



TRI LAYERED SECURITY IMPLEMENTATION IN BANK LOCKER

**Mrs. K. SARADA¹, O. BHARGAVI², K. K. HARSHINI³,
M. RAJESH⁴, P. AKASH⁵**

¹ ASSISTANT PROFESSOR, Dept of Electronics & Communication Engineering,
Tirumala Engineering College,

^{2, 3, 4, 5} UG STUDENTS, Dept of Electronics & Communication Engineering,
Tirumala Engineering College.

Abstract -

The main aim of the project is development of a system with high level security for restricted areas with the help of fingerprint detection, OTP, Password. Fingerprint recognition technology allows access to only those whose fingerprints that are pre stored in the memory. Stored fingerprints are retained even in the event of complete power failure or battery drain. These eliminates the need for keeping track of keys or remembering a combination password, or PIN. It can only be opened when an authorized user is present, since there are no keys or combinations to be copied or stolen, or locks that can be picked. The fingerprint-based lock therefore provides a wonderful solution to conventionally encountered inconveniences. This report focuses on the use of fingerprints to unlock locks, as opposed to the established method of using keys. Here we are using RFID for recognition of authorized persons. GSM module will be generate the different OTP for every person.

Keywords— RFID CARDS, GSM, DC MOTOR

I INTRODUCTION

Theft is one of the major problem in today's world places like in offices and other public places should not be secured so that issues to make secure our documents and precious things so we have decided to make this type of security system that will be more usable to all the people . This system assures the perfect use on the fingerprints for door opening and closing. Through the project we can provide high security to users. The fingerprint most of the banks have lockers such that one key is with the user and the bank has a master key. They also have password which the user has to tell the bank before going in the locker room, now if the user loses the key then, it is a big security risk. there are many thieves around us that they can easily or forcefully break our lockers so we can lost our property so to overcome this problem we are creating this type of security system Many of the bank lockers do not



guarantee full safety of the user. In the fingerprint bank locker system we can easily add more than 1 fingerprint in the system so we can add our family member fingerprint as a nominee. And we can insert our multi hand fingerprint if we are facing accident and if we wound or a cut in our finger so we can use our nominee fingerprint or other multi hand fingerprint. If we are away from our house and we required urgent document or property so our family members can also use our lockers. This is a very unique idea instead to keep keys or to protect that keys. Biometric devices are highly secured security identification and authentication device. Such devices use automated methods of verifying and recognising the identity of a living person based on a physiological behavioural characteristic. These characteristics include fingerprints, facial images, iris and voice recognition.

II EXISTING METHODS

A. *Design and Implementation of a Fingerprint Based Lock System for Shared Access*

Nowadays office/corporate territory security is a

vital problem faced by everyone when far from home or at the home. When it comes to the security systems, it is one of the key worries in this occupied-merciless world, where people cannot get ways to provide security to their important possessions manually. Instead, they find a different solution that provides better, dependable and atomized security. This is a time, where everything is attached through network, where anyone can get hands on information from any place around the globe. Thus possibilities of one's information being hacked are a serious affair. Due to these chances, it's very crucial to have some kind of personal recognition to enter one's own info.

B. *Arduino Based Smart Fingerprint Authentication System*

In today's world Home, offices, shops, banks need excessive security measure for safety motive. To supply security for these areas, smart lock system is initiated. There are numerous innovational smart doorlocks are created to lock and unlock the system. This type of locks has fingerprint, RFID card, pin, password or IOT by unlocking the system using mobile phone. User using these kinds of bolting system either utilize pin number or fingerprint or RFID card to unlock the system. These system does not have security pecking order to grow the security.

C. *A smart door access system using finger print biometric system.*

In this paper a survey is done to provide high security for such high end security applications. The aim of this study is to design a smart door access system using finger print module. Both hardware and software technology are used to design it. An emergency beep sound is provided to protect the system by giving alarm if any unauthorised person intrudes into the system. An indicator indicates for any emergency condition. In this paper author used the finger print sensor, R305 uses unique biological



features to take images and can store up to 128 images which reduces fraud and saves time. This device provides better security by raising alarm and indication for an emergency condition. This system can be installed in defence offices, intensive care units (ICUs), child care units (CCUs) and research laboratories, etc When matching user enters the finger through optical sensor and system will generate a template of the finger image and compare it with templates present in the finger library.

D . On securing a door with finger print biometric technique.

In this paper, the project was constructed done in three different stages, the writing of the code (driver) which controls the Microcontroller using C language, the implementation of the whole project on a solder-less experiment board, the soldering of the circuits on Vero-boards and the coupling of the entire project to the casing. The implementation of this project was done on the breadboard as a prototype, the power supply was first derived from a bench power supply in the electronics laboratory, in all the development guaranteed security for illegal intrusion of illegal entity to room, the mechanism can be implemented in a broader sense on a door where a there is restriction of access.

E . Implementation of biometric security in a smartphone based domotic.

In this paper a cost effective Home Automation System which is secured by a biometric system is proposed. The circuit design, simulation and experimental analysis of the proposed system are discussed. This work proposes a home automation system in which the home appliances can be controlled remotely using the Bluetooth technology through an android app. A fingerprint based biometric system is also employed for providing robust security to the home. This security system provides only authentic access to the door lock of the home as well as the automation circuitry.

III COMPONENTS REQUIRED

- A. *RFID Cards*
- B. *Relay board*
- C. *GSM Module*
- D. *Buzzer*
- E. *Arduino IDE (Software)*
- A. *RFID CARD*

An optical fingerprint scanner works based on the principle of Total Internal Reflection (TIR). In an optical fingerprint scanner, a glass prism is used to facilitate TIR. Light from an LED (usually blue color) is allowed to enter through one face of the prism at a certain angle for the TIR to occur. The reflected light exits the prism through the other face where a lens and an image sensor (essentially camera) are placed. When there's no finger on the prism, the light will be completely reflected off from



the surface, producing a plain image in the image sensor. When TIR occurs, a small amount of light leaked to the external medium and it is called the Evanescent Wave. Materials with different refractive indexes (RI) interact with the evanescent wave differently. When we touch a glass surface, only the ridges make good contact with it. The valleys remain separated from the surface by air packets. Our skin and air have different RIs and thus affect the evanescent field differently. This effect is called Frustrated Total Internal Reflection (FTIR). This effect alters the intensities of the internally reflected light and is detected by the image sensor. The image sensor data is processed to produce a high contrast image which will be the digital version of the fingerprint. The first step is to collect the finger print by using a special or different sensing device. This process is referred to as enrolment. In this step, the finger print is taken for confirmation or authentication. The images we have captured which is called the finger print template can be save directly as an image or it can be save as a biometric algorithm. In this biometric algorithm, various data points on the finger print template are clearly studied and stored, as a result of that the leading to discarding of the real finger print.



Fig.1 FINGERPRINT MODULE

B. Relay board

A relay is an electromagnetic switching device consisting of an armature which is moved by an electromagnet to operate one or more switch contacts. Some advantages of relays are that they provide amplification and isolation and are straight forward. Here we are using 5v 4- channel relay interface board, and each channel needs a 15-20mA driver current. it can be used to control various appliances and equipment with large current relays that work under AC250V 10A or DC30V 10A. it has a standard interface that can be controlled directly by microcontroller.



Fig.2 Relay Board

C. Buzzer

Basically, the sound source of a piezoelectric sound component is a piezoelectric diaphragm. A piezoelectric diaphragm consists of a piezoelectric ceramic plate which has electrodes on both sides and a metal plate (brass or stainless steel, etc.). A piezoelectric ceramic plate is attached to a metal plate with adhesives. Applying D.C. voltage between electrodes of a piezoelectric diaphragm causes mechanical distortion due to the piezoelectric effect. For a misshaped piezoelectric element, the distortion of the piezoelectric element expands in a radial direction. And the piezoelectric diaphragm bends toward the direction. The metal plate bonded to the piezoelectric element does not expand. Conversely, when the piezoelectric element shrinks, the piezoelectric diaphragm bends in the direction. Thus, when AC voltage is applied across electrodes, the bending is repeated, producing sound waves in the air.



Fig 3. Buzzer

PROPOSED SYSTEM

The core section of the project; software part utilizes two different programs-enroll and fingerprint. Get Fingerprint Enroll, Adafruit Fingerprint and get Fingerprint Enroll are some of the different functions syntax used in those programs. These are in-built functions found in library and they pass arguments when these functions are called at different locations of programs. Once the enroll part of the program has been uploaded in the Arduino Uno, go through the Arduino IDE and then open the serial monitor by opening tabs like tools and then select serial monitor options. It is necessary to set the baud rate to a value lower than the serial monitor window to 38400. At the same time choose Newline option. And now, one by one execute the instructions given on the serial monitor. Once you place a finger on the fingerprint module, type an ID number. It can be any whole number. Then when send key is entered, the corresponding ID number is transmitted to the main portion i.e. Arduino Uno from the serial monitor section. Thus sent information (fingerprint) is digitized and converted into storable form which is piled up in R305 module database. This system can withstand a total of 200+ fingerprints which is remarkable. However, each fingerprint must have unique ID number assigned since this is the prime factor to be utilized in identification of the valid individual's name. The serial monitor assists the client in an effective way. Every real-time information of when to place the finger on the sensing module and



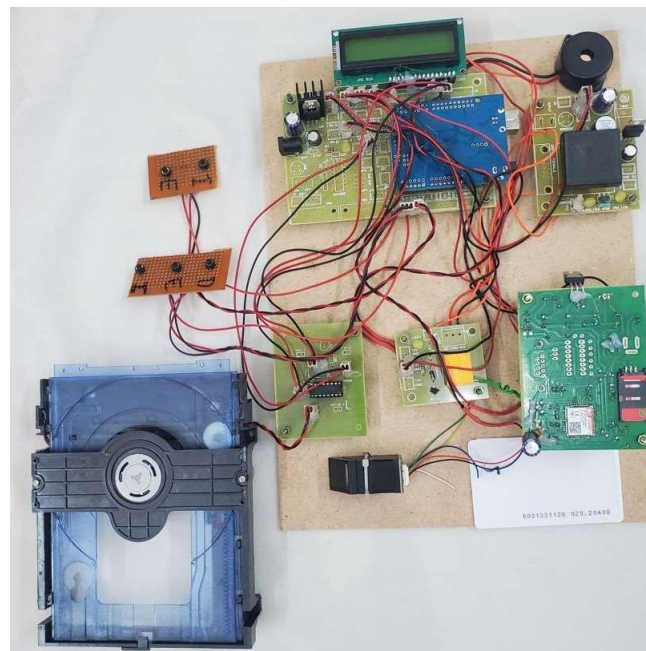
when it is okay to remove, is all provided by the serial monitor which makes this project more user-friendly. If you prefer to debug the system without implementing LCD display, initially upload the fingerprint program and then set the same settings as mentioned above for the serial monitor configuration. Here again the serial monitor performs the guide function. This technique of implementing circuit is employed to make necessary comparisons between the current sensed fingerprint sample with the samples already stored in the database.

WORKING

The first step is collecting the finger print using a special sensing device. This process is referred to as enrolment. In this step, the finger print is acquired for authentication. The captured image (called the finger print template) can be stored directly as an image or can be stored as a biometric algorithm. In the case of a biometric algorithm, several data points on the finger print template are scientifically measured and stored, thereby leading to discarding of the actual finger print. Algorithm software measures 40 or more data points for each finger print and may store these measurements as data coordinates or encrypt them into a digital certificate for future authentication. When the mathematical representation of the finger print, not the actual finger print, is used to prove identity, a higher level of reliability is realised (<http://biometr> The design of security door lock using the finger print technology was built around a Micro- Controller Unit (MCU), ARDUINO, which reads in finger prints from finger print scanner and grant access, to a protected compartment, only to pre-registered finger prints. The finger print scanner serves as the main input into this embedded security system. Finger prints read are compared to those ones pre-programmed into the memory of the microcontroller. When a match is made, the microcontroller outputs a HIGH which activates the transistor-relay switching stage that controls opening and closing of the modelled motorized door granting access into the protected building. An alphanumeric liquid crystal display (LCD) is used in this design to show the operating status of this embedded security system. By default it displays a welcome message requesting that the user should enter a finger print. And when a match is made it displays "ACCESS GRANTED" otherwise it displays "ACCESS DENIED". The design of security door lock using the finger print technology was built around a Micro- Controller Unit (MCU), ARDUINO, which reads in finger prints from finger print scanner and grant access, to a protected compartment, only to pre-registered finger prints. The finger print scanner serves as the main input into this embedded security system. Finger prints read are compared to those ones pre-programmed into the memory of the microcontroller. When a match is made, the microcontroller outputs a HIGH which activates the transistor relay switching stage that controls opening and closing of the modelled motorized door granting access into the protected building. An alphanumeric liquid crystal display (LCD) is used in this design to show the operating status of this

embedded security system. By default it displays a welcome message requesting that the user should enter a finger print. And when a match is made it displays “The design of security door lock using the finger print technology was built around a MicroController Unit (MCU), ARDUINO, which reads in finger prints from finger print scanner and grant access, to a protected compartment, only to pre-registered finger prints. The finger print scanner serves as the main input into this embedded security system. Finger prints read are compared to those ones pre-programmed into the memory of the microcontroller. When a match is made, the microcontroller outputs a HIGH which activates the transistor-relay switching stage that controls opening and closing of the modelled motorized door granting access into the protected building. An alphanumeric liquid crystal display (LCD) is used in this design to show the operating status of this embedded security system. By default it displays a welcome message requesting that the user should enter a finger print. And when a match is made it displays “ACCESS GRANTED” otherwise it displays “ACCESS.

RESULT



A three-layered security system for bank lockers, utilizing fingerprint recognition, one-time passwords (OTP), and a password, offers an exceptionally strong defense against unauthorized access. Fingerprint scanners provide a highly secure biometric verification method, as fingerprints are unique to each individual. This significantly reduces the risk of someone replicating a key or compromising a simple password. Furthermore, OTPs add a dynamic layer of security by requiring a temporary code, delivered via a secure channel like a user's registered phone, to be entered alongside the fingerprint and



password. This eliminates the vulnerability of static passwords being stolen or guessed through brute force attacks.

VI. CONCLUSION AND FUTURE SCOPE





In this project, we reviewed some papers which have worked on this project. In our paper we introduced biometric based locker which provide high degree of security. Any authorized user will unable to access the locker. We use fingerprint as the verification system as duplication of fingerprint is like unable. The system is cheap and easy to use. This system can be mounted anywhere, where you need high degree of security the low cost of the project is very important factor in this project. This locker system is very reliable and safe. We can use thisbiometric system in bikes for antitheft system, thisbiometric system will use in bike locking and to ignite the engine of the bike to provide an advancement in car biometric system can be implement which is good idea forignite the engine and to run the car so that only owner of thecar can drive the car. Retina scanner can be implemented atthe place of fingerprint.

REFERENCES

- [1] IEEE paper on “Iris based human identification” of 2015 by Madhulika Pandey of computer science and engineering department, Amity University, Noida , India.
- [2] IEEE paper on “The human iris structure and its application in security system of car” by Sreekala.P, Victor Jose, assistant professor, Electrical and ElectronicsDept. kanjirapally.
- [3] IEEE paper on “A Broad Survey on Fingerprint Recognition Systems” by Subba Reddy Borra and G. Jagadeeswar Reddy.
- [4] IEEE paper on “Fingerprint Recognition Techniques and its Applications” by Priyanka.
- [5] Pramila D Kamble and Dr. Bharti W. Gawali Fingerprint Verification of ATM Security System by Using Biometric and Hybridization International Journal of Science and Research Publications, Volume 2, Issue 11,November 2012.
- [6] Gyanendra K Verma, Pawan Tripathi, A Digital Security System with Door Lock System Using RFID Technology, International Journal of Computer Applications (IJCA) (0975 8887), Volume 5 No.11, August 2010.
- [7] IEEE paper on “Physical Authentication using RandomNumber Generated (RNG) Keypad based on One Time Pad (OTP) Concept” by Heryn Ramadhani Mohd Husny Hamid and Norhaiza Ya Abdullah.



VII. AUTHOR PROFILES

	<p>Mrs. K. Sarada is currently working as Assistant professor in Department of ECE, Tirumala Engineering College, Jonnalagadda, Narasaraopet, Palnadu (dt). She pursued her M. Tech in JNTU campus, Ananthapur. Her area of interest is Digital electronics and communication.</p>
	<p>Mrs. O. Bhargavi is a student currently pursuing B. Tech in the stream of ECE in Tirumala Engineering College, Jonnalagadda, Narasaraopet, Palnadu(dt).</p>
	<p>Mr. M. Rajesh is a student currently pursuing B. Tech in the stream of ECE in Tirumala Engineering College, Jonnalagadda, Narasaraopet, Palnadu(dt).</p>
	<p>P. Akash is a student currently pursuing B.Tech in the stream of ECE in Tirumala Engineering College, Jonnalagadda, Narasaraopet, Palnadu(dt).</p>