable booking. This made it hard to integrate with these processes that were crucial for students learning and overall management and administration of students' welfare.

The other method identified for classroom attendance was use of smartcards, this was also prone to abuse since the cards could be shared or one clock in for their colleagues. Use of name calling as an identification method could only be used in small classrooms since it was very time consuming in the large classrooms environment. The near field communication (NFC) technology that was developed to try and sort out the manual process proposed use of students' smartphones to capture their registration number and then join the classroom. The challenges with this method is that not only was one required to have a smartphone where the application would be installed, but also had a drawback of students giving their phones and registration details to their colleagues in order to be marked as present.

In regards to objective number two whose aim was to develop a biometric system of student authentication during class attendance, the system was developed using PHP programming language for the web system that required the main user/actor of the system who is the administrator to first register on the system after which they would register the other users i.e. lecturers and the students. The administrator was also required to register courses, units, classrooms, departments and campuses. The sample considered was BSC information technology year 1 semester one students. Units for the same were also registered. This was saved in MySQL database that was sitting on XAMPP server. For the biometric fingerprints enrollment and identification, development was done using java programming language i.e. Java Netbeans IDE 8.2. The fingerprint biometric reader that was used was Secugen Hamster-Plus reader which was integrated to the java program using FDxSDK pro for Java. The administrator was required to login to the system first after which they would proceed to either enroll students fingerprint or perform class attendance. During fingerprints enrollment, the students were required to give their registration number which was verified if it is in the saved database of users i.e. those allowed to sit for the course. If the records were present, fingerprints capturing was done using any of the fingers. A match was done after which the image template was stored in the database.

For the third objective that required to test the developed system and understand the challenges, the system was tested with students undertaking BSC information technology in Year 1, Semester 1. A sample of twenty students from this population was used which was randomly selected from the nominal roll for the first twenty registration numbers for the year 2017. The unit in consideration was Introduction to Computers. The system took in consideration the lecture room where the lesson was to be conducted. The lesson had been scheduled in the timetable that it was happening within the time of testing. Once the students comes in, it already shows the lesson that is taking place in that classroom and the registered students are the only ones that are allowed to check in for lesson attendance. Once attendance happens, a track of attendance is maintained in the database for the lessons attended versus the total number of lessons the unit is assigned. This helps to pull the student report on percentage attendance for the particular lesson. If the two thirds required policy has been met, the student is considered fit to sit for the exam in that unit, otherwise the students gets a fail and cannot be allowed to sit for the exam for the unit unless lesson attendance is repeated.

To test the system challenges, an experiment was conducted with the selected sample which was testing the rate of False Acceptance, False Rejection, Weighted Error Rate, True Acceptance Rate, Failure to Capture, Crossover Error Rate, Failure to Capture, non-identifiable users, non-cooperative users and the overall Weighted Error Rate that was computed from the sum of the FAR and the FRR. From the results, the system had no false positives or false negatives. Some few users (10% of the sample) were not cooperative since they found it intrusive and their crucial data being taken. All users from the selected sample could be identified with the device meaning the entire sample had fingerprints. The weighted Error Rate (WER) on the system was zero meaning no errors were experienced. The True Acceptance Rate (TAR) which was computed as  $1 - \text{FRR}$  gave a result of 1 meaning the system accuracy was 100% and no error was experienced. The Crossover Error Rate was at 0%. During capture, the device could experience some slight delays especially where the fingerprints were not clean or they were poorly placed. Users were required to use clean fingerprints and the device was also wiped of any dirt including excessive oil from previous users that could make the capturing process a problem.

Overall, the system was found to be quite effective while being used for class attendance because other than positively identifying the users, it did not allow or leave out any genuine user. The accuracy of the system was found to be high since the Crossover Error Rate was zero. The system throughput (Rate of registration per given time) was high as it could register several users in a minute meaning learning time would not be wasted. The high throughput also indicated that the system is easy to use. Performance matching was high since the False Acceptance rate and False Rejection Rate were at zero while the True Acceptance Rate was at 1. Performance capture measured through Failure to Acquire was also found to be high. The system is also easy to learn and does not take a lot of time for users to get around with the system meaning efficiency is high.

Comparing with the existing methods, the system is able to positively identify the actual users i.e. students registered for the course are authenticated and authorized by the biometric device and hence “What a user is” identification mechanism is achieved. The system is also able to incorporate timetable and classroom where the lesson is happening. Analysis of student attendance is also easy since the total attendance versus expected attendance is saved in the database. This can be retrieved



to show whether each student has met the expected two thirds attendance policy and hence if they have qualified to sit for an exam for that particular unit. Additionally, the implementation is not very costly as the fingerprint reader is quite affordable. For very large classrooms especially the introductory courses, several devices are required in order to have more identification points thus helping to save time for the lesson. The identification process for individual takes a few seconds and therefore class time is not wasted while trying to identify users.

This system can be used in a university setup to manage classroom attendance. A database server can be placed in the datacenter and the system can be accessed remotely via the web. The additional resources required would be internet connectivity either wired or wireless and the URL that points to the server housing the system. The internet connection should be available where the lesson is taking place i.e. the classroom. An end user Personal computer should also be provided.

## **5.2 Challenges**

Some of the challenges with the system is that the students are only allowed to check-in to the classroom. This implies one would check in and later leave the class since the system will have already marked in the user as having attended the lesson.

The other challenge is with the manning of the biometric device. An administrator or tutor is required to be present in the classroom in order to mark attendance. This also works with the existing methods. In an ideal situation, the system should just allow registration without having a third party control.

Constant tampering and movement of the device also makes it ineffective since it uses a USB cable to connect to the end user computer. With a lot of movement, the USB cable becomes loose making the biometric device undiscoverable by the end computer. This will therefore mean purchase of a new biometric device reader since cable alone cannot be changed.

### **5.3 Recommendation**

So that students can fully attend the class and not just check in for the purpose of being identified, the system should incorporate a check-out button where students will identify again after having been in the classroom for a given amount of time say a half of the lesson. This will achieve the objective of ensuring that knowledge is transferred as expected as the student will have participated on the better part of the lesson.

To eliminate the issue of manning, the biometric fingerprint reader can also incorporate access control mechanism. This will be placed on the entry of the classroom where the lesson is taking place and students who are positively identified will be allowed in. This will also ensure no impostor will get into the classroom.

## REFERENCES

- Academy, M. and Point, W. (2012) 'Biometrics Metrics Report', (December).
- Awedh, M. and Mueen, A. (2015) 'Electronic attendance system using nfc 1', (9), pp. 30–32.
- Bati, A. H. *et al.* (2013) 'Why do students miss lectures? A study of lecture attendance amongst students of health science', *Nurse Education Today*. Elsevier Ltd, 33(6), pp. 596–601. doi: 10.1016/j.nedt.2012.07.010.
- Behara, A. and Raghunadh, M. V (2013) 'Real Time Face Recognition System For Time and Attendance Applications', *International Journal of Electrical*, 1(14), pp. 2320–2084.
- Bhalla, V. *et al.* (2013) 'Bluetooth Based Attendance Management System', *International Journal of Innovations in Engineering and Technology (IJJET)*, 3(1), pp. 227–233. Available at: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.645.1573&rep=rep1&type=pdf>.
- C R Kothari (2015) *Research Methodology Methods and Techniques (SECOND REVISED EDITION)*, *Statewide Agricultural Land Use Baseline 2015*. doi: 10.1017/CBO9781107415324.004.
- St. Clair, K. L. (1999) 'A Case Against Compulsory Class Attendance Policies in Higher Education.', *Innovative Higher Education*, pp. 171–180. doi: 10.1023/A:1022942400812.
- Foldnes, N. (2017) 'The impact of class attendance on student learning in a flipped classroom', *Nordic Journal of Digital Literacy*, 12(1–2), pp. 8–18. doi: 10.18261/ISSN.1891-943X-2017-01-02-02.
- Guleker, R. and Keci, J. (2014) 'The Effect of Attendance on Academic Performance', *American Journal of Clinical Hypnosis*, 5(23), pp. 961–966. doi: 10.1080/00029157.1968.10401998.
- Kant, C. and Dr. Nath, R. (2006) 'Synopsis on Biometrics for User Authentication'.
- Kelly, G. E. (2012) 'Lecture attendance rates at university and related factors', *Journal of Further and Higher Education*, 36(1), pp. 17–40. doi: 10.1080/0309877X.2011.596196.
- Kumar, R. (2015) *RESEARCH METHODOLOGY a step-by-step guide for beginners*, *CEUR Workshop Proceedings*. doi: 10.1017/CBO9781107415324.004.
- Lodha, R. *et al.* (2015) 'Bluetooth Smart based attendance management system', *Procedia Computer Science*. Elsevier Masson SAS, 45(C), pp. 524–527. doi: 10.1016/j.procs.2015.03.094.
- Patel, U. A. and Priya, R. S. (2014) 'Development of a Student Attendance Management System Using RFID and Face Recognition: A Review', *International Journal of Advance ...*, pp. 109–119.
- Poh, N. *et al.* (2012) 'Biometrics Evaluation and Testing D3 . 3 : Description of Metrics For the

Evaluation of Biometric Performance’, pp. 1–22.

Robert, L. L. (2007) ‘Class Attendance : Is It Important ?’, pp. 1–9.

Saheed, Y. K. *et al.* (2016) ‘Attendance Management System Using Barcode Identification on Students ’ Identity Cards .’, 17(2), pp. 224–230.

Saheed, Y. K. *et al.* (2017) ‘Fingerprint Based Approach for Examination Clearance in Higher Institutions 1\*’, 2(1), pp. 2–5.

Schmidt, H. G. *et al.* (2015) ‘On the Use and Misuse of Lectures in Higher Education’, *Health Professions Education*. Elsevier, 1(1), pp. 12–18. doi: 10.1016/j.hpe.2015.11.010.

Somasundaram, V., Kannan, M. and Sriram, V. (2016) ‘Mobile based Attendance Management System’, *Indian Journal of Science and Technology*, 9(35). doi: 10.17485/ijst/2016/v9i35/101807.

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

Tiwari, T., Tiwari, T. and Tiwari, S. (2015) ‘Biometrics Based User Authentication’, (10), pp. 148–159.

Zarina, K. N. and Abdel, S. (2015) ‘Review of User Authentication Methods in Online Examination.pdf’, *Asian Journal of Information Technology* 14 (5): 166-175, 14(5), pp. 166–175.