# IMPLEMENTATION OF BIOMETRIC ACCESS CONTROL FOR DEPARTMENTAL ENTRY DOOR

**BY**


| | |
|---|---|
| **JOSIAH CHINONSO EDMUND** | **ENG1805489** |
| **MADAMEDON AYIRIORITSE ISAAC** | **ENG1805491** |
| **ASIJE IMOHIMI MISHAEL** | **ENG1805356** |
| **OSHIOGWEMO SHEM OSEMUDIAMEN** | **ENG1905739** |

**DEPARTMENT OF MECHANICAL ENGINEERING**

**FACULTY OF ENGINEERING**

**UNIVERSITY OF BENIN,**

**BENIN CITY.**


**APRIL, 2024.**

# IMPLEMENTATION OF BIOMETRIC ACCESS CONTROL FOR DEPARTMENTAL ENTRY DOOR

**BY**


| | |
|---|---|
| **JOSIAH CHINONSO EDMUND** | **ENG1805489** |
| **MADAMEDON AYIRIORITSE ISAAC** | **ENG1805491** |
| **ASIJE IMOHIMI MISHAEL** | **ENG1805356** |
| **OSHIOGWEMO SHEM OSEMUDIAMEN** | **ENG1905739** |


**TO**


**DEPARTMENT OF MECHANICAL ENGINEERING FACULTY OF ENGINEERING**

**UNIVERSITY OF BENIN, BENIN-CITY.**


**IN PARTIAL FULFILLMENT OF THE REQUIREMENST FOR THE AWARD OF BACHELOR IN ENGINEERING DEGREE**

**DEPARTMENT OF MECHANICAL ENGINEERING, UNIVERSITY OF BENIN.**

**APRIL, 2024.**

## CERTIFICATION

This is to certify that this project submitted to the Department of Mechanical Engineering was carried out by JOSIAH CHINONSO EDMUND, MADAMEDON AYIRIORITSE, OSHIOGWEMO SHEM OSEMUDIAMEN, and ASIJE IMOHIMI MISHAEL of the Department of Mechatronics Engineering and Mechanical Engineering, University of Benin, Benin City, Edo State, Nigeria, under the supervision of Engr. P. O. OLAGBEGI.

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

**ENGR. P. O. OLAGBEGI**

PROJECT SUPERVISOR

Date

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

**ENGR. DR. I. B. OWUNNA**

PROJECT COORDINATOR

Date

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

**PROF. E.G SADJERE**

HEAD OF DEPARTMENT

Date

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

**EXTERNAL EXAMINER**

Date

## DEDICATION

We gratefully acknowledge the grace of God Almighty and the unwavering support of our parents and family who have nurtured us throughout our time at the University of Benin.

## ACKNOWLEDGEMENT

We would like to express our sincere gratitude to our project supervisor, Engr. P. O. Olagbegi, for his invaluable guidance and support throughout this project. Your insightful feedback, technical expertise, and encouragement were instrumental in the successful completion of this project. We are particularly grateful for your patience in guiding me through the process of installation of the Biometric system.

We would like to express our sincere appreciation to God Almighty for watching over us throughout our stay in the university and all those who have supported us in completing this project. We also thank our classmates for their valuable suggestions.

Finally, we are thankful to our families and friends for their unwavering support and encouragement throughout this journey.

## ABSTRACT

In an era marked by increasing concerns for security and accessibility, the implementation of robust access control systems stands as a paramount necessity. This project focuses on the integration of biometric access control technology, specifically the X6 Access Control system, for departmental entry doors. The objectives encompassed comprehensive research on biometric access control, assessment of the entry door's condition, replacement of access cards with a fingerprint-enabled security system, and organization of user training sessions to ensure effective adoption.

The methodology employed involved a systematic approach, beginning with thorough research to understand the principles and technologies underlying biometric access control. Subsequently, the condition of the entry door was assessed, ensuring its suitability for the installation of the new system. The X6 Access Control system was then meticulously integrated, involving installation, configuration, and functional testing to ensure seamless operation. User training sessions were conducted to acquaint departmental staff with the new system, addressing concerns and facilitating its adoption.

Data collection methods included user feedback, system performance metrics, and security incident reports, analyzed using statistical techniques to evaluate the system's effectiveness. Throughout the project, references to relevant literature and industry standards guided decision-making and methodology implementation.

This project contributes to enhancing security measures and improving access control mechanisms within departmental environments, fostering efficiency, convenience, and user acceptance through the implementation of biometric technology.

# TABLE OF CONTENT

## LIST OF FIGURES

## LIST OF TABLES

# CHAPTER ONE

# INTRODUCTION

## 1.1 BACKGROUND TO THE STUDY

Security has been one of the fundamental needs of man from time immemorial. Humans have always sought for ways to secure their lives and properties from harm sources which could be from humans, animals and even nature. Any system put in place to protect or secure anything is called a security system. Security systems can be used for humans, animals, physical assets, data or information. The purpose of security spans from protection to privacy to preservation, however the object of protection determines the means.

It is no longer news that the global crime rate has seen a significant rise in recent years. This issue is turning more severe every day. To get away with this problem, there is need to take help from technology. It's always wiser to prevent problems than to deal with their consequences. Taking proactive steps to eliminate issues before they arise is far better than facing the negative outcomes later.

The door access control is a physical security that assures the security of a building by limiting access to the building to specific people and by keeping records of such entries [Mohammed, S. 2007]. The Door lock system of security has been in existence for decades, however several improvement has been made to improve this door lock systems. The door lock system finds use at homes, commercial environment, industrial environment, in the military and in almost all areas of life.

Security describes protection of life and property. The security sector is experiencing diversification as it has never seen before. This has brought about the need to review the

reliability of already existing systems and look into the possibility of creating better systems that are smarter and more secure Ushie, et al, (2015).

The present electronic security systems we now enjoy have unequivocally been around for a very long time, although it has gone through a series of evolutionary changes to cater for the needs and security concerns of the present generation Tamunowari, (2018).

From using sticks to wedge doors to using mechanical locks, security systems have transformed into using electronic equipment such as the microcontrollers to achieve a satisfactory security system Tamunowari, (2018).

Due to the drawback of other various form of door lock system; these nurture the needs for the implementation of a digital door lock system. Hence, this project work caption "implementation of biometric access control for departmental entry door". The term "biometrics" refers to a technology that makes use of physiological and behavioral traits of humans for a variety of functions which includes identification, verification, access control, user authorization, data protection, and security management [Shelar, (2013)]. Biometric characteristics are significantly more difficult to fake, reproduce, share, lose, or guess [PRABHAKAR, (2003)]. The individual being authenticated must be present during the authentication process using a biometric system making it more reliable than old fashioned systems such as keys, passwords, cards etc. [PRABHAKAR, (2003)] Currently, there are six main biometric technologies in the market. They are: Facial recognition, Voice recognition, Hand geometry recognition, fingerprint recognition, Iris and Retina recognition. The most widely applied of these recognition technologies are facial recognition, fingerprint recognition, and iris recognition [H. Wechsler, (2007)] When compared to other biometric systems, fingerprint recognition systems are fairly affordable, and user

acceptance is very high. The versatility of fingerprint identification makes it effective in a wide range of settings. Additionally, it is a tried-and-true core technology, and the capability of registering many fingers can significantly improve system accuracy and adaptability [Y. Wang, (2012)]. Strong security systems are currently in demand in both homes and organizations. To avoid unauthorized entry, the need of developing and implementing a biometric security system incorporating fingerprint technology cannot be overstated.

This approach to identity verification operates on the principles of inherent biological differences among individuals within a given society. Leveraging human variation in access control represents the most dependable method for regulating entry to a particular building structure because each person in the world possesses distinct characteristics. For example, in the utilization of fingerprints for this project, every individual has a unique fingerprint, distinguishing them from every other person globally. This provides an ideal mechanism for controlling access to a facility.

This thesis presents a fingerprint-based security system and door lock designed to protect buildings from intruders. By using biometric identification, specifically fingerprint recognition, the system controls access to the building, granting entry only to authorized individuals whose fingerprints are registered. The core component is a fingerprint module responsible for scanning and verifying fingerprints to determine access privileges.

The system functions by initially registering a master fingerprint, which serves as the primary default access to the structure. This master fingerprint then registers the necessary access permissions for individuals to enter the building. Consequently, anyone seeking access to the building structure must be registered by the master fingerprint before being

granted entry. Upon installation, the user simply places their hand on the module, which scans the fingerprint and compares it to its stored records. If the fingerprint matches any of the records, the door lock unlocks, granting access to the individual.

Fingerprint-based access control offers superior security compared to traditional swipe cards or ID cards due to the unique nature of each individual's fingerprint. This biometric technology has captivated human interest for centuries, with fingerprints serving as a reliable form of personal identification since ancient times.

## 1.2 STATEMENT OF PROBLEM

Through observation, one could attest to the fact that the key cards used to access the departmental doors are very susceptible to getting lost, moreover, such access keys can be duplicated by unauthorized users. Also passwords used to access the doors could be transferred to unauthorized users. This jeopardizes the safety of sensitive information and resources within the department.

Hence, there is a pressing need to implement a more secure, efficient, and reliable access control system for the departmental door. A biometric solution utilizing fingerprint recognition technology presents an opportunity to enhance security while streamlining access management processes. However, the successful implementation of such a system requires addressing several key challenges, including hardware compatibility, software integration, user enrollment processes, and system reliability.

## 1.3 AIM AND OBJECTIVES

### 1.3.1 AIM

This project aims to implement a fingerprint-based access control system for the department.

### 1.3.2 OBJECTIVES

The objectives are as follows:

i. Conducting research on biometric access control.

ii. Ensuring that the door is in good condition.

iii. Replace access cards by implementing a comprehensive fingerprint-enabled electronic security system.

iv. Organize training sessions to acquaint users with the new system, encouraging its adoption and resolving any concerns or inquiries.

## 1.4 SIGNIFICANCE OF STUDY

There are a lot of reasons why the implementation of biometric access control is needed for the departmental entry door. These reasons range from challenges that the existing mode of access have faced, and still facing.

Firstly, by employing fingerprint recognition technology, the system ensures a higher level of security as fingerprints are unique to individuals, significantly reducing the risk of unauthorized access Jain, A. K., Ross, A., & Nandakumar, K. (2016). Secondly, fingerprint access control offers a more streamlined and efficient means of entry compared to manual methods. Authorized personnel can gain access without the need for physical keys or cards, reducing the likelihood of delays or inconveniences associated with misplaced or forgotten

credentials Rathgeb, C., & Busch, C. (2017). Thirdly, this study will help improve access control as the system can be programmed to grant access based on specific user permissions Kaur, P., & Kaur, A. (2016). Lastly, this project contributes to the body of knowledge in the field of biometric security systems by exploring the practical implementation of fingerprint recognition technology in a specific organizational context. Findings from this study can inform future research and development efforts aimed at improving access control systems Li, S. Z., & Jain, A. K. (Eds.). (2011).

## 1.5 SCOPE OF PROJECT

The scope of this project includes the implementation of a biometric access control system on the departmental entry door and how to configure it . It also includes carrying out literature review to understand previous works done. This project will focus exclusively on a fingerprint-based electronic door access system. More complex security features such as iris scanning or facial recognition will not be included.

# CHAPTER TWO

# LITERATURE REVIEW

## 2.1 REVIEW OF RELATED WORKS

Umar et al [B. U. Umar, (2018)] developed a fingerprint door access control system which incorporates D.C motor, LED, microcontroller and fingerprint sensor as major components. The design was made into sub-circuits comprising of input and output sub-systems. The input sub systems include the fingerprint sensor and keypad buttons while the output subsystems is interfaced on the output port of the microcontroller unit. This includes the 12v relay, dc motor, LED display and buzzer alarm. The system works by authorizing registered prints to unlock the door and denying access to unauthorized persons in addition to setting off an alarm. The system was able to function as intended. However, it employs single step authentication in its approach.

Okeimute and his colleagues [O. A. Okeimute, (2018)] developed a system using biometric finger print. User is required to scan finger for authentication, if a matching finger is obtained, access is granted. Access is denied for an unauthorized person and the buzzer is activated to alert the user of an intrusion. There is no provision of adding more fingerprints using this system.

Komol et al [M. M. R. Komol, (2018)] developed a two-step verification system using RFID and finger print sensor to access a door. In this system, user is first required to scan their RFID card. If a valid id is matched, the finger print scanner is then activated further prompting the user to scan their finger. If the right match is obtained, the microcontroller which operates the motor connected to the door latch opens the door. Security is raised

using two-step verification. The system however has its limitations in the sense that, it creates the necessity of carrying RFID card. The system is also incapable of adding more users.

Ahmad and his team [S. U. Ahmad, (2019)] in their work “security lock with effective verification traits”, implemented a five step verification security system. The five levels of security includes entering of password on interactive GUI, thumbprint, facial recognition, speech pattern recognition, and vein pattern recognition. The traits used involves checking, training and verifying processes with application of machine learning operations. Security verification is optimal in this system. However the implementation cost of this system is high.

A system designed by Rajesh and colleagues [K.Rajesh, (2019)] using finger print to control the opening of vehicle door. The microcontroller stores the data equivalent of fingerprint of the master user. The control circuitry sends appropriate signals to the motor relays operating the door of the vehicle. The system is able to provide security. However Alarm system is absent in the design.

Paul et al [P. Paul, (2019)] in their work ‘smart door lock using finger print sensor’ implemented a system using finger print and GSM technology. This system operates by scanning a user's fingerprint using a fingerprint scanner connected to a microcontroller. The microcontroller then compares the scanned fingerprint to a stored database. If there's a match, the microcontroller signals the door latch to open, unlocking the door. If a wrong finger print is entered, the system beeps the buzzer showing ‘try again’ on the LCD display.

If five consecutive attempt is made, the system activates a secure mode, triggering an alarm and displaying "panic mode" on the LCD screen. Simultaneously, a notification is sent to the owner alerting them of a potential break-in attempt. The project was a success. However more prints cannot be added if required however has its limitations in the sense that, it creates the necessity of carrying RFID card. The system is also incapable of adding more users.

Alghamdi [A. Alghamdi, (2020) ] proposed a security lock system which incorporates the keypad, fingerprint, face ID and user phone. Additional features such as camera and motion sensor is also included for monitoring purposes. The use of mobile is to allow for remote control and giving multiple users privileges such as remote unlocking, granting authority to other users, and knowing the situation at the door using the established monitoring systems. The system adopts modern technological components. ZigBee receives and send signals to the STM32 microcontroller which is connected to every other components, TFT touch screen is used to provide LCD display. The system is capable of providing robust security. However, cost of components is high.

Sarma et [M. sarma, (2020) ] Proposed a system based on fingerprint, GSM technology with the incorporation of a camera to capture images of unauthorized persons. The system is capable of capturing the finger print image of unauthorized person in addition to sending notification message to registered phone number. However, Power failure will make the system inoperative.

Ipilakyaa et [T. D. Ipilakyaa, (2020)] Designed a security system based on finger print and GSM technology. The first step is the enrolment of user. The keypad is used to enrol a new fingerprint. After the finger has been successfully registered, user now has access. Once a finger is placed on the sensor, the microcontroller tries to verify the print by matching it with the one stored in its memory. Once a match is found, access is granted with a welcome message on the LCD screen. However, if there is no matching print, the SIM card module automatically sends a notification message to the registered number notifying of a break in attempt. The system is able to provide reliable security at low cost. Nonetheless power failure will make the system inaccessible.

Mahjabeen and his colleague [D. Mahjabeen, (2021)] implemented a door lock system using fingerprint, microcontroller, LCD and motor for locking and unlocking of a door. The system works by taking the fingerprint of a user and matching it against its stored templates. If the entered fingerprint matches, the microcontroller sends two signals, one to the LCD and another to the motor operating the locking and unlocking process. The system was able to function as designed. However, no provision for adding more prints was made.

A system designed by chandhru and his colleagues [V. Chandru, (2021)] using a mobile application and Bluetooth wireless module. Here user must first connect their phone to the system and log into the application. An OTP will be sent to their registered mobile number as a further means of verification. Next user is required to enter finger print scanner on their mobile to unlock the door. User also can view and remove any person who have logged in the system by using fire base. Security at minimal cost is achieved in this system. Short

range of Bluetooth however can make establishing connection difficult in addition to creating the necessity of carrying the phone.

Okoduwa and his colleague [E. O. Okoduwa (2022)] developed a fingerprint based biometric access control system which employs microcontroller, fingerprint module, LCD, H-bridge motor, control buttons and signal LEDs. Using a controlled 5v, the supply unit supplies power to the LCD, fingerprint sensor, and microcontroller. The system database is used to check a fingerprint image with previously stored image scans. Upon recognition, the microcontroller enables the H-bridge motor to control the automated sliding door opening. The control buttons were used for administrative purposes to add or remove users as required. Overall, the projects performance was evaluated and was determined to be adequate. Nonetheless, it adopts a single step authentication approach in its operation.

Raghu and his colleague [R. G. Raghu (2013)] proposed a locker system that employs RFID, fingerprint, password and GSM. In this system, RFID module reads the ID number from passive tag and sends it to the LPC2148 microcontroller. A valid ID will activate the fingerprint sensor else, the process is terminated. If the scanned fingerprint matches, the microcontroller sends a password to the registered phone number. The authenticated user enters the password and the locker gets unlocked. Security is enhanced using this multi-step authentication. However, the system application is restricted to areas requiring high security like vaults, ATM and safes but not suitable for use in residential homes. No provision is made to register more prints.

## 2.2 FINGERPRINT RECOGNITION

Fingerprints are unique patterns formed by raised ridges and valleys on the fingertips**.** These patterns are categorized into three main types: arches, loops, and whorls. Additionally, core (the center) and delta (the point where patterns diverge) can be used for fingerprint alignment, though they aren't present in all prints. These characteristics, illustrated in Figure 1, are the basis for fingerprint recognition.

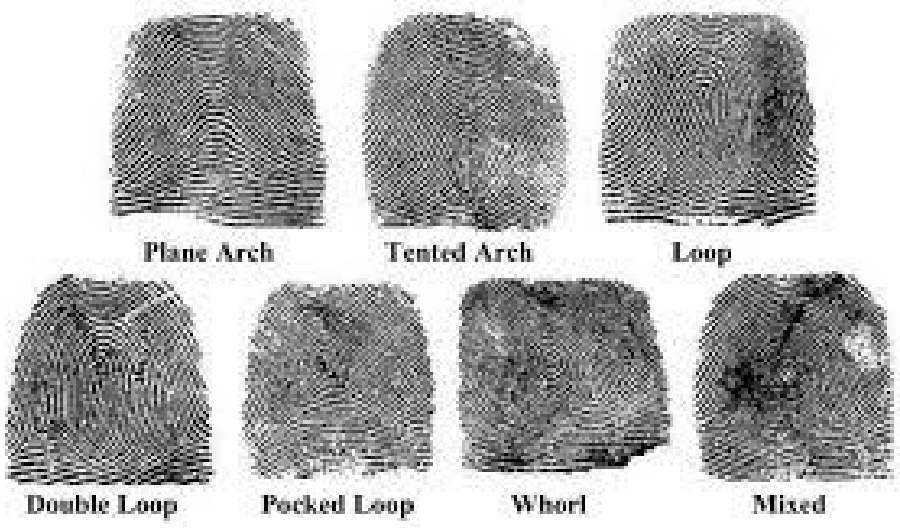



*Figure 1: Fingerprint patterns*

Fingerprint recognition relies on unique patterns called minutiae (see Figure 2), hence the term "minutiae matching." These minutiae are distinctive points where the fingerprint ridge structure is interrupted. The two primary types are endings, where a ridge stops, and bifurcations, where a ridge splits into two.

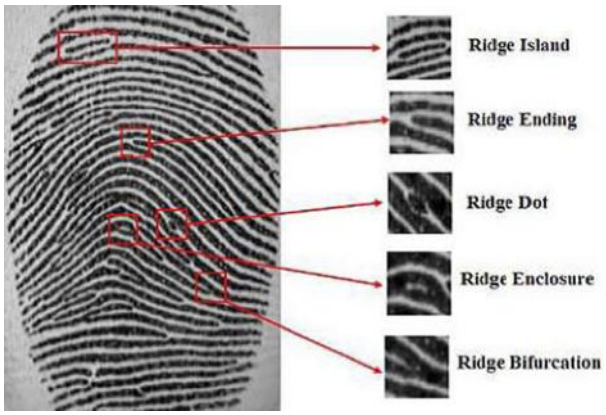



*Figure 2: Fingerprint characteristics (minutiae)*

Both pattern and minutiae matching include the same fundamental procedures in the recognition of a fingerprint. One of the three available sensor types optical, silicon (capacitance), or ultrasound is used to first capture a high-quality image. With an optical sensor, the user places their finger on the sensor surface (platen), and a laser illuminates the fingerprint. The ridges on the fingerprint reflect this light, which is then transformed into a digital signal [Irish Council for Bioethics, Dublin].

### 2.2.1 HISTORY OF FINGERPRINT RECOGNITION

With a history that dates back to at least 6000 B.C. [ J. L. Wayman, (1981)] , finger-print recognition is the oldest form of biometric identification. The Assyrians, Babylonians, Japanese, and Chinese were the first civilizations to employ fingerprints to sign legal documents, according to historical records. The usage of fingerprints on clay tablets for business transactions dates back to ancient Babylon. According to explorer Joao de Barros, fingerprinting was practiced in China. He said that Chinese merchants used ink to stamp children's footprints and palm prints to differentiate one youngster from another. Sir Francis Galton published a thorough examination of fingerprints in the late 19th century and

proposed a new classification scheme that made use of the prints from all 10 fingers. Galton calculated that the probability of two distinct fingerprints being identical was one in 64 billion. The traits used to identify fingerprints today (minutia) were first identified by Galton. Galton's Details is a term used frequently to describe this minutiae classification. The first systematic use of fingerprints to identify convicts in the United States occurred in 1903 with the New York State Prison System. During the next 25 years, increasing numbers of law enforcement agencies joined in the use of fingerprints as a means of personal identification [National Biometric Security Project].

The State of California started requesting fingerprints as part of its driving license application process in the middle of the 1980s [National Biometric Security Project]. The International Biometrics Association (IBA), the first industrial association for biometrics, was established between 1986 and 1987 [National Biometric Security Project]. After the beginning of the 20th century, many biometric techniques were being employed by people in their daily lives.

## 2.3 FINGERPRINT DOOR LOCKS

Modern fingerprint door locks aim to combine the benefits of secure, convenient access control with the capabilities of internet connectivity and remote operation. Several products offering these features are available on the market, and we will discuss some of them.

### 2.3.1 SIFELY SMART LOCK

The Sifely Smart Lock is packed with features aimed at offering multiple ways of accessing your property. The Sifely X Smart Lock houses a fingerprint scanner in the handle, allowing you to quickly gain access to the property. In addition to the fingerprint scanner,

you can unlock the Sifely smart lock with a pin code, key card, or mobile app. Furthermore, Sifely's smart lock connects to the internet via a WiFi gateway, granting you remote capabilities. Users can unlock or lock the door remotely, grant access to visitors, or control the lock with a compatible voice assistant like Alexa or Google.


*Figure 3: Sifely smart lock*

### 2.3.2 CATCHFACE FINGERPRINT DOOR LOCK

The CatchFace fingerprint door handle encompasses a variety of smart lock features. Above all, the CatchFace's touch ID door lock can connect to the internet via a WiFi gateway. In turn, you can remotely manage your lock from anywhere using the mobile app.

*Figure 4: Catchface fingerprint door lock*

### 2.3.3 WYZE LOCK BOLT

The Wyze Lock Bolt is a Bluetooth-enabled smart lock that is a modern replacement for existing deadbolt. It allows the use of fingerprint as mode of access. The biometric deadbolt lock is equipped with the auto-lock feature which ensures that the door is locked even if you forget to lock the door yourself.

*Figure 5: Wyze lock bolt*

### 2.3.4 MASTER LOCK BIOMETRIC PADLOCK

The Master Lock Biometric Padlock is a great mobile lock solution for a variety of situations. Up to 10 different users may use their fingerprints to unlock the padlock. It's powered by a button battery, so it should last up to a year. In the event that the battery is low, the padlock will notify the light indicators around the scanner, and you may use the directional keypad to unlock it.


*Figure 6: Master lock biometric padlock*

### 2.3.5 GEEK SMART FINGERPRINT DOOR LOCK

The Geek Smart Fingerprint Door Lock is battery-powered, requiring four AAA batteries. If the batteries die, a USB-C cable is included to connect the fingerprint door handle to a power source.

*Figure 7: Geek smart fingerprint door lock*

## 2.4 DESCRIPTION OF COMPONENTS

In implementing the biometric access control on the departmental entry door, some components were made use of. These components were selected in line with the requirements of the implementation, specification and also the cost effectiveness and durability of the materials. The subsequent section gives a description of the major hardware components used in the implementation.

### 2.4.1 X6 FINGERPRINT ACCESS CONTROL

The X6 fingerprint access control system is the core component of this project. This advanced device employs cutting-edge biometric technology to provide highly accurate and rapid fingerprint matching for access control. The X6 operates independently and can be integrated with various security components such as electric locks, alarms, door sensors, exit buttons, and doorbells. Its user-friendly keypad allows for easy management of user data, including enrollment, deletion, and access control settings.


*Figure 8: X6 fingerprint access control*

The X6 access control comprises of various components. These includes :

#### 2.4.1.1 FINGERPRINT SENSOR

A fingerprint sensor (Figure 9) is an electronic device that captures a digital image of a fingerprint, known as a live scan. This image undergoes digital processing to create a biometric template, a set of extracted features stored for comparison purposes. The fingerprint sensor used in this project is the ZK optical sensor. This provide a wide range of non-invasive sensors, among all the ones that are the most important. They are characterized of the optical sensors provide, and have a strong light transmission. However, they are less expensive than high-sensitive materials, and one of the most common ones.


*Figure 9: Fingerprint sensor*

#### 2.4.1.2 MICROPROCESSOR

The microprocessor serves as the brain of a biometric lock system, providing the computational power necessary to perform various tasks involved in fingerprint recognition, RFID card and token recognition and lock control.

#### 2.4.1.3 KEYPAD MODULE

A keypad module is a set of button that are arranged in a block or pad and consist of digit. A numeric keypad is a pad that primarily has numbers on it. The keypad is utilized in this project as the input means. There are exactly the same input values because there are a total of 13 keys including the alarm button. It has an adhesive base for simple mounting in a range of application. It's incredibly thin, and is simple to interface with any microcontroller. Its function here is mainly for pin verification and initiating fingerprint enrollment decisions.


*Figure 10: Keypad module*

### 2.4.2 DOOR HANDLE

The function of a push and pull door handle is to provide a means for opening and closing a door by exerting force in either a pushing or pulling motion after biometric authentication.


*Figure 11: Door handles*

### 2.4.3 SOLENOID LOCK

An electronic solenoid is a device that functions essentially as an electromagnet. It is made of a large coil of copper wire with an armature (slug of metal) in the center. When the coil is energized, the slug is drawn or pulled into the center of the coil. This allows the solenoid to move to one end, de-energizing the coil will cause the slug to return to its original position. This feature of solenoid is what is utilized in this design to operate the locking and unlocking process. It operates on a 12vdc supply. Solenoid locks operate on the principle of electromagnetism. When an electric current passes through the coil of wire within the solenoid, it generates a magnetic field. This magnetic field causes a metal core (plunger) to move, either attracting or repelling it, depending on the design.

*Figure 12: Solenoid lock*

# CHAPTER THREE

# MATERIALS AND METHODS

## 3.1 MATERIALS

### 3.1.1 X6 ACCESS CONTROL SYSTEM COMPONENTS

- Control panel
- Fingerprint scanners
- Electronic locks or door strikes
- Power supply unit
- Wiring and cabling

### 3.1.2 DOOR HARDWARE

- Door handles
- Hinges
- Mounting brackets or plates for access control components

### 3.1.3 INSTALLATION AND MOUNTING HARDWARE

- Screws, bolts, and nuts
- Riveting pins
- Anchors and wall plugs
- Cable conduits or raceways
- Mounting brackets or plates
- Cable ties and clips

### 3.1.4 TOOLS AND EQUIPMENT

- Screwdrivers (Phillips, flathead)
- Drill and drill bits
- Hammer
- Riveting gun/Riveter
- Tape measure
- Wire stripper/cutter
- Crimping tool
- Multimeter (for electrical testing)

### 3.1.5 CONSUMABLES

- Electrical tape
- Cable management accessories (cable clips, ties)
- Cleaning supplies (for maintenance of fingerprint scanners)

### 3.1.6 DOCUMENTATION

- User manuals for X6 Access Control system components
- Installation guides
- Maintenance instructions
- System configuration documentation

### 3.1.7 SAFETY EQUIPMENT

- Safety goggles

- Work gloves
- First aid kit

## 3.2 METHODS

### 3.2.1 RESEARCH DESIGN

Objective: To investigate the implementation of biometric access control for departmental entry doors using the X6 Access Control system.

1. Conducted comprehensive research on biometric access control systems, including fingerprint recognition technology, biometric security principles, and industry standards.
2. Reviewed existing literature from academic papers, industry reports, and manufacturer specifications to gain insights into the capabilities and limitations of the X6 Access Control system.
3. Identified key factors influencing the successful implementation of biometric access control, such as accuracy, reliability, user acceptance, and security concerns.

### 3.2.2 CONDITION ASSESSMENT OF ENTRY DOOR

Objective: To ensure the entry door is in good condition for the installation of the biometric access control system.

1. Conducted a thorough visual inspection and assessment of the entry door, focusing on structural integrity, alignment, and functionality of components.
2. Utilized measurement tools such as tape measures, levels, and inspection checklists to document the dimensions, condition, and any existing defects of the entry door.

3. Collaborated with maintenance personnel to address any identified issues and prepare the entry door for the installation of the biometric access control system.

### 3.2.3 REPLACEMENT OF ACCESS CARDS WITH BIOMETRIC SYSTEM

Objective: To replace access cards with a comprehensive fingerprint-enabled electronic security system.

1. Developed a detailed implementation plan outlining the steps for integrating the X6 Access Control system with the existing door infrastructure.
2. Procured necessary materials and equipment, including the X6 Access Control hardware, fingerprint scanners, wiring components, and mounting accessories.
3. Installed and configured the X6 Access Control system according to manufacturer guidelines and industry best practices, ensuring compatibility with existing door hardware and network infrastructure.
4. Conducted functional tests and quality assurance checks to verify the proper operation of the biometric access control system and its integration with door mechanisms.

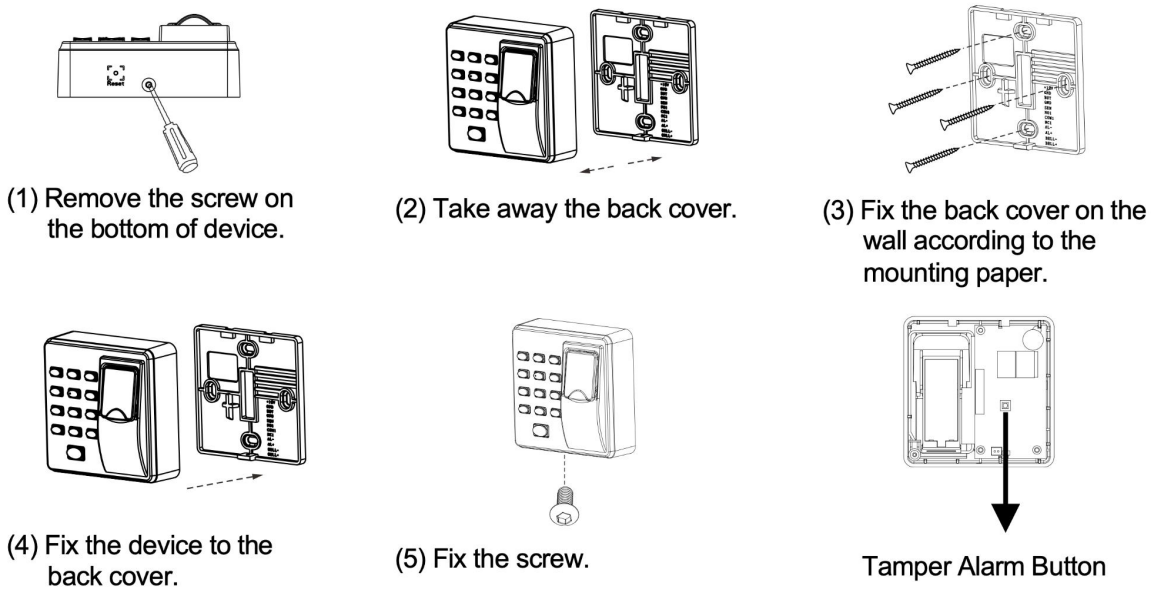
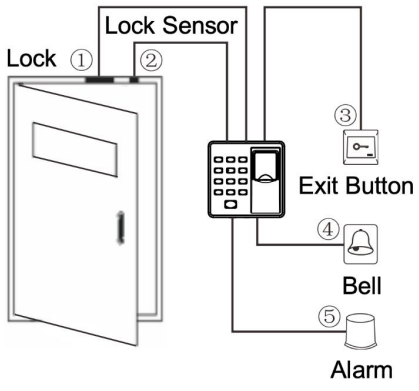



*Figure 13: Steps in mounting the access system*




**Access Control System Function**:

(1) When a registered user's identity is verified, the Access Control device will send out signal to unlock the door.
(2) The door sensor will detect the status of the lock. If the door is unexpectedly opened or improperly closed, the alarm will be triggered.
(3) It supports the exit button for opening the door from inside.
(4) It supports door bell.
(5) If the Access Control device is dismantled, the alarm will be triggered.

*Figure 14:.Access control system functions*

### 3.2.4 USER TRAINING AND FINGERPRINT ENROLLMENT

Objective: To organize training sessions for users to familiarize them with the new biometric access control system and encourage its adoption.

1. Developed comprehensive training modules and instructional materials explaining the operation, enrollment process, and troubleshooting procedures of the X6 Access Control system.
2. Scheduled interactive training sessions with departmental staff, providing hands-on demonstrations and practical exercises to enhance understanding and proficiency.
3. Addressed user concerns, inquiries, and misconceptions regarding the biometric access control system, emphasizing its benefits in terms of security, convenience, and efficiency.
4. Solicited feedback from users to identify areas for improvement and further support their transition to the new system.
5. Explaining the fingerprint enrollment process, including proper finger placement and potential re-enrollment procedures.

### 3.2.5 DATA COLLECTION AND ANALYSIS

Objective: To collect and analyze data pertaining to the implementation and effectiveness of the biometric access control system.

1. Implemented data collection methods, including user surveys, system logs, and performance metrics, to capture quantitative and qualitative data.

2. Utilized spreadsheet software for organizing and managing collected data, categorizing information by user demographics, system events, and operational parameters.
3. Employed statistical analysis techniques, such as descriptive statistics, regression analysis, and hypothesis testing, to interpret the data and evaluate the system's performance against predefined criteria.
4. Generated reports and visualizations to communicate findings effectively and support decision-making processes regarding system optimization and future enhancements.

### 3.3 BLOCK DIAGRAMS

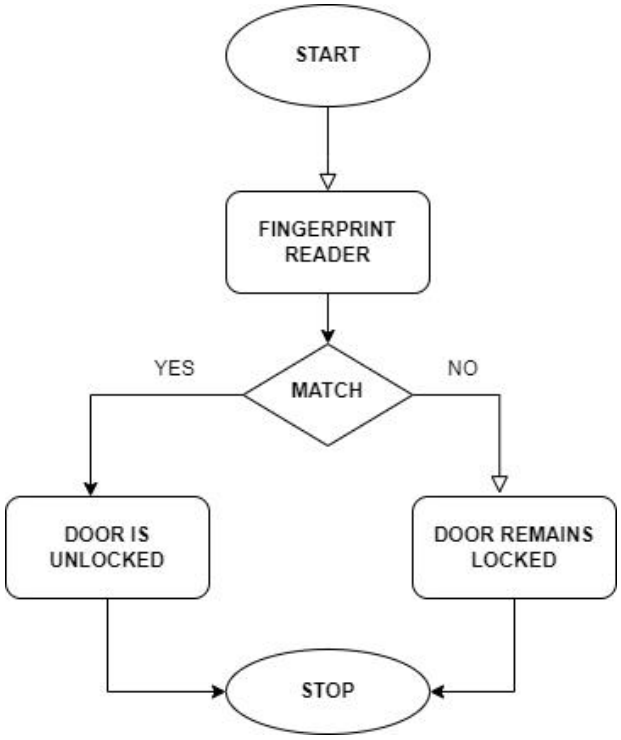



*Figure 15: Flow chart of a biometric access system*

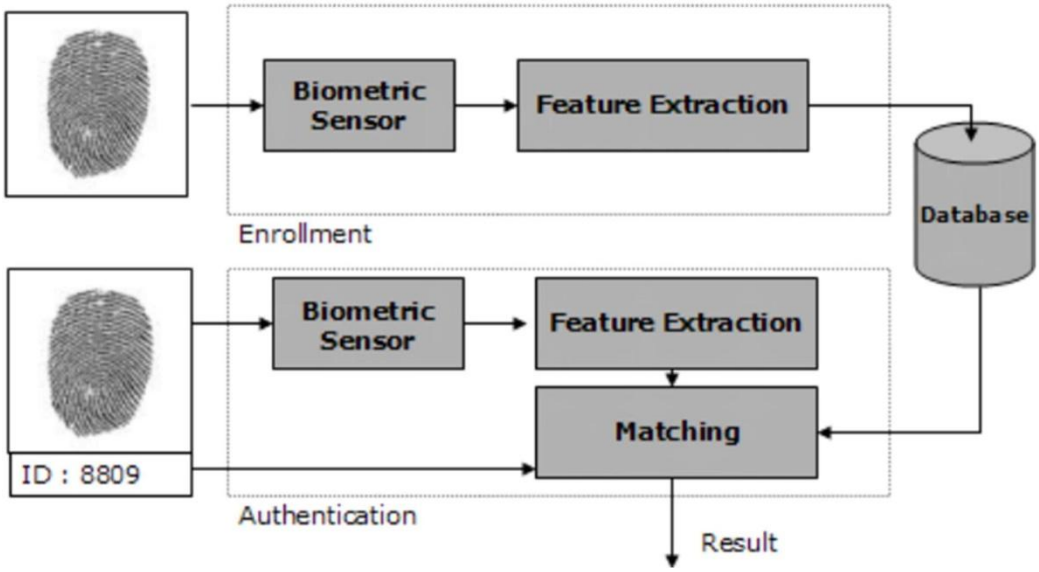



*Figure 16: General architecture of biometric authentication*

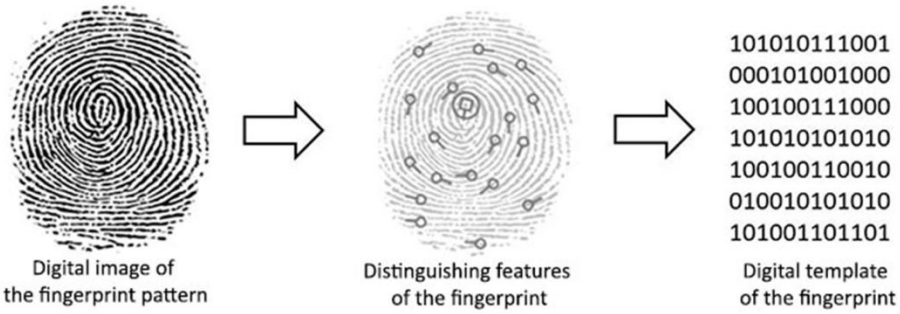



*Figure 17: Digital template of the fingerprint*

# CHAPTER FOUR

# RESULTS AND DISCUSSION

## 4.1 RESULTS

The implementation process involved testing various aspects of the biometric access system which produced satisfactory results. The system when connected had the functions as follows:

1. If the registered user is verified, the device will output a signal to unlock the door.

2. The door sensor will detect the on-off status. If the door opens unexpectedly or closes incorrectly, a warning signal (numeric value) will be activated.

3. If the device is removed illegally, it will output an alarm signal.

So we then subjected the system to tests which would confirm the accuracy of the system in storing and verification of users.

### 4.1.1 STORING TEST

To perform this test, Eight (8) users was allowed to operate the system. Our goal was for us to measure the accuracy and efficiency when storing fingerprints. Each person made a total of Ten (10) trials to store their fingerprints.

***Table 1**: Storing test results*

| Number of users | Attempts | Stored | Not Stored | Average response time (s) | Percentage accuracy |
|---|---|---|---|---|---|
| 1 | 10 | 8 | 2 | 2 | 80 |
| 2 | 10 | 9 | 1 | 1 | 100 |
| 3 | 10 | 10 | 0 | 1 | 100 |
| 4 | 10 | 9 | 1 | 1 | 90 |
| 5 | 10 | 10 | 0 | 1 | 100 |
| 6 | 10 | 10 | 0 | 1 | 100 |
| 7 | 10 | 9 | 1 | 1 | 90 |
| 8 | 10 | 10 | 0 | 1 | 100 |

### 4.1.2 VERIFICATION TEST

To achieve this, Eight (8) users tested the system making a total of Ten (10) trials each. These persons were ensured to have previously stored their fingerprints on the system. The idea was to test the systems effectiveness and responsiveness when it comes to verification of prints. Results obtained were recorded in the table below.

***Table 2**: Verification test results*

| Number of users | Attempts | Verified | Not Verified | Average response time (s) | Percentage accuracy |
|---|---|---|---|---|---|
| 1 | 10 | 10 | 0 | 1 | 100 |
| 2 | 10 | 8 | 2 | 2 | 80 |
| 3 | 10 | 9 | 1 | 1 | 90 |
| 4 | 10 | 10 | 0 | 1 | 100 |
| 5 | 10 | 10 | 0 | 1 | 100 |
| 6 | 10 | 8 | 2 | 2 | 80 |
| 7 | 10 | 10 | 0 | 1 | 100 |
| 8 | 10 | 9 | 1 | 1 | 90 |

### 4.1.3 PERFORMANCE TEST

We also carried out test on the door when the biometric system was implemented to check the performance of the system.

***Table 3**: Performance test results*

| Biometric Scanner | Door Status |
|---|---|
| No scanning of thumbprint | Closed |
| Scanning of thumbprint for identification(registered users) | Open |
| Scanning of thumbprint for identification(unregistered users) | Closed |

## 4.2 DISCUSSION

The results obtained from the storing test shows the system is efficient in storing fingerprints. The average response time for storing ranges between 1-2 seconds. The storing accuracy is quite high using this system. When storing fingerprints, users has too place finger twice in succession in order to store he better image. This will explain the reason why not all fingers were stored for all the attempts made as the fingers applied must be exactly the same while storing. Therefore inconsistent or partial finger placement accounts for the failure of the system inn storing all prints.

The results obtained from the verification test shows that the system is responsive in verifying prints whose prints have been previously stored. The response time is quick and the accuracy is quite high. When verifying fingerprints, the user must place their finger on the sensor and wait so the system to match their print against previously store prints .This will explain why verification failed in some attempts .The reason for this includes sweaty finger, dirt covering the fingerprints sensor, partial finger placement and failure due to fingerprints not properly stored.

The results obtained from the performance test shows that the biometric system performs action of opening and restricting of the departmental door at an optimal level. The door opens when authorized users whose fingerprints have been stored verified by the biometric system. The door fails to open and restricts user who fingerprints are not stored on the system.

# CHAPTER FIVE

# CONCLUSION AND RECOMMENDATION

## 5.1 CONCLUSION

The implementation of a biometric access control system for the departmental entry door signifies a significant step forward in safeguarding sensitive information, assets, and fostering an environment conducive to innovation. This technology offers a multitude of benefits that demonstrably enhance security and position the department as a leader in data protection practices.

Through the development and testing of this system, it has been fully demonstrated that biometric recognition is a reliable and accurate method of authentication with a very low probability of false acceptance and rejection. Additionally, the system is user friendly and easy to operate, requiring minimal training and maintenance. Biometric verification offers unparalleled security by using unique, unchangeable personal traits for identification. Unlike passwords or physical tokens, biometric data cannot be lost, stolen, or copied. This method also ensures the physical presence of the authorized individual, enhancing safety and efficiency compared to traditional verification methods. The system is able to provide authentication in addition to adding more users if required. As technology continues to advance, we can expect even greater improvements in the accuracy, reliability, and convenience of fingerprint recognition systems.

## 5.2 RECOMMENDATIONS

Looking towards the future, the prospects for biometric access system technology is bright. With this, the following are some recommendations provided for organizations considering the implementation of biometric access control systems:

1. Conduct a thorough risk assessment to identify areas where biometric access control systems can provide the most significant security improvements.
2. Conduct a cost-benefit analysis to evaluate the return on investment (ROI) associated with implementing the chosen biometric technology.
3. Collaborate with experienced vendors and service providers with a proven track record in biometric security solutions to ensure successful implementation and ongoing support.
4. Provide comprehensive training programs to educate users on the proper use of biometric technology and address any misconceptions or fears.
5. Regular system maintenance and software updates are crucial to ensure optimal performance and security .Regularly review and update security policies and procedures to adapt to technological advancements.

## REFERENCES


A. Alghamdi, " security lock system ", computer Engineering department, college of computer and information system, umm Al-qura university, makkah saudi Arabia,2020.

B. U. Umar, O. M. Olaniyi, and J. A. Olorunyemi, "Design and development of fingerprint door access control system with buzzer alarm," in international conference on science, technology, Education, Arts, Management and Social sciences(ISTEAMS Nexus), University of illorin, 2018, pp. 1-9.

D. Mahjabeen and M. R. Tarafder, "Unique Authentication for door lock system through bio scanning-fingerprint security sysem "Global Scientific Journal,vol. 9,no. 10, pp. 1559-1565, 10 October, 2021 2021. [Online]. Available:www.globalscientificjounal.com.

E. Esekhaigbe and E. O. Okoduwa, "Design and implementation of a fingerprint- based biometric access control system," Jounal of Advances in Science And Engineering,vol. 7, pp. 18-23, 14th july, 2022 2022.

Jain, A. K., Ross, A., & Nandakumar, K. (2016). Introduction to Biometrics. Springer.

Kaur, P., & Kaur, A. (2016). Secure Access Control System using Fingerprint Recognition Based on LabVIEW. Procedia Computer Science, 85, 307-314.

K.Rajesh, B. V. Rao, P.AV.S.K.Chaitanya, and A. R. Reddy, "smart door unlock system using fingerprint," Pranama Research Journal,vol. 9, no. 3, pp. 756-761,2019. [Online]. Available: https://pramanasearch.org.

Li, S. Z., & Jain, A. K. (Eds.). (2011). Handbook of face recognition. Springer Science & Business Media.

M. M. R. Komol, A. k. Podder, M. N. Ali, and S. M. Ansary, "RFID and Finger print based dual security system: A robust secured control to access through door lock operation," American journal of embedded systems and applications journal vol. 6,no. 1, pp. 15-22, 2018, doi: DOI:10.11648/j.ajesa.20180601.13.

M. sarma, R. salkia, A. Gogoi, and D. j. Bora, "Fingerprint Based Door Access System Using Arduino " International Journal of Scientific Research in Engineering and Management (IJSREM),vol. 4, no. 8, pp. 1-5, 2020. [Online]. Available:www.ijsrem.com.

O. A. Okeimute and E. K. Okeoghene, "property security using a biometric based door system," International Journal of Engineering and Emerging Scientific Discovery, vol. 3, no. 4, pp. 9-19, december 2018 2018.

P. Paul, M. A. A. Achib, H. S. Hossain, and M. K. Hossain, "smart door lock using fingerprint sensor," BRAC University, 2019.

R. Anirudh, V. Chandru, and V. Harish, "multi-level Security Biometric Authentication Locking system using Arduino UNO," Advances in Parallel Computing Technologies and Applications, 2021, doi: 10.3233/APC210121.

Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi, "Locker Opening and Closing System Using RFID, Fingerprint, Password and GSM", International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March – April 2013.

Rathgeb, C., & Busch, C. (2017). How to improve fingerprint-based biometric recognition. IEEE Transactions on Information Forensics and Security, 12(3), 545-559.

S. U. Ahmad, A. Sabir, T. Ashraf, U. Ashraf, S. Sabir, and U. Qureshi, "Security lock with Effective Verification Traits," 2019.

T. D. Ipilakyaa, V. oji, and V. Okeke, "design, construction and performance evaluation of an automated door lock using biometric security system with phone text alert notification," International Journal of Engineering pp. 115-120, may 2020 2020.[Online]. Available: http://wwwannals.fih.upt.ro.

# APPENDIX

## X6 ACCESS CONTROL

## SYSTEM USER MANUAL

### INSTRUCTIONS

**Buttons:** The pound sign (#) confirms, and the asterisk (*) cancels.

**Lights:** Green indicates success, red signifies an error.

**Numbers:** Passwords are four digits long, and operation codes can't exceed five digits.

**Sounds:** A long buzz means success, two short buzzes mean failure, and four short buzzes indicate a wrong action.

**General:** Always confirm with the pound sign (#) to proceed, and the asterisk (*) resets the system.