



FINGERPRINT BASED SMART BANK LOCKER SYSTEM WITH IMAGE CAPTURE SYSTEM

¹ Geddami Gowthami, ²Dr.K.Dhanumjaya, ³ Mr.R.Rama Mohan

¹M.tech Scholar, Dept. Of ECE,Audisankara College of Engineering and Technology, Gudur, Andhra Pradesh

² Professor, Dept. Of ECE, Audisankara College of Engineering and Technology, Gudur, Andhra Pradesh

³ Assistant Professor, Dept. Of ECE,Audisankara College of Engineering and Technology, Gudur, Andhra Pradesh

ABSTRACT

As today fingerprint based system provides high accuracy in terms of security. Also there is a high demand for integration of fingerprint matching techniques for making secure authentication systems. Therefore we have introduced this bank locker system which integrates fingerprint reader in it so as to provide a good level of security. The main goal of fingerprint bank locker with image capture project is to provide security with no manual security flaws. It's simple to use and doesn't need any special tools or training. This system needs fingerprint authentication while operating the bank locker as well as captures the images of person who is handling the locker and saves it in memory card which can be later viewed with card reader to the bank authorized person. The functionality of system is that it will scan the fingerprint and if it matches with registered fingerprint the bank locker opens and also captures the image of user.

INTRODUCTION

The Finger Print Sensor Module, also known as the Finger Print Scanner, is a module that takes a picture of your finger's print, transforms it into an equivalent template, and then stores those templates in its memory at a specific ID (location) chosen by Arduino. Here all the process is commanded by Arduino. The use of embedded systems in household appliances is now possible thanks to advancements in technology. In our homes, we use a lot of electrical appliances to help with various tasks. The majority of these appliances operate independently. However, the recent trend of making these appliances smart and interconnected has made

their operation even simpler. This paper explains various security issues in the existing home automation systems and proposes the use of fingerprint based security algorithms to improve home security. Implementation of this project is done by using as a controller to which the devices are directly interfaced.

Motivation:

The automated identification or verification of individuals based on their unique physiological or behavioral characteristics such as fingerprints, gait, iris etc. is referred to as biometric authentication. The idea of using fingerprints as biometrics dates back thousands of years. Potters from East Asia used to place their fingerprints on clay as it cured. Fingerprints were also used in the 19th century by criminologists for identification of habitual criminals. However, biometrics first emerged as an automated technology in the 1970s. Biometrics were first used in commercial applications to control physical building access. This trend continues to expand as technology advances. The increasing need to reduce instances of fraud as well as to provide secured access to physical and logical assets have made fingerprint biometrics a very popular and widely used technology.

Fingerprint is a very strong authentication mechanism as it based on something that you are as opposed to something you know or something you have. Tokens and passwords are extremely susceptible to theft or loss. A weak or compromised password is the primary reason for the rising cases of security and data breaches. In an organization's

security system, passwords are the weakest link, and even strong passwords cannot withstand sophisticated hacker attacks. Further, the costs of maintaining password and token based systems are very high and inefficient. Resetting lost or forgotten passwords takes up IT support time and reduces employee productivity.

OBJECTIVE: The main aim of the project is to improve the home security system by using advanced technologies. In our project the fingerprint of particular people is detected and stored as a data and it is use to detect the fingerprint of other people and compare it to the already stored data using optical fingerprint.

II.LITERATURE SURVEY:

Aditya Shankar et al. focused on the project related to the replacement of conventional techniques of locking system. The biometric system took the place of previous methods like the lock and key system and password authentication system. They basically used fingerprints for the authentication system, the person whose fingerprint saved in the database can easily access the locker. They also provide an alarm system to alerting the neighbors if an unauthorized person or thief tries to access the locker. They must scan their fingerprints to demonstrate that they are authorized to open the locker door. The scanner is interfaced to 8051 microcontroller; this controller will be controlling the scanning process. They also provided a keypad for password after the fingerprint scanning. This two-step verification is for the double security and a buzzer is provided for alarm in case of unauthorized access of locker. [1]

Omidiora E.O. et al. refused the traditional methods of locking system for the bikes, they introduced finger print based locker which is the robust security mechanism in various security domain. In their prototype software module is used for the database storage of valid users and hardware is provided for the interfacing. Visual C++, Visual Basic, and Visual Basic were used for programming. The programming of this prototype was done in Visual Basic 6.0 Enterprise Edition. The prototype was tested with 20 test images stored in the database. The implementation went well, and the microcontroller could tell the difference between users who were authorized and those who were not.

Transfer of logic 1 for the authorized user and logic 0 for the unauthorized user [2]

Karthikeyan. A et al .told that every person has unique fingerprint. They added a secured keypad for adding and deleting number of users from database which is very good concept. FIM3030 fingerprint module by NITGEN is used in this purpose. Microcontroller AT89C52 is utilized for controlling the entire driving unit. LCD is also provided for showing the information about the authorized and unauthorized user. Due to its short propagation delay, the decoder DM742S138 can be used for data routing and interface with fast memory units. Latch 74HC373 is provided which is high-speed Si-gate CMOS devices. A relay is used as an interfacing circuitry between the microcontroller output and the ignition system of the car.

[3] Pavithra .b.c et al .mainly focused in this project on security. As a scanner, R303A was used. This module has in-built ROM, DSP and RAM. The fingerprint module has a capacity of storage 100 user's fingerprint. This module operates in 2 modes they are Master mode and User mode. Master mode is used to uniquely identify the fingerprints that will be stored in the scanner's ROM. They provided a unique identification number for the last step of verification, which provides three wrong attempts. They provide a digital code lock at every locker's door, which is operated by the password. The password included six mandatory numeric numbers without any character. This locking system is interfaced with microcontroller for the password storage and verification. A microcontroller 8051, a keyboard, and an LCD screen make up this lock. This can be implemented at every door locker because it is commercially available. [4]

III.EXISTING SYSTEM:

In automatic security systems generally passwords, identification cards and PIN verification techniques are being used but the disadvantage is that the passwords could be hacked and a card may be stolen or lost.

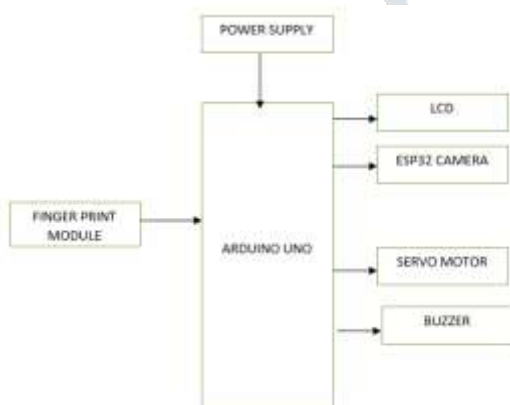
IV.PROPOSED METHODOLOGY:

The proposed system uses an atmega 328 microcontroller for this purpose. The microcontroller processes data sent by the fingerprint reader to check if user is registered,

unregistered users are not allowed access. Controller operates the motors to open the locker door on encountering registered valid users.

If the fingerprint does not matches with register fingerprint of user it will shows the error message as unauthorized user and immediately saves the picture in memory card. So, the system is very beneficial for stopping the bank locker robbery by providing security.

BLOCK DIAGRAM:



V. MODULE DESCRIPTION:

A. Arduino Uno Microcontroller :

Based on the 8-bit ATmega328P microcontroller, the Arduino Uno is a microcontroller board. Along with ATmega328P, it consists other components such as crystal oscillator, serial communication, voltage regulator, etc. to support the microcontroller. The Arduino Uno has a reset button, six analog input pins, a USB connection, a Power barrel jack, an ICSP header, and 14 digital input/output pins, six of which can be used as PWM outputs. Arduino can be used to communicate with a computer, another Arduino board or other microcontrollers. The ATmega328P microcontroller provides UART TTL (5V) serial communication which can be done using digital pin 0 (Rx) and digital pin 1 (Tx). An ATmega16U2 on the board channels this serial communication over USB and appears as a virtual com port to software on the computer. There is no need for an external driver because the ATmega16U2 firmware makes use of standard USB COM drivers. However, on Windows, a .inf file is required. A serial monitor is included in the Arduino software, making it easy to **textual data to be sent to and from the Arduino board.**



Fig 1:Arduino UNO controller

B.R307S Optical Fingerprint Reader Sensor Module

This is the R307S Optical Fingerprint Reader Sensor Module. R307S fingerprint module is a fingerprint sensor with a TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the fingerprint data in the module and can configure it in 1:1 or 1: N mode for identifying the person.

The FP module can directly interface with a 3.3 or 5v [Microcontroller](#). A level converter (like MAX232) is required for interfacing with PC serial port.

Integrated image collecting and algorithm chip together, ALL-in-One Fingerprint reader can conduct secondary development, can be embedded into a variety of end products. Users can conduct secondary development, can be embedded into a variety of end products, such as access control, attendance, safety deposit box, car door locks.



Fig 2:Fingerprint Module

C.ESP32 CAM WiFi Module

The ESP32 CAM WiFi Module Bluetooth with OV2640 Camera Module 2MP For Face Recognition has a very competitive small-size camera module that can operate independently as a minimum system with a footprint of only 40 x 27 mm; a deep sleep current of up to 6mA and is widely used in various IoT applications.

It is suitable for home smart devices, industrial wireless control, wireless monitoring, and other IoT applications.



Fig 3:ESP32 CAM WiFi Module

ESP32 CAM WiFi Module Bluetooth adopts a DIP package and can be directly inserted into the backplane to realize rapid production of products, providing customers with high-reliability connection mode, which is convenient for application in various IoT hardware terminals.

Applications:

- It can be used to provide security in Banks.
- It is used for home security.
- Security offices and recommended to use fingerprint technology.
- Most of the hospital chambers are secured using this technology.
- Generally, this technology is used in the places where the security is required.

VI.RESULTS:

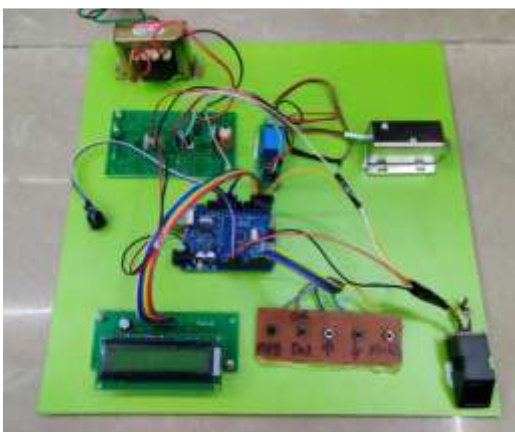


Fig 4:Hardware implementation

VII.CONCLUSION:

Fingerprint identification enhances the security of a locker and makes it possible only for some authorized people to use the locker. Thus, by implementing this relatively cheap and easily available system on a locker, one can ensure much greater security and exclusivity than that offered by a conventional lock and key. It can be deduced that the use of biometric security systems offers a much better and fool proof means of restricting the use of locker by unauthorized users. The developed prototype serves as an impetus to drive future research, geared towards developing a more robust and embedded real-time fingerprint based automatic door lock systems in bank locker.

REFERENCES

- 1.Iftikhar, Umar, Kashif Asrar, Maria Waqas and Syed Abbas Ali. "Evaluating the Performance Parameters of Cryptographic Algorithms for IOT-based Devices." *Engineering, Technology & Applied Science Research* 11, no. 6 (2021): 7867 - 7874.
- 2.Lande, Rani S., Susmita A. Meshram, and Pranita P. Deshmukh. "Smart banking using IoT." In 2018 International Conference on Research in Intelligent and Computing in Engineering (RICE), pp. 1 - 4. IEEE, 2018.
- 3.Ammirato, Salvatore, Francesco Sofo, Alberto Michele Felicetti and Cinzia Raso. "The potential of IoT in redesigning the bank branch protection system: An Italian case study." *Business Process Management Journal* 25, no. 7 (2019): 1441 - 1473.
- 4.Bansal, Malti, Naman Oberoi, and Mohd Sameer. "IoT in online banking." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 2, no. 04 (2020): 219 - 222.
- 5.Alti, Adel and Ahmed Almuhrat. "An Advanced IoT-Based Tool for Effective Employee Performance Evaluation in the Banking Sector." *Ingénierie des Systèmes d'Inf.* 26, no. 1 (2021): 103 - 108.
- 6.A. Kaur, A. Jadli A. Sadhu, S. Goyal A. Mehra and Rahul, "Cloud Based Surveillance using ESP32 CAM," 2021 International Conference on Intelligent Technology, System and Service for Internet of Everything (ITSS-IoE), Sana'a, Yemen, 2021, pp. 1 - 5, doi: 10.1109/ITSS-IoE53029.2021.9615334.
- 7.Cahyono, Filantropi Yusuf Aji, Nugroho Suharto, and Lis Diana Mustafa. "Design and build a home security system based on an esp32 cam microcontroller with telegram notification." *Journal of Telecommunication Network (Jurnal Jaringan Telekomunikasi)* 12. 2 (2022): 58 - 64.

8. Salikhov, R. B., V. Kh Abdrakhmanov, and I. N. Safargalin. "Internet of things (IoT) security alarms on ESP32-CAM." *Journal of Physics: Conference Series*. Vol. 2096. No. 1. IOP Publishing, 2021.
9. B. Jayaram, D. A. Subhahan S. B, T. A. Mohanaprakash S. Joshi and M. J. Kumar, "IoT and Image Processing based Smart Door Locking System," 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2022, pp. 291 - 295, doi: 10.1109/ICACRS55517.2022.10029199.
10. F. Aman and C. Anitha, "Motion sensing and image capturing based smart door system on android platform," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 2346 - 2350, doi: 10.1109/ICECDS.2017.8389871.
11. Dasmien, Rahmat Novrianda and Sandy Prayitno. "Task collection monitoring system on lockers with notifications on Telegram." *PROtek: Jurnal Ilmiah Teknik Elektro* 10. 2 (2023): 107 - 112.
12. G. Soni, S. S. Saini S. S. Malhi, B. K. Srao A. Sharma and D. Puri, "Design and Implementation of Object Motion Detection Using Telegram," 2021 International Conference on Technological Advancements and Innovations (ICTAI), Tashkent, Uzbekistan, 2021, pp. 203 - 206, doi: 10.1109/ICTAI53825.2021.9673226.
13. B. Siddineni, R. Nanditha T. J. Satyanarayana and V. S. Rama Krishna Sighakolli, "Design of an IoT based Surveillance System using Blynk, IFTTT, and Telegram," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2021, pp. 01 - 06, doi: 10.1109/ICCCNT51525.2021.9579790.
14. N. Y. L. Venkata, C. Rupa B. Dharmika, T. G. Nithin and N. Vineela, "Intelligent Secure Smart Locking System using Face Biometrics," 2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT), Bangalore, India, 2021, pp. 268 - 273, doi: 10.1109/RTEICT52294.2021.9573869.
15. Prathapagiri, Dilip and Eethamakula Kosalendra. "Wi-Fi Door Lock System Using ESP32 CAM Based on IoT." *The International journal of analytical and experimental modal analysis*. XIII. 20002003 (2021).

