UNIVERSITY OF NAIROBI

COLLEGE OF BIOLOGICAL AND PHYSICAL SCIENCES

SCHOOL OF COMPUTING AND INFORMATICS

LEVERAGING BIOMETRICS FOR ACCESS CONTROL MANAGEMENT IN LEARNING INSTITUTIONS

By

ALAN SYENGO MALUKI

P53/6623/2017

Supervised by

PROF. WAGACHA PETER WAIGANJO

A research project report submitted to the School of Computing and Informatics in partial fulfillment of the requirements for the award of the Degree of Master of Science in Distributed Computing Technology at the University of Nairobi, Nairobi, Kenya.

DECLARATION

I, Alan Syengo Maluki, do hereby state that this research project report is my original work and any contribution of other researchers has been acknowledged accordingly. To the best of my knowledge, this research work has not been previously submitted or presented to any other academic forum or institution.

Signature..... Date.....

Alan Syengo Maluki
University of Nairobi, Kenya

I, Prof. Wagacha Peter Waiganjo, do hereby certify that this Masters research has been presented for the award of Master of Science in Distributed Computing Technology with my approval as the University of Nairobi Supervisor.

Signature..... Date.....

Prof. Wagacha Peter Waiganjo
School of Computing and Informatics
University of Nairobi, Kenya

DEDICATION

This thesis is dedicated to my father, who taught me that the best kind of knowledge to have is that which is learned for its own sake. It is also dedicated to my mother, who taught me that even the largest task can be accomplished if it is done one step at a time.

ACKNOWLEDGMENT

Prof. Wagacha Peter Waiganjo has been the ideal thesis supervisor. His sage advice, insightful criticisms, and patient encouragement aided the writing of this thesis in innumerable ways. I would also like to thank the evaluation panel led by Dr. Ruhiu whose steadfast support of this project was greatly needed and deeply appreciated.

ABSTRACT

A common problem plaguing institutions of higher learning is how to monitor and manage student and staff attendance and access to key location, especially in institutions with multiple locations and the high population. Currently, institutions of higher learning in Kenya use paper-based attendance records coupled with verification of personal documents to control access and monitor attendance, however, this is subject to falsification and inaccurate data. Analysis of such data requires the transfer of the data to tools such as spreadsheets, a process that is subject to errors, missing file, tedious, and time-consuming.

This research work focused on coming up with a low-cost scalable biometric identification solution utilizing distributed technology. This would greatly benefit institutions of higher learning seeking to gain accurate and quick facility access and attendance insights on their employees and students. The prototype developed was then evaluated in terms of accuracy and performance to determine its suitability in the identification and processing of data. To test accuracy, 20 participants were enrolled with the system able to effectively verify 97% of the registered users. A simulation of 200 users using *JMeter* sending HTTP requests through the middleware to the database showed that the system could process data at the rate of up to 450MB per second with a maximum latency of 0.1 seconds. The results demonstrate that the adopted distributed architecture leads to not only low-cost but also an effective system for recording and processing facility access and attendance data.

TABLE OF CONTENT

List of Tables

List of Figures

List of Abbreviations

ACID	Atomicity, Consistency, Isolation, Durability
API	Application Programming Interface
ATV	Ability to Verify
FA	False Acceptance Rate
FRR	False Rejection Rate
FTE	Failure to Enroll
GSM	Global System for Mobile communication
IOT	Internet of Things
LCD	liquid crystal display
PIN	Personal Identification Number
RAD	Rapid Application Development
REST	Representational State Transfer
RFID	Radio-frequency identification
RMI	Remote Method Invocation
RPC	Remote Procedure Call
RTC	Real-time clock
SMS	Short message service
SOAP	Simple Object Access Protocol
SDLC	Software Development Life Cycle

CHAPTER ONE: INTRODUCTION

1.0 Background

Currently, virtually all institutions of higher learning in Kenya utilize the conventional paper-based registers to monitor students and staff attendance. Similarly, access to key sites such as examination rooms is also based on physical verification of details. There are many disadvantages of conventional access control and paper-based registers which make them unsuitable for monitoring students' attendance. For example, the registers are not uploaded to the central repository where data can be accessed for analysis. This affects the effective lecture time since the data has to be analyzed through a tedious process that is subject to errors. Similarly, the traditional system can be manipulated. An observation of the University of Nairobi also revealed that critical sites such as library and laboratories access are controlled through verification of student identity cards. While this may not be a major problem, the researcher observed that most of the guards manning these sites do not pay much attention to the details of the students' card so it is easy for a stolen or forged card to be used as means to access the sites.

Biometrics can deal with the problems associated with conventional access control. The approach involves the use of physiological and behavioral features to establish the identity of an individual. Since it depends on the individual person, biometric identification can be more reliable than the traditional attendance and access control systems. Biometric focuses on intrinsic characteristics associated with an individual hence cannot be copied, transferred, or disassociated with the owner making them ideal for verification of identity claims (Ahmad et al., 2015). Biometrics is changing the way identification is performed. It has become part of most security system, particularly in access control and forensic applications. A wide range of biometric traits have been used such as the face, iris, fingerprint, voice, and many others. Fingerprint recognition is one of the oldest and most widely used biometric traits in user identification hence it has gained wide user acceptability and security. Its implementation is also relatively inexpensive and can be done at different levels of details. First, at the global level, the important information is related to the physical orientation patterns of the ridge flow. Secondly, at the local level, minutiae are quite prevalent features guaranteeing the individuality of the fingerprint. The third level is the finer level in which pores and ridge contours play a role.

1. 1 Problem Statement

With the growing prevalence of physical security concerns and the need to monitor attendance in institutions of higher learning, utilizing the engineering process to capture and analyze data has become inevitable. In an environment where attendance is captured using conventional paper-based records the major challenge faced by the administrators is how to consolidate and analyze the records. In addition, restricting access to key sites such as library and laboratory is based on manual verification of student card details which poses great security challenge since such details can be forged. While institutions have widely adopted some systems to manage processes and automate daily activities in the workplace, the issue of identification remains largely unattended. Fundamental security principles such as non-repudiation cannot be guaranteed with the conventional identification systems. Attendance has a direct implication on student performance. It is important to properly manage site access and attendance since they significantly impacted retention and completion rate in higher education. In institutions of higher learning with a large number of students and staff, distributed biometric identification can go a long way in increasing security, combating identify-theft, increase accountability, reduce negative recognition, and enforce non-repudiation as well as ensuring the students attain the three-quarter rule of attendance. Notably, the existing access control systems are highly centralized which imposes constraints on data control and processing especially in an environment where there are multiple data sources.

1.2 Objectives

This research project aimed to accomplish the following objectives, which incorporates security principles, algorithm design, and automation of the identification process.

General Objective

The overall objective of the study is to design and implement a distributed biometric identification solution for higher learning instructions.

Specific Objectives

1) To design a biometric identification that utilizes distributed technology and techniques to effectively collect, analyze, and report identification data.

2) To develop a prototype based on the proposed techniques for the purpose of validation.
3) Evaluate the performance of the different components of the biometric system to establish its feasibility.

1.3 Research Questions

Research questions were used to guides research in the investigation of the state-of-the-art tools and techniques for identification, and formulation of an alternative approach to traditional ones. Thus, the following research questions helped the research study to design and implement a distributed biometric identification for a higher learning institution:

1) How can distributed biometrics technology and techniques be used to identify individuals and provide real-time visualization based on the captured data?
2) How can distributed biometrics be used to enhance security in access control and automate attendance management?
3) What is the performance of the proposed solution as a substitute for the conventional system?

1.4 Significance of the Study

Security provided by manual identification of individuals is limited since students' cards can be forged and details are difficult to verify. Terror attacks and threats targeting learning institutions such as Garissa University attack in 2015 shaped security strategies in Kenya. Many learning institutions responded by putting up measures to beef up security. However, most of them rely heavily on traditional security approaches such as the use of student identification cards that can be easy to circumvent. The current solution seeks to seal such loopholes by utilizing biometric identification. In addition, identification for attendance purposes can be manipulated and offer false data for students' records. Additionally, students cannot be guaranteed access to key services such as the library and laboratory if they lose their identity cards. In paper-based attendance, individuals can sign twice to get illegally supplement advantage of absenteeism. They can also deny illegal entry of records and disassociate themselves or avoid taking responsibilities for an act such as lack of sitting for exams. With biometrics, intrinsic traits cannot be guessed, copied, forged, stolen, or forgotten. Since these characteristics cannot be separated from the owner, they can offer

a crucial method of identification. Biometrics can be used to enhance attendance management and access control in learning institutions. A distributed access control system ensures that the highest level of precision is achieved in the identification and also the processing of the data from different check-in points.

1.5 Scope of the Study

The study focused on the design, development, and modeling of distributed biometric identification model for an institution of higher learning. A prototype to test the architecture adopted for the project was implemented in a single point of entry in the Computer Laboratory to determine its efficiency.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

Institutions have become more concerned with the issue of security control and monitoring of attendance among students and staff. Although there is limited research in Kenya to provide a link between absenteeism and work or student performance, literature from scholars across the world reveals that attendance affects students' retention and performance. Many researchers have designed and implemented a biometric attendance system which uses the fingerprint sensor along with different technologies. This section explores related systems and theories suggested and adopted by researchers in recent years.

2.1 Biometrics

Biometric technology has been widely adopted in various industries for different purposes including identification of staff. Biometrics can be categorized based on the level of engagement with systems (Contact and non-contact) or body shape and behavior (behavioral and physiological) (Thepade & Bhondave, 2015). Traditionally, biometrics was a technology for militaries and other highly important agencies. However, with the advent of technology and increasing security challenges, biometrics have become regular security process nowadays. Focusing on physiological and behavioral classification, several biometric traits can be adapted to facilitate the authentication of users. Physiological biometrics are related to the body organs which can be used to distinguish the identity of an individual based on who he/she is instead of what he has (token, card) or what he knows (password, PIN) (Thepade & Bhondave, 2015). They include fingerprint, retina, palm, face, iris, and other physical body parts that are can be used to uniquely identify a user. Behavioral biometrics, on the other hand, may include the signature, movement, heart rate, and voice recognition. It is an ongoing and active area of research. Most biometric devices can be of many types which basically recognize the traits unique to humans as shown in figure 1. Besides attendance, biometric technology is used to restrict access to places that are perceived to be part of valuable assets and information.

2.1.1 Retina Scanner

A retina scan biometrics utilizes the unique patterns of an individual's retina to identify them. In the human being, a retina contains thin tissue with neural cells located within the posterior section of the eye (Kalyani, 2017). The capillaries that deliver blood to the retina have complex shapes, making it (retina) unique for every person. The network of capillaries within the retina is so

complex that even identical twins cannot proportion a comparable sample. Although the retinal styles can be altered by critical conditions such as diabetes, the retina itself remains unaffected from birth till death.

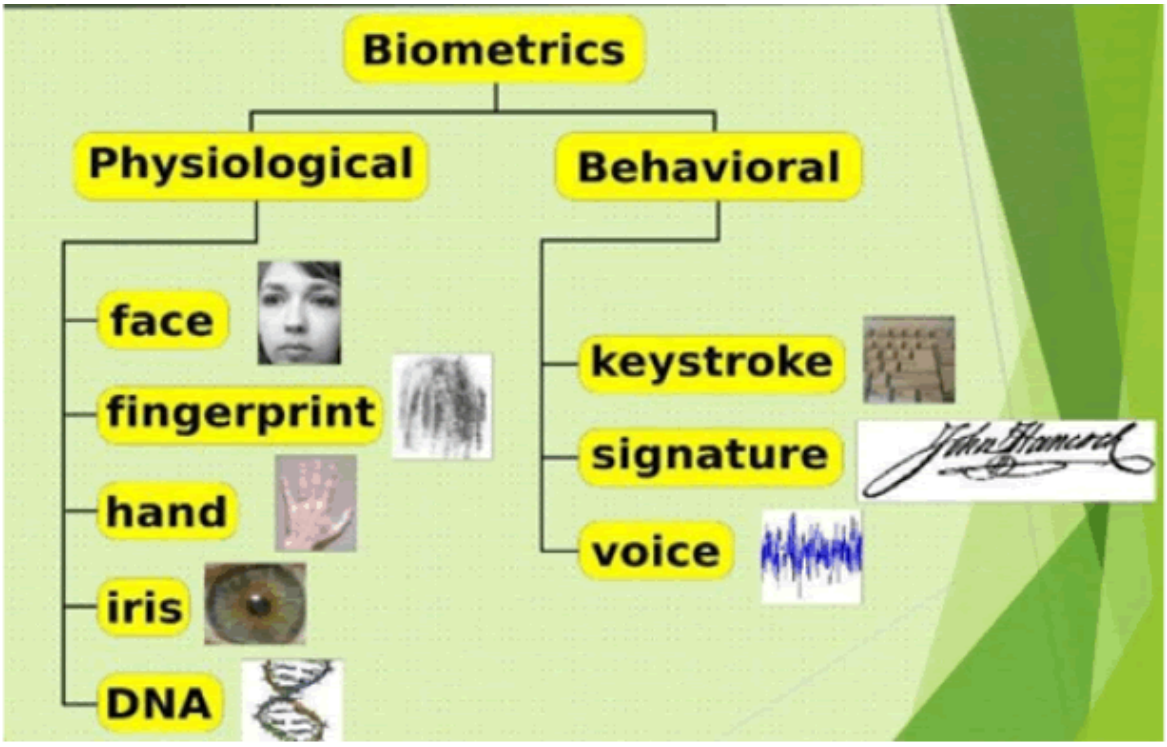

Figure 1. Types of biometrics. Source (Kalyani, 2017)

Due to its uniqueness and inability to change, the retina has been perceived to offer the maximum precise and reliable biometric. The benefits of using retinal experiment include low fake bad charges, low incidence of false rejection, and high reliability. However, this approach has been criticized as intrusive. In addition, it is prone to dangers such as cataracts sickness which could potentially affect the measurement of accuracy. It is less consumer-friendly and users have to be close to the dig cam optics.

2.1.2 Iris Scanning

Iris recognition utilizes digital camera technology infrared coupled with minimal infrared illumination reducing specular reflection the convex cornea, to come up with a detail-rich image (Vorona & Kostenko, 2016). Converting the photographs into digital templates leads to mathematical representations of the iris, yielding unambiguous individual identity. Interestingly,

iris reputation efficiency cannot be impeded by contact lenses or glasses. Hence, iris identification has the lowest outlier group compared to other biometric technologies. Iris offers immense benefits due to its balance and template sturdiness. Unlike the touchy membrane (cornea), the iris is a far inner organ protected against wear or damage. These features distinguish it from other biometrics such as fingerprints which can be difficult to recognize after years of exposing hands to manual labor. Typically, the iris is flat with handiest geometric configuration succeeded by complimentary muscle groups to model the diameter of an individual. The arrangement and positioning of the iris shape make it highly predictable than, for example, the face. The pleasant texture of the iris gets determined at a random stage during embryonic gestation. Being a contactless feature, the iris has been lauded as a better method of identification that offers high precision and acceptability in cultures where fingerprint scanners have been opposed. However, iris scanning technology is still in its infancy, less popular, and comparatively expensive. It is also considered intrusive compared to fingerprint, something that affects its overall acceptability.

2.1.3 Fingerprint scanner

Fingerprint scanners exploit the graphical glide-like ranges of the human fingers. Typically, the configuration of the finger ridges does not change throughout the life of a person. They also rarely get affected by incidents such as bruises and cuts making them an attractive option for biometric identification. Furthermore, fingerprint scanners are less expensive compared to other biometric options (Unar, Seng, & Abbasi, 2014). However, cost varies depending on the level of precision, with the costly ones having the ability to explore blood veins in a fingerprint as well as the shape and scale of fingers besides other deeper features.

2.1.4 Facial biometrics

Globally, every individual has distinctly unique facial features. Different features can exist depending on the structure of the eyebrows, the breadth of the face or the nose, and width of the eyes (Koong, Yang, & Tseng, 2014). Although facial biometrics have been widely applied especially in government and military, they are hardly used in attendance monitoring because they are considered intrusive. However, some manufacturers have created scanners which can uniquely identify individuals by examining the facial elements with low false positives or false negatives.

2.1.5 Voice recognition

Although the human ear may not accurately differentiate the uniqueness of sound patterns, every person around the globe has a distinct voice regardless of how similar it might sound to another.

With proper training of models and programming techniques, each contrast in individuals' voice can be captured and validated. Voice recognition techniques exploit voice levels and quality of pitch to identify individuals. This technique has been applied in forensics to match voices with speakers and general audit or verification process to arrive at a meaningful match. However, voice recognition is prone to interference or distortion of sound and also the voice detection device has to be close to the user.

2.1.6 Keystroke

In recent years, advancement in technology has led to gadgets that utilize keyboards. It has been noted that human beings have different ways of pressing keys and this can form the basis for unique identification. However, this method of identification has limited applicability.

2.1.7 Hand/Palmprint patterns

Like in the case of fingerprint, people have unique patterns and shape of the hand. Palms have unique features such as indents, symbols, and touch which differ from one person to the other. Although hand palms have unique features, they have largely been applied in criminal, forensics, and commercial auditing. The downside of hand/palm print is that it is susceptible to change over time depending on the physical activities that one engages in.

2.1.8 Signature scanning

Advancement in technology has made it possible to extract more features from behaviors such as signature patterns of a person. Signature not only provides an exclusive claim of the identity of a person but also acts as evidence of deliberation and informed consent to perform an action such as entering a contract. Hence, technology has enabled the development of software-based systems that can recognize the unique signature features of a person.

2.2 Related Work

Various approaches have been used to implement biometric authentication systems. For example, a *LabVIEW* approach has been used to implement attendance management with user-friendly graphical interfaces. The system utilizes two microcontrollers for hardware implementation but with limited functionalities. Similarly, a novel system based on the internet of things (IoT) technology has been adopted for the collaboration of different devices of the identification system. The system allows for real-time monitoring and analysis of attendance based on a website. These approaches have been presented in this section.

2.2.1 LabVIEW

LabVIEW provides a graphical programming approach that allows users to visualize different aspects of an application. It has been used for hardware configuration, debugging, and measurement data. Due to its visualization ability, LabVIEW is easy to integrate with measurement hardware from different vendors. One of the systems designed using this approach utilized LabVIEW, 8051 microcontrollers, and an R5305 optical fingerprint (Yadav et al., 2015). In this regard, the programmable microcontroller communicates with the PC running LabVIEW while a RS 232 acts as the serial communication channel between the PC and the microcontroller. On the other hand, LabVIEW is the system design software that stores the attendance records in a text file and displaying them through a user interface. An LCD screen displays the student ID when the fingerprint matching. Figure 1 below shows the LabVIEW based system.

The LabVIEW based system offers a user-friendly graphical interface, easy generation of attendance reports, and low power consumption. However, it is only suitable for small databases and offers limited functionalities.

2.2.2 Internet of things (IoT)

The internet of things technology has been also applied in which the hardware components include an ARM9 S3C2440 processor board and an FPS200 solid-state fingerprint sensor (Shah, 2016). The attendance data is stored in an SQLite database tool. The system provides automation of attendance and login of grades. It facilitates real-time monitoring of attendance data and viewing of the processed data through a website. All attendance data can be accessed through the internet (website). In this approach, security is enhanced through the use of additional vein recognition (multi-modal approach) and everything can be done through the website. In addition, attendance data can be accessed remotely. However, the implementation cost is high due to the inherent complexity of the software system architecture.

2.2.3 GSM and ZigBee

A system designed based on GSM and ZigBee consists of a low power consumption 2138 microcontroller, ZigBee series 2 OEM RF module, and SIM 900 GSM module (Talaviya, Ramteke, & Shete, 2013). The architecture of this implementation is shown in figure 2.

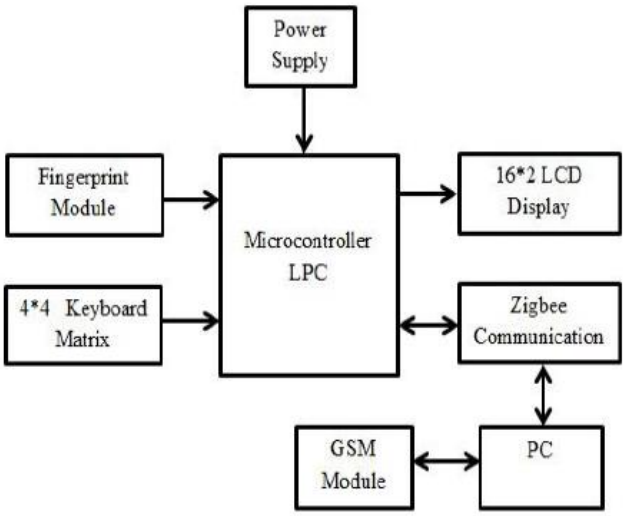

Figure 2. GSM and ZigBee based system.

In this architecture, the GSM module communicates the daily attendance information to the department head regarding the start and the end time of lectures. ZigBee utilizes low power radios to receive and transmit signals wirelessly. The attendance data is analyzed and stored in a centralized repository. The system is easy to use, use low power consumption technology, portable and has additional functionality due to the incorporation of the GSM. However, ZigBee functions in a low range of about 10 to 20 meters and have a low data rate.

2.2.4 RFID and Android

An attendance system developed using the RFID technology requires students to swipe RFID card as well as fingerprint detection to mark their attendance (Kumbhar et al., 2014). In addition, Android application interfaces with the hardware system (as shown in figure 3) to allow users to access the attendance records from any remote location. The system can also detect the user's location within the campus. A web-based SMS service is incorporated into inform parents and guardians about the student's attendance.

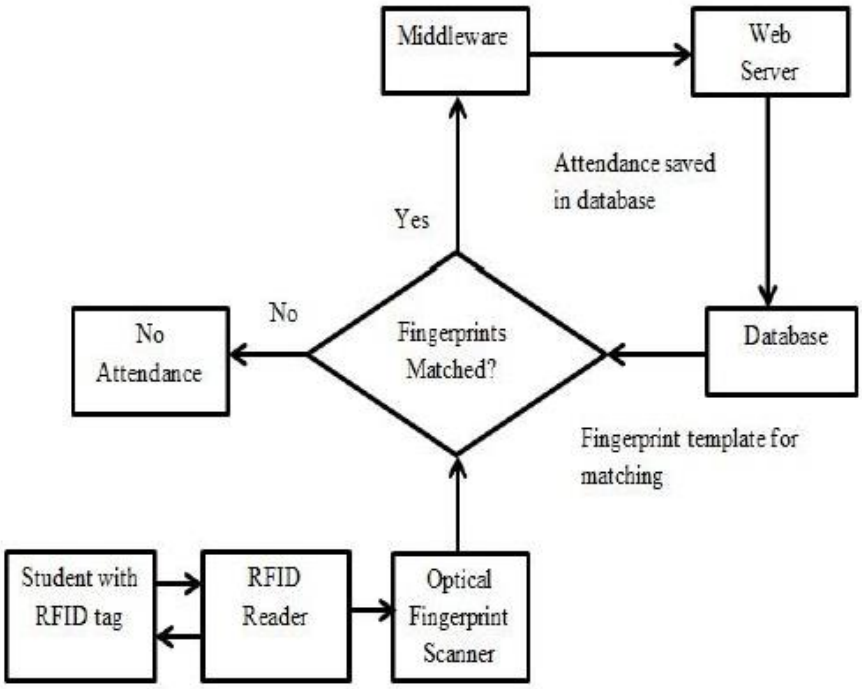

Figure 3. RFID and Android attendance system flowchart

The incorporation of RFID and biometrics makes it more secure. The Android app allows remote access hence offering additional functionality. The system is also designed to generate attendance performance graphs. The RFID based cards can be used in diverse areas including the laboratory, mess, and library. However, the integration of Android increases the complexity of system development.

2.2.5 ZigBee, DSP, and MATLAB

The system comprising of these technologies has been designed with receiver, transmitter, and attendance supervision components. The transmitter consists of optical fingerprint sensor OP-100N, ZigBee transmitter, and ADSP-BF532 (Walia & Jain, 2016). On the other hand, a digital signal processor facilitates faster processing. The receiver competent is made of ZigBee receiver and microcontroller. MATLAB is used for image enhancement. The system utilizes MS-access and Visual basic for database implementation. ZigBee can be replaced by Radiofrequency (RF) to increase range. The design leverages various sets of technologies to provide high accuracy environment. It has flexible user modes and is highly portable. However, the use of multiple power supply voltages (3.3V, 5V, 12V) increases power consumption and the cost of implementation.

2.2.6 Cryptography

The cryptography-based fingerprint attendance system is developed using the Arduino board with ATmega1280 (Ahmed et al., 2016). The system uses ZFM 20 fingerprint scanner with its memory and processor. It integrates with a TFT touch screen that offers a user-friendly interface. In addition, an SD card stores the student attendance records while a real-time clock (RTC) offers a record of exact attendance date and time. It uses the Caesar cipher cryptographic technique to ensure data does not get manipulated by unauthorized individuals. The integration of these techniques offers a portable, small-sized system with user-friendly design and enhanced security. However, the high consumption of power due to the integration of multiple hardware reduces battery life and also offers limited functionality.

2.2.7 RFID, GSM and.Net

The system utilizes GSM technology and RFID with biometrics to manage attendance. The student ID card has the RFID tag which is matched with records in the database and attendance completed once the fingerprint is verified using the fingerprint sensor (Srinidhi & Roy, 2015). On the other hand, the GSM Modem broadcasts SMS to parents about student attendance. The system requires the installation of RFID transponders in the classrooms, laboratories, libraries, and staffrooms to trace the location of student and staff. A web portal developed using vb.net (server-side) and asp.net (website) provides parents, students, and staff with real-time data about the location of students within the campus and can also be used to retrieve attendance records. Thus, the system is more secure and utilizes small-sized RFID cards. It also offers fast attendance processing speed. In addition, it can read multiple tags simultaneously while .net framework simplifies debugging. However, it has to remain ON and it can be costly to implement in addition to its complex software design.

2.3 Distributed Systems Architecture

Distributed systems can be classified into different categories. In terms of architectural styles, there are four different types that exist as well as an additional hybrid architecture. Architecture, in this case, denotes the logical organization of different components distributed over various machines. According to Tanenbaum and Van Steen (2007), these architectures include Layered Architecture, Object-Based Architecture, Data-centered Architecture, Event-Based Architecture, and Hybrid Architecture.

2.3.1 Layered Architecture

In a layered architecture, layers of components exist separately from each other, creating a relatively more modular approach. A classic example of this approach is the OSI model that combines different components into a layered architecture to enable them to interact with each other. In this architecture, interaction follows a sequential approach where a layer can only communicate with the adjacent layer. The process continues until the message is delivered or the connection is broken. However, some implementation can adapt the model in such a manner that skips some layers, an approach called cross-layer coordination. Cross-layer coordination provides better results due to an increase in performance. In this approach, layers on the bottom offer services to those on top. The layered approach offers benefits in that calls follow a predefined path and each layer can be modified or replaced easily without having any impact on the entire architecture.

2.3.2 Object-Based Architecture

The object-based architecture involves loosely coupled combination of objects with no specific architecture such as layers. In this architecture, no sequential set of steps that should be followed for any call. Reference to the component is done through objects and components can interact with one another through an interface or connector. This is a more direct approach in which various components can interact with each other through a direct method call. In addition, objects communicate in the form of method invocations, approaches commonly known as Remote Procedure Calls (RPC). Common examples include REST API Calls, Web Services, and Java RMI. However, as technology advances and security become a major concern, users now prefer decoupled processes where components anonymous and replaceable. Similarly, a shift from processes that communicate synchronously to asynchronous communication necessitated the need for Data Centered and Event-Based Architectures.

2.3.3 Data Centered Architecture

Data-centered architecture places emphasis on the data-centered and primary communication takes place through the centralized data repository. In this approach, the data repository can be passive or active. The architecture takes the form of a producer-consumer approach in which the producer releases items to a centralized data store while the consumers request data from it. The central repository can be a simple database or a complex data center. However, the central idea is that communication between components occurs through the shared common data store. The data-centered architecture supports different objects (or components) by availing persistent storage

space for each of them. The persistent storage stores information regarding the nodes in the system. Components have to subscribe to the storage so the data can only be sent and received by the subscribed components. Examples systems with such architecture include web-based data services, producer-consumer, and distributed file systems.

2.3.4 Event-Based Architecture

Communication in event-based architecture happens through triggered actions. A generated event is transmitted through the bus system and components in the network get notified about the occurrence. Such events can be URL to resources or data from a user application. Hence, the receiver can access the information provided in the process and the event accordingly. Communication between processes occur through event propagation and they occasionally carry data. The benefit of this architectural style is that components objects are loosely coupled and communication can asynchronous. As a result, adding, removing, or modifying components can be done without affecting the other components. In addition, the heterogeneous components can contact the communication bus using any communication protocol. Notably, direct communication cannot occur between each node so coordination can be a challenge. Instead, objects subscribe to the service to allow communication through the event bus. The event-based architecture supports various communication styles such as Publisher-subscriber, Enterprise Services Bus (ESB) Broadcast, and Point-to-Point.

2.4 Gap Identification

A review of the related work shows that biometric identification is an ongoing field with endless opportunities to explore. The focus now is to improve functionalities and increase scalability. In addition, there is a need to use modern programming languages to design scalable software that integrates with the hardware components to offer a user-friendly interface. The current study seeks to leverage the power of distributed technology to design a rich application with a high level of performance and scalability. The system capture should capture a fingerprint, perform feature extraction, perform feature comparison based on the fingerprint information in the database, and authentic or reject the user. The literature has revealed a useful distributed computing feature that can be integrated into the biometric system to offer enhanced synchronization, scalability, and security. The hardware components include the Arduino Uno hardware and a fingerprint scanner.

To facilitate integration and scalability, there is a need to leverage the available distributed technologies.

Another important aspect of distributed systems is database design. The systems reviewed utilized SQL databases for implementation. In large corporations where data is expected to grow to multiple records and also the presence of unstructured data. Non-relational databases become handy in such cases. Non-relational databases are distributed and typically document-structured, making it possible to hold data in a folder-like hierarchy. This makes it possible to hold unstructured data. Unlike relational databases, non-relational databases prevent databases from being the architectural bottleneck, particularly in a high volume environment. Also known as NoSQL databases, are not limited to specific storable data types. It becomes possible to add new types as organizational needs change. Besides, NoSQL databases offer high scalability compared to SQL databases. For example, MongoDB has an in-built capability to handle replication through horizontal partitioning of data (sharding) to facilitate scalability. Although these features are available to some extent in SQL databases, they require extensive human and hardware resources investment.

2.5 Conceptual Design

This research sought to utilize distributed technology integrated with biometrics to design and implement access control and management application. The project utilized a middleware as an infrastructure for distributed authentication. The importance of a distributed architecture is its reliability, availability, and transparency. If we look at Distributed systems today, they lack uniformity and consistency. Various heterogeneous devices have taken over the world where distributed system caters to all these devices in a common way. One-way distributed systems can achieve uniformity is through a common layer to support the underlying hardware and operating systems. This common layer is known as a middleware, where it provides services beyond what is already provided by Operating systems, to enable various features and components of a distributed system to enhance its functionality better. The layer offers certain data structures and operations that enable users and processes on wide-ranging machines to interoperate and work together in a consistent way. Figure 4 depicts the usage of middleware to inter-connect various kinds of nodes together. According to Andrew Tannenbaum, middleware is like the operating system of distributed systems.

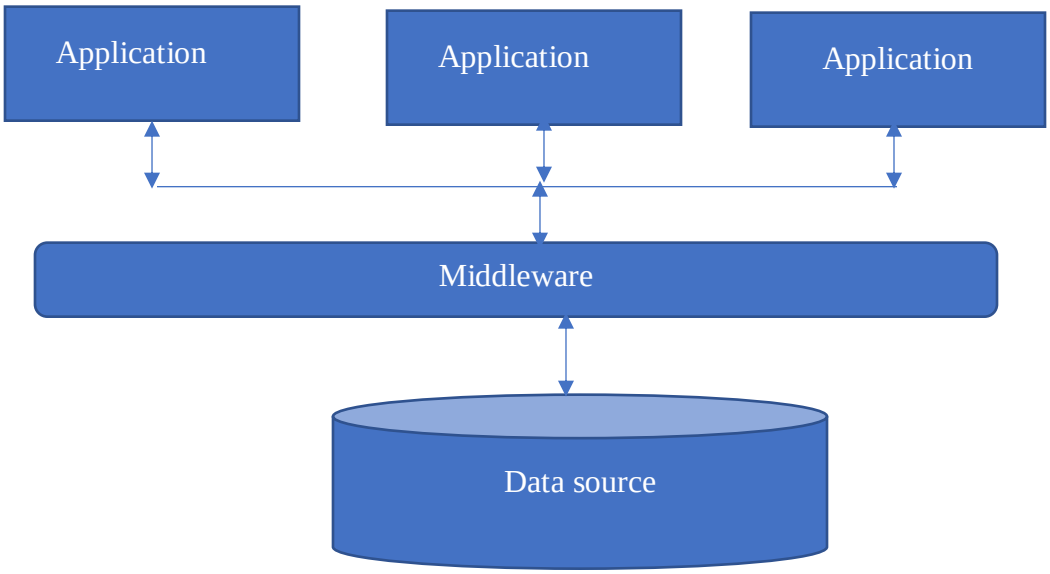

Figure 4. Conceptual Design

CHAPTER THREE: RESEARCH METHODOLOGY

This chapter describes the methodology adopted in the design, implementation, and testing of based biometric access control for a university. It includes research, application development, and testing methodology.

3.1 Research Design

The research project consists of various main elements: comparative evaluation and justification for use of selected technology, design and implementation of a distributed-based biometric access control system, and evaluation of the prototype to determine how the results relate with the selected architecture.

3.2. Rapid Application Development

Rapid Application Development (RAD) was selected for the development of the prototype. This method emphasizes rapid prototyping and iterative delivery. Therefore, the RAD model is a sharp contrast to the classic waterfall development model which is characterized by sequential activities from design to deployment. According to Maheshwaran et al. (2017), RAD offers a wide range of benefits compared to other traditional methods. Due to the heavy focus on speedy delivery, it provides an opportunity for cost-effective and time-effective SDLC. A complete life cycle consists of two to three months (60-90 days) hence being an ideal model for the project. Besides, it reduces development risk through iterative processes. Since the method encourages modularity and prototyping, reusability of components becomes a major benefit of this approach. Originally invented by James Martin, RAD has four stages which include planning requirements, user design, rapid construction, and cutover.

3.3 Requirement Planning

Requirement planning was perhaps the most critical stage where multiple decisions were made regarding the choice of function and non-functional requirements as well as the tools to be used. In this stage, the researcher conducted a student, a staff, and subordinate staff in the University of Nairobi. The three were conducted on different dates between January and February 2019 for a duration of 20 minutes each. During the discussion, the research sought to understand three key things: the challenges or frustrations in physical identification of users, the perceived need for change from the manual system, and recommendations for change. In conducting the interview, the researcher went one senior employee at the University to determine the needs and issues in monitoring students/employee attendance. In addition, the researcher observed how employees in

some departments record their arrival and departure time record in the Daily Time Record Form for triangulation.

3.3.1 Interview

Interviews with knowledgeable individuals were the main source of data needed to formulate functional and non-functional requirements. In this research, face-to-face interviews were conducted at the University of Nairobi using open-ended questions to obtain meaningful information. This section presents areas of questions few relevant to detecting problems in the University context and seeking a solution to reduce issues. The questions focused on several topics:

- The role of the interviewee in the University
- Technologies currently used by the University to control access or attendance in the university
- Procedure for verifying real identity in case of lack of essential identification document.
- Written or unwritten procedures for allowing access into the University by new members with no University documents
- Synchronization and aggregation of records at the end of a certain period to monitor attendance or access.

3.3.2 Data Analysis

The interviews were conducted in line with the data analysis to facilitate building requirements. The detailed notes collected during the interviews were analyzed to identify interesting topics. Affinity diagrams were used to organize the topics identified in the interviews based on the analysis of comments, issues, and suggested solutions. Each topic was written on a different sticky note and organized into groups of similar topics. The group clusters on the affinity diagram were reviewed to identify redundancy in problems and solutions as well as the presence of solutions without a problem. Using the affinity diagram, the researcher was able to identify the problem and suggested a solution (if any) represented by each topic. Using the list of problems and solutions discussed during the interviews, the researcher identified common problem themes and grouped them based on similarities or causation to understand the larger issues.

A. Inefficacious Manual Access Control

Control of access to institutions of higher learning and management of employees' attendance is an expensive affair. Although cost data were not available, the number of resources invested do not yield considerable benefits. During the interviews with on subordinate staff and a student, it was apparent that access to the institution is based on possession of University Documents which may be a Student identity card or any document to prove that one is part of the University community. Asked whether there are security measures and policies beyond the use of University documents, it emerged that there are written and unwritten rules governing access to key sites in the University. However, several challenges existent in relation to verification of people' details. In particular, there is no existing method, policy, or strategy to immediately verify the validity of identification cards issued in the University. The problem is even worsened by when the person cannot produce an identification document and can cause massive delays, frustration, and a threat to the security of the University security. It was established that there is a biometric database of students with plans to enroll the entire student and staff body in the future. A senior staff believed that such measures could be leveraged to streamline security access control.

B. Problems in Manual Records

Although students' attendance records are maintained by each Faculty, such records are non-existent for staff in nearly all departments. Records maintained in attendance sheets have to be manually typed and analyzed usually using Microsoft Excel for various reasons such as making decisions about the eligibility to sit for the exam. The major issues observed in manual records include dishonesty, errors, and missing files. Dishonest students tend to cheat about attendance by signing for their friends. This is a major problem in the current system since it is difficult to establish actual attendance figures. The senior staff also talked of missing attendance files which affects the decision about attendance management. Besides, errors occur when transferring data from manual files to electronic document for analysis. These errors can have an adverse impact on the performance of students. In addition, if they occur on the side of staff attendance, they could affect annual performance appraisal. Automating the process was long overdue according to the staff and this would simplify the process of recording and management of records.

C. Aggregation of Attendance Data

In essence, access control data plays a key role in the monitoring of people in a facility. However, institutions of higher learning want more than just monitoring access. In the case of staff attendance (though not frequently practiced in most Department), aggregating the data becomes a major challenge due to the bulkiness of records in a month. It becomes even costly and time consuming to aggregate students' attendance data. Due to the huge amount of data handled, it gets subject to errors in the aggregation and the possibility of making skewed decisions. Handling a huge amount of data becomes difficult to organize and visualize the data for making important decisions. A major problem here is that errors occurring in the process of converting the manual records to digital form can be difficult to detect immediately. Similarly, files meant that the aggregated data never represented a true picture of the student attendance. The interviewed students talked of students being victims when the aggregated data does not capture all attendance data, leading to inconsistent reporting. Manual records do not leave trails so any missing files or errors can have an unprecedented effect on those involved. Similarly, a small error when entering the data or aggregating it can also lead to incorrect reports and less meaningful results. Although no substantial recommendations were made to solve this problem, there was the mention of automation of visualization of data and reporting, which was perceived as a measure that can be taken to reduce errors in aggregation.

D. Growth of Data

University population growth is another challenge that affects the monitoring of attendance or access control. This is a multifaceted problem in that it affects the various decision made from a lower level to the management level. It affects among other things the control of people access the facility and attendance. The senior staff talked of the high cost of complete automation if such a decision was to be made. To the staff, automating the high number of data meant investing in high-end infrastructure with high development cost. A cost-effective method has to be sought to manage hundreds to thousands of staff and students who access the institution every day. The high number of people translates to massive data that also requires proper management decisions, policies and guidelines to ensure availability, integrity, and confidentiality of records. That is a decision that needs to be when conceiving the idea of automation in such an environment. Table 1 summarizes the findings of as shown.

Table 1. *Classification of User Stories (Requirements) and Possible Solutions*

Category	Problems	Proposed/Perceived Solution
Inefficacious Manual Access Control	-Access to University based on possession of documents -Not necessary adhered to -Existence of written and unwritten rules on attendance/access control mostly not enforceable	Existence of biometric database
Problems in Manual Records	-Dishonest in attendance records -Errors in transferring data to excel for analysis -Missing files	
Aggregation of Attendance Data	-Tedious processes of aggregating -Aggregate data not always a true picture of real-data -Errors in the aggregation process -Missing files affect analyzed data	Automation/better visualization
Growth of Data	-Population growth affecting the monitoring of people -Huge population require high investment in technology	Cost-effective automation solution

3.4 User Design

The data collected from interviews was first analyzed and converted to user functional and non-functional requirements presented in the next chapter 3. The requirements were further analyzed and converted to designs. During user design, the requirements were grouped into components and design focused on each component. Requirements were addressed by different components throughout the designs. At the top level, the design focused on five key aspects:

- **Accurate Identification:** Design of biometric components for accurate identification of users.
- **Friendly interface:** Design of user-friendly designs for system administration.
- **Interactive reports:** Design of system with the ability to generate interactive reports for key decisions such as people who have accessed a facility for a month.
- **Scalable system:** Design of a scalable system to deal with the growing population of the University community and distributed nature of Universities.
- **Scalable database:** Design of distributed, scalable database with the ability to accommodate the massive growth of users, support multiple entries and queries, and facilitate the high performance of the entire system.

Detailed design of the system was undertaken in the next chapter based on the requirements formulated. This included activity diagrams, schemas, mockups and much more. The overall analysis and design focused on the inexpensive approach to the development of the physical access control system utilizing distributed technology. Nevertheless, a high-level architecture of the project based on the requirements gathered is as shown in figure 5.

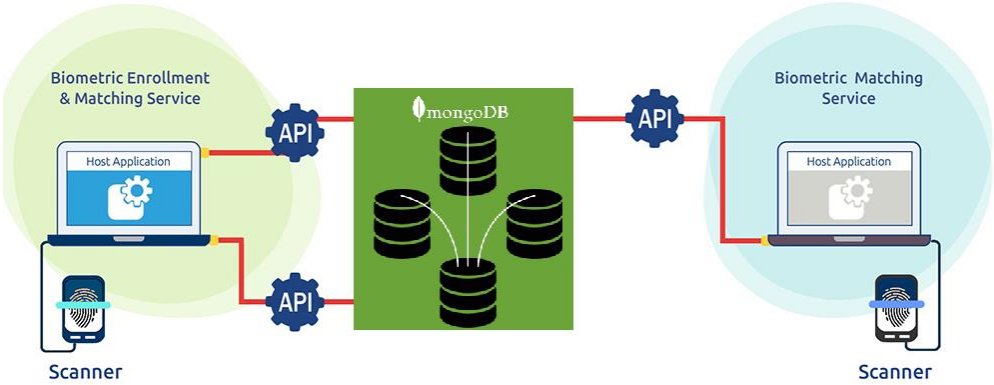

Figure 5. The high-level architecture of the Prototype

3.5 Rapid Construction

After the designs, rapid prototyping kicked off with different modules ready for execution. The first component to develop was the fingerprint reader module which included a fingerprint scanner and Arduino microcontroller. Secondly, a database was created with the required documents as it is discussed in the implementation chapter. The third component was the development of a RESTful API as middleware and the decisions made during the development are presented in the subsequent chapters. Finally, the interactive user interfaces were designed and integrated with the other components to come up with the complete system.

3.5 Cutover

The developed prototype was used to evaluate the feasibility of implementing a distributed biometric authentication system. Testing focused on two major things: the accuracy of the system in terms of ability to enroll or authenticate users; and the performance of the system in terms of resource consumption and other metrics such as throughput, multithreading, latency, and average response rates.

3.5.1 Test Parameters

Various aspects of performance measures were conducted after completion of the project. Some measures are defined for clarity. False accept rate measured the expected portion of authentication with wrongful claims of identity (unenrolled finger) are incorrectly confirmed.

$$FAR = \frac{\text{number of successful authentications by impostors}}{\text{number of attempts at authentication by impostors}}$$

False reject rate measured the portion of transactions bearing truthful claims of identity or non-identity that are incorrectly denied.

$$FRR = \frac{\text{number of failed attempts at authentication by authorized users}}{\text{number of attempts at authentication by authorized users}}$$

Failure to enroll/failure to capture rate measured the expected proportion of the population for which the biometric system could not extract sufficient features for enrollment as well as those who could not reliably match their details in an attempt to confirm their enrollment.

$$FTE = \frac{\text{number of users who fail in their attempts at enroll}}{\text{number of users who attempt to enroll}}$$

Ability to verify rate gives the proportion of the enrolled users for whom the biometric system worked property.

$$ATV = (1 - FTE)(1 - FRR)$$

Besides, the load testing focused on metrics to measure the performance of the developed middleware. The key performance metrics used include average response time, error rates, and throughput. Average response time was defined as the measure the cumulative mean of all request/response cycles. Throughput was used as the measure of bandwidth consumed during the test. Average latency was also evaluated to determine the time it would take from when a request is sent until the first is received.

CHAPTER FOUR: ANALYSIS AND DESIGN

4.1 Analysis

As part of the system analysis, the research focused on the prototype's external and internal behavior. Functional and non-functional requirements were outlined for the complete prototype.

4.1.1 Feasibility Study

Utilization of middleware in the processing of access control offers unprecedented benefits compared to traditional centralized architecture. It combines the benefits of a centralized system with an enhanced distributed capability. In particular, scalability is enhanced since multiple biometric user authentication nodes can be added without having to resign the system. Hence, a single node failure does not affect the middleware. It offers infinite scalability and tremendous evolution. A feasibility study based on research shows the benefits and the practicability of implementing the proposed prototype in an organization.

The proposed system is economically feasible due to the low cost of implementation compared to a centralized processing system. It is economical in the sense that it eliminates paperwork or manual attendance monitoring. With a single processing unit, data from different terminals can be processed and stored in a central repository housing data from all nodes. The results of the processed data are highly accurate due to the utilization of biometric features. Besides, the system is technically feasible since there is minimal hardware required to support its operation. A fingerprint scanner and Arduino Uno are the primary hardware components needed for the development. However, a complete set of the fingerprint scanner and Arduino Uno board are required for each terminal. As a result, to minimize the cost of development, a single set was used to integrate with the middleware. In regard to behavioral feasibility, the proposed system offers benefit in that there is minimal interaction with the user. As a result, it easy to use and also easy to learn due to a simple but attractive administrative interface.

4.1.2 Requirements

4.1.2.1 Functional Requirements

The functional requirements specifications documents what the proposed prototype should perform. This section also includes the type of data that can be entered in the system, flow of data, operations, reports, and users and their roles or user groups. The system consists of a variety of functionalities designed to ensure the system works as it is meant to. Notably, the system has several components. The key functionalities that the system should have include:

- Fingerprint scanner to capture and extract features from users for storage into the database and feature comparison during authentication.
- A user interfaces with interactive features for various activities. This includes the login page to authenticate users based on username and password. Once the user logs in, they can access two sections: one with gate pass programs and another with office utilities. Under the gate pass programs, there should be several program modules to offer functionalities such as changing password, registering new users, viewing records, monitoring continuous attendance, and reports such as daily, monthly attendance, special reports, and visitors reports. Such tools should also be available under the office utility programs.

4.1.2.2 Non-Functional Requirements

The non-functional requirements include the requirements that outline the criteria for evaluation of the system operations rather than the specific behavior. Although functional requirements are important, most requirement gathering techniques tend to ignore non-functional requirements leading to gaps in non-functional aspects of the system requirements. The main focus of the current project is to create a scalable system with improved performance and reliability. Hence:

- The prototype development utilizes multithreading capabilities to improve performance and response rate.
- Use of scalable database technology also guarantees better scalability through replication and sharding which can be an incredible way to reduce latency during mass processing of requests.

4.1.3. Database Requirements

Traditionally, developers have been utilizing SQL databases (also known as relational databases) such as MySQL. Over time, the growth of unstructured data (such as social media posts, images, texts, video, and email) has necessitated the need for non-relational databases. Such databases include the MongoDB which was selected for this prototype due to its benefits over the relational databases such as MySQL for the corporate environment. MongoDB is a non-relational database management system and a prominent NoSQL database. Instead of using database tables and static schemas commonly used in the relational database management system (RDBMS), MongoDB utilizes key-value storage in the collection of documents. Unlike RDBMS, MongoDB supports

several options for horizontal scaling in a large production environment, enabling a more reliable, scalable, and cost-effective substitute to relational databases. Scaling in relational databases typically occur vertically. This means that data resides in a single server and scaling requires more hardware like a larger server which can be expensive.

4. 1.4. Domain Requirements

Domain requirements specify the environment under which the system operates. In this system as it involves biometrics so much attention has been put into designing a system that corresponds to the expected application domain. Such domain requirement includes part 8 of ISO/IEC 19794-8:2006 on the exchange of biometric data which specifies how to exchange of pattern-based skeletal fingerprint recognition data.

4.1.5 Hardware Requirements

During the implementation of the system, various components shall be used.

1. Biometric fingerprint reader
2. A computer for the program to run.
3. An Arduino Uno Microcontroller

4.1.6 Middleware/API Requirements

Middleware was another central focus of the development process in this porotype. In system analysis of the middleware, it is expected to allow communication and data management of the distributed application, acting as a hidden translation layer. It delivers the messages thereby allowing the application to send and retrieve data from the database. The primary messaging frameworks used was JavaScript Object Notation (JSON). Acting as the request broker, the middleware should process user data from each terminal, filter database requests, and perform forwarding of data for storage. The middleware should also provide integration capability and runtime services for communication.

Typically, there are two options for API that have been widely adopted in distributed systems. SOAP (Simple Object Access Protocol) and REST (Representational State Transfer) are two API styles that address data transmission from a different perspective (Tihomirovs & Grabis, 2016). SOAP is a standardized protocol capable of sending messages based on protocols such as HTTP and SMTP. Specifications for SOAP are recognized as formal web standards, developed and maintained by the World Wide Web Consortium (W3C). Unlike SOAP, REST is an architectural

style rather than a protocol. The REST architecture has laid down guidelines (such as, the use of HTTPS status codes and stateless existence) that need to be followed to create a RESTful web service.

Since SOAP represents an official protocol, it has strict rules, procedures, and advanced security measures such as built-in ACID authorization and compliance. Due to the complexity of the protocol, it has high complexity which requires more bandwidth and resources leading to slower page load times (Tihomirovs & Grabis, 2016). In this regard, REST was developed to address these challenges, providing a more flexible architecture with loose guidelines. REST allows developers to implement recommendations based on custom requirements. Unlike SOAP which allows only XML messaging format, REST allows a wide range of messaging technologies such as HTML, JSON, XML, and plain text. In addition, REST offers lightweight architecture leading to better performance if RESTful web services (Kumari & Rath, 2015).

4.2. Design

This section gives a detailed design of the proposed prototype based on the requirements gathered and analyzed.

4.2.1 Description of the Proposed System

The proposed system explores the use of fingerprint biometrics to record attendance. The fingerprint is the single most method of identification so the system should authenticate users based on whether they are registered or not. The registration of users is done by a user with administrative rights. The data is then sent through a secure RESTful tunnel to the database for storage. Biometrics can combat non-repudiation and errors in manual identification. The REST API offers an added advantage in that data from different terminals can be synchronized and stored in a single repository. Any database request must go through the middleware. This adds a high level of security, protecting data from attacks such as SQL injection.

The system has such a simplified interface that shall make it easy for use by any persons that is using it. High attention is paid to the security and high ability to generate efficient and precise reports. The system shall have the capability to search and compare between different tables, that is, the student table, the lecturer's table, and the staff table. Such capabilities ensure that security is maintained around the school. The design focuses on accuracy, better performance, and simplicity of use. The fingerprint scanner utilizes serial communication such that it can be connected to the Arduino microprocessor and communicate with the software component through

COM ports. An integrated alarm notification ensures security personnel can be easily notified in case an unauthorized person tries to circumvent security checks.

4.2.2 Process Design

Process design illustrates the flow of events and data across the system. It demonstrated through activity diagrams and flow-charts showing actions that can be taken by a user depending on resources exposed to them.

4.2.2.1 Activity Diagrams

Admin Login

The administrator has full rights as shown in figure 6. This super user can manage all tasks in the system.

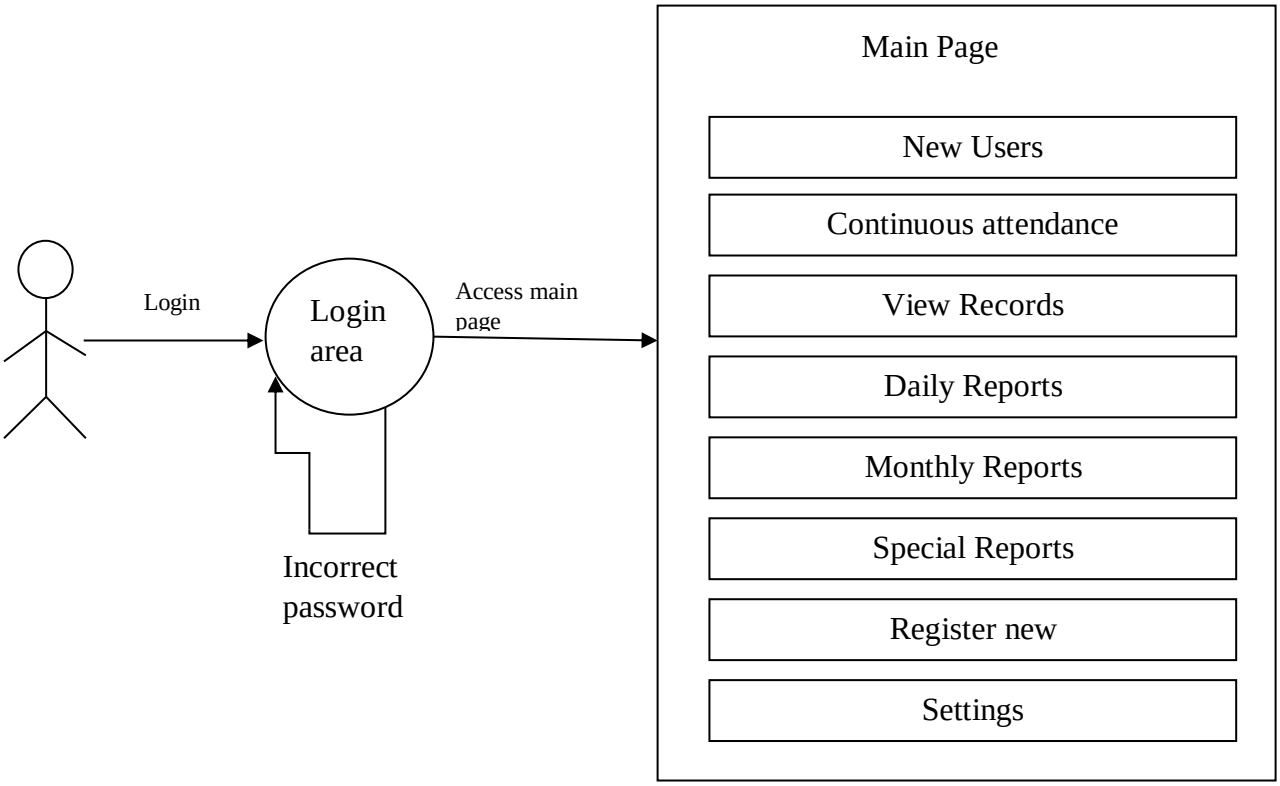

Figure 6. This diagram shows how the Admin access and uses the system. (Full access rights)

User Login (Restricted access)

Figure 7 shows the restricted rights of a user. Users can only view reports and access settings for their page.

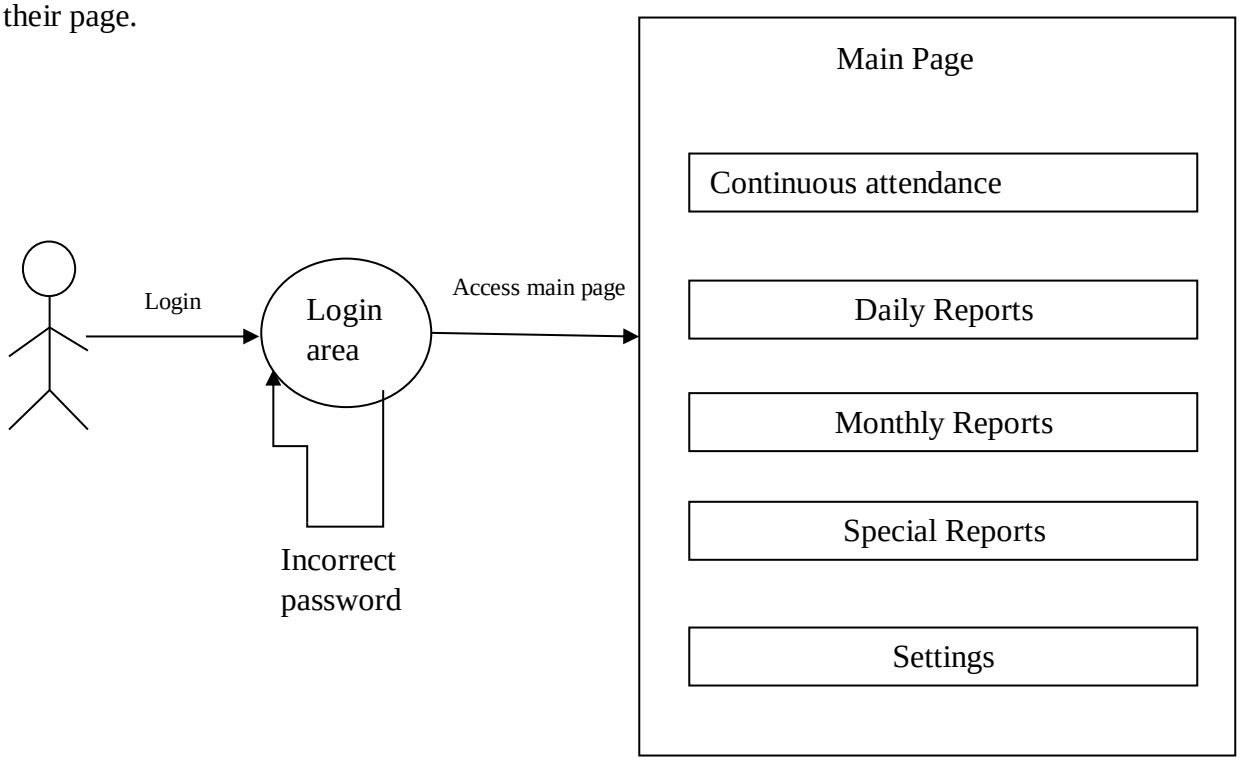

Figure 7. Show a user case diagram of how a common added user has limited privileges.

Generating Reports

Figure 8 shows the reports that can be accessed by users.

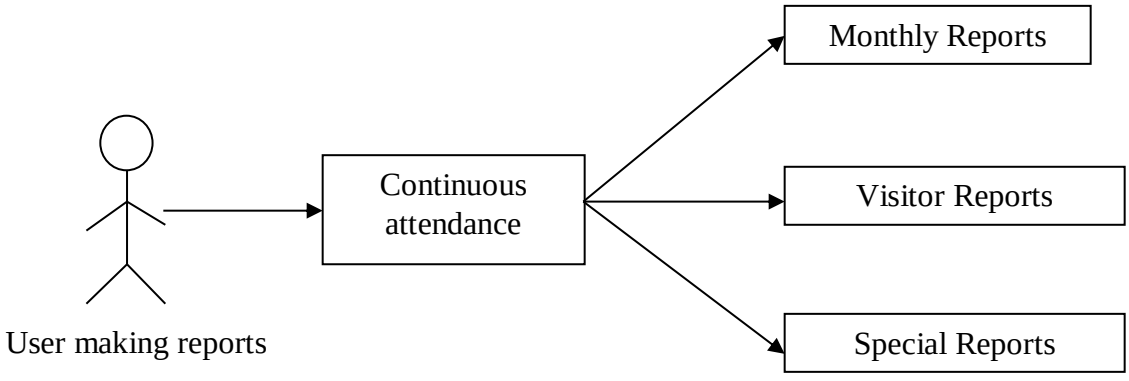

Figure 8. From continuous attendance all report s are easily generated

On the other hand, Figure 9 illustrates the registration of new user biometrically

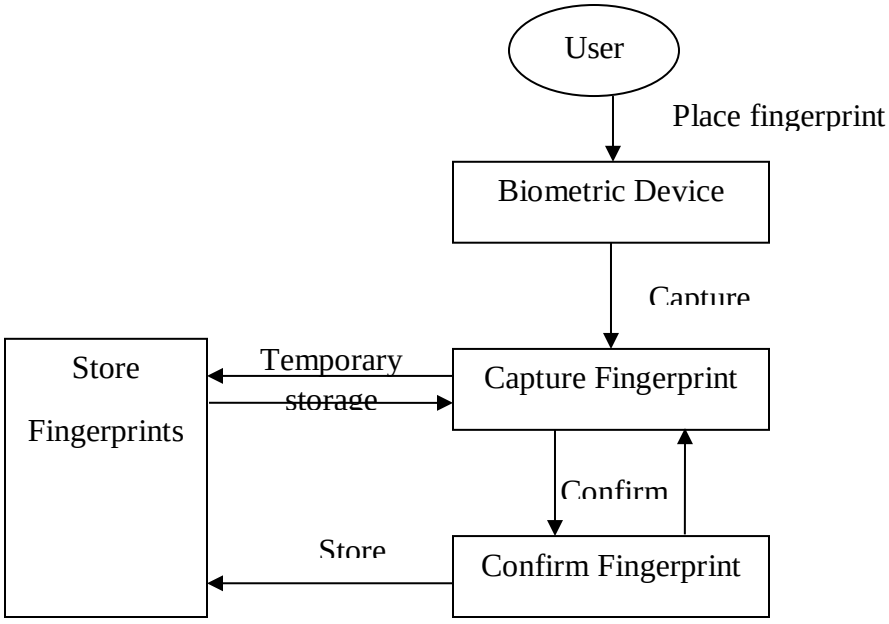

Figure 9. Biometric Registration of New User

Figure 10 shows how the entities access the Office/ Gate

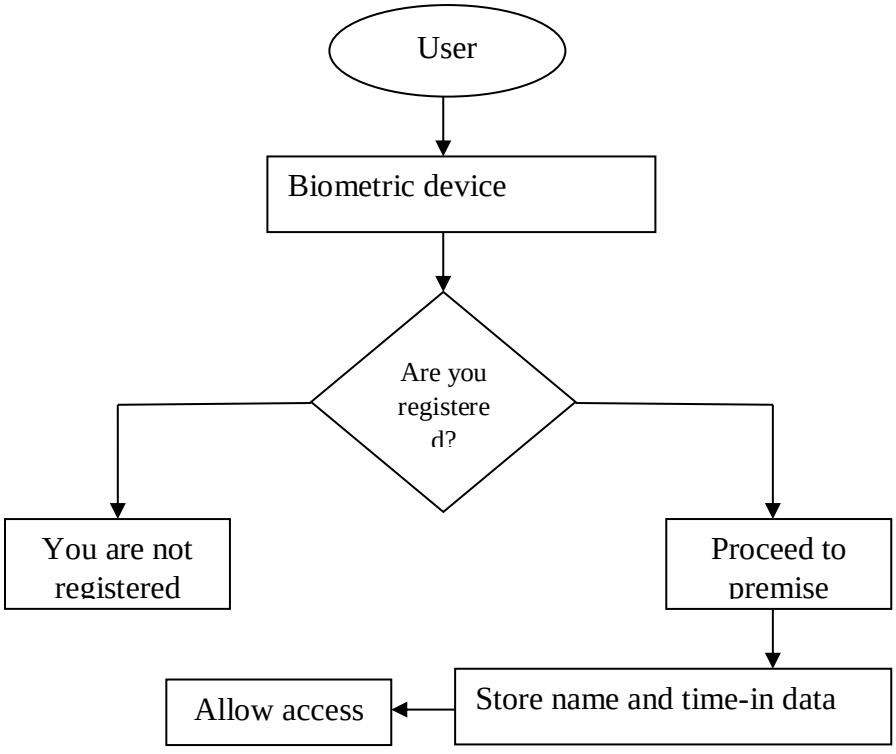

Figure 10. Show how the office shall be accessed biometrically

4.2.3. Database Design

4.2.3.1. Conceptual View

The conceptual view of the database provides a perspective of the key collections and documents as well as the type of information contained in those documents. Notably, Non-relational databases are schemaless. Hence, this conceptual view only provides an overview of the database documents in terms of the keys used as shown in figure 11.

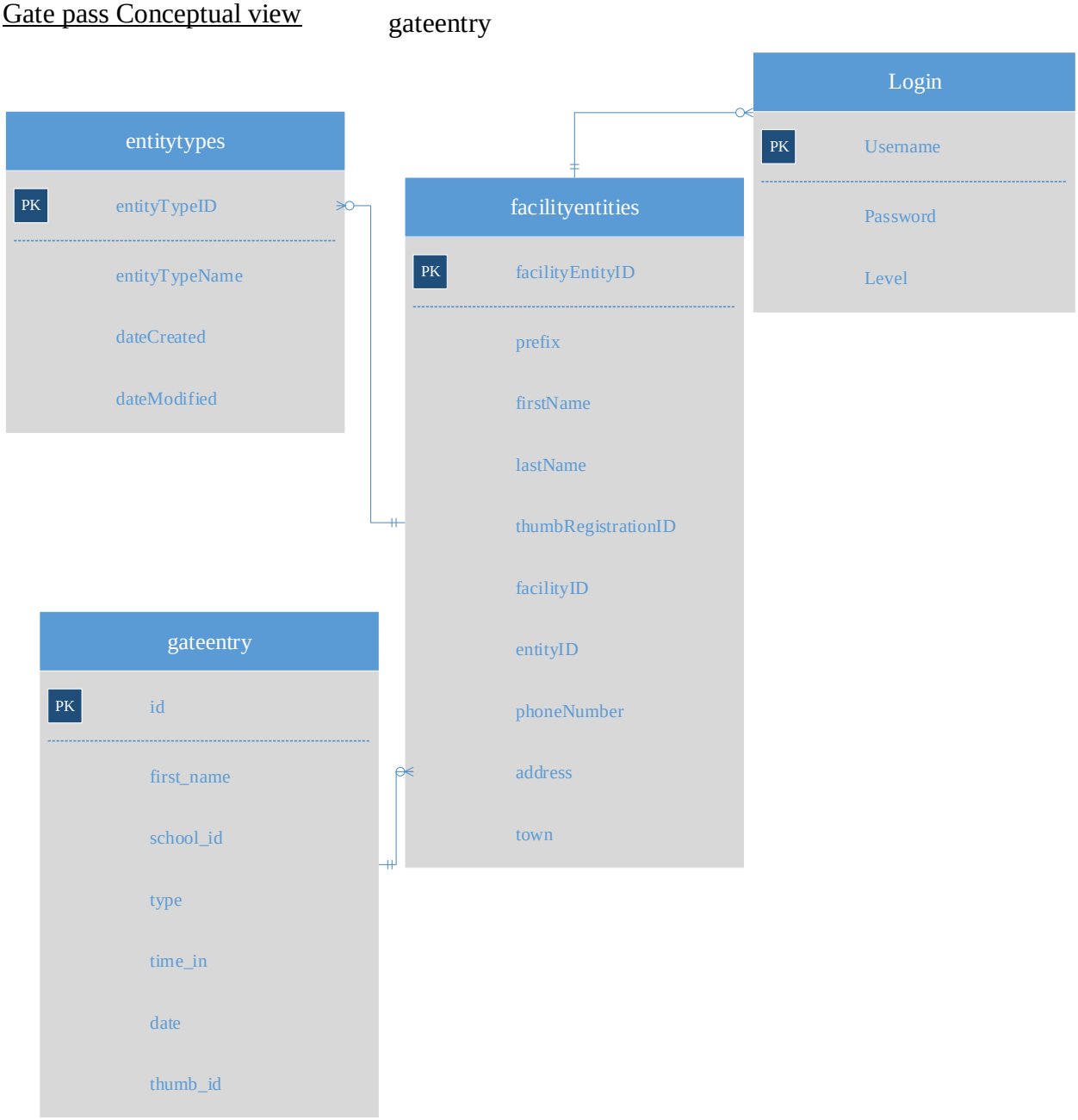

Figure 11. Conceptual view of the database

4.2.4. Interface Design

The interface has been designed based on what users find simple to use and access with much ease. In order to create a system that performs and works well better than the previous versions, a lot of attention has been paid on how to make a system that shall ease all fundamental processes and ensure manual processes are partially done away with to improve the services the university offers. This shall mean the creation of interactive user interfaces and the inclusion of all requirements that were based on previous studies. The Biometric System in construction shall require more attention to detail in order to achieve the best result. Selected interfaces for login, main page, and registration page are shown in figures 12-14.

Login Interface

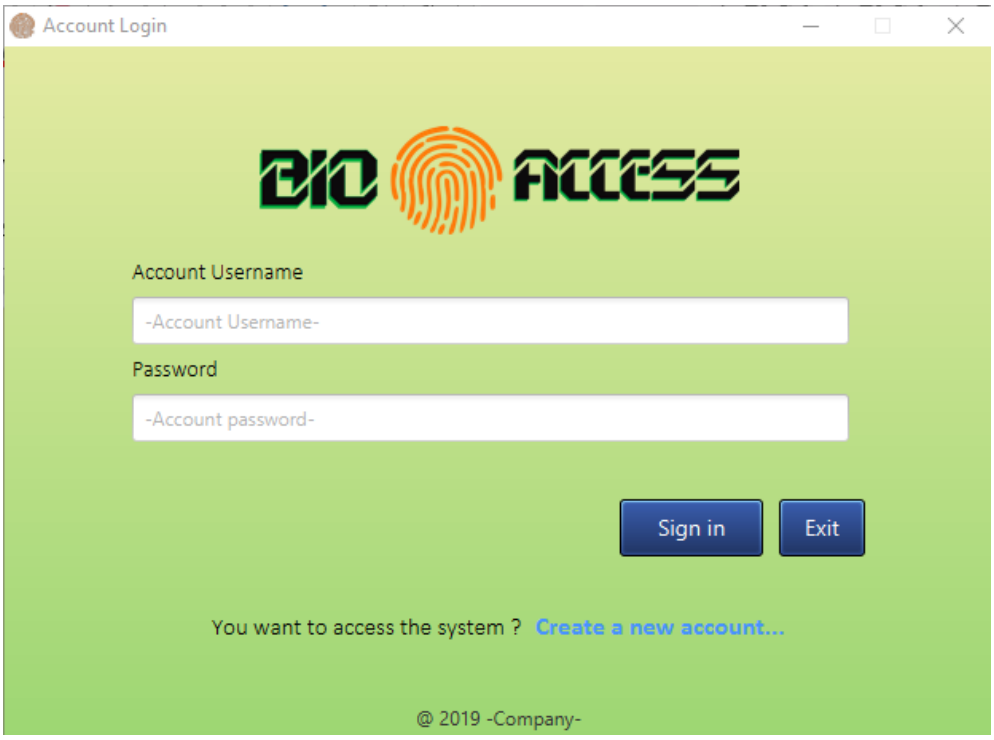

Figure 12. Login Page

The Main Page on Viewing Gate Programs

Figure 13 Main Page

Registering New Student

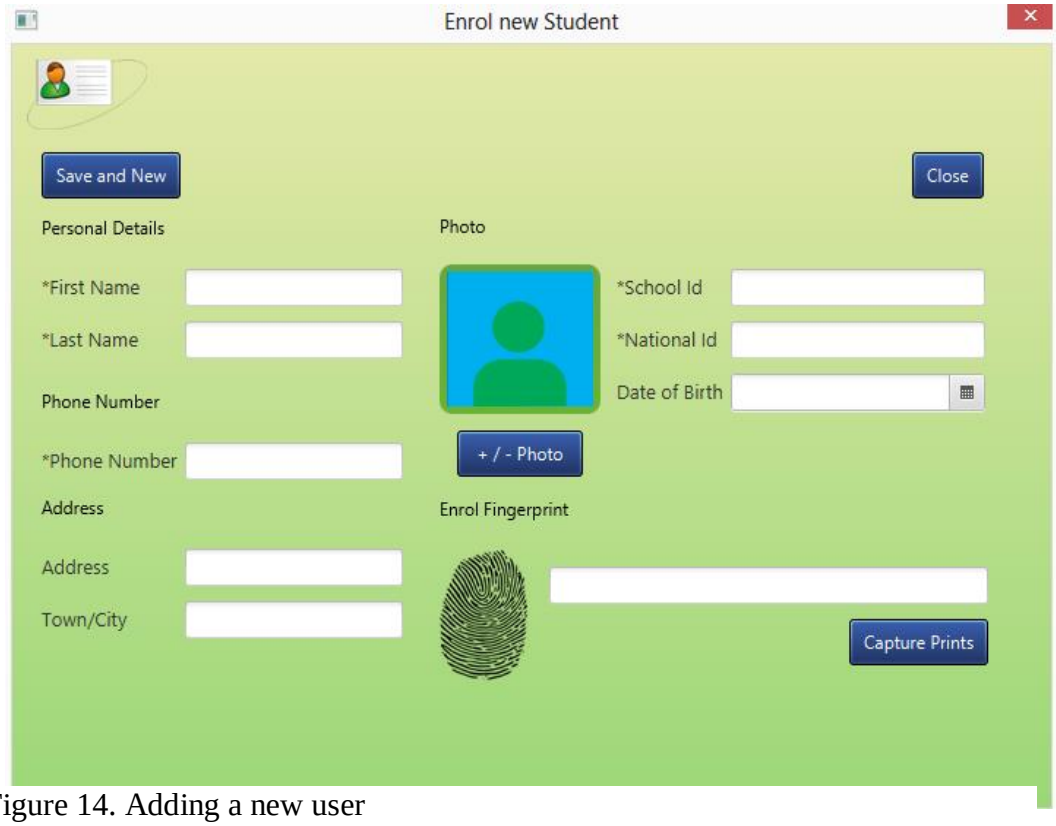

Figure 14. Adding a new user

4.2.5. RESTful API Design for Middleware

Besides the user interfaces and databases, the middleware layer added in the system increases scalability, ensuring that multiple terminals can utilize a central database with high precision in the communication. The middleware server piece exposes the application components as Web services, hence different terminals can share the same data effectively. The primary purpose of the middleware is in this project is to facilitate communication functions between the application (terminals) and the database. This communication includes user authentication, management of transitions, managing message queues, and directories. The middleware here is a distributed processing of requests in real-time. Conventionally, REST-style architectures are based on the client-server model (Kumari & Rath, 2015). The client can initiate requests to servers while the servers process the requests and respond appropriately. In this approach, the requests and responses are based on the transfer of representations of resources. Typically, the user requests take the form of HTTP verbs such as GET (read from database), PUT (update/replace row in database), PATCH (update/modify a row in database), POST (create a new record in the database), or DELETE (delete from the database). When the REST API gets the results, it sends back the response to the client in JSON format. This is illustrated in Figure 15

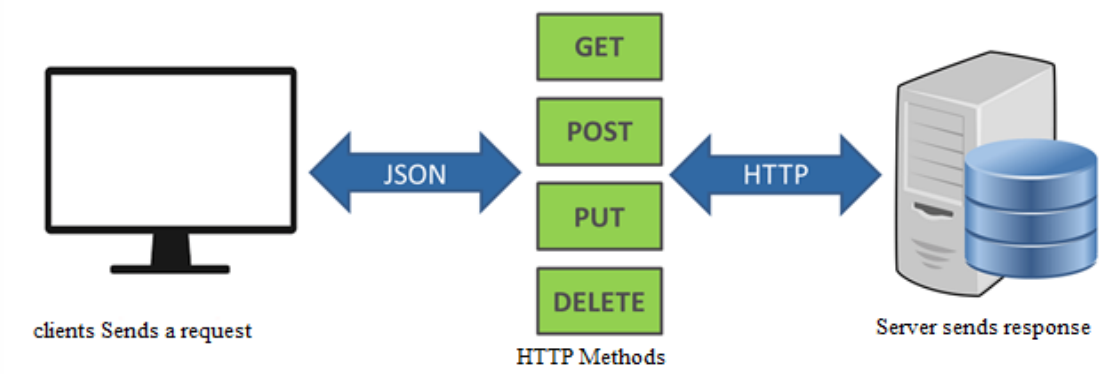

Figure 15. REST API Middleware

CHAPTER FIVE: IMPLEMENTATION

This chapter describes how the design was implemented. It encompasses the set of tools and technology used in the project lifecycle.

5.1 System Development

Biometric Security Access for Gate Pass and Access to Examinations Office has been developed using JavaFX. JavaFX is a programming language developed by Oracle. It is an improvement of Java in terms of how it utilizes computer resources, size of application developed, platform independence and ability to run in both mobile, desktop and web environment.

A REST-style architecture was used for the middleware. The JSON REST middleware achieves two crucial practices: JSON encoded bodies and JSON only responses. Hence, it is added in the PHP file as:

```
$app->add(new API\Middleware\JSON());
```

Hence, it is added in the PHP file as:

```
class ReceiveRequest {
    function __construct() {
        $rawParams = file_get_contents("php://input");;
        $params = json_decode($rawParams);

        $tempPassword = null;
        if(isset($params->password)) {
            code;
        }
        Utils::logToFile("Request Params:
".json_encode($params), __CLASS__, __FUNCTION__, __LINE__);
.
.
.
private function returnResponse($response) {
        code;
          }
```

The development processes incorporate measures to report errors to the users in case of unsuccessful operation. For example, for a write-enabled (PUT, POST, PATCH) request, the content must type head should be JSON, otherwise the program exists with “There was an error processing your request. Please try again” error. If the request header contains the correct content, the statement $this->next->call() executes the middleware module in the chain. A third-party library (JWT Authentication Middleware for Slim) was used for authentication of API users.

```
$app->add(new \Slim\Middleware\JwtAuthentication([
    "secret" => "supersecretkeyyoushouldnotcommittogithub"
]));
```

Hence, the middleware utilizes JSON Web Token Authentication for Slim Framework rather than the OAuth 2.0 authorization server. It does not provide mechanisms to generate, issue, or store the authentication tokens. The REST middleware parses and authenticates tokens that get passed through cookie or header.

The backed database was done in MongoDB to primarily deal with the storage of data recorded by the fingerprint scanner and the administration as well as the attendance information. The primary database was created and collections added based on the requirements defined and modeled in the analysis and design phase. A collection is an equivalent of a database table in the relational databases. A collection can store multiple documents, why by a document represents an entity like a user. MongoDB supports different ways of distributing data for enhanced availability. At lower level demands, replication can be done based on slave-master architecture. The replication was done for testing purposes to ensure data recorded in the primary database can be read in the secondary database for increased availability. This is a better way to deal with latency in a distributed environment in case of multiple reads. Notably, MongoDB provides another approach to distributing databases across multiple clusters with no redundancy, a method called sharding. Sharding allows both read and write operations to occur in any database and synchronization is facilitated by a set of techniques including the sharding key.

5.2 Hardware Components

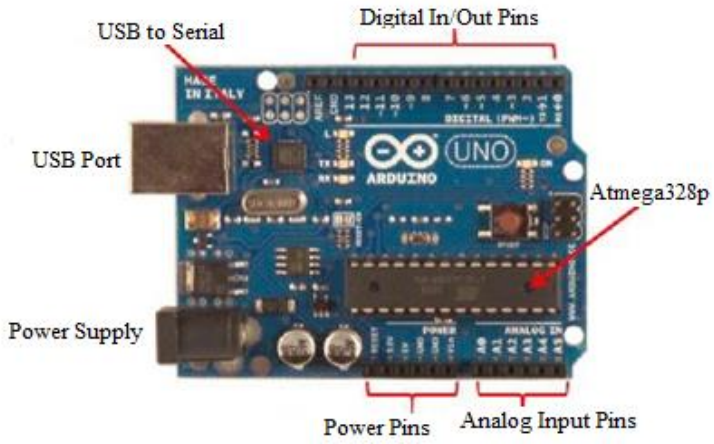

Figure 16. Arduino Uno

Arduino Uno is open-source electronics prototyping tool built on the principles of flexibility and ease-of-use technology. The microcontroller on the Arduino board is programmed using the Arduino programming language based on Wiring. In the system, this is used to receive data from the fingerprint scanner which processes and compares it to the pre-defined programmed logic codes and transmits a signal from its digital PIN 0 to the CMO3 in the application. See an image of this in Figure 16

5.3 Serial Communication

As noted earlier, JavaFX was the core programming language for the front-end components. The fingerprint scanning device utilizes serial communication. The fingerprint scanner connects to the Arduino microcontroller which connects with the computer COM port through serial communication. The fingerprint scanner communicated with the JavaFX through a Java serial port communication defined in the code. The RXTX library facilitates connection with the serial port (COM3 for Windows) to connect to the Arduino.

```
public static String fingerPrintPort = "COM3";
```

When the application starts up, it iterates through all of the system ports looking for a match for the OS and then attempts to connect to it. If it finds a match, it will break out of the “for” and “while” loops, and then connect on that port. Once the connection has been established, the user can perform any operation in the application that requires the fingerprint scanning. Error and exceptions are also defined if the connection is not established. The readers are connected to the application through the RXTX library which provides many controlling features. Using JavaFX,

the application logic was developed to ensure minimum privilege access for all user. The super admin has absolute rights and is responsible for the registration of other group admins. Notably, access to the system is primarily through username and password. Admins can register any category of users including lecturers, staff, students, and visitors. Admin can also update and delete records, view daily/monthly attendance report, and see students list selected by name, date, or month. Search can be done using the name or the fingerprint. If the fingerprint ID is matched with information stored in the database, the user data is retrieved and the same case applies to attendance.

CHAPTER SIX: RESULTS AND DISCUSSION

6.1 Results

6.1.1 Setting the Test Environment

The evaluation of the system is based on Phillips et al (2002) recommendation of the testing biometric system which focuses on technology, scenario, and operation evaluation. The goal of technology evaluation is to compare competing matching algorithm based on the standardize database collected by the fingerprint scanner. Scenario evaluation evaluates the overall system performance in a simulated application. In other words, the scenario testing should test the system in an environment that models the real-world target population. Operational evaluation determines the performance of the complete system based on the specific application domain. In particular, testing done on the biometric system was majorly offline and within a limited computing environment.

To facilitate testing, the researcher invited 20 participants to enroll and simulate attendance in the system. The attendance report is as shown in figure 17. The same number of random users also participated in the random testing of various metrics explored in here.

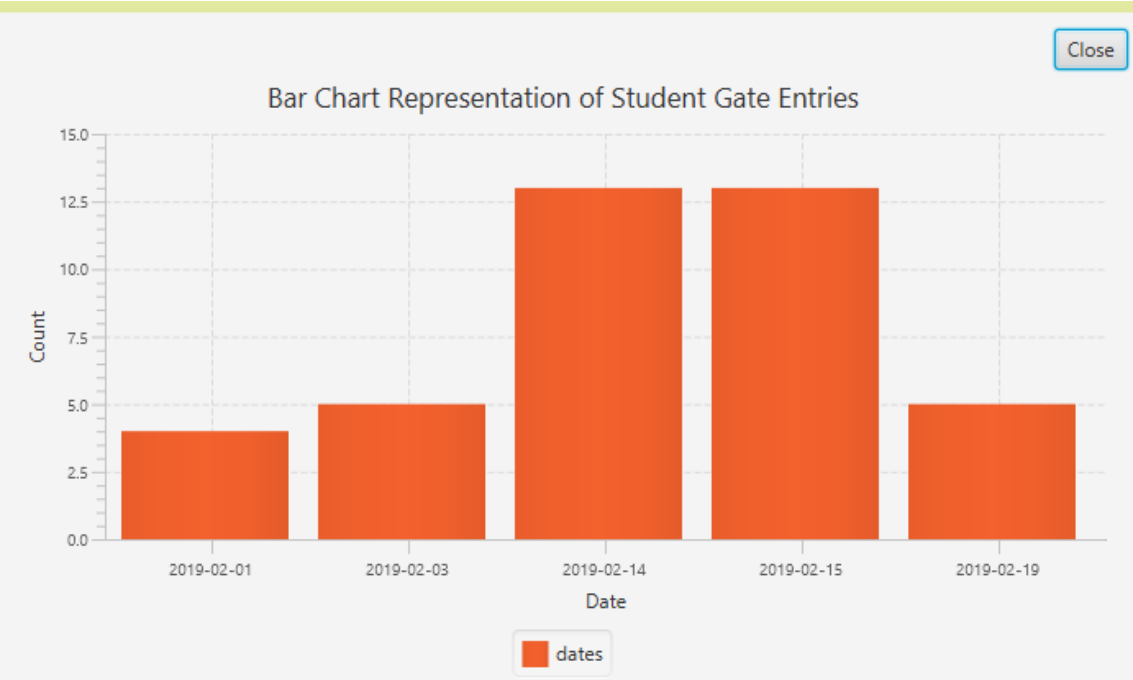

Figure 17. Sample Attendance Graph

Apache JMeter was also used for load and performance testing. Apache JMeter is the leading open-source tool for centralized and distributed load and performance testing. JMeter is a pure Java

application so setting it up required only downloading the binary and extracting it on the preferred location. A thread group of 300 users was created to simulate real traffic. HTTP Request was set as the sampler, recording start time, duration, success, response messages, and errors.

6.1.2 Biometrics Test Results

The graph below shows False accept rate (FAR), False reject rate (FRR), Failure to Enroll (FTE), and Ability to verify rate (ATV) average results for the first three attempts. The data from 50 volunteer participants were used to measure these decision rates for biometric identification. From the sample data collected, the FAR remained significantly low at 2 %.

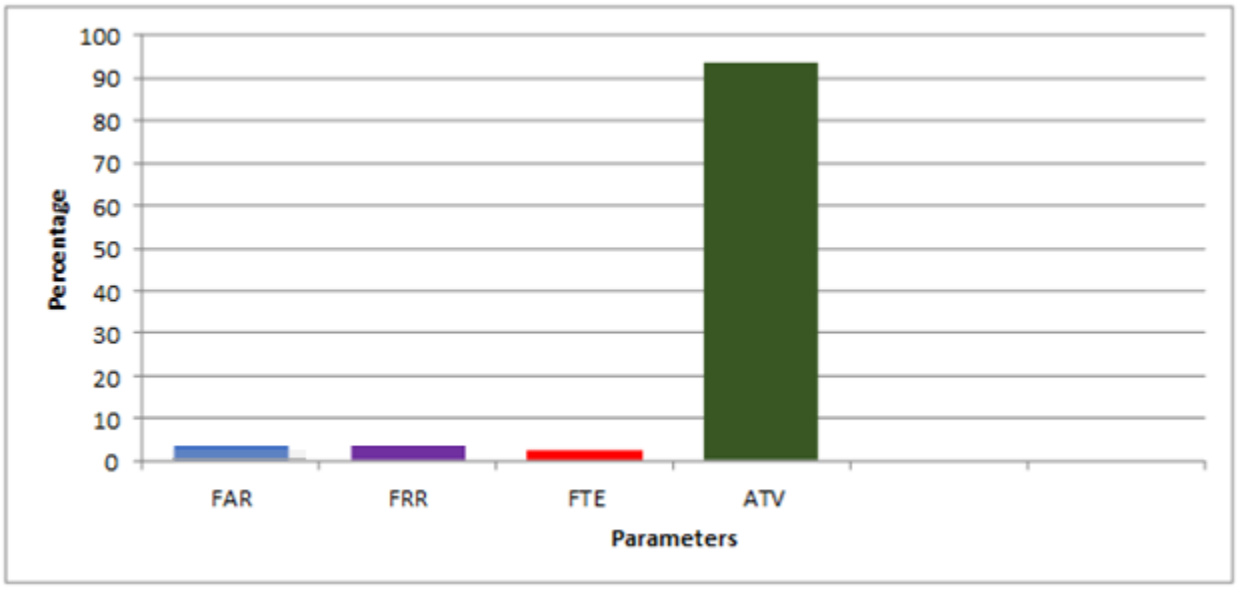

Figure 18. Biometric Test Results Graph

The system also portrayed low failure to enroll, at the rate of 1.5% while the force rejects rate was at 2%. The increased false rejection rate can be attributed to failure to place the figure at the rate position on the fingerprint scanner. On the other hand, the ability to verify rate was at 97%, showing a high confidence level and efficiency of the system to effectively identify registered users. Figure 18 shows the FAR, FRR, FTE, and ATV results.

6.1.4 Middleware Test Results

Average Response Time

The *JMeter* was configured to measure the average response time, throughput, and latency. JMeter is a powerful tool for the evaluation of performance metrics involving HTPP requests. As a result, the tool was configured to listen to specific events on some target application interfaces that interact with the middleware. The JMeter simulates actual traffic sending requests to middleware and waiting for the response. As a result, the number of thread users was configured to 300. The average response time was recorded as follows. From the graph above, the average response rate remained relatively the same as the number of users increased as shown in figure 18.

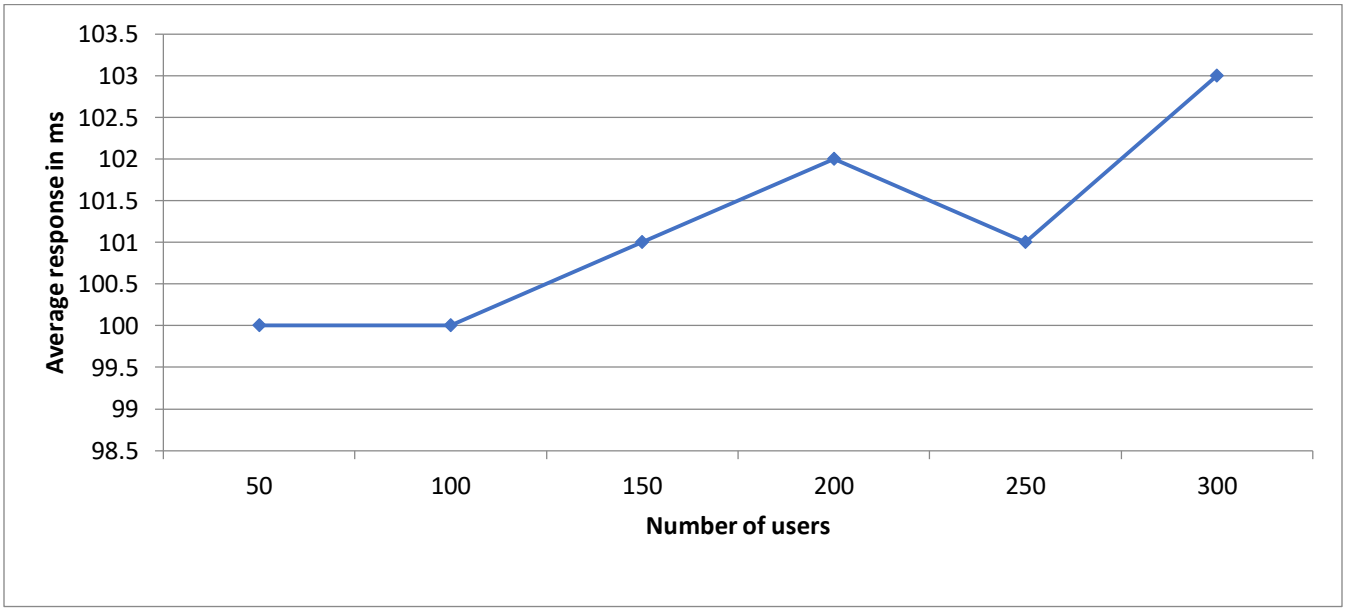

Figure 19. Average response time graph

Throughput and Latency

For meaningful results, the researcher sought to establish the relationship between throughput and latency as the load increases. The simulation results show throughput vs latency, parameterized by the injected workload. Notably, there was no clear pattern for throughput so the figures used were average rates. Throughput depends on the workload per second but in this case, workload varies

depending on the HTTP request. As a result, the researcher considered throughput at a specific level compared to latency at that level.

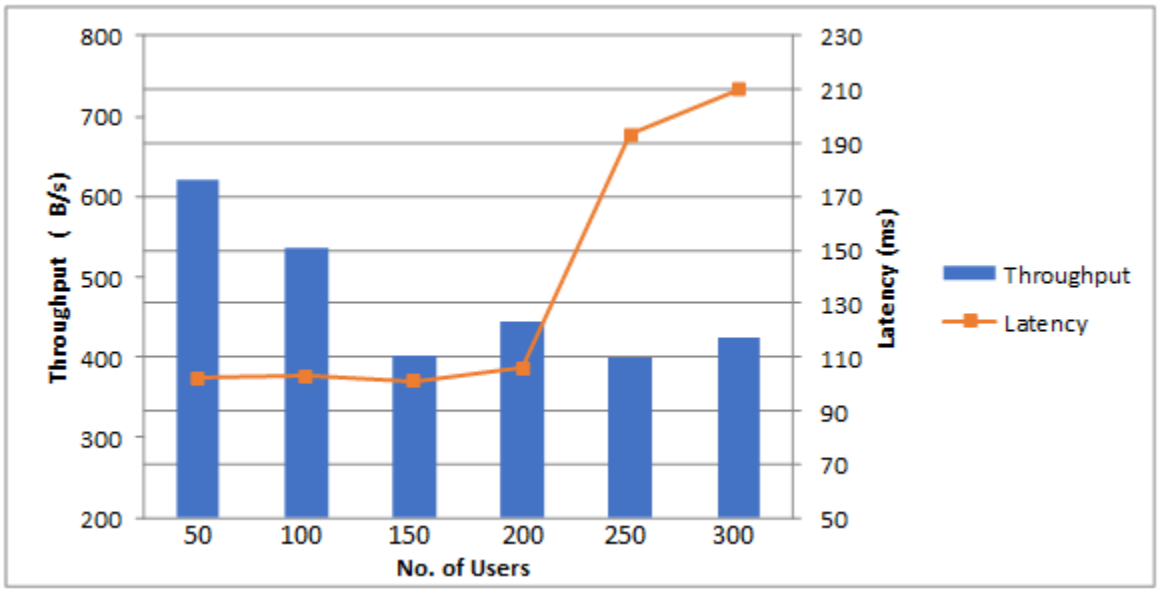

Figure 20. Throughput and Latency graph

Nevertheless, the latency remained considerably uniform as the number of users increased but began to increase exponential at some point. See Figure 20 for illustration. The middleware, in the simulated environment, was able to maintain at least 400Bytes per second throughput with an insignificant effect on latency. Throughput remained fairly consistent even as the number of simulated users grows to 300. However, latency remained fairly constant but starts to grow linearly as the number of users reached 200. This is expected as a larger number of users may be requesting the same service which leads to congestion of the channel.

6.1 Discussion

The discussion section begins with the discussion on the performance of the metrics of the complete system starting with biometric performance to average response time then throughput and latency. Thereafter, the outcomes of the prototype development are presented. To begin with, the fingerprint results showed good performance. All three errors measured (False accept rate (FAR), False reject rate (FRR), and Failure to Enroll (FTE)) remained relatively low at 0.02, 0.02,

and 0.015 respectively. The ability to verify rate (ATV) was quite high (0.97). These figures show that the performance of the biometric system is consistently superior. A biometric device is considered accurate and reliable when FAR and FTE rate figures go down. AR occurs when we accept a user whom we should actually have rejected. This type of issue is also referred to as a false positive. FRR is the problem of rejecting a legitimate user when we should have accepted him. This type of issue is commonly known outside the world of biometrics as a false negative. Either of these situations is undesirable in excess. What we try to achieve with such systems is a balance between the two error types, referred to as an equal error rate (ERR). EER is usually used as the measure of the accuracy of biometric systems. It is computed as:

$$EER = \frac{FAR+FRR}{2}$$

In the case of this project, the EER is 0.02 which is considerably low, hence the biometric system can be considered accurate and reliable. On the other hand, Ability to Verify (ATV) is a performance measure with a direct impact on system costs, security, and convenience. Mathematically, the ATV was supposed to be 0.9653 i.e. (1-0.015) (1-0.02) from the formula:

$$ATV = (1 - FTE)(1 - FRR)$$

In addition, no system can be 100 percent AVT rate but a high ATV rate is a sign of a more effective system. AVT impacts cost in that implementing a biometric system can be highly expensive due to exception processing. Any user that unable to be processed by the biometric must be processed by a fallback procedure, meaning that a dual system must be maintained. This can be an alternative biometric, a password, or a live verification which can increase the overhead cost. Hence, high ATV shows that the biometric system developed is quite useful. In terms of security, low ATV shows that a substantial percentage of users are not being verified by the implemented system. A biometric system that verifies up to 97% of the registered users in the first three attempts can be acceptable in most institutions. In regard to convenience, a low ATV reflects a difficult-to-use system. In learning institutions, convenience is paramount hence a high ATV is necessary.

In regard to the middleware performance, the average response time was relatively remained between in the range of 100 to 103 milliseconds as the simulated user's workload grew to 300. The interest here was on user growth, scalability, and user satisfaction. Timeliness and speed have

a direct correlation with satisfaction. A first response perceived as fast can set the system on the right track for a positive first impression. Fast response time also is an opportunity for growth. It shows that the system can accommodate a wide array of users without affecting performance. A middleware-based application must be able to handle large increases in simultaneous users, data volume and other workloads. Linearly scalable applications are perfectly scalable in that their performance degrades at a constant rate directly proportional to their demands. The graph of response time shows that the middleware begins to deviate from linear scalability after about 200 users.

The middleware was able to process requests from users at the rate of at least 400 MB in less than a second even as the user base grows. It also recorded low latency of about 100 milliseconds, with the highest being 210 milliseconds for simulated number of 300 users. However, since latency began to increase linearly after 200 users, it selected as the ideal number of concurrent users that the middleware can support at a given time. At this point, latency remained at 100 milliseconds, with a throughput of 460 MB per second. Another observation is that when latency begins to increase, throughput starts to decrease. This is attributed to the middleware controlling HTTP requests to avoid overloading the system. This enables the middleware to control HTTP requests per given time to maintain a stable processing time.

To this end, the research has successfully demonstrated a working low-cost scalable prototype with high-performance features and accuracy. The product is low cost in the sense that it leverages low-cost and opensource components to create a high-performance prototype. Compared to other biometric technologies such as iris scanners, fingerprint scanners are considerably inexpensive, less intrusive, and with high acceptability. Similarly, the prototype used open-source database management system. MongoDB has a built-in capacity for replication and sharding to deal with growth in population and distribution of data centers. On the other hand, the use of RESTful API offers great benefits to the distribution of application and controlling access to the database. This is a low-cost approach for distributed architecture providing security and processing of data from multiple sources. Hence, this is an access control and attendance management solution that can offer the low-cost scalable option to institutions of higher learning with a high population.

CHAPTER SEVEN: CONCLUSION

This research and prototype study was able to achieve three objectives. The project involved designing, developing, and testing a low-cost scalable biometric user access control system that utilizes distributed technology. As a result, there were several components of the project. After a detailed study of the biometrics, the fingerprint was found to be less intrusive and offering a cost-effective method of user identification. A REST API was designed as a middleware to facilitate communication between the client-side and the server-side component of the prototype. The API was based on PHP and JSON for data parsing. The REST middleware/API allow integration of multiple client-side terminals. In the backend, the MongoDB was utilized as the database to store information about the users. MongoDB is a distributed NoSQL database management system that allows a high level of scalability and performance. These technologies allowed the development of a highly scalable system that can facilitate fast identification with high precision, accuracy, and speed. The scalability of the design allows the system to be implemented in large corporations and institutions of higher learning.

7.1 Future Work

Future projects can focus on multi-modal biometric identification. Multi-modal biometrics involves using more than open behavioral or physiological characteristics for enrollment, verification, and identification. This is an emerging trend and there is a growing demand to combine various modalities to improve recognition accuracy. The multi-modal approach can be appropriate for unique deployment scenarios and when security is a major concern. Currently, multi-modal biometrics have been designed for identification but not all are suitable for universal application. Biometrics aside, researchers can explore the effectiveness of distributed clusters of MongoDB in the authentication of users. Also known as sharding, clustering distributes data across the shards in the cluster, enabling a shard to host a subset of the total cluster data. As the data set grows, additional shards increase the storage capacity of the cluster and can be useful in organizations that have huge sources of data.

BIBLIOGRAPHY

Ahmad, F., Abbas, S. W., Singh, J., & Mishra, N. K. (2015). Students Attendance Monitoring System Based on RFID and GSM Network. In *International Journal of Emerging Technologies and Innovative Research JETIR* (Vol. 2, No. 4 (April-2015)). JETIR.

Ahmed, A., Mikail, O. O., Kolo, J. G., & Durugo, C. (2016, November). A Multifactor Student Attendance Management System Using Fingerprint Biometrics and RFID Techniques. In *International Conference on Information and Communication Technology and Its Applications. 11th.*

Dalwadi, D., Guriwala, I., Chaudhary, S., Kapadia, M., & Savalia, M. (2016). Implementation of Attendance System based on RFID and GSM with respect to Power Saving Concept. *International Journal of Current Engineering and Technology*, 6(2), 539-541.

Hasan, R., Khan, M. M., Ashek, A., & Rumpa, I. J. (2015). Microcontroller Based Home Security System with GSM Technology. *Open Journal of Safety Science and Technology*, *5*(02), 55.

Kalyani, C., H. (2017). Various Biometric Authentication Techniques: A Review. *Journal of Biometrics & Biostatistics*. 8(5): 371 DOI: 10.4172/2155-6180.1000371

Koong, C. S., Yang, T. I., & Tseng, C. C. (2014). A user authentication scheme using physiological and behavioral biometrics for multitouch devices. *The Scientific World Journal*, *2014*.

Kumari, S., & Rath, S. K. (2015). Performance comparison of soap and rest based web services for enterprise application integration. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1656-1660). IEEE.

Kumbhar, A. A., Wanjara, K. S., Trivedi, D. H., Khairatkar, A. U., & Sharma, D. (2014). Automated attendance monitoring system using the android platform. *International Journal of Current Engineering and Technology*, *4*(2), 1096-1099.

Maheshwaran, P., Kumar, R., Rajeswari., & Mungara, J. (2017). A Review on Requirement Engineering in Rapid Application Development. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 2(3), 742-746.

Phillips, P. J., Martin, A., Wilson, C. L., & Przybocki, M. (2000). An introduction to evaluating biometric systems. *Computer*, (2), 56-63.

Shah, D. (2016). IoT based biometrics implementation on Raspberry Pi. *Procedia Computer Science*, *79*, 328-336.

Srinidhi, M. B., & Roy, R. (2015). A web enabled secured system for attendance monitoring and real-time location tracking using Biometric and Radio Frequency Identification (RFID) technology. In *Computer Communication and Informatics (ICCCI), 2015 International Conference on*(pp. 1-5). IEEE.

Talaviya, G., Ramteke, R., & Shete, A. K. (2013). Wireless fingerprint based college attendance system using Zigbee technology. *International Journal of Engineering and Advanced Technology (IJEAT) ISSN*, *2249*, 8958.

Tanenbaum, A. S., & Van Steen, M. (2007). *Distributed systems: principles and paradigms*. Prentice-Hall.

Thepade, S. D., & Bhondave, R. K. (2015). Bimodal biometric identification with Palmprint and Iris traits using fractional coefficients of Walsh, Haar and Kekre transform. In *Communication, Information & Computing Technology (ICCICT), 2015 International Conference on* (pp. 1-4). IEEE.

Tihomirovs, J., & Grabis, J. (2016). Comparison of soap and rest based web services using software evaluation metrics. *Information Technology and Management Science*, *19*(1), 92-97.

Ufoaroh, S. U., Oranugo, C. O., & Uchechukwu, M. E. (2015). Heartbeat monitoring and alert system using GSM technology. *International Journal of Engineering Research and General Science*, *3*(4), 26-34.

Unar, J. A., Seng, W. C., & Abbasi, A. (2014). A review of biometric technology along with trends and prospects. *Pattern Recognition*, *47*(8), 2673-2688.

Vorona, V. A., & Kostenko, V. O. (2016). Biometric identification technology in monitoring systems and access control. *Computational nanotechnology*, (3), 224-241.

Walia, H., & Jain, N. (2016). Fingerprint Based Attendance Systems-A Review. *International Research Journal of Engineering and Technology (IRJET) Volume*, *3*. 45-59.

Wallace, L. G., & Sheetz, S. D. (2014). The adoption of software measures: A technology acceptance model (TAM) perspective. *Information & Management*, *51*(2), 249-259.

Yadav, D. K., Singh, S., Pujari, S., & Mishra, P. (2015). Fingerprint Based Attendance System Using Microcontroller and LabView. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, *4*(6), 5111-5121.

APPENDICES

Appendix A Hardware Components (Fingerprint Scanner and Arduino Microcontroller)

An illustration of the hardware component that acts as the fingerprint scanner to identify/authenticate.

Appendix B Real-time View of Successful Identification

The administrators can view live authentication data from the fingerprint identification module. It shows the attendance data such as name and time as the show.