Fingerprint Based Secure Identification System using IoT

Dr. Praveen Kumar K V
Professor, Dept. of Computer Science, Sapthagiri College of Engineering, Bangalore, India

Kumar Abhijeet, Saurabh Dokaniya, Saurav Sirohi, and Unnati Gupta
Final Year Students, Dept. of Computer Science, Sapthagiri College of Engineering, Bangalore, India

Abstract - **Fingerprint scanners have become the norm in recent times when it comes to security. Most of the identification devices still are susceptible to attack and vulnerable to some extent. Thus, regular attempts to upgrade the existing systems keep being made. So, a system is proposed in this paper which overcomes the major flaws in the existing systems by introducing new technologies such as Capacitive Fingerprint Sensor and IoT to create a cost effective, more secure identification system. It can also be used to prevent unauthorized access in any facility by attaching it to a door lock.**

Keywords – Capacitive, Arduino, Fingerprint, Identification, IoT, Authentication..

I. Introduction

In recent years, The Internet of things (IoT) has proven itself to be a platform to be considered among the preferable devices to be used for solving problems. IoT technology is widely associated with products such as smart lighting bulbs, home security systems and cameras that can be controlled via devices associated with that ecosystem, such as smartphones. But the area of applications for IoT is much larger than that. IoT is a class of computing which fuses the use of the internet onto typical day to day machines to enhance the usage of devices. These devices move information collected through the sensors and send it to an online repository to reduce as much human intervention as possible. Today, we are using Internet of Things technology towards creating a secure authentication device to prevent unauthorized access in any organization.

Arduino is a microcontroller used for creating electronics projects. It has an IDE and a programmable circuit board that runs on a computer. It is different from most existing programmable circuit boards as the Arduino does not bother with an equipment known as the programmer. Thus, to stack new code onto the board a USB link is utilized instead. The IDE for Arduino makes use of a simpler version of C++ which is pretty easy to learn. The arduino board can interact with buttons, LEDs, motors, the internet, and even a smartphone along with many other types of accessories and components. This adaptability combined with the fact that the Arduino software is open-source,free,easily available and the hardware boards are pretty cheap has made it a very popular choice for users as it can be used for any kind of electronics project.

Capacitive Fingerprint sensor has advantage over Optical Fingerprint sensors. It contains an array of capacitors. The capacitors measure the capacitance of the fingerprint ridges and valleys instead of taking a 2D image. It makes it secure compared to other forms of biometric identification. When combined with a device like Arduino, it can be developed into a very robust identification system.

In modern times, privacy has become a very vital part of our lives. Humans put some form of security check in every device they use. Hence, an universal identification system is required. Places such as Hospitals, Airports and Offices often have private areas which can only be accessed by authorized members. Such places can benefit from a fingerprint identification system. Obsolete systems use keys and keycards (RFID) to identify, such objects can be stolen and duplicated. A Capacitive fingerprint based identification system is protected from such flaws as it cannot be duplicated.

II. Relatedworksinthefield

The existing fingerprint based identification systems currently available in the market are based on Optical Fingerprint scanners. The major flaw in the current system is that it can be spoofed. It uses fingerprint images which are 2-Dimensional in nature. A dedicated hacker with social engineering skills can acquire the fingerprint of the victim. The hacker can recreate the acquired fingerprint into a high quality image and print it on a thumbprint model. Thus, the security is breached.

A scene from the accurate TV series "Mr. Robot" consists of the protagonists breaking into a facility by using hacking, social engineering to get the fingerprint and using an imaging program and a 3D printer to hack into the Fingerprint system. It could have been prevented if Capacitive sensors were used instead. This scene inspired us to work on a secure identification system.

III. PROPOSEDSYSTEM

The proposed system consists of an Arduino board, a capacitive fingerprint sensor, a WiFi module board, LCD display. The system works as a cost effective and easy to implement identification system to be used by organisations and individuals (for home security purpose).

A. Hardware Implementation

1. *Arduino Mega 2560 R3* - It is a programmable microcontroller board. It uses C and C++ as the programming language. The compiler supports various libraries to support the external modules connected to the board. It has the benefit of being cheaper in cost. It is responsible for the overall implementation of the system.

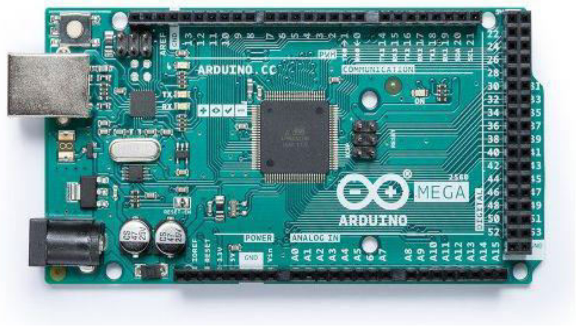


Figure 1: Arduino Mega 2560 R3

2. *R302 Fingerprint Module* - It is the capacitive fingerprint sensor which can read the capacitance values of the fingerprint. It does not work on imagery technology. It consists of a tiny array of capacitors to acquire the fingerprint data in matrix form. It securely stores the fingerprint data in the inbuilt memory. Thus, the seek time is reduced marginally.

Figure 2: R302 Fingerprint Module

3. *NodeMCU ESP8266 ESP-12E Board* - It is a Wi-Fi development board used to connect the system to the Internet. It supports 2.4 GHz 802.11 b/g/n wireless standard.

Figure 3: NodeMCU ESP8266 ESP-12E Module

4. *LCD 1602 Parallel Display Module* - It is a dot matrix type Liquid Crystal Display. It can display up to 16 characters in 2 rows. It has parallel ports to support multiple I/O read and write operations. It can display the ID of the registered fingerprint while matching.

Figure 4: LCD 1602 Parallel Display Module

5. *LED Lights* - It is a light emitting diode used to indicate matching results of the fingerprint sensor. It turns green when a fingerprint is identified otherwise it turns red.

Figure 5: LED Lights

6. *4-Channel Push Button Switch* - It has 4 reprogrammable buttons which are programmed to run functions such as enroll, match, navigate up and down and enter button.

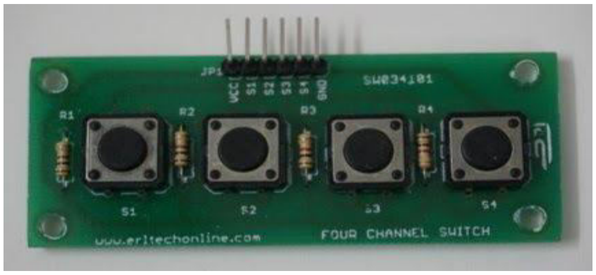
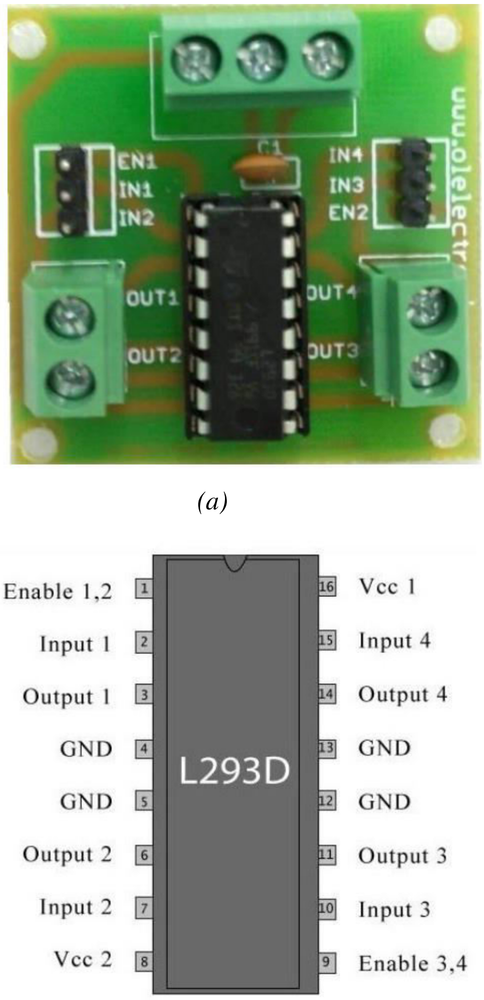


Figure 6: 4-Channel Push Button Switch

7. *DC Motor (12 Volt)* - It is a type of rotary motor which can spin the spindle. Spindle can be connected to door locks.

Figure 7: DC Motor (12 Volt)

8. *L293D Motor Driver IC* - It is an integrated circuit chip designed to control the motor. It is placed on the Motor driver board which provides protection from electrostatic discharge and performs thermal shutdown.



(a)

(b)

Figure 8: (a) L293D Motor Driver IC, (b) Pin Description of the L293D Motor Driver IC

B. **Modules Implementation**

1. *<Adafruit_Fingerprint.h>* - It is a sensor library for the fingerprint module. It can enroll, save, match, delete fingerprints and similar other functions. It can detect when a fingerprint is pressed on the sensor and lights up the LED. It enrolls new fingerprints and links them with an unique id number. It also calculates the accuracy value of the fingerprint while matching to existing ones.

2. *<LiquidCrystal.h>* - It is a library that works on the text based LCDs. It can display the result after matching. It displays the current status of the program. It can autoscroll and clear text when required. It displays the serial input taken from the

4 button switch and also manages the underscore cursor.

3. *<Keypad.h>* - It is a library for supporting the 4 channel push button switch. It can program the buttons to activate different functions. Navigation button and Accept button are programmed to perform their functions.

4. *<ESP8266WiFi.h>* - It is a library for the Node MCU board. It allows the module to connect to the internet via WiFi. It takes SSID and password as input in the program. It can connect to servers for sending and receiving messages.

5. *<BlynkSimpleEsp8266.h>* - It is a library to connect the system to the Blynk server. It can send the access logs to the Blynk Cloud. It can send notification for unrecognized fingerprints to the mobile phone application.

IV. Methodology

A. System Flowchart

Prerequisites require the system to have a database of stored fingerprints of the authorized users. This will be done by the enrollment process. The users will be marked with unique ids in the database.

It starts with the user putting his finger on the fingerprint sensor. Then the fingerprint sensor recognizes the finger on the sensor, it then starts to capture the data from the fingerprint. At which point the sensor matches the data with the existing database.

If the input fingerprint matches with the existing data, then the id of the user is taken from the database and shown on the LCD display. Therefore, the id of the user will be sent to the Blynk application. At which point the motor will spin to unlock the connected lock.

If the input fingerprint does not match with any of the stored fingerprints. Then it is considered to be an unauthorised attempt and a notification will be sent to the Blynk application.

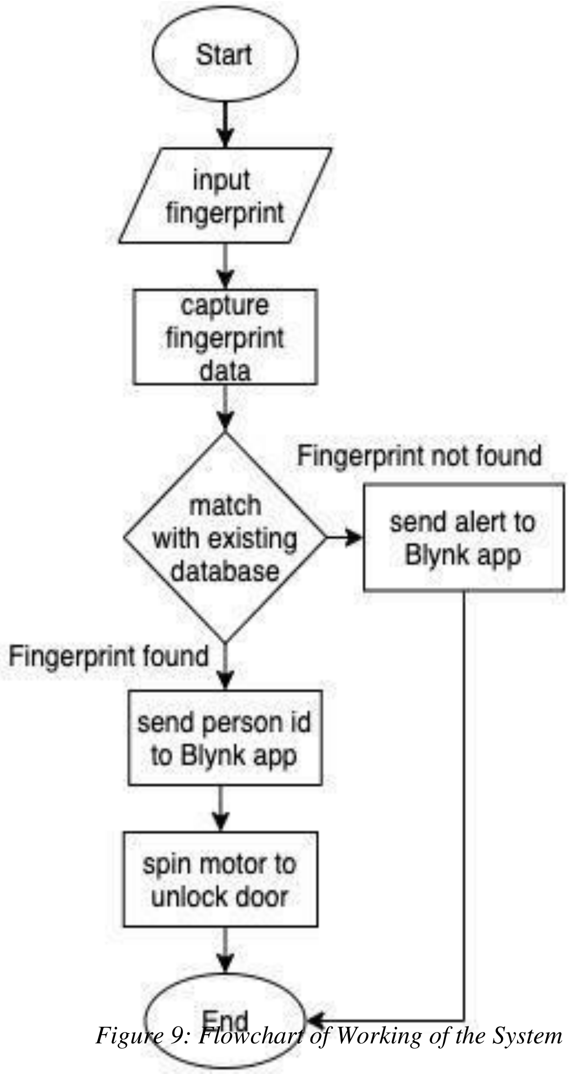


Figure 9: Flowchart of Working of the System

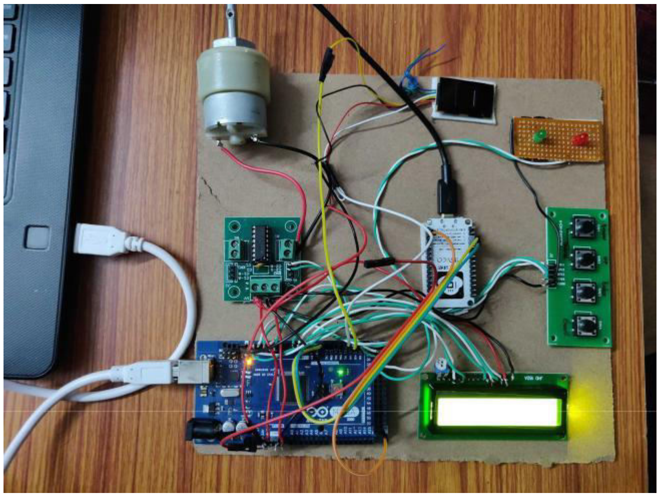


Figure 10: The Proposed System

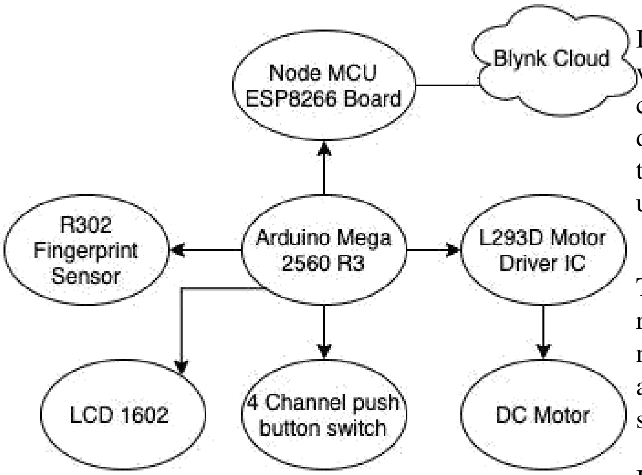


Figure 11: Overall Architecture

B. Fingerprint Detection during Enrollment

For enrollment of new users, the fingerprint sensor takes fingerprint as the input from multiple angles. It is done to get accurate fingerprint data.

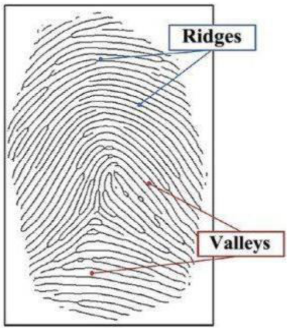


Figure 12: Ridges and Valleys in a Fingerprint

The fingerprint consists of several minutiae such as ridges (outward lines of the fingerprint) and valleys (gaps between two ridges). The ridges touch the capacitive arrays in the sensor and the individual capacitors get charged up. Different values for the measured capacitance are given for each two adjacent rows for each element which can be ridge-ridge, ridge-valley and valley-valley. The values are then combined to be written in a matrix form. This matrix is stored for each user id in the built in flash memory.

C. Fingerprint Recognition

During the matching process, the user puts the finger on the sensor. The sensor extracts the fingerprint data in the way explained in the previous subtopic. The extracted data is matched against the existing database. The matrix data is compared to calculate the confidence value. Confidence value defines the accuracy range of the fingerprint data. If the matrix value is above a certain threshold confidence value of the existing fingerprint matrix data, then it is considered as a positive match. At which point, the LCD displays the id no. of the user. If the matrix value is below the threshold confidence value, then it is considered as an unrecognized fingerprint.

V. Result

The identification system works when a fingerprint is recognized with a high confidence value. It will send the id no. of the user to the Blynk Cloud which thereafter can be accessed on the Blynk phone application. The result is shown on the LCD display as well.

In the Blynk phone application, the logs are entered in real time. It also shows the log for an unrecognized fingerprint. Thus, the admin can know that a breach in the system has been attempted and can take proper action.

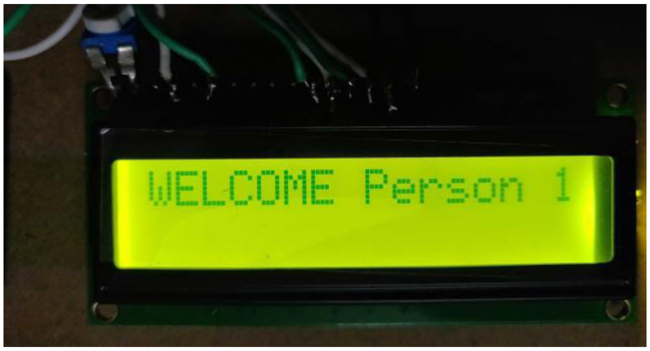
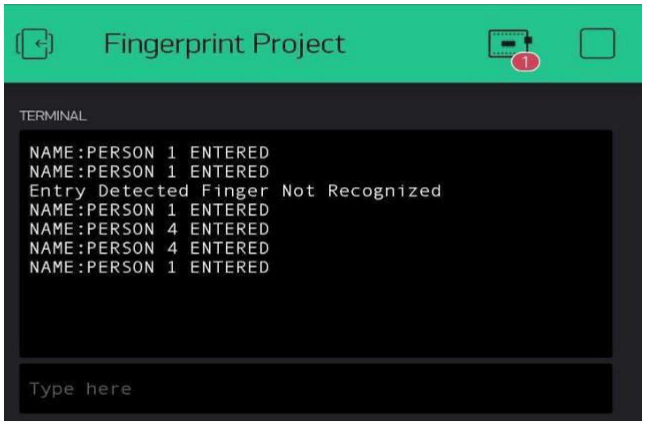


Figure 13: Output on the LCD Display



```
NAME:PERSON 1 ENTERED
NAME:PERSON 1 ENTERED
Entry Detected Finger Not Recognized
NAME:PERSON 1 ENTERED
NAME:PERSON 4 ENTERED
NAME:PERSON 4 ENTERED
NAME:PERSON 1 ENTERED
```

Figure 14: Logs shown in Blynk Application

The connected motor starts to spin when a fingerprint is recognized and thus, if a physical lock is connected to the motor, it will open the lock.

VI. ConclusionandFutureWorks

The Fingerprint based secure identification system has been developed using Open-Source libraries for Arduino programming. Compared to existing systems, our system is affordable in pricing. The components chosen for the system were not expensive. Even the Blynk Cloud service is free to use.

Decision to use capacitive sensors turned out to be fruitful as it is very accurate and overcomes some of the major flaws of the Optical sensors used in existing systems.

Overall, our system is easy to build and implement as an identification tool and security measure in a real world scenario.

For future work, implementation of a RTC (Real Time Clock) module can be done to keep track of time. Support for MicroSD can be added to extend the storage of the fingerprint database. A web application can be developed to monitor the system. A GSM module can be implemented to add the functionality of sending SMS to the admin.

References

[1] Wenchen Yang, Song Wang, Jiankun Hu, Guanglou Zheng Craig Valli "Security and Accuracy of Fingerprint-Based Biometrics" *MDPI*,2019

[2] Tanjarul Islam Mishu, Dr. Md. Mijanur Rahman, "Vulnerabilities of Fingerprint Authentication Systems and Their Securities" *IJCSIS,*Vol 16, No 3, 2018

[3] Hossam Hassan, Hyung-Won Kim "CMOS Capacitive Fingerprint Sensor Based on Differential Sensing Circuit with Noise Cancellation", *MDPI*,2018

[4] Munish Kumar, Priyanka "Fingerprint Recognition System: Issues and Challenges", *IJRASET*,Vol 6, 2018

[5] Farah Dhib Tatar, Mohsen Machhout "Improvement of the Fingerprint Recognition Process", *IJBB*,Vol 7, No 2, 2017

[6] Arduino Reference Documentation for developers https://www.arduino.cc/en/main/docs

[7] Node MCU 8266 Reference Documentation for developers https://arduino-esp8266.readthedocs.io/en/latest/

[8] Official Blynk Starting Guide Manual for developers https://docs.blynk.cc/