MULTILAYER SECURITY SYSTEM

A thesis submitted in partial fulfillment of the requirements for the degree of

B.Sc in Electrical and Electronic Engineering

Submitted By

JABEL RAHMAN

Student ID: 12121180

MOHAMMAD AL-AMIN

Student ID: 10221015

SUROJIT SAHA

Student ID: 10221014

APRIL 2016

DECLARATION

We hereby declare that the thesis titled **"MULTILAYER SECURITY SYSTEM",** submitted to the Department of Electrical and Electronic Engineering, BRAC University for the fulfillment of degree in Bachelors of Science in Electronics and Electronic Engineering, is our original work. Any information used from other sources has been acknowledged in the reference section.

Submitted by:

_____

JABEL RAHMAN

Student ID: 12121180

_____

MOHAMMAD AL-AMIN

Student ID: 10221015

_____

SUROJIT SAHA

Student ID: 10221014

_____

Signature of the Supervisor
Ms. Marzia Alam,
Department of Electrical and Electronic Engineering,
BRAC University

ACKNOWLEDGEMENT

Through the span of this proposal, for as far back as year, we have committed ourselves to this work, the movement of which have made could never have been finished all alone and for that; we have gotten ourselves obligated to our regarded supervisor, Ms. Marzia Alam, Senior Lecturer, Department of Electrical and Electronics Engineering, BRAC UNIVERSITY . For whose without constant positive bolster, direction and advice for the fulfillment of this work would not have been generally conceivable.

Our special thanks to Mr. Wahiduzzman Arup for helping us and giving his important time throughout the project.

Lastly we would deeply like to convey our thanks to all the faculty members, the lecturers and our university for assisting us with their help and with the required equipment, which was required during the completion of our thesis.

ABSTRACT

The main goal of this paper is to design and implement a multilayer security system, which can be used in bank, secured offices and homes. The system is based on RFID, Keypad and a fingerprint scanner technology containing door-locking system, which can activate, authenticate, and validate the user and unlock the door in real time. This system consists of microcontroller, RFID reader, Fingerprint scanner, keypad locker, and display module. The RFID reader reads the id number from passive RFID tag and send to the microcontroller, if the id number is valid then the user will be asked to enter the keypad password and after the password is verified the user will be asked to use the fingerprint scanner which will match the fingerprint and if user gives a wrong input then alarm will be generated and a blue tooth connection will be established with an android device which will take a picture of the unauthorized person. After completing all the security check successfully, the locker system will be accessible to the user and the system will be prevented from any unauthorized access.

TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION 7

1.1 BACKGROUND AND MOTIVATION 9

1.2 DESCRIPTION 10

1.3 OBJECTIVE OF THE PROJECT 11

CHAPTER 2: OVERVIEW OF THE PROJECT 12

2.1 COMPONENTS *13*

2.2.1 ARDUINO *13*

2.2.2 LCD *14*

2.2.3 CONNECTING WIRES *15*

2.3 KEYPAD SYSTEMS *15*

CHAPTER 3: SENSORS 18

3.1 FINGERPRINT (BIOMETRIC SYSTEM) 19

3.1.1 INTRODUCTION TO FINGERPRINT 22

3.1.2 FINGERPRINT PATTERNS 25

3.1.3 FINGERPRINT RECOGNITION 28

3.2 RFID 29

3.2.1 HISTORY OF RFID 30

3.2.2 RFID THEORY 31

3.2.3 TYPES OF RFID 32

3.2.4 RFID READER 33

3.2.5 CLASSIGICATION 34

3.2.6 RFID APPLICATION 35

3.2.7 BENEFITS AND CHARACTERISTICS OF RFID 36

3.2.8 PROBLEMS WITH RFID 37

CHAPTER 4: BLUETOOTH SYSTEM 39

4.1. PIN CONFIGURATION 40

4.2 WORKING PROCESS 42

4.3 FLOWCHART 44

CHAPTER 5: CONCLUSION AND FUTURE WORKS 45

APPENDIX 47

REFERENCES 52

Chapter 1: Introduction

In this present age, safety has becomes an essential issue for most of the people especially in the rural and urban areas. Some people try to cheat or steal the property, which may endanger the safety of money and valuable assets in the bank, house, and office. To overcome the security threat, a most of people will install bunch of locks or alarm system. There are many types of alarm systems available in the market, which utilizes different types of sensor. The sensor can detect different types of changes occur in the surrounding and the changes will be processed to be given out an alert according to the pre-set value. By the same time this system may not be good for all the time. Theft is one of the major problems in schools and offices. To minimize these incidents, different ways to secure belongings and documents were done. Most universities and offices use lockers and cabinets for storing files, securing belongings and keeping of important documents for privacy and security purposes. However, some lockers used ordinary padlocks and were shared by two or more users. Common lockers do not guarantee full safety and security of property because ordinary padlocks can be opened by force In this thesis we have implemented safety of the valuable belongings in the bank locker, house, and office (treasury) by using RFID, Keypad and a fingerprint scanner based multilayered security system.

The word ‘security system’ suggests for itself that it is associated with the safeguard of valuable things. Bangladesh is a developing country with many security problems, which are still to overcome. We are still lacking in technological fields where many nations have already explored. This is happening due to lack of awareness among the people of our nation. The carelessness have got us to this position now from which we are facing trouble to recover ourselves as a nation. But we can all take steps to make our nation a safer place to live in so we need security in every sector of our life. The most important place where safety is required is our households and the place where we store our valuables. The old types of security are no longer strong enough to safeguard such valuables so we must thing digitally and use technology to make security systems much stronger. This types of security may involve using digitals locks, various locks using keypad or word security, using microcontroller, RFID, biometric process, etc.

1.1 BACKGROUNDS AND MOTIVATION

Bangladesh is country where theft is a major issue nowadays. Every now and then we can see that there are several news on the TV regarding theft in the banks, offices and even in some households. The people associated with such crime, there are hardly any steps to catch them when stealing or neither there is any evidence out of which they can be caught. They can easily break through the security systems, which are there to safeguard the place because in most of the places in our country there are old conventional methods, which are used for security systems.

So we have considered something, which will help people to increase their security systems using latest technology at a cheaper rate. Cost is also a major factor, which forbids people from switching to such types of security systems. So we have kept that in mind and have come out with a project, which will help people to start using such equipment eventually and help them in the long run.

In our project we have made a security system, which uses a keypad system, an RFID and a fingerprint scanner, which are simultaneously set to make it a stronger multilayered security system.

1.2 DESCRIPTION

Biometric is considered as one of the most effective method when it comes to security. Biometric is an automated technique of recognizing a person based on his physical attributes which includes face, fingerprint, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric data are considered as different and distinct from personal information because it cannot be reverse-engineered to recreate any personal information and cannot be stolen to attempt theft. Fingerprints are the most common biometric technology used in many applications. The fingerprints recognition and matching is one of the simplest ways of verifying a person's identity. It requires the imaging and comparison of the print pattern, which includes the ridges and minutia points. These patterns are unique to every individual.

RFID module consists of RFID tag and RFID reader. When the user punches his card (containing the tag), the 12-byte serial number of the tag is read by the RFID reader and is sent to the

microcontroller. The microcontroller then compares the data with the existing data stored in the EEPROM memory (internal memory of the microcontroller). If the data matches with the existing data in the memory, it means the person is authorized and the user enters the second stage of the security system. If the data is not matched then the user will not be permitted to enter the premises. The buzzer starts ringing to provide an alarm indicating the presence of an unauthorized person.

The user uses the keypad system to manually enter the password. The keypad is used to make the security system much stronger as using a keypad makes the user to remember the password he had been using for accessing into the security system. The keypad also restricts an unauthorized person from entering into the security system as a person who fails to remember the password cannot go to the next step of the system. If the user inserts any wrong input then the blue tooth device will connect to the android camera and will take a picture.

1.3. OBJECTIVE OF THE PROJECT

We live in a country where we have so many places to develop, so we all need to take initiative to make progress to stay in par with the rest of the world. As the youth of the society of our country it us our responsibility to start the progress. We need to show the path to the people of our country. Thus making more of such projects will enable us to know more about the technology of the modern world and its utilization of such technology in various places and sectors. Making strong security systems will help our nation in many ways. The most important thing is that it will make people believe in such systems and they will use more of such systems in their daily life.

Chapter 2: OVERVIEW OF THE PROJECT

2.1. Components

- Sensors
    - Fingerprint sensor (Biometric System)
    - RFID
- Keypad system
- LCD Display
- Arduino Mega 2560(2 pcs)
- AC & DC source
- Variable resistor
- Connecting wires

2.2.1. Arduino

The Arduino mega 2560:

The Mega 2560 is a microcontroller board based on the ATmega2560. It has 54 digital input/output pins (of which 15 can be used as PWM outputs), 16 analog inputs, 4 UARTs (hardware serial ports), a 16 MHz crystal oscillator, a USB connection, a power jack, an ICSP header, and a reset button. It contains everything needed to support the microcontroller; simply connect it to a computer with a USB cable or power it with a AC-to-DC adapter or battery to get started. The Mega 2560 board is compatible with most shields designed for connect with any device.

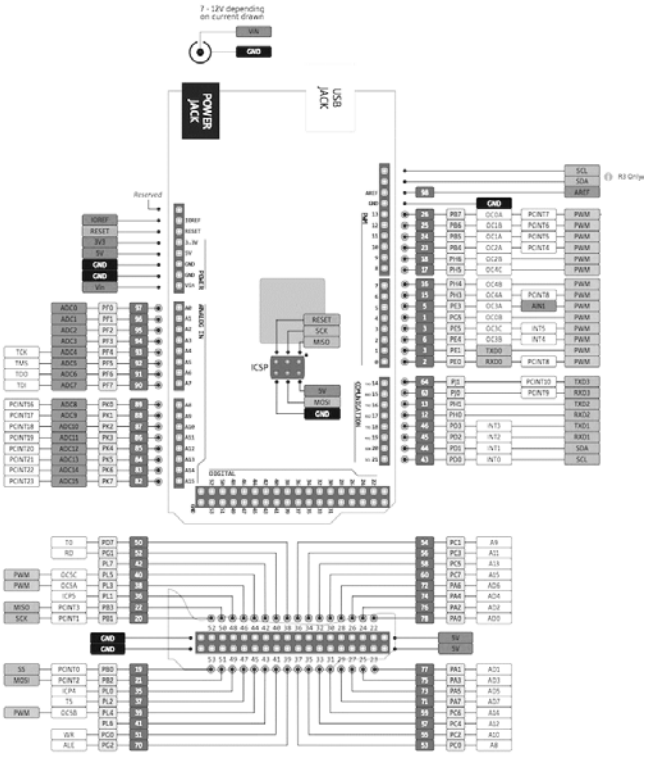


Figure [2.1]: Block diagram of Arduino

2.2.2 LCD

A Liquid crystal display is used to indicate the present status of parameters and the respective AC devises (simulated using bulbs). The information is displayed in two modes, which can be selected using a push button switch which toggles between the modes. Any display can be interfaced to the system with respective changes in driver circuitry and code.

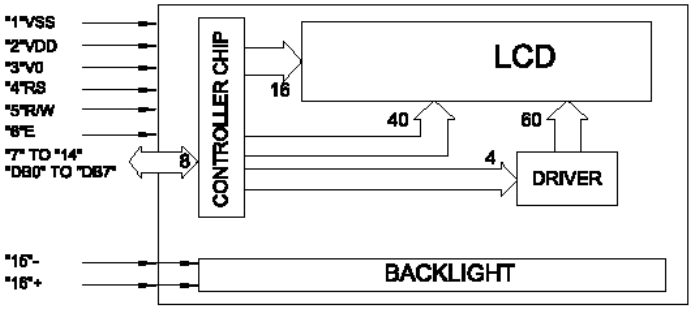


Figure [2.2]: Block diagram of LCD Module

2.2.3. Connecting wires

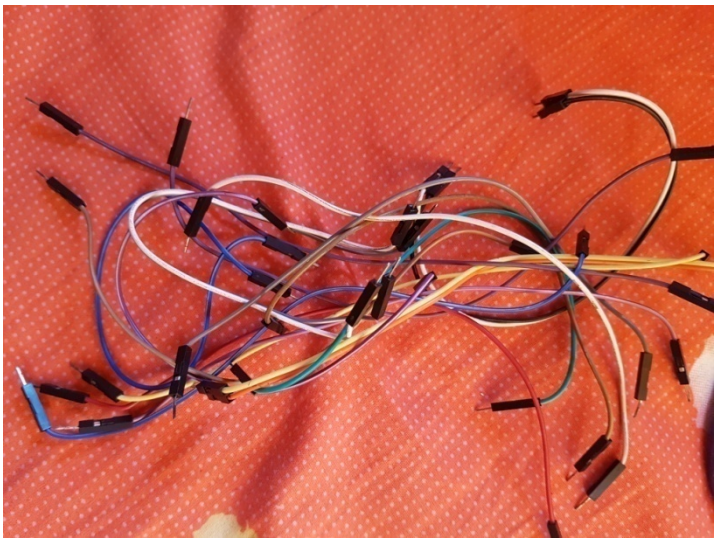


Figure [2.3]: Connecting wires.

2.3 Keypad System

A keypad is a set of buttons or keys bearing digits, symbols and/or alphabetical letters placed in order on a pad, which can be used as an efficient input device. A keypad may be purely numeric, as that found on a calculator or a digital door lock, or alphanumeric as those used on cellular phones. A keypad system is very vulnerable equipment, which can be used in many places effectively. Thus in a nutshell we can say that keypad system also helps a lot to secure the security systems.

Here are the advantages and disadvantages of using a digital door lock:

- **Advantages**

Pick-proof: Because there is no place for a key with these locks, that prevent lock breaking because burglars are unable to pick or ‘bump’ the lock. Criminal’s methods of breaking and entering are improving and the majority of criminals can pick an ordinary key lock.

NO MORE KEYS: Someone won't have to carry around a large set of keys and they will be less likely to be lost or stolen. Also, a landlord won't have to give residents keys or replace them if they lose them.

Control: In a company building, it can be controlled and restrict who goes into what part of the building. Also residents and landlords of apartments and flat can control who can enter their room with one PIN code and it reduces the risk of anything getting stolen. It is incredibly easy to change the PIN code whenever someone like. The combination door locks from the Workplace Depot have over 8,000 possible code combinations with a simple code change facility.

Aesthetically Pleasing: Door locks can come in a range of stylish colors that look smart and professional.

Perfect for the elderly or disabled: The extra investment into a door lock could bring massive advantages to those who are unable to get to the door quickly and/or who struggle with keys.

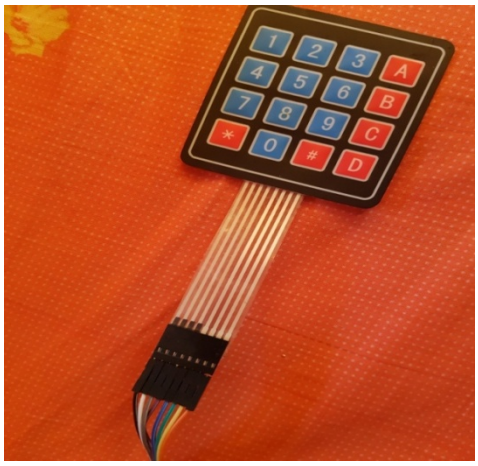
- ## Disadvantages

Forgetfulness: It is easy to forget PIN code for the lock and when someone is in a rush to get into the room or building or it is nighttime and dark, someone won't want to change the code in the middle of the night or when it's raining!

Power Failure: Some digital door locks are powered by electricity, if any house or building has a power failure, then the door lock will not work which restricts from entering the building.

Limit the PIN Code Length: Some digital door locks have a PIN code length up to 10 digits digital Door Locks will be much more secure if they are only 4 digits long.

In this project we used digital keypad

: 

Figure[2.4]: Keypad

Chapter 3: Sensors

3.1 Fingerprint (Biometric System)

Positive identification of individuals is crucial societal requirement. Until recently, automatic personal identification technologies followed two approaches:

i) A token based approach and

ii) A knowledge based approach.

Token-based approaches are based on identification using tokens such as a magnetic swipe card, key, driver's license, etc. knowledge-based approaches use passwords and personal identification numbers (PINs) to identify or validate a person's identify. Both these forms of identification are not secure, because this credential's can be lost, stolen or duplicated. On the other hand, biometrics is a science of verifying and establishing the identity of an individual through physiological features or behavioral characteristics that are unique to that individual and hence cannot be stolen, lost or misused. The word "Biometric" is derived from the Ancient Greek language where "Bio" means "life "and "Metric" means "To measure". All Biometric systems compare a biometric sample against a previously stored template to determine a level of similarity. Biometric identification works on the principle of a threshold. Because, it is nearly

impossible to capture the biometric the same way every time it is used for access. Therefore, the system cannot expect a 100% match. Instead, a threshold system is used that can be modified depending on the security level of the applications. If the score exceeds the threshold, the result is a match and if the score falls below the threshold, the result is non-match

Biometric characteristics can be divided in to two main classes, as represented in the following figure [3.1]

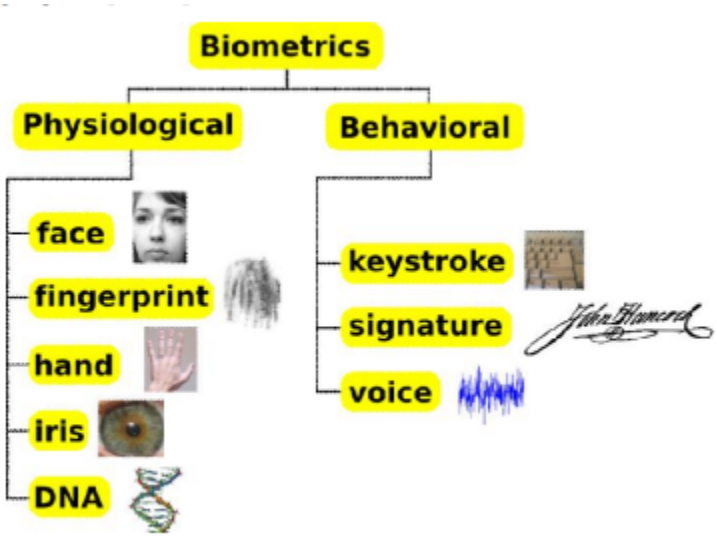


Fig 3.1: Classification of Biometrics

• **Physiological Biometrics**: These characteristics are related to the structure of the body, such as, Fingerprint, face, Irish, Hand geometry, DNA, etc.

• **Behavioral Biometrics**: These characteristics are related to the behavior of a person, such as, Handwriting, Voice, Gait, Signature, keystroke, etc.

Fingerprints are Good for use in Biometrics because there are many criteria that must be accounted before a physical or behavioral trait can be considered suitable for use in biometrics.

Perhaps the most important criteria are “Uniqueness” and “Permanence”. Fingerprints have been well proven on both counts.

• **Uniqueness**: Uniqueness of fingerprint is not an established fact but an empirical observation. Fingerprints have been routinely compared worldwide for more than

140 years. In that time, no two fingerprints on any two persons have been found to be identical. Even identical twins who shared same DNA structure have different finger prints; they tend to have fingerprints that are similar globally, i.e. have the same fingerprint classes (e.g.. whorl, loop, arch, etc) but ridge structures are very different. The true is also holds for the right and left finger and can be anticipated for clones.

• **Permanence**: Fingerprints are fully formed at about seven months of fetus development and finger ridge configuration do not change throughout the life of an individual except due to accidents such as bruises and deep physical injuries. They simply expand proportionately in all directions as we grow, means fingerprints maintains a proportional scale for its entire existence. The other advantages of fingerprints as a biometric are stated bellow:

• **High Universality**: Within human population every individual has fingerprint which can be easily used for their authentication.

• **High Indispensability**: Like token-based authentications fingerprints for human identification do not lead problems of being stolen or lost. On the other hand fingerprints would never be forgotten like PINs, password, or other knowledge-based systems. Actually in most cases, fingerprints would accompany the individual throughout his/her life time unless there is some serious injury to their fingers.

• **High Collectability**: Fingerprints can be easily collected compared to other biometric samples, such as Retina, DNA, Irish, etc. which require complete cooperation and high cost special equipment to acquire the biometric samples. On the other hand the process of fingerprint acquiring requires minimal or no user training and can be collected easily from both cooperative and non-cooperative users.

• **Good Storability**: The database of fingerprints does not require huge space; it depends on the representation of the templates that can be chosen for the system. Depending on the application and way of representation the size of these templates can be from 52 bytes to several megabytes.

• **High Performance**: Fingerprints remain one of the most accurate biometric modalities considering both False Accept Rate (FAR) and False Reject Rate (FRR).

• **Wide Acceptability**: Since the beginning of the twentieth century, fingerprints have been formally accepted as valid personal identification trait and have become a standard routine in forensics.

3.1.1. INTRODUCTION to FINGERPRINT

A fingerprint is an impression of the friction ridges found on the inner surface of a finger or thumb. Fig [3.2.] Finger skin is made of friction ridges, with pores (sweat glands). Friction ridges are created during fetal live and only the general shape is genetically defined.

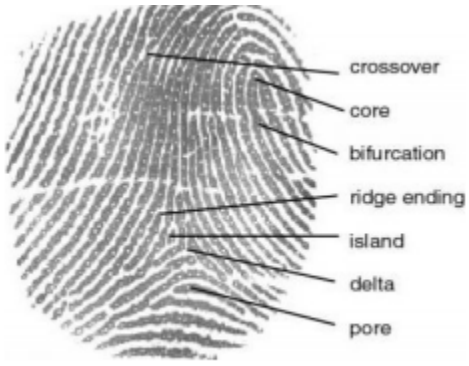


Figure3.2: A fingerprint image labeled with different components.

A fingerprint is composed of different types of components . Those are stated bellow-

• **Ridges**: The lines that flow in various patterns across fingerprints are called ‘Ridges’.

• **Furrows:** The spaces between ridges are called ‘Furrows’ or ‘valleys’. It dos not make contact with a surface under normal touch.

• **Termination**: The point on a fingerprint that a friction ridge begins or ends without splitting into two or more continuing ridges or it is the immediate ending of a ridge, at which a ridge terminates.

• **Bifurcation**: It is the point on the ridge from which two branches derive. Bifurcation is also known as 'Ridge Branch'.

• Dots: They are very small ridges.

• **Islands**: Ridges those are slightly longer than dots, occupying a middle space between two temporarily divergent ridges.

• Ponds or lakes: A notch protruding from a ridge.

• **Bridges**: Small ridges joining two longer adjacent ridges.

• **Crossover**: Two ridges which crosses each other.

• **Core**: The core is the inner point, normally in the middle of the print, around which swirls, loops, and arches center.

• **Delta**: Deltas are the points, normally at the lower left or right hand of the fingerprint, at which a triangular series of ridges center. However, shown by intensive research on fingerprint recognition fingerprints are distinguished by 'MINUTIA', which are some abnormal points or the discontinuities of the ridges. There are among 150 different types of minutiae categorized based on their configuration. [Fig3.3]

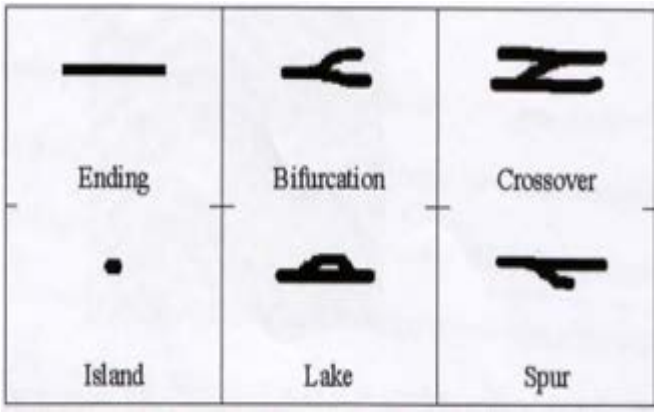
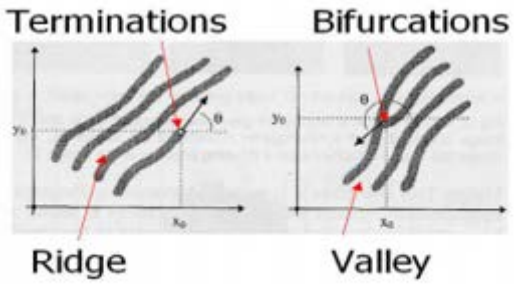


Figure [3.3]: Some of the common minutiae types

Among these minutia types ‘Termination or Ridge Ending’ and ‘Bifurcation’ are mostly significant and have heavy usage [Fig: 3.4]. There are features that can be used for matching such as core, delta, pores but they are not available on all fingerprints beside requires higher resolution scanner and very good image quality. Whereas, minutia is relatively stable and robust to contrast, image resolutions and global distortion compared to other representations. However, to extract the minutia from a poor quality image is not an easy task.



Figure[3.4]: Minutia: Termination and Bifurcation

3.1.2 Fingerprint Patterns:

The ridge flow constitutes a global pattern of the fingerprint and based on the structure of ridges the fingerprints can be categorized in three patterns i) Arch, ii) Loop and iii) Whorl. [Fig1.3.1] Different classification schemes can use up to ten or so pattern classes, but these three are the basic patterns.

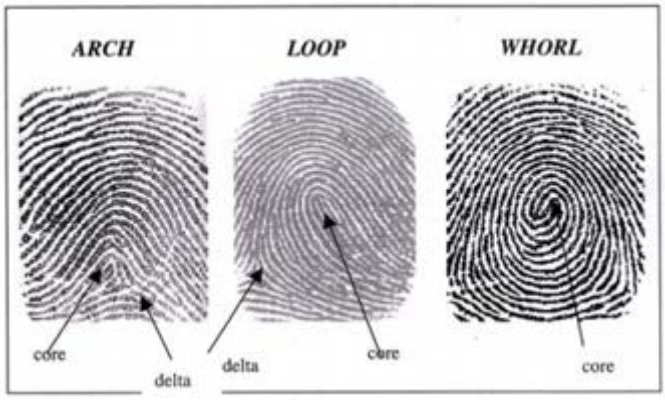


Figure [3.5]: Fingerprint Patterns: Arch, Loop, Whorl.

3.1.3. Fingerprint Recognition

The fingerprint recognition problem can be separated in to two categories:

i) Fingerprint Verification

ii) ii) Fingerprint Identification.

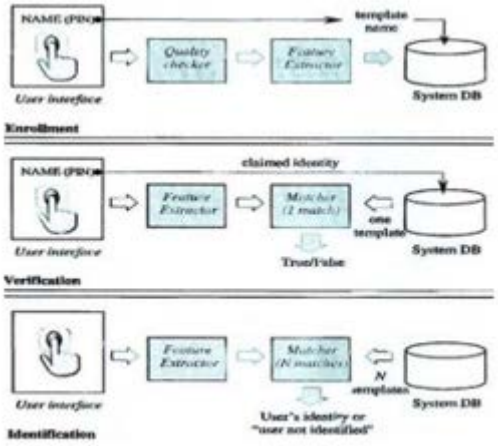


Figure [3.5]: Block diagram of enrollment, verification and identification tasks.

• Fingerprint Verification:

It is the comparison of a claimant fingerprint against an enrollee fingerprint, where the intention is that the claimant fingerprint matches the enrollee fingerprint. A verification system either rejects or accepts the submitted claim or identity (Am I whom I claim I am?) .To prepare for verification, a person initially enrolls his or her fingerprint into the verification system. A representation of that fingerprint is stored in some compressed format along with the person's name or other identity. Subsequently, each access is authenticated by the person identifying him or herself, then applying the fingerprint to the system such that the identity can be verified. Verification is also termed 'one-to-one matching'. It is suitable for used in civilian applications like, PC access, credit cards, personal identification, etc.[1][3][6]

• Fingerprint Identification: Fingerprint Identification is to specify one person's identity by his fingerprint. (Who am I?). Without any information of the person's identity, the fingerprint

Identification system tries to match his fingerprint with those in the whole fingerprint database. It is especially useful for criminal investigation cases. Identification is also termed as ‘one-to-many matching’. There is an informal third type of matching that is termed ‘one-to-few matching’. This is for the practical application where a few users use a fingerprint system, such as by family members to enter their house. A number that constitutes ‘few’ is usually accepted to be somewhere between 5 and 20. However, all fingerprint recognition problems are ultimately based on a well representation of a ‘one-to-one matching’. As long as the representation of fingerprints remains the uniqueness and keeps simple, the fingerprint matching is straightforward and easy.

- **Scheme to avoid False Rejection in a Fingerprint Authentication System**

The finger should be clean that means free of sticky residue and greases and depending on the sensor should not be too damp or too dry. The finger should always be applied on the sensor in the same manner (same position and direction) and with uniform pressure (e.g., avoid pressuring while twisting)

- **Effect of wounds affect Fingerprint Recognition**

If a wound is not too deep, the finger lines will fully regenerate to their original state. Deep cuts leave line-forming scars and should be recognized as such by good identification algorithms, thereby barely impairing the identification performance. Most system offers the possibility to record a ‘Substitute Finger’ in enrollment, so that a fingerprint authentication can still take place during healing process. In our project we have used **FBM10** as fingerprint scanner.

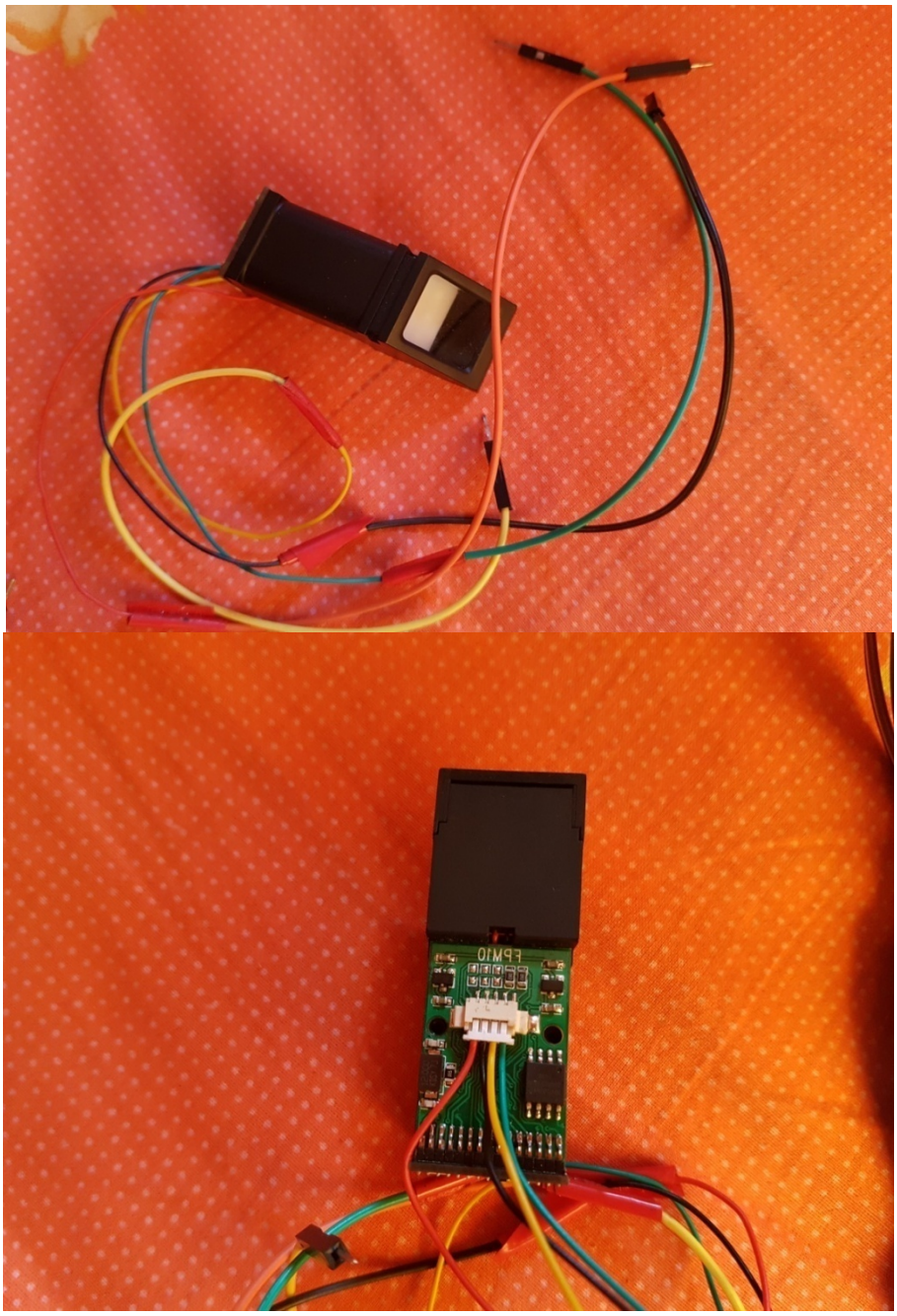


Figure [3.6]: Fingerprint scanner.

3.2 RFID

Radio Frequency Identification (RFID), one member in the family of Automatic Identification and Data Capture (AIDC) technologies, used to describe a system that transmits the identity of an object or people wirelessly without physical contact by radio waves.

There are two components to any RFID system: a transponder called a “Tag”, and an interrogator called a “Reader”. Tags are the antenna enables the chip to transmit the identification information to a reader. With this in mind, each tag carries a unique identification number; which is programmed at the time of manufacturing to ensure the object can carries a distinctive identity and description. Readers are a component to scan the tags for their data, and a series of integration technologies that link the readers back to central systems that track the data being scanned.

3.2.1 History of RFID

RFID technology was invented in 1945, but it was not mainstreamed for commercial applications until the 1980s.

The first similar RFID tag invention was invented in 1945 by Leon Theremin, which the Soviet Union used as an espionage tool, not a RFID tag or chip, but it is accredited to being the technology that was used to develop the current RFID tags or chips.

More relevant technology was during Second World War, called IFF (Identification Friend or Foe), which used by the British in the World War II for the detection of airplanes of both friends and enemies.

In 1973, Mario Cardullo holds the patent for a passive radio transponder with memory- the modern RFID that uses radio waves to collect information from the memory.

In 1987, the first RFID road toll collection implemented in Norway.

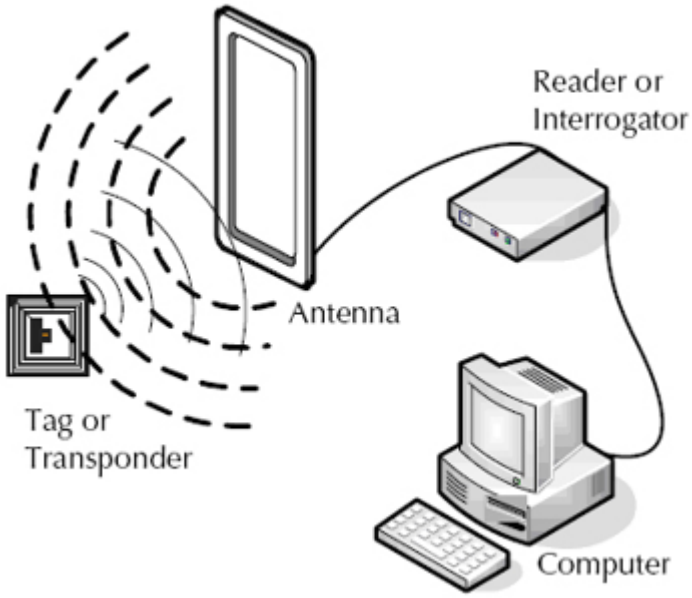
Soon this technology began to invade everything. Nowadays, RFID is used in many applications: identification of all sorts of products, banking (VISA card…), security (E-seal and RFID system for custom, Boiler and equipment monitoring system, fireworks management, logistics management, security system for sections…), personnel identification, medical identification and wine identification.

3.2.2 RFID Theory

The RFID system typically consists of a tag made up of a microchip with an antenna, and an interrogator (reader), which is embedded with a single chip processor and an antenna.

The purpose of an RFID system is to enable data to be transmitted by a tag, which is read by an RFID reader and processed according to the needs of an application. Moreover, the data transmitted by the tag may provide identification or location information, or specifics about the product, for example, price, color, date code, etc. Also, RFID systems can be employed for tracking objects- as an invasion of privacy.

In short, RFID tags can carry data and serve as data transfer agents; a reader in range of the tag’s signal will receive the data, decrypt it, and forward it to the host computer for stores all collected data within a database.



Figure[3.6]: The process of RFID systems.

3.2.3 Types of RFID Tags

Generally, there are two types of RFID tag: active and passive.

- **Active RFID Tags**

Active RFID tags contain an internal power source (battery) to transmit signal to reader. Active tags have greater communication distance and larger memory capacity then Passive RFID tags.

According to own power source, active RFID tags of a range of up to 1,500 feet and have a battery life of up to 10 years. The advantages of active tags are reliability, precision, and superior performance in adverse environments, like metallic and so on.

- **Passive RFID Tags**

  Passive RFID tags have no internal power supply. These passive tags are powered by an incoming radio frequency, which is received through the tag's internal antenna. So, passive tags are read at a relatively short range from a distance of ten millimeters to over six meters away.

  At present, these tags are enough to relay simple information, like number or name. The size of passive tags is small and thin. And, it is the lowest price of RFID tag.

3.2.4 RFID Reader

Basic function of the RFID reader is to converse with the RFID tag by originating radio waves from its antenna.

The RFID readers are classified on their variety, such as Microwave frequency, UHF (Ultra-high frequency), HF (High frequency) and LF (Low frequency) that are 5.8 GHz to 125 KHz. There costs are also reliant on their range; Microwave frequency readers are costliest, LF readers are the cheapest.

Mainly, there are two types of RFID reader: handhold and fixed.

- **Handhold Type Reader**

  The Handheld reader fits comfortably in the palm of our hand. Users carry this portable Reader while looking for specific items such as merchandise, inventory, or other assets.

  The Handheld reader not only can be used to manually scan but also program individual tags. Instead of reading all tags in an area at one time, users can selectively read and program only particular items.

- **Fixed Type Reader**

  The fixed reader is an RFID interrogator mounted to a permanent or non-mobile structure enabling users to read RFID tag numbers attached to movable items.

3.2.5 Classification of RFID Frequency

Different frequencies have different characteristics that make them more effective for different applications.
There are four commonly used frequencies:

- **Low frequency**

  This Low frequency (LF) RFID operates at less in 125 to 134.2 KHz frequency; as well its read range is limited to less than a foot (0.33 meter). This frequency is typically used for short-range RFID applications, for example, Access control. Besides, the LF tags use less power too.

- **High frequency**

  This High frequency (HF) RFID operates at round 1-400 MHz. The common specification is 13.56 MHz frequency, and its read range is longer than LF, generally 6-12 inches (medium read range). This kind of HF RFID tags are best suited for applications and often used in manufacturing processes and tracking and so on. For instance, library book tracking, Smart Cards.

- **Ultra-high frequency**

  This Ultra-high frequency (UHF) RFID operates at round 860 MHz to 960 MHz frequency and can read at long distances, up to 15 feet. This UHF RFID tags are mainly used for tracking cases and pallets. They can offer better range and can transfer information faster and farther than LF and HF RFID tags. But radio wave cannot pass through metallic and liquid items.

- **Microwave frequency**

  This Microwave frequency RFID operates at round between 1 to 5.8 GHz, and can used for long distance.

3.2.6 RFID Applications

RFID has applications in various industries. RFID applications help in tracking products in the supply chain and during the manufacturing process. Different kinds of frequency RFID tags have different applications. Such as, LF (Low frequency) RFID tags are model for scanning objects at close range. UHF (Ultra-high frequency) RFID tags are best for scanning boxes of goods, and so on.

Some applications can be summarized as follows.

- Supply chain automation
- Warehouse control system
- Retail control system
- Manufacturing
- Industrial automation
- Custom management
- Asset management
- Security systems
- Medical applications
- People tracking
- Location control
- Logistics management
- Passenger and transportation management
- Animal Identification
- Container control (E-seal…)
- Harbor container management system

- Boiler and equipment monitoring system
- Automatic monitoring management system
- Timing

The above list is only small representation of RFID applications in the RFID market. RFID applications are still being developed and improved as the technology advances.

Moreover, the RFID technology is advancing day-by-day and researches are on to help reduce the cost that can lead to easy availability of the RFID services. Thousands of worldwide companies have renovated to RFID systems to improve efficiency in production and security features.

3.2.7 Benefits and Characteristics of RFID

Nowadays, RFID is already having a significant impact on many businesses. RFID can deliver benefits in many areas from tracking work in progress to speeding up throughput in a warehouse and so on.

Here is the list of RFID benefits and features.

- RFID (Tag) can be read from a distance and from any orientation
- RFID(Tag) do not require line of sight to read
- RFID (Tag) have both read and write capabilities
- RFID (Tag) Can provide large amounts of data
- RFID (Tag) can be embedded easily into different objects
- RFID (Tag) can read at rapid rates- at a speed of up to 1,000 tags per second
- RFID (Tag) can be read in harsh environments where operating temperatures range from 22 degree Fahrenheit to +159 degree Fahrenheit
- RFID (Tag) is costly but efficient
- RFID (Tag) do not get damaged easily
- RFID system offers permanent identification- tags encrypt information with unique identification

- RFID reduces administrative error, labor costs associated with scanning, reading and shipping
- RFID improves businesses and guarantee traceability
- RFID can help to improve the forecasting

3.2.8 Problems with RFID

RFID technology has a lot of benefits, but it also has several drawbacks that have limited its adoption on a more widespread scale.
There are some problems with RFID:

About privacy problem, RFID tags can be read without the knowledge and agreement of authorized user.
Because of the tags can be read without obviously scanned, anyone with an RFID tag reader can read the tags embedded in our belongings without our agreement.

About security problem, RFID tags are difficult to for consumers to remove: some are tiny; others may be embedded inside a product where consumers cannot notice it.

About standard problem, different manufacturers have manufactured RFID in different ways: this issue may be cause problems for companies.

About interference problem, RFID systems can be easily disrupted: the electromagnetic spectrum is easy to jam at the right frequency, and active RFID tags can be repeatedly disrupted to wear the battery down.

About reader collision problem, RFID reader collision occurs when the signals from two or more readers overlap: the tag is unable to respond to simultaneous queries.

About tag collision problem, RFID tag collision occurs when many tags in a small area meanwhile: it is easier for vendors to develop systems to respond one at a time.

In this project we used RFID reader and tag(RC522):

Figure [3.7]: RFID

CHAPTER 4: BLUETOOTH SYSTEMS

4.1 Bluetooth device:

HC-05 module is an easy to use Bluetooth SPP (Serial Port Protocol) module, designed for transparent wireless serial connection setup.

Serial port Bluetooth module is fully qualified Bluetooth V2.0+EDR (Enhanced Data Rate) 3Mbps Modulation with complete 2.4GHz radio transceiver and baseband. It uses CSR Bluecore 04-External single chip Bluetooth system with CMOS technology and with AFH(Adaptive Frequency Hopping Feature). It has the footprint as small as 12.7mmx27mm. Hope it will simplify our overall design/development cycle.

Hardware Features

- Typical -80dBm sensitivity
- Up to +4dBm RF transmit power
- Low Power 1.8V Operation ,1.8 to 3.6V I/O
- PIO control
- UART interface with programmable baud rate
- With integrated antenna
- With edge connector

Software Features

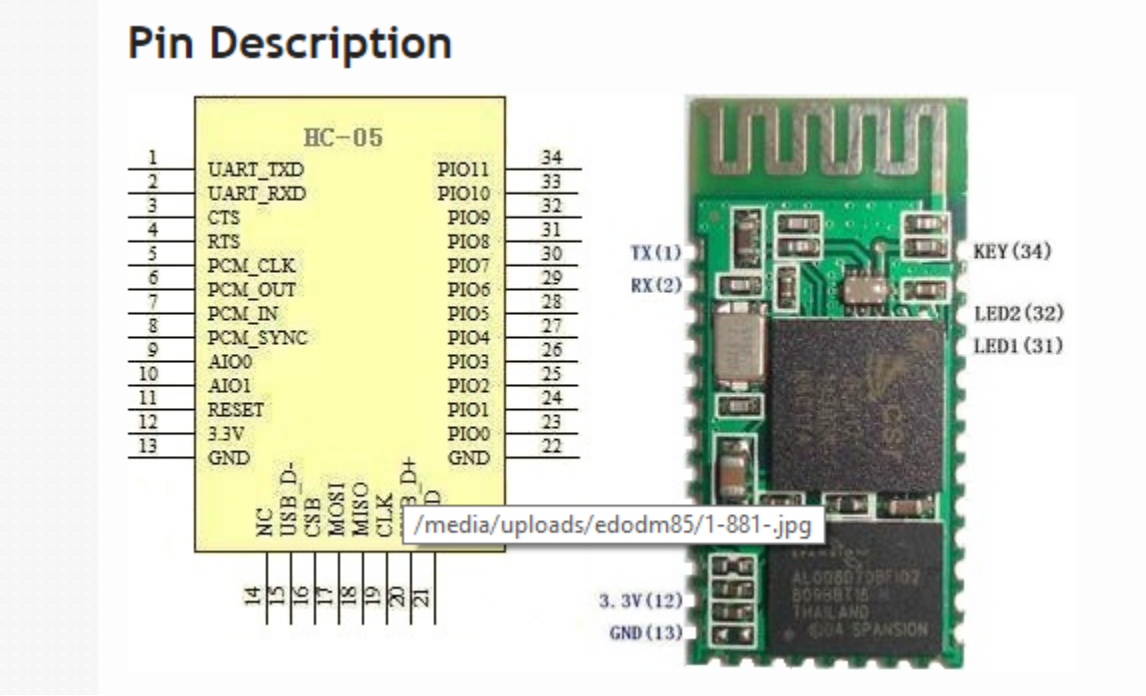
- Default Baud rate: 38400, Data bits:8, Stop bit:1,Parity:No parity, Data control: has.

Supported baud rate: 9600,19200,38400,57600,115200,230400,460800.

- Given a rising pulse in PIO0, device will be disconnected.
- Status instruction port PIO1: low-disconnected, high-connected;
- PIO10 and PIO11 can be connected to red and blue led separately. When master and slave

are paired, red and blue led blinks 1time/2s in interval, while disconnected only blue led blinks 2times/s.

- Auto-connect to the last device on power as default.
- Permit pairing device to connect as default.
- Auto-pairing PINCODE:”0000” as default
- Auto-reconnect in 30 min when disconnected as a result of beyond the range of connection.



4.2 Device work process:

At first the device will initialize all its components (counter,timer, LCD, RFID,fingerprint sensor etc.). Then the system will search for fingerprint if it get the fingerprint matched then it will search for rfid ,if it is match then it will go for keypad ,as the keypad is the most secured part that's why it is placed at the last part. If everything is correct then the door or the lock will be opened. On the other hand if an user put a wrong fingerprint or any of these wrong input then the device will automatically connect to the bluetooth of the android device and it will take a picture.

PIN configuration of the device:

LCD to ARDUINO:

LCD		ARD 1
VSS		GND
VDD		5V
RS		POT
RW		12
E		GND
D4		11
D5		6
D		4
D7		3
A		2
K		5V
		GND

RFID to ARDUINO 1:

RFID		ARD 1
SDA		53
SCK		52
MOSI		51
MISO		50
RQ		
GND		GND
RST		5
3.3V		3.3N

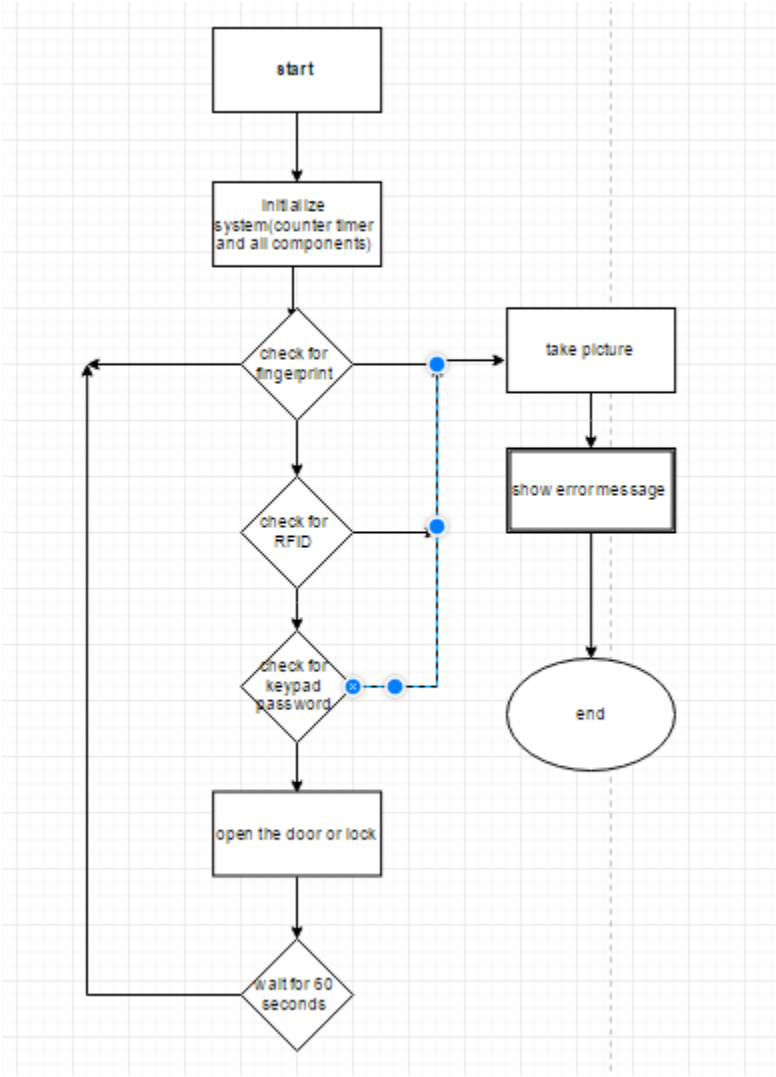
FINGERPRINT to ARDUINO 2:

FINGERPRINT		ARD 2
GND		GND
5V		5V
3		50
4		52

BLUETOOTH to ARDUINO 2:

BLUETOOTH		ARD 2
GND		GND
5V		5V
TX		1
RX		7

4.3 FLOW CHART OF OUR DEVICE:



Chapter 5: Conclusion and Future work

Security is an integral part of our life, be it personal or providing it for our belongings. Constant technological advancements have been made in the field of developing security systems over the past few years. 'Radio frequency identification' (RFID), fingerprint, keypad and a Bluetooth camera. These has been used widely for database management in places like malls and office areas. Our project is the first of its kind, which brings together these popularly, used systems in developing a three level security system. To give a complete overview of our project, the individual needs to have the pre-defined card, an RFID tag. Thus there are three levels of security for the secured place. It is a great pleasure that we have successfully completed our project, which we had proposed before. We have made this project keeping in mind that our country needs such security system, which can be cheap and effective, and thus coming out with such a solution is very much required for the betterment of our country.

This security system can be used in banks and internal secured offices where security is very much required. Our main objective was to provide a secure system as we have used multilayer so it works logically, when one wants to use a locker they will have to pass three layers of security, and this is very rare in our country. We mainly want to provide our security system as a versatile project, which can be used in many sectors.

Thus our main goal was to provide the small companies of our country who cannot use security system due to cost factor, as our project is very chap and secure.

Future work of our paper is planned to a developed security system based on iris scanner for visual identification of the person, and also using motion sensor in the device, which will detect unwanted movement. Finally we have proposed to create a central sever where the picture will be stored for reference.

APPENDIX

```
#include <Adafruit_Fingerprint.h>
#include <SoftwareSerial.h>
#include <Wire.h>

SoftwareSerialmySerial(52, 50);
Adafruit_Fingerprint finger = Adafruit_Fingerprint(&mySerial);
void setup(){
Serial.begin(9600);
Wire.begin();
while (!Serial);

  // set the data rate for the sensor serial port
finger.begin(57600);

  //outputStream.begin(9600);
}
void loop(){
getFingerprintID();
delay(50);
}
uint8_tgetFingerprintID() {
uint8_t p = finger.getImage();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image taken");
break;
case FINGERPRINT_NOFINGER:
Serial.println("No finger detected");
return p;
```

```
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_IMAGEFAIL:
Serial.println("Imaging error");
return p;
default:
Serial.println("Unknown error");
return p;
  }
  // OK success!
p = finger.image2Tz();
switch (p) {
case FINGERPRINT_OK:
Serial.println("Image converted");
break;
case FINGERPRINT_IMAGEMESS:
Serial.println("Image too messy");
return p;
case FINGERPRINT_PACKETRECIEVEERR:
Serial.println("Communication error");
return p;
case FINGERPRINT_FEATUREFAIL:
Serial.println("Could not find fingerprint features");
return p;
case FINGERPRINT_INVALIDIMAGE:
Serial.println("Could not find fingerprint features");
return p;
default:
Serial.println("Unknown error");
return p;
```

```
  }
  // OK converted!
  p = finger.fingerFastSearch();
if (p == FINGERPRINT_OK) {
Serial.println("Found a print match!");
Wire.beginTransmission(9);
Wire.write(1);
Wire.flush();
Wire.endTransmission();
  } else if (p == FINGERPRINT_PACKETRECIEVEERR) {
Serial.println("Communication error");
return p;
  } else if (p == FINGERPRINT_NOTFOUND) {
Serial.println("Did not find a match");
Wire.beginTransmission(9);
Wire.write(2);
Wire.flush();
Wire.endTransmission();
return p;
  } else {
Serial.println("Unknown error");
return p;
  }

  // found a match!
Serial.print("Found ID #"); Serial.print(finger.fingerID);
Serial.print(" with confidence of "); Serial.println(finger.confidence);
}
#include <SPI.h>
#include <MFRC522.h>
```

```
#define RST_PIN         5
#define SS_PIN          53
MFRC522 mfrc522(SS_PIN, RST_PIN);

/*
* ---------------------------------------------------------------------------------------
 *           MFRC522      ArduinoArduinoArduinoArduinoArduino
 *           Reader/PCD   Uno          Mega      Nano v3    Leonardo/Micro   Pro Micro
 * Signal      Pin          PinPinPinPinPin
 * ---------------------------------------------------------------------------------------
 * RST/Reset   RST          9            5         D9         RESET/ICSP-5     RST
 * SPI SS      SDA(SS)      10           53        D10        10               10
 * SPI MOSI    MOSI         11 / ICSP-4  51        D11        ICSP-4           16
 * SPI MISO    MISO         12 / ICSP-1  50        D12        ICSP-1           14
 * SPI SCK     SCK          13 / ICSP-3  52        D13        ICSP-3           15
 *
 */
void setup(){
Serial.begin(9600);
SPI.begin();                    // Init SPI bus
  mfrc522.PCD_Init();           // Init MFRC522
}
void loop(){
if (  mfrc522.PICC_IsNewCardPresent()) {
Serial.println("Password Accepted");
 }
}
```

REFERENCE

1. Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. jain, Salil Prabhakar.

2. http://en.wikipedia.org/wiki/Biometrics

3. http://pagesperso-orange.fr/fingerchip/biometrics/types/fingerprint.htm

4. http://www.robotshop.com/media/files/pdf/ -sensor-sen92355p.pdf.

5. http://playground.arduino.cc/Learning/PRFID

6. http://bildr.org/2011/02/rfid-arduino

7. “Microcontroller”. Wikipedia.<2012 wikipedia, The Free Encyclopaedia 26 Nov 2012 http://www.wikipedia.org/microcontroller.html>.

8. https://en.wikipedia.org/wiki/Bluetooth