USMANU DANFODIYO UNIVERSITY SOKOTO, NIGERIA

(POSTGRADUATE SCHOOL)

DESIGN AND CONSTRUCTION OF A FINGER BASED MULTI-USER BIOMETRIC ACCESS CONTROL SYSTEM

A Dissertation

Submitted to the

Postgraduate School

USMANU DANFODIYO UNIVERSITY SOKOTO, NIGERIA

In Partial Fulfilment of Requirements

For the Award of the Degree of

MASTER OF SCIENCE (PHYSICS)

BY

SULE, OJONUGWA SAMUEL

(ADM. NO: 12210305015)

DEPARTMENT OF PHYSICS

APRIL, 2019

DEDICATION

This work is specially dedicated to Almighty God by whose Grace I made this research, to my wife and daughters and finally to my late father, my mother and the entire family.

CERTIFICATION

This dissertation by Sule, Ojonugwa Samuel (Admission number 12210305015 has met the requirements for the award of the degree of Master of Science (Physics) of the post graduate school, Usmanu Danfodiyo University, Sokoto and is approved for its contribution to knowledge

Prof Musa Momoh **Major Supervisor**	**Date**
Dr. A U Moreh **Co-supervisor I**	**Date**
Prof. Hassan Yahaya **Co- Supervisor II**	**Date**
External Examiner	**Date**
Head of Department	**Date**

ACKNOWLEDGEMENTS

More often a time, the task of a research work is usually not a single person's effort and credit of such research work goes to people who one way or the other contributed towards the success of the work.

Therefore I acknowledge the contributions of my able and dynamic supervisor professor Musa Momoh for his useful support, I also acknowledge the contributions of my co-supervisors Prof. Hassan N. Yahaya, Dr. Abubakar Umar Moreh for their co-operations and patience in reading through my work and most especially their constructive criticisms that guided me in realizing the present quality of this research work.

I also acknowledge my PG coordinator Dr. Garba Musa Argungu, My Lecturers Mal. Ismaila Garba Saidu, Dr. Sanusi Abdullahi and my ever able departmental staff Ahmad Abdullahi for their support and guidance throughout my Programme.

My profound appreciation goes to my Wife and daughters for their support/patience and prayers and also to my parent and family for their support throughout my academic pursuits.

I finally acknowledge the authors whose ideas were used to accomplish my research

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT

Traditional personal authentication systems that are based on knowledge (e.g., password) or physical tokens (e.g., ID card) are not able to meet strict security performance requirements of a number of modern applications such as internet network security, e-commerce, private related tasks, etc. Hence biometric –based authentication systems that use physiological and/or behavioral traits (e.g., fingerprint, face, and signature) are good alternatives to traditional methods. However, these systems have their own drawbacks such as system hacks leading to invading privacy rights, exorbitant cost, etc. In this work, we designed an integrating systems combining fingerprint biometric and cryptography based multiuser biometric access control system for improved security. Firstly, we analyze attack robustness of fingerprint matchers, and develop algorithms for circumventing them.. Secondly, we developed algorithms for increasing the security of image-based (e.g., fingerprint and face) biometric templates, via embedding additional information in them. Thirdly, we worked on a secure multimedia content distribution framework that includes fingerprint matching. This provides another line of defense against the piracy of copyrighted data. Finally, this provides developed hybrid system that combines traditional cryptography with fingerprint biometrics. The results showed that the system would authenticate persons accurately, rapidly ,reliably cost effectively as well as user friendly. The two major errors associated with biometrics were also found to have reduced to the minimal level

CHAPTER ONE

INTRODUCTION

1.1 Background of the study

With the proliferation of large-scale computer networks (e.g., internet), the increasing number of applications making use of such networks (e.g., e-commerce, e-learning), and the growing concern for identity theft problems, the design of appropriate personal authentication systems is becoming more and more important. Systems that have the ability to authenticate persons accurately, rapidly, reliably, without invading privacy rights, cost effectively, user-friendly, and without drastic changes to the existing infrastructures are desired.(Diaz, 2007) The traditional personal authentication systems that make use of either a (secret) piece of knowledge (e.g., password) and/or a physical token (e.g., ID card) that are assumed to be utilized only by the legitimate users of the system and cannot provide the desired improve security..

Biometrics-based personal authentication systems that use physiological and/or behavioral traits (e.g., fingerprint, face, iris, hand geometry, signature and voice) of individuals have been shown to be promising. (Diaz,2007). They lead to increased user convenience as there is nothing to remember or carry. They improve the authentication accuracy: the system parameters can be modified so that the probability of illicit use of the system can be reduced. Further, the cost of incorporating biometric components into an authentication system is continually decreasing, whereas the cost of relying on traditional authentication mechanisms is increasing.

One of the biggest challenges facing society today is confirming the true identity of a person. There are several identification verification schemes that exist today but one of the most accurate identification schemes are in the area of biometrics (Diaz, 2007). A

simple example of the application of biometric system is in the banking sector where it is used as an Automated Teller Machine (ATM) card. When a person wishes to use his ATM card, he is required to enter in a personal identification number (PIN) in order to begin transaction(s). This type of identification verification is given by what that person has (card) and what that person knows (PIN). There may be a potential problem to this ATM scheme. For instance, the card could be stolen. It would be difficult for the thief to use this ATM card unless he or she knew the PIN; however the PIN is vulnerable to theft especially if someone is looking over ones shoulder while you are entering PIN number. It is practicable to use two types of identity verification method, biometric alone or used with another type of identification verification method.

Some examples of identifying biometric characteristics are fingerprints, handgeometry, retina and iris patterns, facial geometry, and signature and voice recognition. (Abhisek,2013)

Biometric identification may be preferred over traditional methods (e.g. passwords, smart-cards) because its information is virtually impossible to steal. Although in some cases it may become possible to impersonate a biometric (e.g. replicating legitimate user's fingerprints to fool the fingerprint scanning device) this is however a very difficult exercise (Jain and Aron, 2009).

Two interesting properties of biometric identification are that the person to be identified is required to be physically present at the point of identification and identification based on biometric techniques does not depend on password and token..

The two distinct functions for biometric devices are to prove that a personnel is who he say he was and to prove that the personnel is not who he say he is not (Mazumdar and Dhulipala,2008).

The purpose of the first function is to prevent the use of a single identity by multiple people. In this case it is important that the biometric device be able to differentiate between a live biometric presented to the scanner (i.e. a real finger) or a spoofed biometric trying to fool the scanner (i.e. a photograph of a legitimate user used to fool a facial scanner). The second function is used to prevent the use of multiple identities by a single person (Setlak,2010). It would have to be ensured that the biometric system either automatically cross checks the enrolled characteristics for duplicates, or otherwise does not allow a person to register their biometric (i.e. fingerprint) under two different names.

For positive identification, there are also multiple supplemental technologies such as passwords, tokens, and cryptographic keys (Adolp, 2009). An enticing feature of biometric identification is that it could take the place of millions of passwords (e.g. long, hard to remember passwords used to gain access to sensitive information stored on a computer in a large corporation).

As a banker issue of security is always of paramount importance. The motivation for this research is therefore born out of the desire to help meet the number one challenge to the banking sector which is security and access right to restricted rooms, places or safe boxes which is presently being accessed using Keys and combination locks. To provide improved security, biometrics could be used in addition to these alternative technologies and provide information needed to achieve continuous authentication.

1.2 Statement of the Problem

With control system hacks on the rise and increasing cost of relying on traditional authentication mechanisms, an alternative system that can authenticate persons accurately, rapidly, reliably, without invading privacy right, cost effectively, in a user friendly manner is much needed/desired (Elsevier, 2007).Biometric authentication

measures unique human's traits such as finger print, voice, and iris but biometric data are noisy and inconsistent, biometric systems allow minor errors while maintaining high authentication accuracy (Mazumdar and Dhulipala, 2008).

Therefore, integrating biometric and cryptographic schemes (which encrypt and decrypt secret information using cryptographic keys and does not tolerate even a single bit of error) technology is a challenging task.

1.3 Significance of the Study

Specifically, this thesis is concerned with the improvement of security systems in homes or organizations. The work will be significant as it is aimed at achieving a fingerprint-based multi-user biometric access control system with the capability of the transmission of encrypted user print templates in contact smart cards. It also integrates a wireless (Wi-Fi) network for remote monitoring and observation of access events.

The design and development of a practical biometric cryptosystem utilizing fingerprint features that combine the benefits of biometric systems with the security of cryptographic systems should prove very useful.

1.4 Aim and objectives

The aim of this study is to design and construct a finger based multiuser biometric access control system.

The objectives of this work are:

i. To assemble a fingerprint multiuser biometric access control system for improved security.
ii. To test and access the system's performance after construction.

1.5 Scope and Limitation of the Study

This design is to provide a fingerprint access control device to improve security system for

i. Homes and organizations
ii. Safe box
iii. Door lock system
iv. Vehicle control
v. ATM and POS

The system is capable of giving access to authorized users while denying all those that are not registered .however it is limited to 500 users at a time and not suitable for larger population. Also physically challenged aren't fortunate enough to be able to participate in the enrollment process.

CHAPTER TWO

LITERATURE REVIEW

2.1 Theoretical fundamentals

The term "biometrics" is derived from the Greek words "bio" meaning life and "metric" meaning to measure (Diaz,2007). Biometrics is the measurement and statistical analysis of people's physical and behavioral characteristics. The technology is mainly used for identification and access control, or for identifying individuals that are under surveillance. The basic premise of biometric authentication is that everyone is unique and an individual can be identified by his or her intrinsic physical or behavioral traits (Anil and Karthik, 2013).

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the eccrine glands that are present in epidermal ridges (Karthik, 2014)

In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primatehand. A print from the sole of the foot can also leave an impression of friction ridges.

Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers.

Human fingerprints are detailed, unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves.

Fingerprints offer a reliable means of personal identification. That is the essential explanation for fingerprints having replaced other methods of establishing the identities of criminals reluctant to admit previous arrests. The science of fingerprint Identification stands out among all other forensic sciences for many reasons (marco and marcos, 2014).

Other visible human characteristics such as facial features tend to change with age, but fingerprints are relatively persistent. Barring injuries or surgery causing deep scarring, or diseases such as leprosy damaging the formative layers of friction ridge skin, finger and palm print features have never been shown to move about or change their unit relationship throughout the life of a person (injuries, scarring and diseases tend to exhibit telltale indicators of unnatural change).

In earlier civilizations, branding or maiming was used to mark the criminal for what he or she was. The thief was deprived of the hand which committed the thievery. Ancient Romans employed the tattoo needle to identify and prevent desertion of mercenary soldiers from their ranks.

Before the mid-1800s, law enforcement officers with extraordinary visual memories, so-called "camera eyes," identified previously arrested offenders by sight alone. Photography lessened the burden on memory but was not the answer to the criminal identification problem. Personal appearances change (Christian and christoph, 2014)

Around 1870, French anthropologist Alphonse Bertillon devised a system to measure and record the dimensions of certain bony parts of the body. Theoretically, would apply only to one person and would not change during his/her adult life.

The Bertillon system was generally accepted for thirty years. But the anthropometric measurement system never recovered from the events of 1903, when a man named Will West was sentenced to the US Penitentiary at Leavenworth, Kansas. It was discovered there was already a prisoner at the penitentiary, whose Bertillon measurements were nearly the same, and his name was William West (Neylre, 2014).

Upon investigation, there were indeed two men who looked very similar. Their names were William and Will West. Their Bertillon measurements were close enough to identify them as the same person. However, a fingerprint comparison quickly and correctly identified them as two different people. (Per prison records publicized years later, the West men were apparently identical twin brothers and each had a record of correspondence with the same immediate family relatives).

2.1.1 Types of Biometric identification

The following are types of biometric identification (Abhisek,2013):

- DNA Matching (Deoxyribonucleic acid) matching it's a chemical biometric type of identification of an individual that uses the analysis of segments from DNA which is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same **DNA.**
- Ear Matching, it's a visual biometric type of identification of an individual by using the shape of the ear .

- Eyes –Iris, recognition it's a visual biometric type of identification of an individual which uses the features found in the iris to identify an individual.
- Eye –Retina, Recognition it's a visual biometric identification type that uses the patterns of veins in the back of the eye to accomplish recognition.
- Face recognition, it's a visual type of biometric identification that uses the analysis of facial features of patterns for the authentication or recognition of an individual's identity. (Abhisek,2013)
- Fingerprint recognition, it's a visual biometric identification type that uses the ridges and valleys (Minutiae) found on the surface tips of a human finger to identify an individual.

2.1.2 Biometric fingerprint identification

Biometric fingerprints are unique to each individual and each individual has their own pattern in their fingerprints. This type of identification has been successfully used by the police to capture criminals and to find missing children. A fingerprint records the patterns found on a fingertip. The traditional method, which is used by police, matches details of the fingerprint (Thornton, 2010). Some other approaches are pattern matching, and moiré fringe patterns. There are some verification approaches that can detect if a live finger is presented, but not all of these approaches can provide this type of information. Live fingers detecting and testing requirement should be incorporated if fingerprint-scanning techniques were to be incorporated into an access control system. (Thornton, 2010)

Fingerprints serve to reveal an individual's true identity and the practice of using fingerprints as a means of identification has been a helpful aid to those who chose to use this type of identification. Fingerprints are unique in the sense that there has not been any

type of pattern duplication by two different people. Not even a single instance hasbeen identified or discovered at this time. This uniqueness also applies to identical twins, as well as triplets, quadruplets, and quintuplets. (Christian and christoph, 2014)

One good thing about fingerprints is thatany type of burn (superficial), abrasions, or cuts do not affect the ridge structure, thus thefingerprint pattern is unaffected (Neylre,2014)

2.1.3 Review of Biometric Fingerprint Identification Systems

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of forensic science. Fingerprints are easily deposited on suitable surfaces (such as glass or metal or polished stone) by the natural secretions of sweat from the endocrine that are present in epidermal ridges (karthik ,2014)

In a wider use of the term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primatehand. A print from the sole of the foot can also leave an impression of friction ridges.

Deliberate impressions of fingerprints may be formed by ink or other substances transferred from the peaks of friction ridges on the skin to a relatively smooth surface such as a fingerprint card. Fingerprint records normally contain impressions from the pad on the last joint of fingers and thumbs, although fingerprint cards also typically record portions of lower joint areas of the fingers (Langenburg, 2010)

Human fingerprints are detailed, unique, difficult to alter, and durable over the life of an individual, making them suitable as long-term markers of human identity. They may be employed by police or other authorities to identify individuals who wish to conceal their

identity, or to identify people who are incapacitated or deceased and thus unable to identify themselves, as in the aftermath of a natural disaster.

2.1.4 Biometric performance measurements

The performance of biometric systems is tested usually in terms of false rejection rate (FRR), false acceptance rate (FAR), failure to enroll rate (FER), Receiver operating characteristics (ROC), Equal error rate (EER) and Failure to capture rate (FTC)(Langenburg, 2010)

i. **False acceptance rate (FAR):** It is also called false match rate (FMR) is the probability that the system incorrectly matches the input pattern to a non-matching template in the data base. It measures the percent of invalid inputs that are incorrectly accepted. In the case of similarity scale, if the persons is an imposter in reality, but the matching score is higher than the threshold, then he is treated as genuine. This increases the FAR, which thus depends upon the threshold value (Anil and Karthik, 2013)

ii. **False rejection rate (FRR**): It is also called false non match rate (FNMR) is the probability that the system fails to detect a match between the input pattern and a matching template in the data base. It measures the percent of valid inputs that are incorrectly rejected (Anil and Karthik, 2013)

iii. **Receiver operating characteristics (ROC) :**It is also called relative operating characteristics (ROC) it is a plot of visual characterization of the tradeoff between the FMR and the FNMR. In general, the matching algorithm performs a decision based on a threshold that determines how close to a template the input needs to be for it to be considered a match. If the threshold is reduced, there will be a fewer false non match but more false accepts. Conversely, a higher threshold will

reduce the FMR but increase the FNMR. A common variation is the Detection error trade off (DET), which is obtained using normal scales, on both axes (Anil and Karlhik,2013)

iv. **Equal error rate (EER):**It is also called cross over error rate (CER) is the rate at which both acceptance and rejection errors are equal. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate (Anil and Karthik, 2013)

v. **Failure to enroll rate (FTE OR FER) :**The rate at which attempts to create a template from an input is unsuccessful and this is most common by low quality inputs (Anil and Karthik, 2013)

vi. **Failure to capture rate (FTC) :**The probability that the systems fails to detect a biometric input when presented correctly within automatic system (Anil and Karthik, 2013)

2.2 Literature review of past work

Review of past work done on biometrics and their limitations

i. Adewole et al. (2014) reported work was based on the design and implementation of staff biometric attendance system using fingerprint authentication. The proposed system can be used to monitor, identify and check the IN and OUT timings of non-academic staff in tertiary institution. The system requires that all non-academic staff enroll his/her fingerprint for the device to identify and verify if he is a valid staff and also to record daily resumption and closure timings for the staff for a whole month, before payment of salaries are affected. The primary idea behind their design was to avoid a situation where staff records fake timings in the manual register and yet receiving full payment for the month. This greatly

affects output to input ratio of staffs and in earnest the institution as a whole. The design enhances compilation of each staff's attendance by remote workstations, which was then sent to the central database server at the end of each month for easy processing of salaries and allowances. The result of each staff clocking in and out timing is captured via a fingerprint device at each terminal and stored in the central database server. Each Department remote terminal is interconnected to the central database server via a shared network.

The work did not in any way address the staff access security measure.

ii. Ashraf (2009) developed a biometric access control system for restricted areas based on individual finger print and Gabor filter for enhancement process. Gabon filter is a linear filter used for texture analysis.The developed system architecture, demonstrated the components, enhancement, minutiae extraction and matching techniques are presented. A software application was written in Matlab and C++ to implement algorithms for enhancement, minutiae extraction and matching processing. The resulting minutiae information was used as a method of identifying matching fingerprints. Also it was used to register this fingerprint in system database. Finally, verification system, and identification system was implemented. Registration system has facilities namely; automatic registration, manual registration and update for the database to help the administrator to update required information. Based on that processing, an integrated secure system for biometric access control was developed for restricted area with acceptable security level.

The work is purely on biometrics access control system but did not address the limitation associated with biometric error.

iii. Shoewu et al (2016), presents the design and construction of a fingerprint based biometrics attendance system. The model includes fingerprint model use for taking the fingerprint of each student and also a graphic LCD to display the registered students or none. Its process entails taking attendance of each student and it searches for it in the database to confirm if the student has registered or not. It marks attendance for the registered student and displays results not found for the unregistered student. It has a biometric data capturing database memory that stores about 200 students data (fingerprint, name, matric, sex, faculty, department, blood group etc). It uses a USB computer keyboard as input and has a big 240 128 pixel graphic LCD as output. It has a Bluetooth or serial port to transfer attendance result to a phone or computer for printing.

iv. Ogherohwo and Ezeoba (2011) designed and constructed a biometric device to be used for the authentication of the student's eligibility for an examination. The system requires that the students, during their registration for a particular course will have their finger prints taken and registered against their name. Subsequently, during an examination or a test, the students are verified using their finger prints. The system was also designed with an external display unit, which displays information about the validity of the finger scan

The research was designed and constructs a device that uses the unique, distinguishable and permanent marker, in this case, the fingerprint to automatically verify the identity of a student during examination and the same system should be able to register the same person, for more than one course using the same finger during enrollment

2.3 Research Gap

From the foregoing a fingerprint access control system can make two major types of error which are a false match, when a match occurs between images from two different fingers, and a false non –match, when images from the same finger are not match. This research work is to design a good matching biometric access control system to reduce to the lowest minimum these two errors and provide access to dully enrolled and registered personnel while denying access to unregistered personnel. However both errors cannot be reduced simultaneously as they are inversely dependent on each other.

Also from the forgoing, the gap of biometric system robustness against attacks, protecting biometric templates, integrating fingerprint registration and authentication components into existing computing architectures, combining cryptography with biometrics, will be analyzed and appropriate solutions for them will be proposed and developed

CHAPTER THREE
MATERIALS AND METHOD

3.1Materials

The design is aimed at improving the security system of homes and organizations by designing a finger print system that is based on digital signal processor (DSP) processing unit.

The access control system embodies different subsystems integrated to achieve a fully-functional unit. These subsystems are:

a. Power supply - To supply power to the system

b. Fingerprint scanner/sensor - MIAXI SM630 sensor

c. Microcontroller - Atmega328 8-bit single-chip computer

d. Liquid crystal display - 4-line 20-character alphanumeric LCD

e. Multiplexer - CD4052 DUAL 1 OF 5 CMOS Multiplexer

f. Contact memory card - smart card

To design and construct a networked multi user biometric access control system. The system is to use MIAXI SM630 biometric sensor with a TCP-IP communication network and a wireless LAN network interface capable of giving access to authorized users while denying all those that are not registered. Other specifications include encrypted card resident user data storage, a 4-line character LCD with scrolling marquee system information update and an auto recovery firmware that ensures stable all year round with zero maintenance. It could also keep access log record with time and date stamps that is expandable to about 4000 records. To meet this specification, the general requirements are:

- A Wi-Fi communication system that allows for communication between a connected PC and the control unit forair interface
- Acontact card reader for data retention
- A provision switch to open or close a door
- A programmable controller to reduce circuit complexity
- A power supply unit to meet the power requirement of all the sections
- A display unit that providesinterface for system information, communication and update

3.2 System design

3.2.1 ATMEGA328 Microcontroller

In this application a microcontroller is utilized for power economy, weight, and reduced component counts. The microcontroller is essentially a one-chip computer. It has functional hardware functions that are implemented using external peripheral devices on full-fledged microprocessor incorporation onto a single die.

It embodies a re-programmable memory unit, designed around a FLASH memory device because of its easy in-circuit electrical programmability during code updates. Microcontrollers can handle complex algorithms and cope with more input and output signals that are necessary for medium-complexity control systems. Different functions can be implemented by altering the programs that drive the microcontrollers, and the capability of performing variable functions makes a microcontroller a nearly universal device in many industrial and domestic applications.

For this purpose an AVR microcontroller (ATmega32) was selected, programmed and used to direct the operations of the other sections of the system. The choice was due to its numerous features, reliability, low cost and availability.

The microcontroller also has embedded into its package random access memory (RAM) for program execution on high-end 32-bit versions, or temporary data storage on lower devices (Adolph, 2009).

The Atmega32 is one of Atmel's newest and most powerful 8-bit microprocessors (Adolph, 2009). Not only does it have a more advanced Central Processing Unit (CPU), and features such as two index registers that greatly simplify programming, it also has the following main functional components (Atmega32 datasheet, 2017):

1. An On-Chip RAM mainly reserved for interrupt vectors and for some monitor variables.
2. An On-Chip EEPROM. The user can write small programs to this area
3. An On-Chip FLASH ROM
4. An asynchronous Serial Communications Interface (SCI) that allows the Atmega32 to transmit and receive serial data in an asynchronous format.
5. A synchronous Serial Peripheral Interface (SPI). These parallel channels allow an Atmega32 to communicate with other microcontrollers or outside devices such as a keypad, serial SPI memory, ADCs, etc.
6. A 8-Channel, 10-Bit Analog-to-Digital (A/D) Converter.
7. A 16-Bit Pulse Accumulator, which can count pulses by capturing the falling or rising edge of a pulse signal.
8. A Real-Time Interrupt Circuit
9. A 16 bit Timer with Capture and Compare.
10. Power Saving SLEEP that dramatically reduces power consumption.

The Atmega32 device as shown in fig 3.2 has the following hardware ports(Atmega32 datasheet, 2017):

a) Port B – SPI/ISP programming interface, Output Compare pins

b) Port C- JTAG/Debug port, I2C hardware port

c) Port D – Serial port, external interrupts (INT0/INT1). This port is used as a serial communication Interface (SCI) if the SCI function is enabled. Otherwise it serves as a general I/O port for digital signals.

d) Port A - A/D. It is a 8-channel A/D converter/serial interface for I2c devices.

has 14 digital I/O pins, of which 6 can be used as PWM outputs and 6 analog input pins. These I/O pins account for 20 of the pins.

The Pinout for the Atmega328 is shown Figure 3.1.

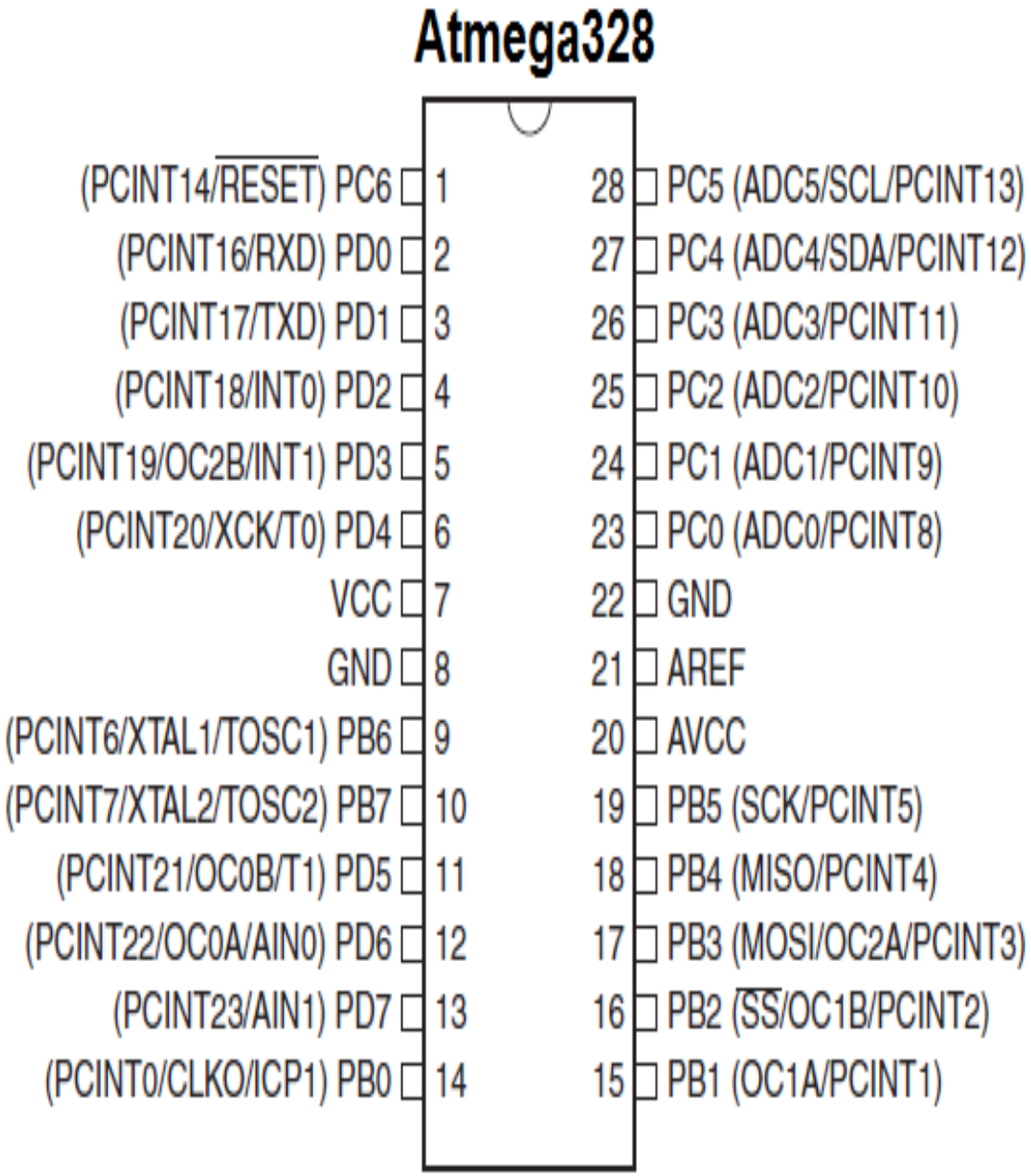

Figure 3.1 Pinout for Atmega328

The table below gives a description for each of the ATMGA328 pins, along with their function.

Table 3.1 Microcontroller Pinout Functions

Pin Number	Description	Function
1	PC6	Reset
2	PD0	Digital Pin (RX)
3	PD1	Digital Pin (TX)
4	PD2	Digital Pin
5	PD3	Digital Pin (PWM)
6	PD4	Digital Pin
7	Vcc	Positive Voltage (Power)
8	GND	Ground
9	XTAL 1	Crystal Oscillator
10	XTAL 2	Crystal Oscillator
11	PD5	Digital Pin (PWM)
12	PD6	Digital Pin (PWM)
13	PD7	Digital Pin
14	PB0	Digital Pin
15	PB1	Digital Pin (PWM)
16	PB2	Digital Pin (PWM)
17	PB3	Digital Pin (PWM)
18	PB4	Digital Pin
19	PB5	Digital Pin
20	AVCC	Positive voltage for ADC (power)
21	AREF	Reference Voltage
22	GND	Ground
23	PC0	Analog Input
24	PC1	Analog Input
25	PC2	Analog Input
26	PC3	Analog Input
27	PC4	Analog Input
28	PC5	Analog Input

For the hardware design the considerations were (Atmega32 datasheet, 2017):

• Operating Voltages

1. 2.7 - 5.5V (ATmega32L)
2. 4.5 - 5.5V (ATmega32A)

• Speed Grades

1. 0 - 8 MHz (ATmega32L)
2. 0 - 16 MHz (ATmega32A)

• Power Consumption at 4 MHz, 3V, 25°C

1. Active: 3.6 mA
2. Idle Mode: 1.0 mA
3. Power-down Mode: 0.5 μA

A power supply capable of meeting the above requirement was designed and used to power the microcontroller. An external crystal was used due to the need to achieve synchronization clock with the mains, and repeatability of the different timing used when executing portions of the code blocks.

Integration between the different system components was achieved in software. The device also has rich plethora of on-chip hardware.

Firmware for the microcontroller was compartmentalized for ease of testing, debugging, and modifications. The microcontroller was programmed using ICC AVR C compiler and development studio. The compiler was chosen as it supports standard C libraries with optimized code footprint and reasonable execution speed, even on an 8-bit machine that the microcontroller is.

The firmware is broken down into code blocks:

Hardware configuration code block handles the I/O pin configuration. Pins designated as outputs are set up by writing '1' to their bit positions in the Data Direction Registers

(DDRx), port pins used as inputs are likewise configured by writing an '0' to their bit positions in the DDRx.

System operation was based on an externally-connected 11.0592MHz crystal device. At this crystal value, the system achieves about 11MIPS at single-cycle instruction execution (Neylre, 2014).

The Baud rate was configured using the formula derived from Table 3.2 (ATmega 32 data book, 2018)

Table 3.2 Baud rate (Atmega32 datasheet, 2017)

Operating Mode	Equation for Calculating Baud Rate[1]	Equation for Calculating UBRRn Value
Asynchronous Normal mode (U2Xn = 0)	$BAUD = \frac{f_{OSC}}{16(\boldsymbol{UBRR}n + 1)}$	$\boldsymbol{UBRR}n = \frac{f_{OSC}}{16BAUD} - 1$
Asynchronous Double Speed mode (U2Xn = 1)	$BAUD = \frac{f_{OSC}}{8(\boldsymbol{UBRR}n + 1)}$	$\boldsymbol{UBRR}n = \frac{f_{OSC}}{8BAUD} - 1$
Synchronous Master mode	$BAUD = \frac{f_{OSC}}{2(\boldsymbol{UBRR}n + 1)}$	$\boldsymbol{UBRR}n = \frac{f_{OSC}}{2BAUD} - 1$

Where:

The baud rate is defined to be the transfer rate in bits per second (bps)

BAUD: Baud rate (in bits per second, bps)

f_{OSC}: System oscillator clock frequency

UBRRn: Contents of the UBRRnH and UBRRnL Registers, (0-4095)

The USART has to be initialized before any communication can take place. The initialization process was achieved by setting the baud rate, setting frame format and enabling the Transmitter or the Receiver based on the usage. For interrupt driven

USART operation, the Global Interrupt Flag was cleared (and interrupts globally disabled) during initialization.

Before doing a re-initialization with changed baud rate or frame format, it was ensured that there were no ongoing transmissions during the period the registers are changed. The TXCn Flag is used in this design to check that the Transmitter has completed all transfers, and the RXC Flag to check that there are no unread data in the receive buffer. The TXCn Flag was always cleared before each transmission before UDRn is written.

The baud rate is given as a function parameter (Mazumber and Dhulipala, 2008).

Table 3.3 UBRRn Settings for Commonly Used Oscillator Frequencies

Baud Rate (bps)	f_{osc} = 8.0000 MHz				f_{osc} = 11.0592 MHz				f_{osc} = 14.7456 MHz			
	U2Xn = 0		U2Xn = 1		U2Xn = 0		U2Xn = 1		U2Xn = 0		U2Xn = 1	
	UBRRn	Error	UBRRn	Error	UBRRn	Error	UBRRn	Error	UBRRn	Error	UBRRn	Error
2400	207	0.2%	416	-0.1%	287	0.0%	575	0.0%	383	0.0%	767	0.0%
4800	103	0.2%	207	0.2%	143	0.0%	287	0.0%	191	0.0%	383	0.0%
9600	51	0.2%	103	0.2%	71	0.0%	143	0.0%	95	0.0%	191	0.0%
14.4k	34	-0.8%	68	0.6%	47	0.0%	95	0.0%	63	0.0%	127	0.0%
19.2k	25	0.2%	51	0.2%	35	0.0%	71	0.0%	47	0.0%	95	0.0%
28.8k	16	2.1%	34	-0.8%	23	0.0%	47	0.0%	31	0.0%	63	0.0%
38.4k	12	0.2%	25	0.2%	17	0.0%	35	0.0%	23	0.0%	47	0.0%
57.6k	8	-3.5%	16	2.1%	11	0.0%	23	0.0%	15	0.0%	31	0.0%
76.8k	6	-7.0%	12	0.2%	8	0.0%	17	0.0%	11	0.0%	23	0.0%
115.2k	3	8.5%	8	-3.5%	5	0.0%	11	0.0%	7	0.0%	15	0.0%
230.4k	1	8.5%	3	8.5%	2	0.0%	5	0.0%	3	0.0%	7	0.0%
250k	1	0.0%	3	0.0%	2	-7.8%	5	-7.8%	3	-7.8%	6	5.3%
0.5M	0	0.0%	1	0.0%	–	–	2	-7.8%	1	-7.8%	3	-7.8%
1M	–	–	0	0.0%	–	–	–	–	0	-7.8%	1	-7.8%
Max. (1)	0.5 Mbps		1 Mbps		691.2 kbps		1.3824 Mbps		921.6 kbps		1.8432 Mbps	

3.2.2 Finger Scanner Design

The next requirement of this design is a biometric security fingerprintscanner that `is designed to use the distinct features of the fingerprints of individual's to provide security. There are Fingerprintscanners now being used in police stations, security-intensive industries and, most recently, on computer shops as a peripheral device for computers. The fingerprints scanner is a device that works based on aperson's fingerprint that is determined by his or her genetic makeup and other factors in his or her mother womb (Neylre, 2014).

. Because there are countless combinations between these two sets of factors, a fingerprint is unique. As such, fingerprints have become an ideal means of identification. One of the commonest finger print scanners in the market today is the SM630 finger print sensor. Due to its availability, cost and features it was used in this research as the fingerprint scanner.

The SM630 background highlight optic fingerprint verification module is the latest release of Miaxis Biometrics Co., Ltd. From its specification (SM630 Datasheet), it consists of optic fingerprint sensor, high performance DSP processor and Flash. It boasts of functions such as fingerprint Login, fingerprint deletion, fingerprint verification, fingerprint upload, fingerprint download, etc. (Jain and Aron, 2009)

The technical specification of the SM630 (SM630 datasheet,) are:

- Operating Voltage: 4.3V～6V
- Operating Current：<80mA（Input voltage 5V）
- Fingerprint Template： 768 templates
- Search Time：<1.5s（200 fingerprint, average value in test）
- Power-on Time：<200ms（Time lapse between module power-on to module ready to receiveinstructions）
- User Flash Memory：64KByte

- Interface Protocol: Standard serial interface (TTL level)
- Communication Baud Rate: 57600bps
- Operating Environment: Temperature: -10℃～+50℃
- Relative humidity: 40%RH～85%RH（no dew）

These features make the scanner very suitable for our design as both the operating weather conditions are very suitable for the design location. The internal memory is also adequate for the design.

Interfacing with the SM630 was done over a two-wire TTL serial interface at 57600bps. Since the microcontroller used has only one serial port, this interfaced was multiplexed using a CD4052 dual 1-of-4 selector, enabling the software to talk to two other devices over the time-multiplexed connection, though only the Wi-Fi radio module was utilized as the companion device on the serial port as recommended (Adolph (2009).

The electrical specifications as recommended from the scanner module are in Table 3.4 The module is connected to host via 4pin cables.

Figure 3.2 SM630 Fingerprint scanner

Table 3.4 SM630 electrical connection (SM630, datasheet, 2017)

Module is connected to HOST via 4PIN cable. The PIN definition is as follows:

No.	PIN Definition	Remarks
1	Power supply +	Power supply +
2	Module Tx	Open circuit output, need to use pull-up impedance in application (Typical value: 10KΩ)
3	Module Rx	Wide voltage input, 7V affordable
4	Power supply	Power supply −

Its pin one is connected to the negative terminals of a power supply while terminals 2 and 3 serves as the transmitter and receiver of data to and from the microcomputer respectively as recommended in its datasheet(Jain and Aron, 2009

3.2.3 The WIFI Radio Network Mode

The system includes a provision for wireless communication between it and a computer. For this purpose an infrastructure network mode was used. This mode implements the full Wi-Fi operational capabilities, at the expense of a more costly setup, and greater time investment. The mode selected should provide security, flexibility and range (Karthik, 2014). This mode also provides an easy interface of an already-existing network to the Internet (Karthik ,2014) .

This mode was implemented for the monitoring system. A module that is commonly available in the market is the HLK-WIFI-M04 embedded radio. The module due to its numerous features was used as the communication device for this design. Themodule is a new low-cost embedded UART-ETH-WIFI module (serial port - Ethernet -Wireless network) developed by Shenzhen Hi-Link Electronic co., Ltd. This product is an embedded module based on the universal serial interface network standard, built-in TCP /IP protocol stack, enabling the user serial port, Ethernet, wireless network (WIFI) interface. Through the HLK-RM04 module, the traditional serial devices do not need to change any configuration; data can be transmitted through the Internet network, provide a quick solution for the user's serial devices to transfer data via Ethernet. The block representation of the module (Mazumber and Dhulipala, 2008) is shown in Fig 3.3

Figure 3.3 HLK-RM04 WiFi radio

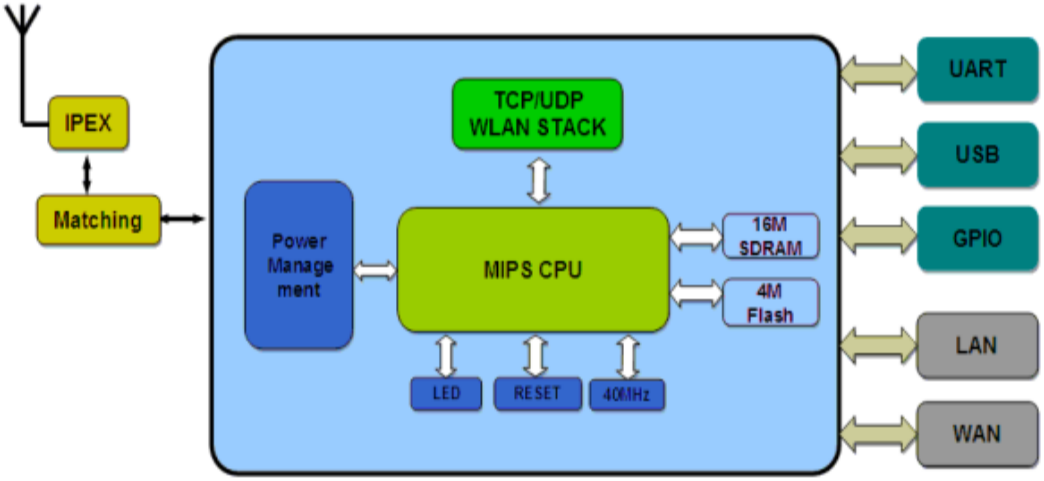

Figure 3.4 HLK-RM04 WiFi radio/AP/router block diagram

Some of the application features that make the HLK-RM04 suitable are **:**

• WiFi Led Control

• WiFi Power Switch

• Home and Commercial buildingautomation

• OBDII WiFi Diagnose

• RFID Data Transfer

• Toys and gaming peripherals

• Industrial systems

• Telemetry

• Remote Control

The device was interfaced to the microcontroller through a multiplexer IC. The power requirement of the device is 5Vand does not require any external component (Mazumber and Dhulipala,2008). The hardware configuration is shown in figure 3.5

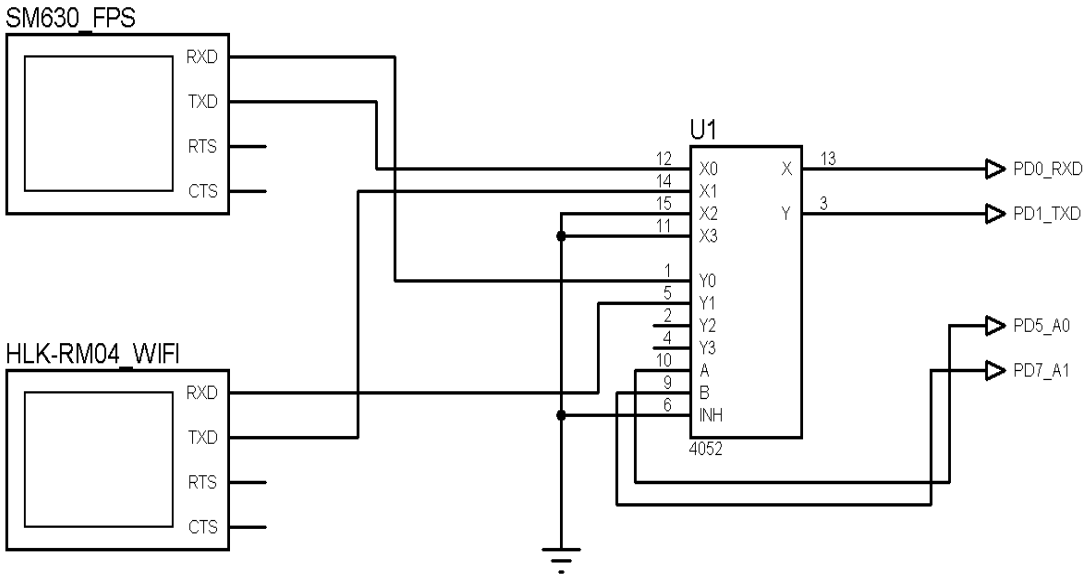

Figure 3.5 WiFi radio circuit configurations

3.2.4CD4052 DUAL 1-OF-4 CMOS Multiplexer

Since the hardware also has to interface with a radio and the finger print sensor, and the Atmega32 has only a single USART in the hardware, a simple means of communicating with both the sensor and the FPS was implemented. This entailed using a multiplexer integrated circuit to time share two signals on the same channel to the microcontroller. The multiplexer used is the CD4052 dual 1-of-4 analog multiplexer. It is used to time-multiplexed the communication between the microcontroller on one hand and the HLK-WIFI-MO4 radio and SM630 fingerprint scanner/sensor units on the other.

The CD4052 device has two address inputs (A1, A0) for selecting the inputs to which a common output is connected. With two address lines, four serial outputs are created by

simply changing the digital logic levels on the address input. The pin configuration of the CD4052 is as shown in figure 3.6

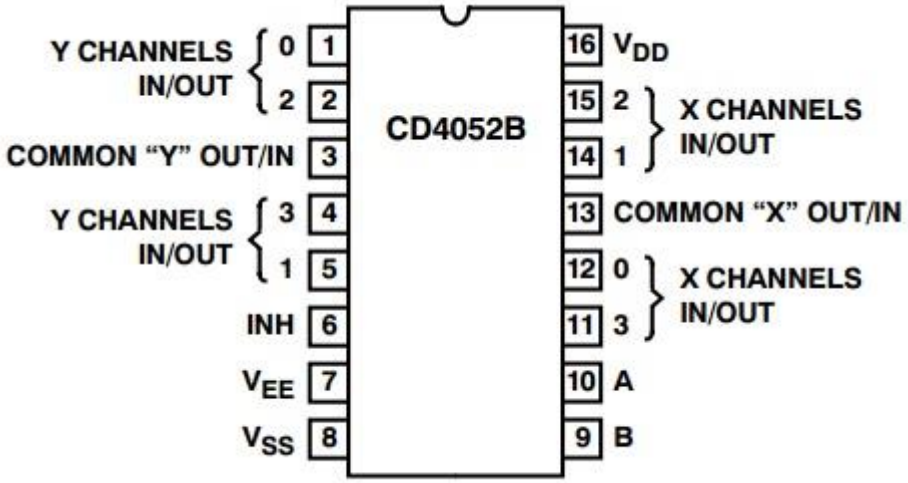

Figure 3.6 CD4052 Multiplexer pinout and fuction

The SM630 sensor was interfaced with the X0/Y0 input, necessitating placing logic 0 on both address input lines. The radio was placed on X1/Y1 hardware pins, and selected by placing logic 1 on A0, and a logic 0 on the A1 pin.

A third output, debug, was used during hardware development for streaming diagnostic data from the hardware ensemble to Hyper terminal on a PC for analysis, especially since the sensor's operation had to be verified. The debug output was selected by making A0 logic 0, and A1 logic 1.

Table 3.5 CD4052 Truth Table (Motorola Semiconductor Databook)

INPUT	**A1**	**A0**	**OUTPUT**
X0/Y0	0	0	X0/Y0
X1/Y1	0	1	X1/Y1
X2/Y2	1	0	X2/Y2
X3/Y3	1	1	X3/Y3

Address selection was done via PD7 and PD5 configured as output pins during hardware initialization at start-up. The hardware connection of the multiplexer circuit is as shown in figure 3.7

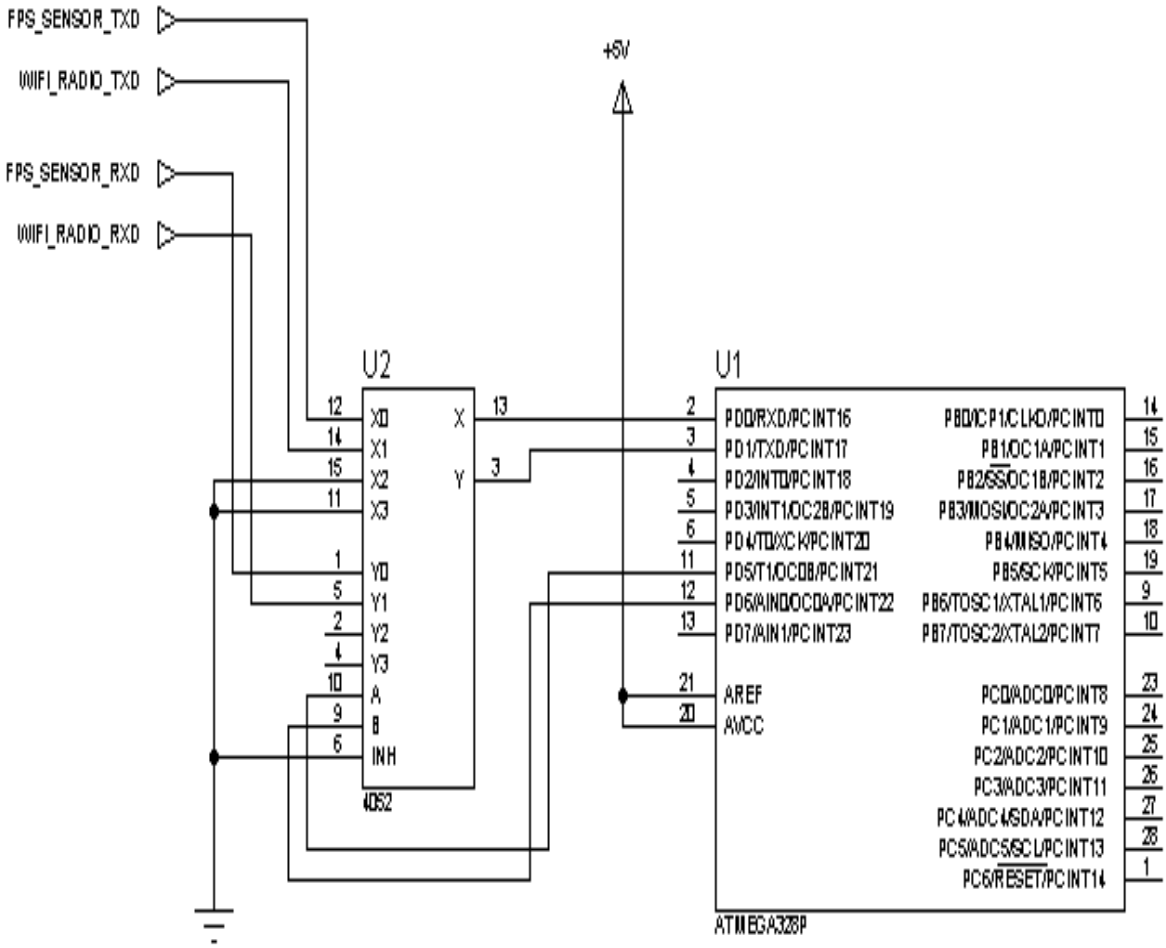

Figure 3.7 CD4052-Microcontroller Interface circuit

3.2.54-line 20-character alphanumeric liquid crystal display

For human-machine interactivity, an alphanumeric LCD was integrated with the system components. The LCD was configured for 4-bit nibble operational mode. The system states were communicated to the user via this component.

Liquid crystal display or LCD as shown in Figure 3.8 is one of the most used devices for alphanumeric output in processor-based circuits. (Desai and Ruchir, 2014)

Figure 3. 8 4-line 20-character alphanumeric LCD

Their LCD are less expensive, reduced size and LCD is classified according to their interface into Parallel and serial. The Serial LCD requires less I/O resources but executes slower than their parallel counterparts and is considerably more costly.

In this work, parallel-driven LCD devices based on the Hitachi HD44780 character-based controller was used. It is by far the most popular controller for microcontroller-driven LCD (Desai and Ruchir, 2014).

The LCD was connected to PORTC of the Atmega32, with JTAG disabled to prevent hardware access conflict. LCD backlight contrast adjustment was provided using a 50-k potentiometers as recommended in the data book of the device (Langenbury, 2010).

The current to the backlight LED was sourced from the 5-volt supply via a series resitance calcukated using the relation:

$Rs = (Vs - V_{LED})/I_{LED}$

Where

Vs = supply voltage across the resistor-LED network

V_{LED} = Forward-voltage drop across the LED

I_{LED} = Forward current through the LED

Using a 5-volt suppy, the resistance was calculated as:

Rs = (5.0 – 2.0)/10mA

Rs = 3.0/0.01 = 300Ω

The nearest available value of 330Ω was used. The eventual circuit diagram is as shown in figure 3.9

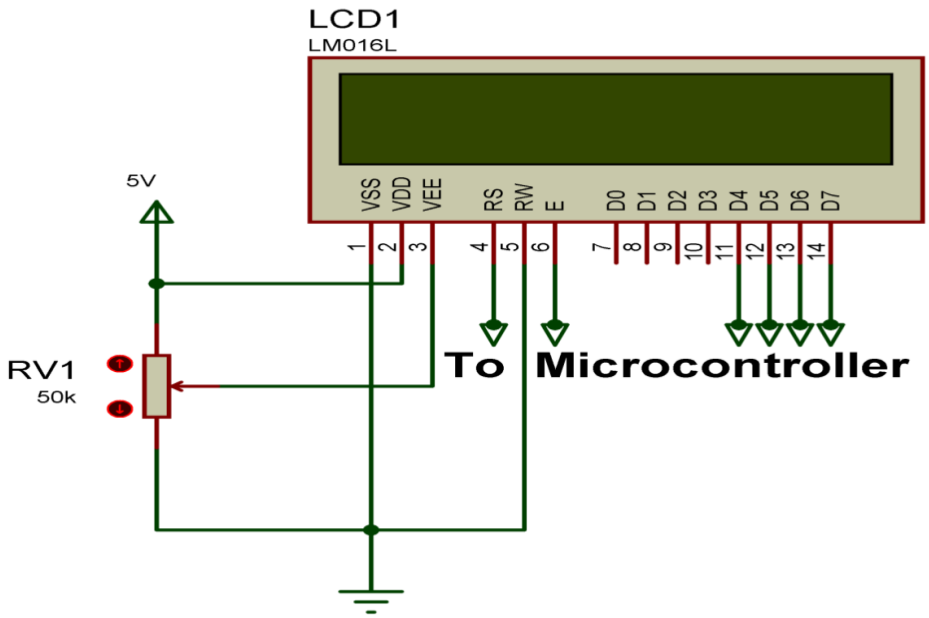

Figure 3.9 LCD Contrast Adjustement circuit

3.2.6 Contact Memory Smart Card

In line with the project objectives and goals, a smart card for data retention was utilized in the design. The memory card was programmed to store data during account registration to be subsequently accessed over a virtual communication port realized using the Wi-Fi radio (Neylre,2014).

An I2C memory card was used as it offered the basic functionality of data storage without the undue software complexity imposed when a true microprocessor card is used. A popular memory card(AT24C16A) was used in this design. The contact memory card has a 2KB non-protected EEPROM cells that are byte-addressable via a 256-byte memory array and 3-bit paging address. Thence, the 2KB memory array was divided into eight 256-byte unique banks (Diaz, 2007). The AT24C16A provides 16384 bits of serial electrically erasable and programmable read only memory (EEPROM) organized as 2048 words of 8 bits each. The AT24C16A is available in space saving 8-pin PDIP, 8-lead JEDEC SOIC, and is accessed via a 2-wire serial interface. In addition, the entire family is available in 2.7V (2.7V to 5.5V) and 1.8V (1.8V to 5.5V) versions.

The features of the selected memory card are:

• Write Protect Pin for Hardware Data Protection

• Low-voltage and Standard-voltage Operation

– 2.7 (VCC = 2.7V to 5.5V)

– 1.8 (VCC = 1.8V to 5.5V)

• Internally Organized 256 x 8 (2K)

• 2-wire Serial Interface

• Schmitt Trigger, Filtered Inputs for Noise Suppression

• Bi-directional Data Transfer Protocol

• 16-byte Page Write Mode

• Partial Page Writes Supported

• Self-timed Write Cycle (10 ms max)

• High Reliability

– Endurance: One Million Write Cycles

– Data Retention: 100 Years

The pin configuration is as depicted in Figure 3.10

Figure 3.10 Smart Card Readers

Figure 3.11 Smart Card (24C16-based, 2KB)

3.2.7 TTL-RS232 logic level converter

To effect communication between the Atmega328 microcontroller and the PC running the VB.Net front-end GUI, a translator was required to transpose the unipolar (0-5V) signaling conventional on the microcontroller to the bipolar (-12V /+12V) signaling required by the IBM PC compatible.

This translation was done using discrete components instead of standard ICs line the MAX232,233, etc. the MAX devices of RS232-TTL transceivers were detected prone to spurious failure after initial operation capability (Neylre, 2014) and thus were not used. A fool-proof transistor-diode assembly was used instead.

3.2.8 Electromechanical relay and Driver Circuit

The system was constructed to provide access by physically controlling a door. This front-end control was implemented using an electronic door lock. The lock was energized/de-energized by passing or blocking current flow into its coil using an electromechanical relay as shown in Figure 3.12

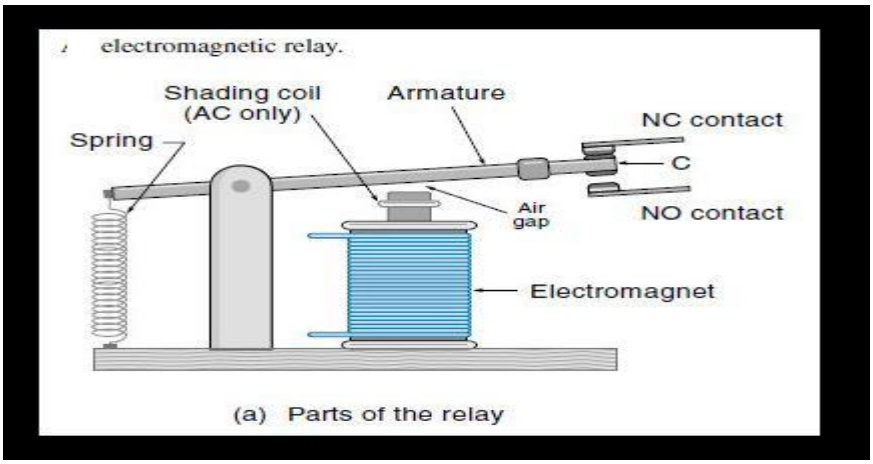

Figure 3.12 Internal assembly of an electromechanical switch

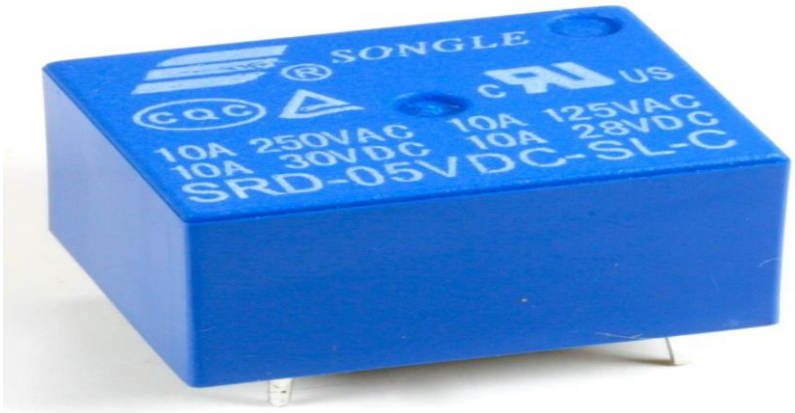

Figure 3.13 5V DC Relay used in the design

Basic parts and functions of electromechanical relays include:

1. **Frame:** Heavy-duty frame that contains and supports the parts of the relay.
2. **Coil:** Wire is wound around a metal core. The coil of wire causes an electromagnetic field.
3. **Armature:** A relays moving part. The armature opens and closes the contacts. An attached spring returns the armature to its original position.
4. **Contacts:** The conducting part of the switch that makes (closes) or breaks (opens) a circuit.

A 5-Volt DC relay was used to control the current to the door strike. A driver circuit was designed and used to drive the relay as the output signal is not sufficient to directly drive it. The driver circuit of which is given in Figure 3.14

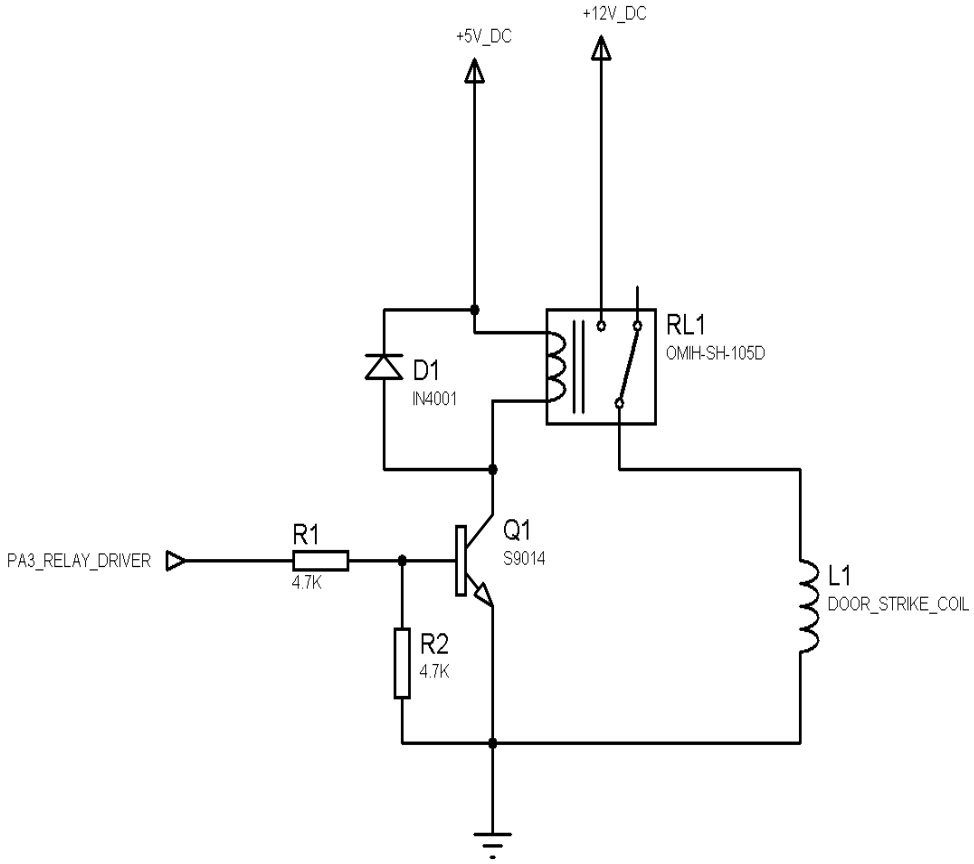

Figure 3.14 Door Strike Relay Drivers

The relay was driven by an S9014 low-power NPN transistor selected because it is a general purpose transistor capable of handling large current. The relay's coil inductance was measured to be 400L, with the rated coil voltage of 5V.

The current required to energize the relay was calculated using the expressions:

$$I = V/R \quad (1)$$

I = current needed to turn on the relay (in amperes)

V = voltage applied across the relay coil (in volts)

R = resistance of the relay coil

Using R = 400Ω, V = 5V;

I = 5/400 = 0.0125A = 12.5mA.

This is the current required to cause an initial latch-on of the relay (latching current). However, once latched on, the coil current can drop to a lesser value (holding current) before the relay de-energizes. The driver transistor (S9014) was chosen based on the maximum continuous current expected to flow through its collector. The S9014 has a continuous-collector-current-handling capability of 150mA, a much larger value than the required latching or holding currents. Since the transistor was operated as a saturated switch, and because in a saturated transistor, the collector current is not dependent on the base current, the requirement was to overdrive the base-emitter junction of the transistor.

Using the advertised gain of 150 for the S9014 (S9014, datasheet, 4444), the maximum base current required to maintain the devices in its linear region is given by

$I_B = IC/\beta$ (2)

I_B = 100uA.

The aim is to drive the base-emitter junction of the transistor with a current much greater than this to cause an overdrive condition.

With a 5-volt Dc supply, the Atmega328 can source a maximum of 10mA per pin.

The value of resistance required to develop a current through the base of the transistor using voltage divider rule and with a current half the microcontroller sourcing current is then given by.

R = V/I = 2.5/0.0005

R = 5KΩ.

This was to ensure that the current drawn from the microcontroller is not too much. This gives the maximum resistance required to develop the required base current to ensure over-drive. This value was reduced to 4.7KΩ, as this was the nearest available value available.

3.2.9 System Power Supply

For the proper operation of the circuit it is required that appropriately rated power supply be provided for the various sections. The primary criterion for selecting the power supply type was voltage, current, power, stability and efficiency. The power requirement of the various sections is:

Microcontroller – 5V 10mA

Relay - 5V 25mA

LCD - 5V 10mA

Sm630 5V 80mA

From the above it was estimated that a well-regulated dc voltage of 5V and current of 2A should be more than adequate. In this regards, switched mode power supplies (SMPS) are far superior to their linear regulator counterparts (Carl, 2013).

The power supply utilized a step-down SMPS commercial off-the-shelf power pack with a nominal output voltage of 12 volts. The 12-volt input was “bucked” down to the 5 volts required for system operation using an LM2576 high-current buck converter.

The LM2576 series of regulators as shown in Fig. 3.17 are monolithic integrated circuits that provide all the active functions for a step-down (buck) switching regulator, capable of driving 3A load with excellent line and load regulation. These devices are available in fixed output voltages of 3.3V, 5V, 12V, 15V, and an adjustable output version.

Requiring a minimum number of external components, these regulators are simple to use and include internal frequency compensation and a fixed-frequency oscillator.

The LM2576 series offers a high-efficiency replacement for popular three-terminal linear regulators. It substantially reduces the size of the heat sink, and in some cases no heat sink is required.

The LM2576 schematic as shown in figure 3.15 Its feature greatly simplifies the design of switch-mode power supplies.

Other features include a guaranteed ±4% tolerance on output voltage within specified input voltages and output load conditions, and ±10% on the oscillator frequency. External shutdown is included, featuring 50 µA (typical) standby current. The output switch includes cycle-by-cycle current limiting, as well as thermal shutdown for full protection under fault conditions.

The features of the LM2576 as listed in the data book are**:**

a. 3.3V, 5V, 12V, 15V, and adjustable output versions
b. Adjustable version output voltage range,
c. 1.23V to 37V (57V for HV version) ±4% max over line and load conditions
d. Guaranteed 3A output current
e. Wide input voltage range, 40V up to 60V for HV version
f. Requires only 4 external components
g. 52 kHz fixed frequency internal oscillator
h. TTL shutdown capability, low power standby mode
i. High efficiency
j. Uses readily available standard inductors

k. Thermal shutdown and current limit protection

The application circuit diagram of figure 3.15 was adopted from the LM257 data sheet. It was found suitable for the design. It provides the required voltage and current.

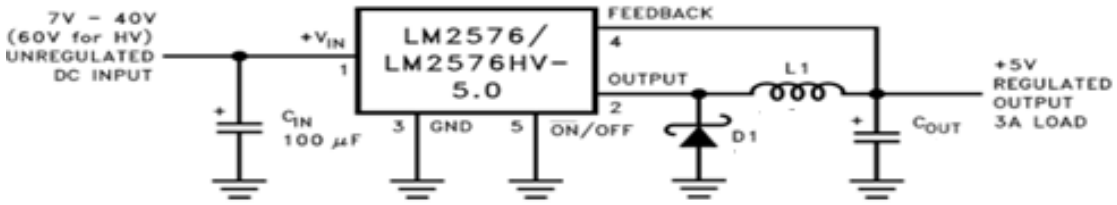

Figure 3.15 LM2576 Buck regulator applications

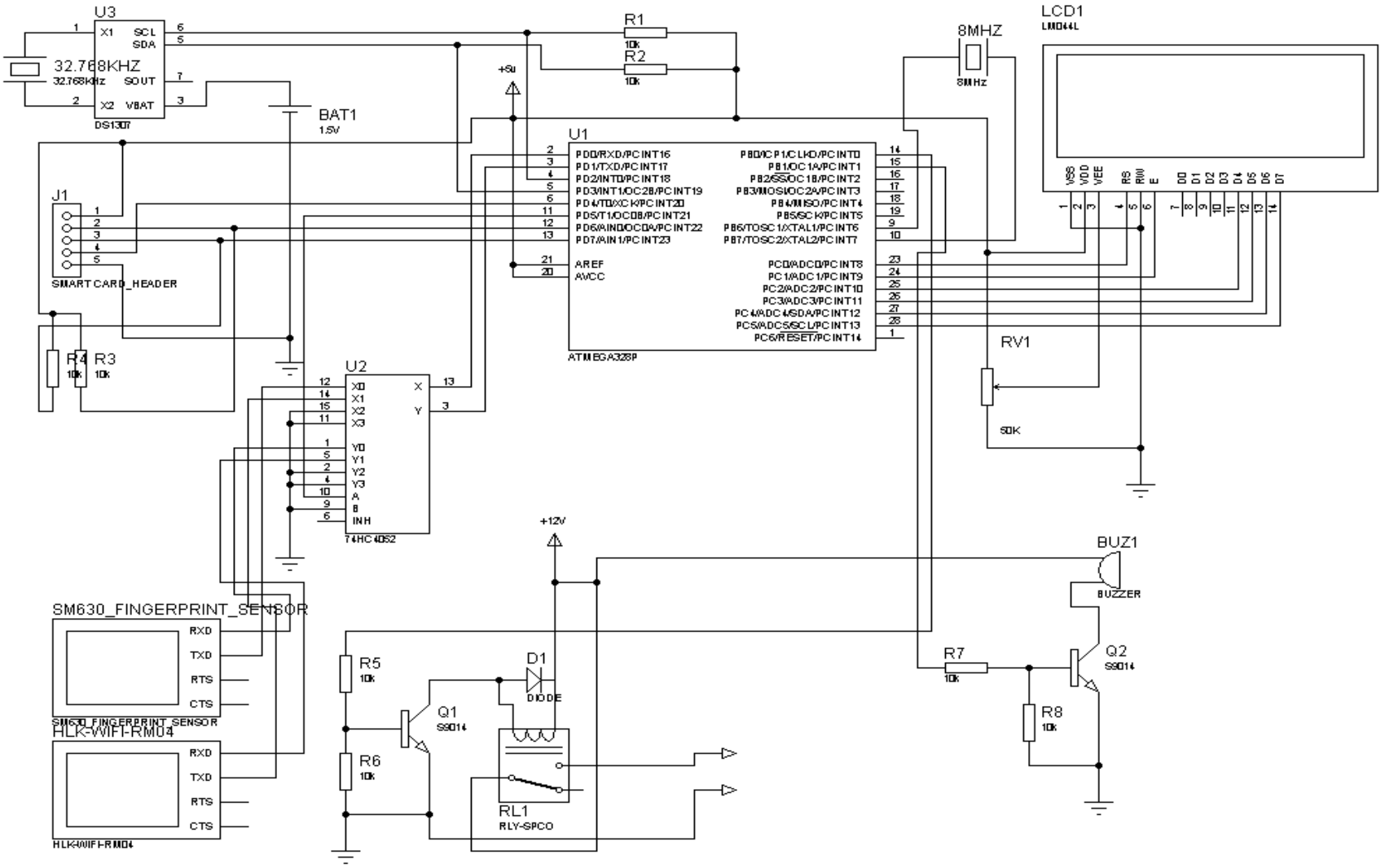

Figure 3.16 System circuit diagram

3.3 Software designs

3.3.1 Software Consideration of the SM630 Scanner

The SM630 biometric sensor relies on a set of commands to perform user-specified operations. These operations include (Mazumber and Dhulipala,2008)

- Add fingerprint
- Delete fingerprint
- Search fingerprint
- Empty fingerprint database
- Search information in fingerprint database
- Download fingerprint template
- Upload fingerprint template
- Read ID number
- Read user Flash
- Write user Flash
- Read product logo

The sensor furnishes a set of response code to the user application, indicating the status of the execution of the user-specified operation(s). The responses are (Jain and Aron, 2009)

- Receive correct
- Receive error
- Operation successful
- Finger detected
- Time out
- Fingerprint process failure

- Parameter error
- Fingerprint matching with this ID found
- No matching fingerprint with this ID
- Fingerprint found
- Fingerprint unfound

Interfacing with the sensor entails formatting the intended operation to be executed by the sensor in a manner expected by the sensor. These packets can be either a command packet, or response packet. A command packet is sent from the application processor and a response packet is sent from the SM630. These packets are coded as indicated below:

One communication packet includes the following (Jain and Aron, 2009):

Packet Head（2 bytes）

Packet flag（1 byte）

Packet length（1 byte）

Packet ContentN bytes）

Check sum（1 byte）

Packet head：0x4D 0x58

Packet flag;

0x10：command packet

0x20：data packet

0x21：last packet

0x30：response packet

Packet length：

Length of the Content in packet

Packet content：

Content of packet

Check sum：

Low 8 bytes of the SUM from packet head to check sum.

(MIAXIS SM630 Fingerprint Verification Module User Manual, 2009)

In interfacing with the fingerprint sensor (FPS) the approach was to maximize flexibility and rapid adaptation top changing requirements if necessary: the command packets were assembled by a core code block, the checksum generated by the same block, and the size of the data bytes to be written to the sensor placed in a strut member. Since the FPS required different commands for operations, while also returning different response packet sizes, the software was coded to deal with these issues as well.

3.3.2 System flowchat

The flowchart for the software is shown in Figure 3.17

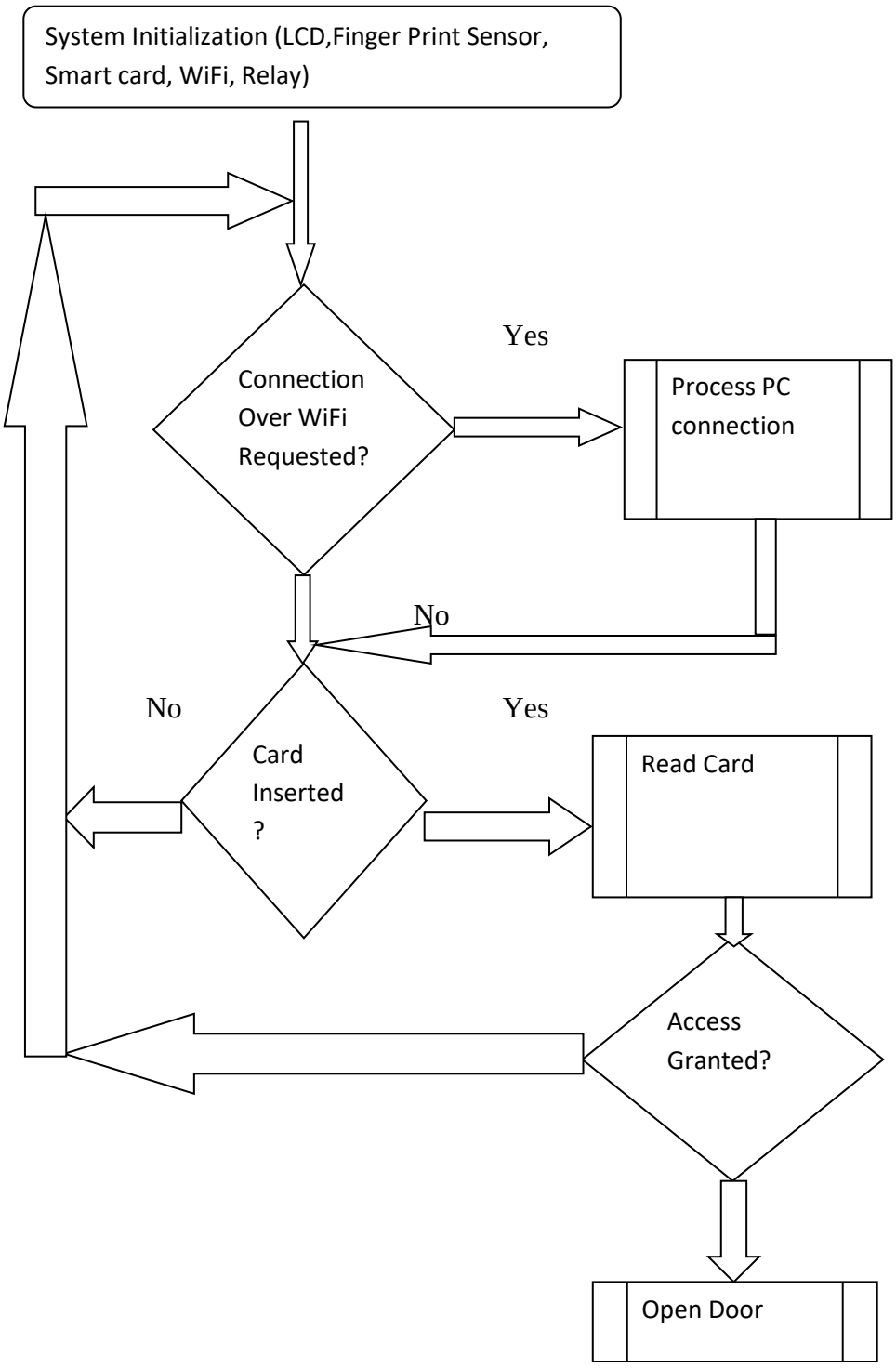

Figure 3.17 Design Flowchart of the microcontroller software

3.4 Method

After the circuit design, each module was constructed on separate modules. The power supply and the main microcontroller module were however constructed on the same board to limit the number of buses. The assembly was carried out module by module. At each stage, tests were conducted to see if the constructed circuit meets the design claim or expectations. Each stage was first connected on a bread board then transferred to permanent circuit board. The completed construction is as shown in fig 3.18

Figure 3.18 Completed WiFi Biometric Access Control system

3.4.1 Design testing of user registration

After the system was constructed it was tested by registering users on the system. A multi-step process was adopted which embodied the creation of a server-side account for an intended card holder andwas carried out through:

a. Image registration and bio data logging into an online database integrated with the graphic user interface was carried out by a user.

b. Registration of the user over the network was tested to ensure that the developed system does not need to have a master unit dedicated to user registration. In essence, similar unit can be used for registration. This is so because the captured templates are not stored locally on the machines, but rather on the card, enabling instant verification of identity at any visited node.
c. Downloading of the server-side information wireless into the control unit.
d. Physical capturing of the user print templates through the FPS was performed, and transferred to the card. The card was inserted into the card reader at the prompt indicated on the screen.

With thisprocess successfully carried out, the card is now deemed valid and verifiable. In addition, the card was digitally-signed using the end-user public key. The prints written to the card were also encoded, the key being generated from the user name, and stored encrypted on the card.

3.4.2 Testing for User Authentication

Test on User authentication was carried out, configured to commence with the detection of an inserted card. A visual notification is printed on the LCD notifying the card holder of this, while background processes run to ascertain the validity of the card holder's information and account.

Validation of the holder's access rights was achieved based on the following steps:

1. Loading user-specific data from the card. The software searches for the programmed access level assigned to the holder. If the access level is lower than that assigned to the access control system, the access is denied.
2. Information on the card is correlated with the information stored in the database on the access system. Primarily, the software confirms if the account ID

associated with the card is active or not.It is possible for the account to be blocked. If the account is active, the user bio data loaded from the card is matched with that downloaded onto the control system over the wireless interface. If there is match, the software then moves on to the next step.

3. Actual authentication using fingerprint templates involves the following intermediate steps:
    a. Loading the two print templates from the card and downloading into the FPS.
    b. Grabbing a fresh scan of the user print via the SM630. If the scanned finger does not match the first template, it is matched against the second downloaded template.
    c. Depending on the matching score generated by the authentication IP core, access is either granted or denied.
    d. If access is denied, the corresponding reason is visually conveyed to the user.
4. After a successful validation of user print, the system date and time of access was saved against the user ID in an access log and uploaded to the server application on instruction. Consequent upon a successful authentication the physical energizing of an electromagnetic lock or door strike interfaced with the system. The lock is energized for a period of time determined by the setting made in the system configuration parameters. This was communicated audibly by two short beeps.

A display of the card holder's name was also printed on the human machine interface (HMI), enabling the opening up the possibilities of more interactive human-machine interfacing.

3.5 Testing of the system

Four tests were carried out on the system after assembly. These tests were to determine the fitness, or otherwise, of the access control system for the intended deployment. The tests are (Mazumber and Dhulipala, 2008).

a. False Match Rate (FMR)
b. False Non-Match Rate (FNMR)
c. Failure-to-Enroll (FTE) Rate
d. Average comparison time

The test sample was drawn from a pool of 40 volunteers. Since a single memory card was available during the testing phase, the software was modified to utilize the fingerprint sensor for print storage. As the sensor could store a maximum of 768 templates in its on-chip memory, restriction on print template data size was not an issue. The templates of the volunteers were saved on the sensor after code modification preparatory to real-life testing. The right thumb was used for registration as this provided the largest surface area for print capture.

3.5.1 False acceptance rate test

This test was performed to evaluate the ability of the sensor to discriminate amongst different prints. Ten non-registered users were asked to authenticate themselves on the system one at a time, and the system response noted as each user was scanned and compared in real-time.

3.5.2 False rejection rate test

This test shows the susceptibility of the sensor to false rejecting a valid authentication credential. The test was carried out using twenty users.

3.5.3 Processing time test

This test was to arrive at the average time expended by the system on a single user during validation. The processing time during registration was not considered as it is not relevant to the “real-timeness” of the system during field usage.

The response of the system can be approximately inferred from the time taken to process a single print template. This time is directly related to the quality of print extracted from the scanner.

3.5.4 Failure to enroll test

The FTE test result was drawn up during the registration phase. Of the forty volunteers prints used on the system, some could not be registered until about the third or fourth attempt.

CHAPTER FOUR
RESULTS AND DISCUSSION

4.1 Results

The performance of the fingerprint based multiuser biometric access control system designed in the course of the work. Data collection and tests carried out on the unit are also expounded upon. A comprehensive discussion of the test results is also included for the purpose of future endeavors in this area of research.

4.1.1 Enrollment Test Result

The result of the test on the Volunteers enrollment is tabulated in Table 4.1

Table 4.1 The result of the enrollment test

S/NO	Volunteers	ENROLLEMENT TRIALS				
		1ST TRIALS	2ND TRIAL	3RD TRIAL	4TH TRIAL	5TH TRIAL
1	Volunteer 1	Fail	Fail	fail	Successful	0
2	Volunteer 2	Fail	Fail	fail	Fail	Successful
3	Volunteer 3	Fail	Successful	0	0	0
4	Volunteer 4	Successful	0	0	0	0
5	Volunteer 5	Fail	Fail	fail	Fail	Successful
6	Volunteer 6	Successful	0	0	0	0
7	Volunteer 7	Fail	Successful	0	0	0
8	Volunteer 8	Successful	0	0	0	0
9	Volunteer 9	Fail	Fail	fail	Successful	0
10	Volunteer 10	Fail	Fail	Fail	Fail	Successful
11	Volunteer 11	Successful	0	0	0	0
12	Volunteer 12	Fail	Fail	successful	0	0
13	Volunteer 13	Fail	Fail	fail	Successful	0
14	Volunteer 14	Successful	0	0	0	0
15	Volunteer 15	Fail	Fail	fail	Successful	0
16	Volunteer 16	Fail	Fail	successful	0	0
17	Volunteer 17	Successful	0	0	0	0

18	Volunteer 18	Fail	Successful	0	0	0
19	Volunteer 19	Fail	Fail	Fail	Fail	Successful
20	Volunteer 20	Fail	Fail	Successful	0	0
21	Volunteer 21	Fail	Successful	0	0	0
22	Volunteer 22	Fail	Successful	0	0	0
23	Volunteer 23	Successful	0	0	0	0
24	Volunteer 24	Fail	Fail	fail	Fail	Successful
25	Volunteer 25	Successful	0	0	0	0
26	Volunteer 26	Fail	Successful	0	0	0
27	Volunteer 27	Fail	Fail	Fail	successful	0
28	Volunteer 28	Fail	Successful	0	0	0
29	Volunteer 29	Fail	Fail	Fail	Fail	Successful
30	Volunteer 30	Successful	0	0	0	0
31	Volunteer 31	Fail	Fail	successful	0	0
32	Volunteer 32	Successful	0	0	0	0
33	Volunteer 33	Fail	Successful	0	0	0
34	Volunteer 34	Fail	Fail	fail	successful	0
35	Volunteer 35	Fail	Fail	successful	0	0
36	Volunteer 36	Fail	Fail	Fail	Fail	Successful
37	Volunteer 37	Successful	0	0	0	0
38	Volunteer 38	Fail	Fail	successful	0	0
39	Volunteer 39	Fail	Fail	fail	Successful	0
40	Volunteer 40	Successful	0	0	0	0

The result presented is summarized in table 4.2. The table shows the number of the volunteers that were successfully enrolled after the different stages of the five trials.

Table 4.2 The summary of the enrollment test result

No of trials	1st trial	2nd trial	3rd trial	4th trial	5th trial	Failure to enroll
No of volunteer enrolled	12	8	6	7	6	1

4.1.2 Failure to enroll test result

The Table 4.3 below gives the overview of the test result of the failure to enroll test conducted.

Table 4.3 The result of the failure to enroll test

No of trials	1st trial	2nd trial	3rd trial	4th trial	5th trial	Failure to enroll
Failure to enroll	28	20	14	7	6	1

From Table 4.1 it could be seen that after the first trial, 12 of the volunteers successfully enrolled indicating that 70% failed to enroll. On the second trial only nine of the remaining volunteers were enrolled indicating that 67% failed to enroll after two tests. The result of the third trial showed that 52% of the volunteers failed to enroll. Of the ten volunteers left for the fourth trial the result showed that 40% failed to enroll. The fifth enrollment test showed that three of the volunteers left only one failed to be enrolled. The result also showed that even after 6th 7th, and 8th trials the remaining volunteer could not be enrolled.

4.1.3 False rejection rate test result

Twenty enrolled volunteers and twenty not registered volunteers were considered under this test to evaluate the false rejection rate as 19 of the registered volunteers was successfully authenticated while one (1) of the registered volunteers was not successfully authenticated and the result is as presented in Table 4.4.

Table 4.4 False rejection rate

NO OF VOLUNTEERS	Authentication Successful	Authentication Failed
20 Registered	19	1
20 Not Registered	0	20

4.1.4 False acceptance rate test result

Twenty non registered volunteers were considered under this test to evaluate the false acceptance rate where a non-registered person can be successfully authenticated and gain access to a restricted place.

As also presented in Table 4.4, of the twenty non registered volunteers, none was successfully authenticated while twenty of the volunteers was not successfully authenticated.

4.1.5 Average comparison time

Ten registered volunteers were used to evaluate this test to determine user processing time for a successfully validation and authentication as shown in Table 4.5 below.

Table 4.5 User Processing time of validation

No volunteers	1st	2nd	3rd	4th	5th	4th	7th	8th	9th	10th
Processing time(seconds)	53	47	30	37	35	44	33	38	40	36

Average comparison time can be calculated in seconds as below

$$\text{Average comparison time} = \frac{Total\ proccessinn\ time}{Total\ number\ of\ volunteers}$$

$$= \frac{53+47+30+37+35+44+33+38+40+36}{10} = \frac{393}{10}$$

= 39.3 sec

4.2 Discussion of result

The results of the False Acceptance rate (FAR) test showed that all of the non-registered volunteers were not accepted by the system. This indicates that the system is highly secured as it will not accept non registered outsiders to a restricted place. The false reject rate (FRR) test produced mixed results, as one registered volunteer failed to be authenticated even after five runs of the same individual were made. The above result is not atypical of print-based access control systems; it merely underscores the fact that many variables come into play during print authentication, variables that were not factored in during print registration. Chief amongst these variables are:

1. Incorrect finger pose

   Some algorithms are every sensitive to discrepancies in finger pose during registration and authentication. As it is impossible to have every user place his/her thumb exactly the way it was during registration, this outcome cannot be entirely eliminated. It should be noted that the results were not strictly monotonic in nature, but rather yielded different responses for the different runs.

2. Dirty finger

   The SM630 scanner is capable of detecting dirty fingers. Cleaning the finger (washing with soap) to eliminate greasy obscurations provided the cure. In the field, users will need to be aware of these requirements for a successful registration and authentication.

After multiple usages, this became a bit of an issue. Print deposits left over from a previous user made the scanner optical assembly insensitive to new prints, with the attendant result that it was not easily possible extracting templates from prints placed on the dirtied glass. However, wiping with a soft cloth corrected this, but not in all cases.These reasons could be any of the following (Mazumber and Dhulipala, 2008)

i. scanner error
ii. validate error
iii. print download error
iv. finger detect error
v. print capture error
vi. print match fail
vii. database access error
viii. print process error

A dirty print will register as validate error. A finger that is not “biologically-active” will register as a finger detect error.

On failure to error (FTE) test result, various reasons could be given as listed below:

a. Fingerprint process failure
b. Timeout
c. Parameter error

Of the errors stated above, the parameter error would silently go away by itself. This error is indicative of a wrong argument sent to the print sensor. However, since it is non-sticky (does not crop up on retries), it is postulated that an internal sensor malfunction is

responsible as a malformed packet sent to the sensor will be rejected over and over again. This was not the case, and thus misbehavior in the sensor was the due cause.

The fingerprint processing failure error was most influenced by the user. This has been enumerated in the FRR section.

Timeout error is typified by a communication break between the system microcontroller and the SM630 sensor. Due to the limitation of the Atmega328 having a single UART while two are needed, a multiplexer was used to expand the UART interface. This IC (CD4052) was fingered in causing data obfuscation in about two occasions.

An enrolment or comparison attempt can fail, thus resulting in a Failure-to-Enroll (FTE) or Failure-to-Compare (FTC) error, respectively. Failures can be reported by the algorithm (which declares itself to be unable to process a given fingerprint), using the following mechanisms:

a. timeout: the algorithm exceeds the maximum processing time allowed;
b. Missing template (only for comparison): the required template has not been created due to enrolment failure, such that the comparison cannot be performed.

Each FTE error produces a “ghost template”, which cannot be matched with any fingerprint (i.e. any comparison attempt involving a ghost template results in a failure to compare). Although using this technique for including Failure-to-Enroll errors in the computation of FMR and FNMR is both useful and easy for the problem at hand, this practice could appear arbitrary. It can be shown that this operational procedure is equivalent to the formulation adopted in (Ratha and Bolle, 2004), which is consistent with current best-practices

Performance evaluation is important for all pattern recognition applications and particularly so for biometrics, which is receiving widespread international attention for citizen identity verification and identification in large-scale applications. Unambiguously and reliably assessing the current state of the technology is mandatory for understanding its limitations and addressing future research requirements.

Performance of SM630 fingerprint algorithms is quite good if we consider that the test regimens have been intentionally made difficult by exaggerating perturbations such as skin distortion and sub-optimal skin conditions (e.g. wet and dry) known to degrade algorithm performance.

CHAPTER FIVE
CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

The design and construction of a finger based multiuser biometric access control syetem was successfully carried for improved security in homes and organization . the various performance test of failure to enroll, false rejection rate, false acceptance rateand average comparison test was done .

The result showed that the device was much secured as it measures individual's unique physical or behavioral characteristics to recognize or authenticate their identity. The work was successful features the major characteristics of p[roving the user claim to be who they said they are and proving the user to be who they said they are not.

. The design has these features:

- The ability to add and delete users
- Enrollment of user
- User’s biometric characteristics that is provided to the sensor during both enrollment and life presentation
- Transmission of captured data
- Matching of captured data

The design system was able to authenticate authorized personal accurately, rapidly, reliably, without invading privacy right , cost effectively, in a user friendly manner and without drastic change to the existing infrastructures.

5.2 Recommendations

i. This work was built with quality wiring and contains many connections, I recommend that if failure occur, it should be troubleshoot by a qualify personnel along with the circuits diagram.

ii. This project was built for Educational purposes. It is recommended that a hook should be attached to the casing and fixed the system on the wall if one wants to use it for industrial or home applications.

iii. In Compliance with privacy law, I recommend more work can be done through privacy by standard which integrates technical measures to mitigate privacy risks.

iv. This work can accommodate up to 500 users at a time, I recommend a further work that can accommodates more than the presents 500 users

REFERENCES

Abhisek, N (2013). Secure biometric recognition. Turkey: Turku University of Applied Science.

Adewole, K.S., Babatunde, R, S and Abdulsalam S.O (2014). Development of fingerprint Biometric attendance system for non-academic staff in a tertiary institution. Ilorin: University Printing Press.

Adolp, M (2009). Biometric and standards. USA: ITU- technology watch report.

Anil, K.J and Karthik, N (2013). Fusion in Multibiometric identification system. USA: Biometric Template Security.

Ashraf, E (2009) Design and implementation biometric access control system using fingerprint for restricted area based on Gabon filter. Egypt: Fingertech.

Carl Z.E (2013). Optical cryptography and biometric based remote authentication protocol. West Sussex: Mag Tek miniwedge publisher.

Chirillo, J. and Scott, B. (2007). Implementing Biometric Security. Indianapolis: John Wiley Publishing Inc.

Christian, R and christoph, B (2014). Multibiometric template protection, issues and challenges. Turkey: voicevault Inc publisher.

Desai,K.R and Ruchir, P (2014) Cryptography and biometric based remote authentication protocol. Kerberos: Voicevault publisher

Diaz, R (2007). Biometric Security Vs Conveniences. USA: Security World Magazine Publisher.

Dubin, C. (2011). Biometrics: Hands Down, ID Management. USA: CMS, Hosting & Web Development, epublishing.

Elsevier, C (2007). The future of Biometric, biometric technology today. USA: Zeus technology.

Jain, A.K (2007). Biometric: providing ground for image and pattern recognition. China: Image and graphics, fourth international conference.

Jain, A.K and Aron, R (2009) Learning user- specific parameter in a multi biometric system. USA: Department of computer and engineering, Michigan state university.

Jianjiang, F. (2007). Combining minutiae descriptors for fingerprint matching. China: Pattern Recognition page 342-352.

Karthik, N (2014). Multibiometric system fusion strategies and template security. Kerberos: feature transformation figures

Langenburg, G (2010). Are one's fingerprints Similar to those of his or her parent in an discernable way? USA: Scientific American.

Marco, G and Marcos, F (2014). A protection scheme for enhancing biometric template security and disccriminability, Kerberos: Voicevault publisher.

Mazumdar, S and Dhulipala, V (2008) Biometric Security Using Fingerprint Recognition. San Diago: University of California.

Neylre, D.S (2014) Practical multi factor biometric remote authentication, Kerberos: Voicevault publisher

Ogherohwo, E.P and Ezeoba E.O (2011). Design and construction of a biometric examination authentication devices. Jos: University of jos Printing Press.

Ratha,N and Bolle,R.M (2004). Authomatic Fingerprint Recognition System. New York: springer

Setlak, D (2010). Advances in Biometric fingerprint technology are driving rapid adoption in consumer marketplace. New York: Authen Tec, Retrieved 4 November 2010.

Shoewu, O., Ogunlewe, O.A and Adebari, F.A (2016) Design and development of an effective and secure fingerprint based biometric attendance device. Lagos: University Press.

Thornton, J (2010) Latent Fingerprint, setting standards in the comparison and identification. California: 84th Annual Training Conference of the California State Division of IAI.