

Biometric Banking: Evaluating the Effectiveness of Arduino-Integrated Fingerprint Systems for Locker Security

Navneet Kaur^{1,*}, Nidhi Ahirwar², Mohini Prasad², Ankit Sharma², Chetan Bhaisare²

Abstract

The aim of this research paper is to implement a fingerprint-based bank locker system using Arduino that provides enhanced security features for users. The proposed system eliminates the need for traditional keys and instead utilizes biometric identification to grant access to the locker. The inexpensive and user-friendly Arduino microcontroller platform is used to design the system. The proposed system is implemented using various sensors, including fingerprint sensors, keypad, and LCD display. The system also includes a GSM module, which sends alerts to the user's mobile phone in case of any unauthorized access attempt. To overcome these issues, the proposed system utilizes biometric identification to grant access to the locker. The system also includes features such as remote monitoring and alerting, making it a highly secure friendly solution. This system is more secure than any other since it makes use of identity, security question approach, RFID technology, and GSM technology.

Keywords: RFID (Radio Frequency Identification), GSM (Global System for Mobile Communication), LCD (Liquid Crystal Display), SMS (Short Message service), Arduino.

INTRODUCTION

With the advancement of technology, the banking sector is shifting towards a more secure and user-friendly approach. Traditional locker systems are becoming outdated due to security concerns and the inconvenience of carrying keys.

Security in the workplace or business setting is a serious risk that everyone must deal with, whether at home or on the road. Security systems represent a major worry in this fast-paced, cutthroat society where people are unable to secure their private items by manual means. Instead, he or she looks for a different approach that offers more atomized, dependable, and superior security. Currently, everything is interconnected via networks, enabling anybody to access information from anywhere in the globe. The possibility of having one's information hacked is therefore a major concern. It is crucial to have a personal identity system in place to access one's own information because of these hazards. Personal identity is becoming a big deal everywhere these days. Password and identity card approaches are the most often used means of personal identification in the mainstream. However, these techniques are highly unreliable because identity cards can be misplaced, and passwords can be easily hacked these days.

*Author for Correspondence

Navneet Kaur
E-mail: navec2000@gmail.com

¹Assistant Professor, Department of Electronics and Communication, Sagar Institute of Research and Technology, Bhopal, Madhya Pradesh, India

²Student, Department of Electronics and Communication, Sagar Institute of Research and Technology, Bhopal, Madhya Pradesh, India

Received Date: November 14, 2023

Accepted Date: November 30, 2023

Published Date: December 20, 2023

Citation: Navneet Kaur, Nidhi Ahirwar, Mohini Prasad, Ankit Sharma, Chetan Bhaisare. Biometric Banking: Evaluating the Effectiveness of Arduino-Integrated Fingerprint Systems for Locker Security. International Journal of Electrical Power and Machine Systems. 2023; 1(1): 16–22p.

The system is more secured as 4 steps are required for verification. RFID technology is used

to verify the RFID tag [1]. A valid user must then answer a security question using software, and the answer must match the one that was initially entered when the account was opened. Next, the password must match to unlock the locker's door. Finally, a scan identification will be performed, and the smell pattern must match the one that was stored in the Arduino UNO.

LITERATURE SURVEY

The literature survey of fingerprint-based bank locker system previous works based on related work is discussed as follows:

A project was developed by Pooja et al. [2] with a primary objective of development and implementation of an OTP and fingerprint-based bank locker security solution. This can be set up in homes, offices, and banks. Under this approach, money or documents can only be retrieved from the lockers by an authenticated individual. Both fingerprints and OTP are employed in this security scheme. First-time users must register with a username, password, and mobile number in their system. A person's fingerprint will be detected and stored with their ID if their username and password match. The authorised person's mobile will then receive a four-digit code to unlock. Thus, compared to other systems, biometric and Bluetooth security have more advantages. Together with basic data, this system can also generate a record that includes each user's check-in and checkout times.

A sturdy and highly secure smart door accessing system with an Android platform has been built by Kashaboina et al. [3]. Applications of this kind are used in banking, homes, and businesses. For increased security, we incorporate a smart security system with a GSM module and Bluetooth in the suggested system. The Raspberry Pi module is used in the hardware implementation to process large amounts of data. In real-time applications, this wireless data access method is incredibly quick and secure.

In Shweta S. Joshi, Vinayak Ekke et al.'s study [4], a randomly generated password using a mobile device is used to establish an authorised locker key system. Only three password entries are permitted; if the password is entered correctly, the locker can be accessed by the designated individual. A buzzer sounds and the lock cannot be opened if the password is entered incorrectly more than three times. The locker door is locked and opened in the reference architecture using a DC motor. Additionally, max-232 is utilised for GSM data exchange.

The "bank locker security system based on RFID and GSM technology" that can be set up in banks, secure offices, and houses is presented by Chandanshive et al. [5]. Through this technique, money from a bank locker can only be retrieved by genuine individuals. They have implemented an RFID and GSM-based bank locker security system that includes a door locking system that can activate, authenticate, and validate users in real time, as well as open the door for secure bank locker access. Using passive RFID and GSM has the primary benefit of being more secure than other systems. Their system includes an LCD, a GSM modem, an RFID reader, a keyboard, and a microcontroller. The RFID reader reads the ID number from the passive tag and sends it to the microcontroller. If the ID number is valid, the microcontroller sends an SMS request to the verified person's mobile number, requesting the original password to open the bank locker. If the verified person sends the password to the microcontroller, it verifies the passwords entered using the keypad and received from the authenticated mobile phone. Because two passwords are needed for verification, this approach is more secure than others.

Detroja et al. [6] developed and installed a high security locker system that can be arranged in banks, safe offices, and houses and is based on RFID, fingerprint, password, and GSM technologies. Only legitimate users of this system can retrieve money from lockers. One type of biometric that is used to identify people and confirm their identities are fingerprints. RFID used radio frequency emission to identify a person or object.

Jadhav and Agrawal developed and put into place a smart bank locker security system that is both

extremely safe and dependable [7]. It will be based on RFID, biometric fingerprint, password, and GSM technology. This can be set up in houses, banks, treasury offices, and schools. Under this approach, only the legitimate user can unlock the lock and take valuables like jewels, cash, or vital documents out of the lockers. This security system makes use of GSM, RFID, biometric fingerprint, and password technologies. The user of our suggested system enrolls first, providing his username, password, and mobile number. Next, the user places his finger on the fingerprint module, whereupon his fingerprint is scanned and stored with his fingerprint identity. The user enrollment process will be finished in this manner.

Use a GSM application to unlock the security logging door by entering a special password over the GSM modem as presented in Leela et al. [8]. Using a GSM application, a security logging door can be opened and closed. Using a GSM modem, the user can connect and send SMS. This is a highly convenient solution since it eliminates the need for the user to physically open or close the door of his car. Using a mobile phone set as a communication device between the user at one end and the object of access (i.e., the door) at the other receiving end, the GSM module functions as both a transmitting and receiving unit.

Verifying the identity of the individual wishing to use the locker is crucial for preventing fraud. It has been suggested by Rajasekaran et al. [9] that a security system utilising voice recognition, face detection, and GSM technologies be used to address this security breach.

In the previous technologies, micro-controller is used which is expensive as compared to Arduino UNO. In this Fingerprint Based Bank Locker System we used Arduino UNO which is cost effective and at the same time it is very easy to use and easy to install. The circuit complexity also reduces.

PROPOSED METHODOLOGY

The proposed system consists of two main parts: hardware and software.

The hardware includes Arduino, fingerprint sensor, keypad, LCD display, and GSM module. The Arduino IDE is used to write C code for the software. To put it another way, radio frequency identification (RFID) is an electrical technique for data exchange using radio waves that may be used to track, identify, and detect a wide range of things. The fingerprint sensor is used to capture the user's fingerprint, which is then stored in the system's memory as shown in Figure 1 [10, 11]. When the user wants to access the locker, the fingerprint sensor compares the input fingerprint with the stored fingerprint as. If the fingerprint matches, the user is granted access to the locker. The keypad is used to enter a PIN code in case the fingerprint sensor fails to recognize the user's fingerprint. The LCD display is used to provide feedback to the user, such as the status of the locker and any errors that may occur. The GSM module is used to send alerts to the user's mobile phone in case of any unauthorized access attempt [12, 13].

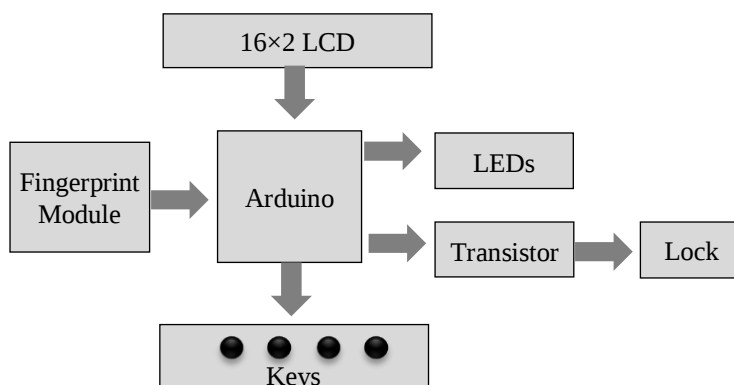


Figure 1. Block Diagram of the System.

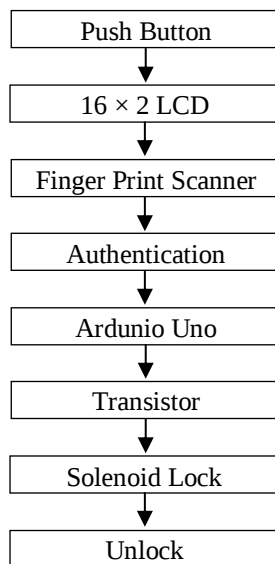


Figure 2. Flow Chart of the proposed system.

In Figure 2, when a saved finger is placed at the fingerprint module, the gate (a solenoid lock) that we have utilised will open. The user must first enrol their finger with the aid of push buttons or keys. Pressing the ENROL key will cause the LCD to ask for the user's location and ID, where their finger will be a store. Thus, the user must now utilise the UP/DOWN keys to enter ID (Location). After choosing Location/ID, the user must hit the OK key (DEL key). The LCD will now request that a finger be placed over the fingerprint module. Currently, the user must place his finger over the fingerprint module. The LCD will then prompt you to take your finger out of the fingerprint module and urge you to put it back in. Now user needs to put his finger again over fingerprint module. The fingerprint module now uses an image to create templates, which it then saves in its memory according to a chosen ID. The user can now unlock the lock by pressing the MATCH key (UP/Down key) with the same finger that they added or registered in the system.

Here, the circuit diagram of this project is shown in Figure 3. This Arduino Biometric authentication system is a very straightforward circuit that consists of an LCD, a push button, a transistor, and an Arduino, which manages the entire project. Arduino controls the complete process.

Fingerprint Sensor

The fingerprint data is accurately captured by the solid-state fingerprint sensor. It is made to be integrated into gadgets for increased convenience and security. The sensor offers a dependable, efficient, and intuitive substitute for PINs, passwords, and other user identification methods.

Energy Source

The regulated power supply provides the circuit's input. The transformer steps down the AC input, or 230 V from the mains supply to 12 V, which is then sent to a rectifier. The rectifier produces a pulsing DC voltage as its output. Therefore, the rectifier's output voltage is sent through a filter to eliminate any remaining AC components in order to obtain a clean DC voltage. This voltage is now applied to a voltage regulator in order to produce a clean, steady DC voltage.

Microcontroller

The project's core is an AVR microcontroller. Embedded C is the programming language utilised. Developed by Atmel in 1996, the AVR is an 8-bit RISC microcontroller on a single chip, based on the modified Harvard design. Unlike other microcontrollers of the era, which used one-time programmable ROM, EPROM, or EEPROM, the AVR was among the first microcontroller families to employ on-chip flash memory for programme storage.

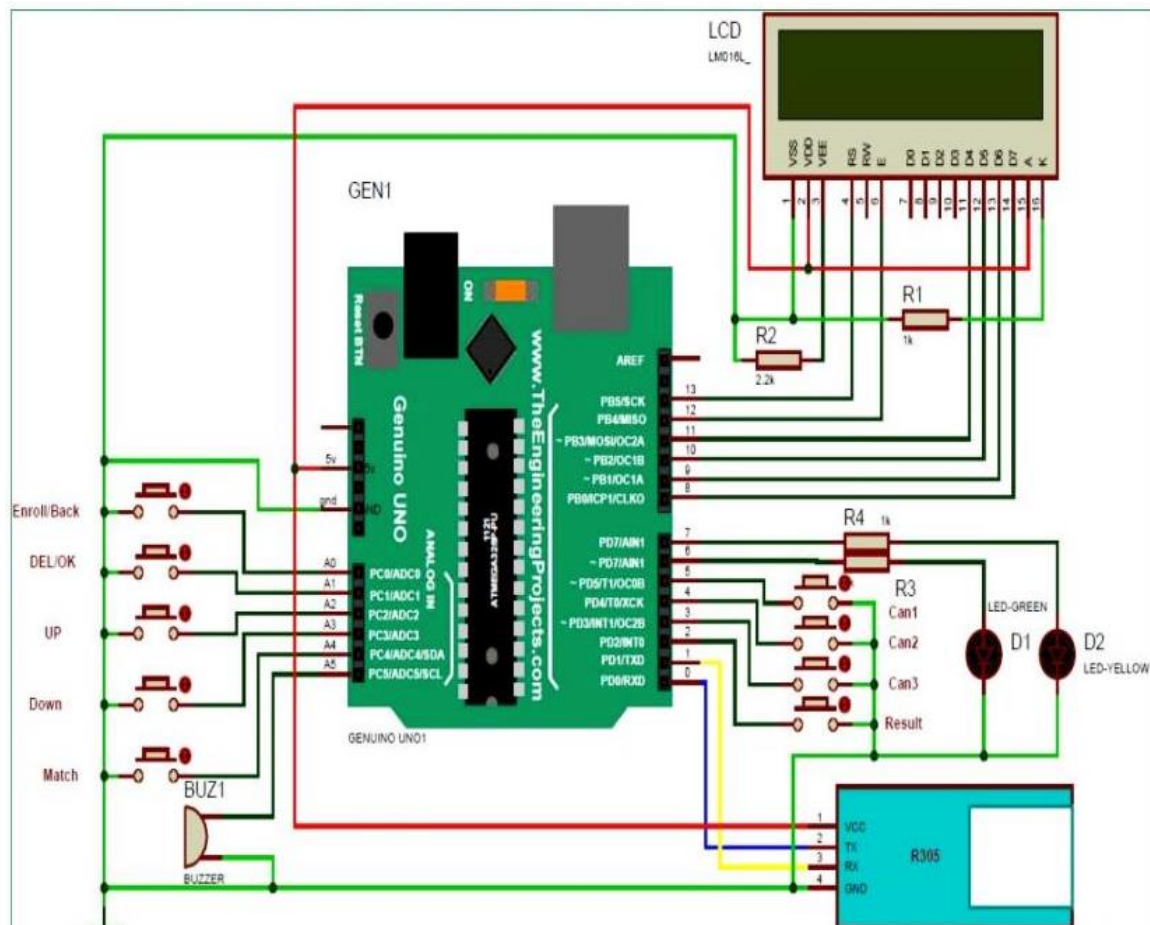


Figure 3. Circuit Diagram of the proposed system.

RESULTS

The proposed system was tested in a laboratory environment, and the results were found to be highly satisfactory shown in Figure 4. The system was able to recognize the user's fingerprint accurately and grant access to the locker. The system was also able to detect any unauthorized access attempts.

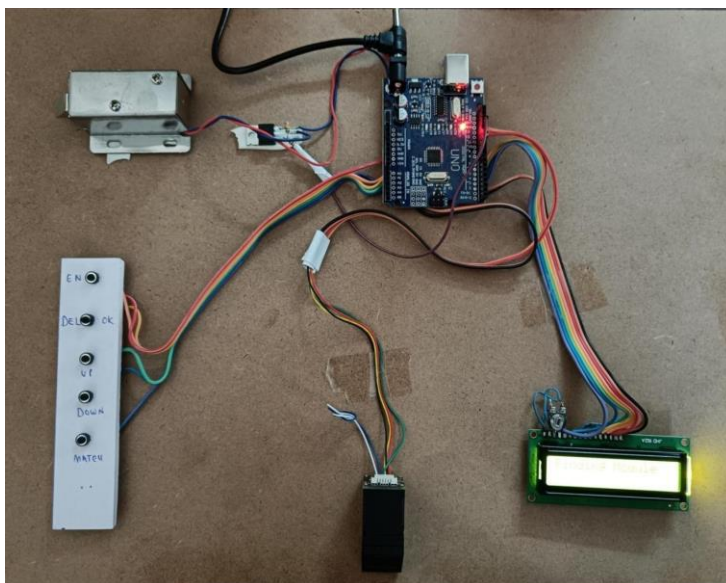


Figure 4. Image of Final Project.

CONCLUSION

The proposed fingerprint-based bank locker system using Arduino provides enhanced security features for users. The system eliminates the need for traditional keys and utilizes biometric identification to grant access to the locker. The system is highly secure and user-friendly, making it a suitable solution for banks and other financial institutions. To improve the system's features and capabilities, more advancements can be made through development and the addition of features like extra locks to the system would improve this concept. Therefore, if a lock can be used to control multiple doors, we won't need to spend as much money on multiple. It might have been possible to create a system that saves prints without using a computer, but it would have needed more parts than we did.

The entire mechanism needs to be mounted on the opposite side of the door or inside the door panel to guarantee sufficient security. It is also possible to create a battery system or even use solar power. This system's adaptability is one of its key benefits. This system can be used with several other systems. The system is very secure. Since each fingerprint is distinct, the sensor can recognise every print while being tested. It provides greater control for access to restricted places.

REFERENCES

1. Reddy JH, Sundar BJ, Evangeline CS, Supragna GB, Evangelin KP. IoT Based Triple Way Access Control for Secured Asset Storage. In 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS) 2023 Mar 17 (Vol. 1, pp. 1923–1928). IEEE.
2. Pooja K M, Chandrakala K G, Nikhitha M A, Anushree P N, 2018, Fingerprint Based Bank Locker Security System, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCESC–2018 (Volume 6–Issue 13).
3. Kashaboina Radhika and Ramasamy Dr Velmani 2020 IOP Conf. Ser.: Mater. Sci. Eng. 981 042009.
4. Shweta S. Joshi, Vinayak Ekke, Pankaj Yedurkar, Ajit Lokhande, "Locker Security System using GSM and Random Password", International Journal of Advanced Research in Electronics and Communication Engineering (IJARECE) Volume 4, Issue 04, April 2015.
5. Parul L. Chandanshive, Varsha V. Chavan, Shital D. Jare. Bank Locker Security System Based on GSM and RFID. International Journal of Research in Engineering and Science. Volume 9 Issue 3. 2021. PP. 30–33.
6. Hiloni S. Detroja, Disha D. Kotadiya, Prutha J. Vasoya, Prof. C. B. Bambhroliya. GSM Based Bank Locker Security System using RFID, Password and Fingerprint Technology. IJIRST –International Journal for Innovative Research in Science & Technology. Volume 2. Issue 11. April 2016. 110–115.
7. Subhash H. Jadhav, S. S. Agrawal. Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology. International Journal of Science and Research. October 2016; Volume 5 Issue 10, 1920–1925.
8. R. Alagu leela, A. Anandhajothei, P. Selvakumari. GSM BASED AUTHORIZED ACCESS WITH SEPARATE USER PASSWORD DOOR LOCK AND UNLOCK CONTROL SYSTEM. International Journal of Electrical and Electronics Engineers. Volume 07, Issue 01, Jan-June 2015. 388–391.
9. Dr. Rajasekaran. A, C. Sai Keerthan, A. Manikanta, D. Sathvikh. Voice Identification based Bank Locker Security System. International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering. Vol. 10, Issue 3, March 2022; 5–9.
10. Prafull Bhatt, Hasan Raza, Hemant Pratap, Rishi Kumar Gupta. GSM Module Technology: A Boon for Advance Security Systems. International Journal of Optical Sciences. 2021; 7(2): 22–26.
11. Mittal Y, Varshney A, Aggarwal P, Matani K, Mittal VK. Fingerprint biometric based access control and classroom attendance management system. In 2015 Annual IEEE India Conference (INDICON) 2015 Dec 17 (pp. 1–6). IEEE.
12. Alothman B, Joumaa C, Alotaibi A, Alotaibi B, Almutairi B, Aldhafairi A, Khan M. Development

- of an electronic smart safe box using private blockchain technology. *Applied Sciences*. 2022 Jun 24;12(13):6445.
13. Nivethika SD, Pandian MS, Parameswaran NG, Elakiya E, Naresh M, Dhamodharan S. Arduino UNO Based OTP Lock for Integrated Home Security System. In 2023 2nd International Conference on Edge Computing and Applications (ICECAA) 2023 Jul 19 (pp. 1342–1347). IEEE.