International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 07 | July 2021 www.irjet.net p-ISSN: 2395-0072

FINGERPRINT BASED BANK LOCKER SECURITY SYSTEM

Akash Thomas[1], Kezia Mariam Varghese[2], Sheba Elizabeth Kurian[3]Er. Ashly John[4]

[1, 2, 3]UG Scholar, Department of ECE, SAINTGITS College of Engineering, Kerala, India
[4]Assistant Professor, Department of ECE, SAINTGITS College of Engineering, Kerala, India

---

Abstract -*The main goal of this project is to design and implement a security system based on fingerprints, which can be organized in banks, offices and apartments.In this system only the authenticated person picks up the documents or the money from the locker.Fingerprints of clients are stored and when the client puts his/her hand over the fingerprint module it reads the digital data and this data is entered into the AVR microcontroller. The microcontroller compares this value with the stored value. If both values are the same, the person's name will be displayed on the LCD screen and the motor will spin and the locker will open. If the values do not match, the motor will not turn and the locker will remain closed.This system also provides enhanced security by means of a Bluetooth module and vibration sensor. If an unauthorized person tries to unlock, a warning message is sent to the mobile phone via Bluetooth in order to monitor the security details of the bank. If the system is hit, the buzzer is activated and an alarm is generated.In this way, a simple and highly secure security system for bank lockers can be implemented.*

***Key Words*: Fingerprints, AVR Microcontroller, LCD Screen, Motor, Bluetooth module, Vibration sensor**

1.INTRODUCTION

In the real world, people are more concerned about the safety of their valuable things like jewelry, money, important documents, etc. which is why safe deposit boxes are the safest place to keep them. The advent of rapidly growing technologies enables users to operate high security systems with electronic identification options .These identification technologies include safe deposit boxes and ATMs as well as other smart cards, user IDs and password-based systems etc., which are unfortunately not protected against hacker attacks, theft and forgotten passwords. All of these failures or faults and malfunctions or crashes of these systems still exist; However, identification based on biometric or fingerprint authentication is the most efficient and reliable solution for strict security. Biometrics measures a person's unique physical characteristics to recognize or authenticate their identity. The physical characteristics are fingerprints of the hand, face, iris, etc., signature, voice keystroke patterns, etc. Biometric systems operate in verification mode or in identification mode. In verification mode, the system validates a person's identity by comparing the captured biometric template previously saved in the system database. In the traditional locker security identification mode, the system recognizes a person by searching the entire template database for matches, and the system performs one of many comparisons to determine the person's identity or fails if the person is not as the system is registered. Our project therefore use a fingerprint security system to improve the security of conventional lockers.

2. LITERATURE SURVEY

R. Ramani (2012) et al. defined a bank locker security system which is based on RFID and GSM technology which can be implemented in banks, secure offices and homes. In this system, only authorized people can get money from a safe deposit box. We have implemented a bank locker security system based on RFID and GSM technology which includes a door locking system with RFID and GSM that can activate, authenticate and validate the user and unlockthe door in real time for safe access to the safe deposit box. The main advantage of using passive RFID and GSM is that it provides more security than other systems. This system consists of a microcontroller, RFID reader, GSM modem, keyboard and LCD, in this system the RFID reader reads the identification number of the passive tag and sends it tothe microcontroller if the identification number is valid, then the microcontroller sends the SMS request to the mobile phone number of the authenticated person, the original password to open and l safe deposit box if the person sends the password to the microcontroller, which is responsible for the the keypad will verify passwords entered and received by an authenticated mobile If these two passwords match, the locker will open; otherwise it will remain in a locked position. This system is more secure than other systems as it requires two passwords for verification. This system also creates a logbook that contains the record and output of each user along with basic user information.

Raghu Ram.Gangi (2013) and others have given a proposal for fingerprint verification of the security system of automatic teller machines using biometrics with hybridization. The fingerprint function is chosen for its availability, reliability and high precision. The fingerprint-based biometric system can easily be implemented to secure the ATM. In this system, the operation of these ATMs is that upon accessing the ATM, the customer inserts the fingerprint module to withdraw the money, then the machine wants the fingerprint of the user using the

machine, check / identify and give accurate with biometric fingerprints results if it's valid or not.In thismanner we can try to control and secure the criminal circle of the ATMs and lockers.

Sanal Malhotra (2014) has given a proposal for a bank locker security system with Odour identification, Security Questions using RFID and GSM technology which can be utilized in banks, companies and at personal secured places. Only the original account holder is able to use his locker. This system uses Odor identification, Security question technique, RFID and GSM technology which makes it more secure than any other system. The system has the capability of providing more security as 4 steps are used for verification. RFID tag can be verified using RFID technology, then valid person has to answer the security question by using Security question software techniques and it should be same as that of already stored then the valid person gets a message in his/her mobile using GSM technology and needs to type password from his/her mobile and keypad of locker, both passwords should match to open the door of the locker, and then odor identification will be done, the odor pattern should match with the odour pattern stored in the microcontroller.

3. OBJECTIVE

Banks offer lockers to people as and when needed. Both public and private banks provide this facility to people in need for a small annual fee. A bank locker has several advantages, some of the best are listed below:

- Softy
- Easy Access
- Available at any bank
- Anyone can use
- Easy nomination available

The fingerprint based bank locker security system is an advanced version of the traditional bank locker system which uses keys. Keys can now be easily copied and made by thieves. In addition, the keys need to be taken care of and they can also be lost through some neglect.The fingerprint based bank locker security system can solve all of these problems. The fingerprint-based bank locker system is more secure and it is easy to use and maintain. Here there is no need for key handling and hence you don't have to worry about losing keys.The system uses fingerprint recognition to read the fingerprints and first stores the registered fingerprints in the bank locker register. The next time when a person scans his/her finger, the sensor reads it and compares it to previous recordings. If a match is now found with the existing fingerprints, it sends the match signal to the microcontroller and the controller displays this data on the LCD screen. The controller also operates the driver motor to open the locker to authorized customers. The locker remains closed for unauthorized customers.

4. METHODOLOGY

There are two types of fingerprint processing: fingerprint registration and fingerprint comparison.

When logging in, users have to enter the fingerprint twice. The system processes the finger image, creates a finger image template based on the processing result, and stores the template. During the comparison, the user holds his finger on the optical sensor and the system displays the fingerprint template and compares this finger with the template already in the "finger" library for a 1: 1 comparison system that the machine uses corresponds to compares the recorded original fingerprint with the clearly defined template, which is sorted in the module, for 1: N match or for the search system, which searches the entire finger library for the matching fingerprint of the user. In both cases, the system returns the match result as a success or failure.

4.1 Fingerprint template

The first step is to collect the fingerprint with another or special recognition device. This process is known as registration. In this step the fingerprint is taken for confirmation or authentication. Images that we have taken that are f The digital artwork can be saved directly as an image or as a biometric algorithm. With this biometric algorithm, various data points in the digital print template are clearly studied and stored, which is the actual fingerprint. The algorithm software measures 40 or more data points for each fingerprint and then stores these measurements while the data is organized or encrypted into a digital certificate for future authentication. If we represent the fingerprint in mathematical form, but the actual fingerprint is not used to

prove a person's name or identity, a higher level of reliability can be clearly understood.

4.2 FINGERPRINT MATCHING

Fingerprint Matching or Matching Techniques can have two types of categories, the first one is based on details and the other one is based on correlations. The minutiae-based technique first finds the minutiae points and then plans their associated position and places them on the finger. When we match the features for the minutiae extraction, you need some kind of processes including orientation calculation, image segmentation, image enhancement, edge and brightness extraction, minutiae extraction, and filtering before the match can be performed. The correlation-based approach is able to solve some of the difficulties of the minute-based approach. Correlation-based techniques require the exact position of a corner or center of an object or a registration point and are overloaded by translation and rotation from the image.

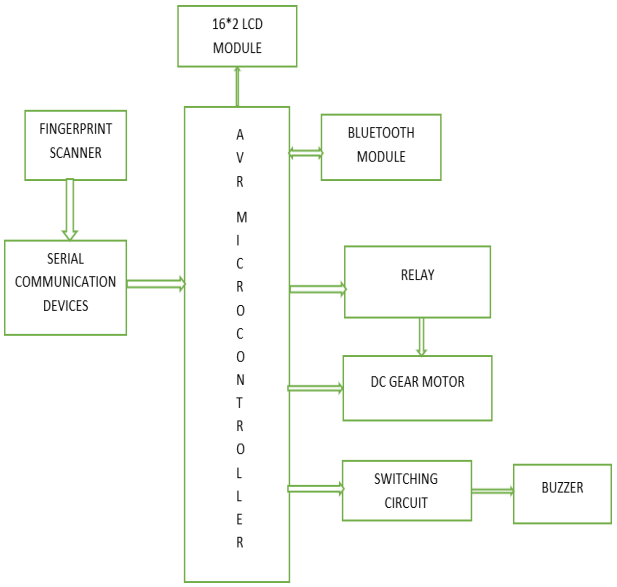

Fig -1: Block Diagram

5. COMPONENTS REQUIRED

5.1 FINGERPRINT SENSOR

The sensor is a solid-type fingerprint sensor that reliably captures fingerprint information. It is designed to be combine into devices for added security and convenience. The sensor offers a reliable, fast and easy-to-use alternative to passwords, PINs and other forms of user authentication.

Fig -2: Fingerprint Sensor

5.2 AVR MICROCONTROLLER

The AVR microcontroller is the heart of the project. The C language is employed to do the programming. This is a modified 8-bit RISC single-chip microcontroller in Harvard design, which was developed by Atmel in 1996. The AVR was one amongst the primary microcontroller families to use on-chip non-volatile storage for program storage, instead of one-time programmable ROM, EPROM, or programmable EEPROM utilized by other microcontrollers at the time.

Fig -3: AVR Microcontroller

5.3 ANDROID

Android is popular with technology companies who need an inexpensive, customizable, out-of-the-box operating system for high-tech devices. Android's openness has encouraged a large community of developers and enthusiasts to use open-

source code as the basis for community-based projects, add new features for power users, or bring Android to devices that are officially released with other operating systems.

Fig -4: Android

5.4 BLUETOOTH

Fig -5: Bluetooth

Bluetooth is a popular wireless technology for exchanging information over short distances from constant and cellular devices and for building personal space networks. It was invented in 1994 by the telecommunications provider Ericsson and was originally designed as a wireless alternative to RS232 data cables. You can connect a variety of devices to troubleshoot sync problems.

5.5 SERIAL COMMUNICATION DEVICE

In telecommunications and computing, serial communication is the process in which data is sent bit by bit sequentially over a communication channel or computer bus, as opposed to parallel communication, in which multiple bits are sent as a whole on one connection. with several parallel channels. Serial communication is used for all long-distance communication and most computer networks where the cost of cables and timing issues make parallel communication impractical.

5.6 POWER SUPPLY

The input to the circuit is applied by the regulated power supply. The AC input voltage, i.e. 230 V from the mains, is reduced to 12 V by the transformer and fed to a rectifier. The voltage from the rectifier is a pulsating DC voltage. In order to obtain a direct voltage, the rectifier output voltage is fed to a filter to remove any alternating current components even after rectification. This voltage is fed to a voltage regulator to obtain a pure constant DC voltage.

5.7 LCD DISPLAY

A liquid crystal display (usually abbreviated as LCD) is a thin flat screen device consisting of many number of monochrome or color pixels arranged in front of a light source or reflector. it is often used in battery-powered electronic devices because it uses very little electrical energy. In this project, the LCD Display is used for monitoring purposes.

Fig -6: LCD Display

5.8 DC MOTOR

The DC motor power vary goes from 45Watt to 1500 Watt. The L293D and L298 are dual H bridge motor driver ICs. We can control the rotation of two motors clockwise and counter clockwise. DC motors are used to physically drive the application according to the system requirements. DC motor runs at 12V. To power a DC motor a DC motor controller, L293D is needed.

Fig -7: DC Motor

5.9 CRYSTAL OSCILLATOR

Crystal oscillators are devices capable of utilizing mechanical resonance of a vibrating crystal made of a piezoelectric material to produce an electrical signal at a precise frequency. This frequency can be used to keep track of time in order to provide a stable clock signal for our AVR microcontroller. The most commonly used Piezoelectric Resonator is quartz crystal, hence the oscillator circuitry that contained this is called as crystal oscillators.

5.10 STEP DOWN TRANSFORMER

Step-down transformers are created to reduce the electrical voltage. Its primary voltage is greater than its secondary voltage. This kind of transformer lowers the voltage applied to it. These transformers reduce the electrical voltage from a level or a phase configuration in general to a lower level.

Fig -8: Step Down Transformer

5.11 RECTIFIER

A rectifier is an electrical device which is capable to convert alternating current (AC) which can periodically reverse its direction into direct current (DC),which flows in only one direction. The process is called as rectification and it has different forms including vacuum tube diodes, mercury arc valves, selenium-copper oxide rectifiers, semiconductor diodes, silicon controlled rectifiers, and other silicon based semiconductor devices.

5.12 FILTER

Electronic filters are analog circuits that does signal processing functions especially to remove undesirable frequency components from the signal in order to enhance the desired ones, or both. Linear filters are the most common electronic filter regardless of other aspects of their design.

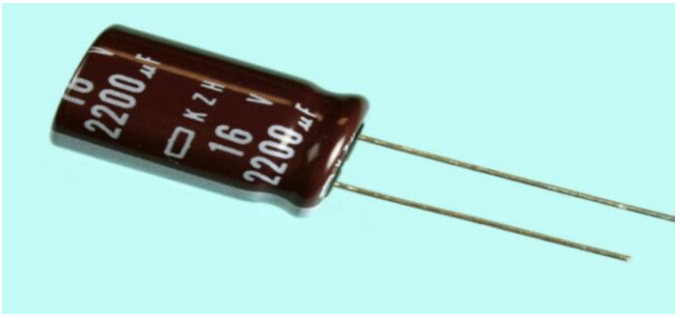

Fig -9: Filter

5.13 REGULATOR

A regulator is a device that can maintain a particular characteristic. It is responsible for managing or preserving a wide range of values in a machine. The quantifiable property of any device is closely managed by specified conditions or an advance value. It may be a fixed value or a variable one based on a predetermined formula.

Fig -10: Regulator

6. WORKING

6.1 BASIC WORKING

The customer's fingerprints are stored in the fingerprint sensor as a database. When the customer places his hand on the fingerprint sensor, it reads the digital data and this data is fed to the microcontroller. The microcontroller compares this value with the stored value. If both values are the same, the motor will turn and the locker will open; otherwise, the motor will not turn and the cabinet will not open.

6.2 MODIFICATIONS

1) VIBRATION SENSOR If the system is damaged or hit multiple times, the buzzer will turn on and an alarm will be generated.

2) LCD DISPLAY Displays the customer's name if their fingerprint matches the stored value.

3) BLUETOOTH MODULE Development of an application on the mobile phone to initiate a call or a message so that a warning message is sent to the mobile phone via Bluetooth if an unauthorized person tries to unlock it.

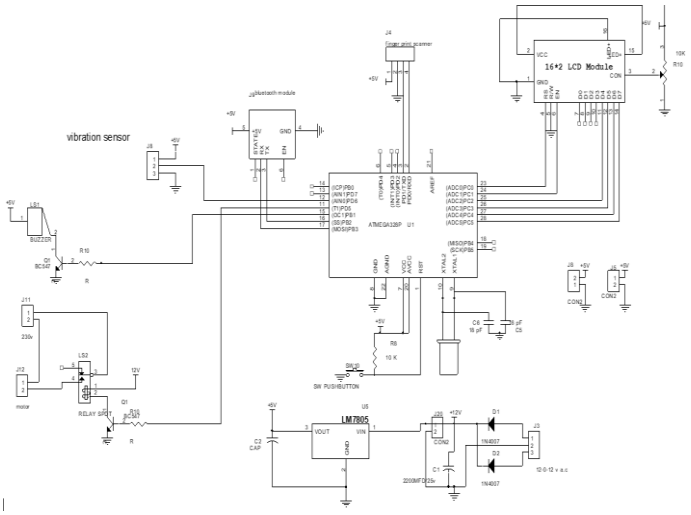

Fig -11: Circuit Diagram

7. RESULT

It is a basic implementation of the proposed hardware system. We have successfully designed and made a hardware of the proposed design. The Fig-12 shows our proposed hardware.

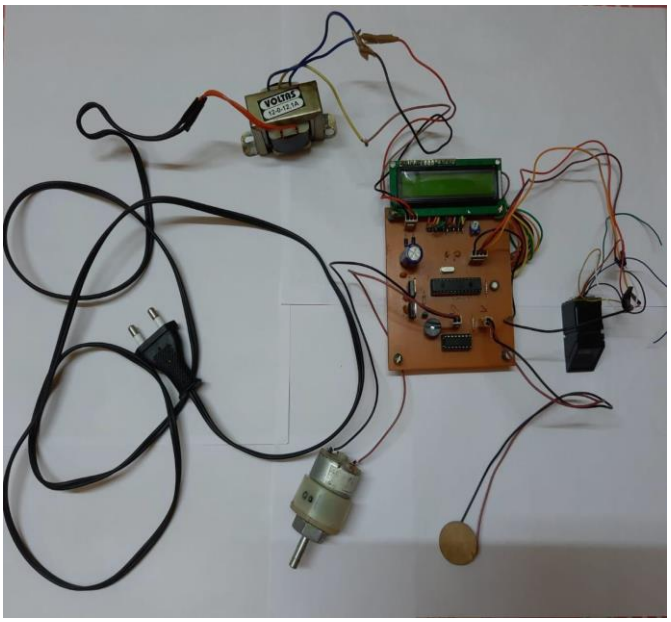

Fig -12: Hardware

8. CONCLUSION

In this article, we're reviewing some of the articles that worked on this project. In our article, we introduced fingerprint-based lockers that offer a high level of security. No unauthorized user can access the locker. Fingerprint is impossible. The system is cheap and easy to use. This system can be installed wherever a high level of security is required. These locker systems are very reliable and secure. In addition, the Bluetooth module and the vibration sensor provide improved protection

REFERENCES

[1] A.Aditya Shankar, P.R.K.Sastry, A.L.Vishnu ram.A.Vamsidhar Fingerprint Based Door Locking System International Journal of Engineering and Computer Sciences ISSN:2319-7242, Volume 4 Issue 3 March 2015

[2] Kanak Chopra, garvit Jain Door Opening System Based On Fingerprint Scanning International Journal of Engineering Research Management Technology, March 2015, Volume 2,Issue-

[3] Pavithra.B.C, Myna.B.C, Kavyashree.M Fingerprint Based Bank Locker System Using Microcontroller Proceedings of IRF International Conference, 5 April-2014, Pondicherry, India, ISBN: 978-93-82702-71-9.

[4] M.Gayathri, P.Selvakumari, R.Brindha Fingerprint and GSM based Security System International Journal of Engineering Sciences Research Technology, ISSN: 2277-9655, Gayathri et al.3(4): April, 2014.

[5] Sagar S. Palsodkar, Prof S.B Patil Biometric and GSM Based Security for lockers International Journal of Engineering Research and Application ISSN: 2248-9622, Vol.4, December 2014.

[6] Raghu Ram.Gangi, Subhramanya Sarma.Gollapudi Locker Opening And Closing Sys-tem Using RFID, Fingerprint, Password And GSM International Journal of Emerging Trends Technology in Computer Science (IJETTCS), Volume 2, Issue 2, March April 2013.

[7] R.Ramani,S.Valarmathy, S. Selvaraju, P.Niranjan Bank Locker Security System based on RFID and GSM Technology International Journal of Computer Applications (09758887) Volume 57 No.18, November 2012 .

[8] 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.

[9] 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.

[10] Mary Lourde R and Dushyant Khosla Fingerprint Identification in Biometric Security Systems International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October,2010.

BIOGRAPHIES

Akash Thomas
Department of ECE
Saintgits College of Engineering

Kezia Mariam Varghese
Department of ECE
Saintgits College of Engineering

Sheba Elizabeth Kurian
Department of ECE
Saintgits College of Engineering

Er. Ashly John
Assistant professor
Department of ECE
Saintgits College of Engineering