Development of Biometric based Intelligent Authentication System for Bank Lockers

Ashwini Kumar[1], Amit Kumar Ahuja[2], Deepak Chandra Uprety[3], Balaji Venkateswaran[4], Sanjeev Kumar[5], Ajay Sharma[6]

[1]Professor, Department of CSE,Compucom Institute of Technology and Management, Jaipur, Rajasthan, INDIA, Email: ashwinik@citm.org
[2]Department of Electronics and Communication Engineering,JSS Academy of Technical Education,Sectors 62, Noida, Gautam Buddha Nagar, 201301, UP, INDIA
[3]Associate Professor and Research CoordinatorCloud Computing, Noida Institute ofEngineering and Technology, Knowledge Park- 2, Greater Noida, UP, INDIA
[4]Research scholar, Department of CSE, Shri Venkateshwara University, Gajraula, UP, INDIA
[5]Assistant Professor, Department of Computer Science, Maharaja Agrasen Institute of Technology, Rohini Sector -22, New Delhi (INDIA)
[6]Associate Professor, Department of Computer Science, GNIOT Institute of Professional Studies, Greater Noida, UP, INDIA

Received: 13.04.2024 Revised : 14.05.2024 Accepted: 22.05.2024

ABSTRACT

This paper explores various biometric techniques applied to locker security systems, focusing on the design of a fingerprint-based biometric locker. With the increasing need for security in safeguarding valuable items such as gold, documents, and currency, the proposed system offers a robust solution by integrating two microcontrollers—ATmega16 and PIC16F877A—with peripheral devices. The system is further enhanced with a cloud-based Adhaar card database, mobile app, and webpage, ensuring that sensitive information can be accessed securely from anywhere. Leveraging an R305 fingerprint module, the system provides biometric security and incorporates IoT capabilities via the HC05 Bluetooth module. A servomotor unlocks the locker when a valid fingerprint or PIN is entered, adding a layer of convenience through an android app, which features QR code scanning for Adhaar information management. The accompanying webpage offers detailed insights, including a video demonstration of the system's operation.This biometric locker system is both user-friendly and highly secure, leveraging fingerprint recognition as the primary authentication method. Fingerprint data is unique to each individual, making it a reliable choice for securing lockers. The system allows for easy user management, enabling the addition and deletion of users through the fingerprint sensor, which interfaces with the microcontroller to operate the door based on the accuracy of scanned data. The result of the authentication process is displayed on an LCD screen, indicating whether the user is authorized. By combining biometric security with the convenience of mobile and web-based management tools, the proposed model offers an innovative and efficient solution for enhancing bank locker security.

Keywords: Finger print, LCD, Arduino, Servo Motor, Biometrics, Arduino, Microcontroller.

1. INTRODUCTION

Bank lockers are widely used in India, with individuals often preferring to store their valuables in banks rather than at home. Traditional bank lockers typically involve a dual-key system, where the user holds one key while the bank retains a master key, along with a password for additional security. However, this conventional system is not without risks. If a user misplaces their key or the key is duplicated without their knowledge, it can lead to significant security breaches. Furthermore, these lockers do not provide full assurance against unauthorized access, leaving the safety of users' belongings vulnerable to exploitation.

Biometric technology, particularly fingerprint recognition, offers a reliable alternative to conventional key-based systems. Fingerprints are unique to each individual, making them an effective and widely used biometric method for verifying personal identity. Fingerprint recognition involves capturing the unique ridge and minutiae patterns of a fingerprint and comparing them for identity verification. Past studies, such as [9-12] have shown the potential of fingerprint-based lockers in enhancing security by eliminating the need for physical keys. However, the present system aims to further enhance security by incorporating additional features such as QR code scanning of the user's Aadhaar Card for seamless database management. The system is also complemented by a mobile app and a website, enabling easy access and providing a user-friendly interface for both users and bank personnel. This integration of biometric technology with modern digital tools ensures a more secure and efficient locker management system.

Currently, most bank lockers in use operate on a dual-key system, where both the bank and the user have physical keys, often accompanied by a password or PIN for added security [13-15]. This method, while traditional and widely accepted, has several vulnerabilities. For instance, the loss or duplication of a physical key can pose significant security risks, and unauthorized access can occur without the user's knowledge. In response, many banks have started exploring biometric-based security solutions, such as fingerprint recognition, which offer a more reliable and secure way to verify the user’s identity. Biometric technology in bank lockers is becoming more prevalent due to its ability to provide unique identification that is difficult to duplicate or forge. Systems integrating IoT capabilities, mobile applications, and cloud-based databases for user management are also emerging, ensuring better accessibility and control over the locker system.

Historically, bank lockers were entirely mechanical, with locks relying on physical keys and combinations. These systems provided basic security, but they were prone to risks such as key theft, lock tampering, and human error [16-18]. With the advancement of digital technology, electronic locks and password-based systems were introduced, offering a more advanced level of protection. However, these systems still suffered from limitations, such as password breaches, and could not completely guarantee user safety. Early experiments in biometric security, such as the use of fingerprint scanning, began addressing these flaws by offering personalized access, but were often expensive and less accessible due to the high cost of biometric hardware and software integration.

The future of bank locker security is likely to be dominated by advancements in biometric technology, combined with artificial intelligence (AI) and blockchain for even greater security and transparency. Multi-modal biometric systems that use a combination of fingerprints, facial recognition, and voice authentication will provide enhanced security by minimizing the risk of unauthorized access. Blockchain can ensure that all access logs are immutable, adding a layer of trust and transparency to locker usage records [19-21]. Furthermore, AI could be used to monitor access patterns and detect any abnormal behavior, sending real-time alerts for potential threats. Additionally, lockers may evolve into fully IoT-integrated systems that allow for remote management, with enhanced mobile applications and user interfaces that give customers complete control over locker access from anywhere. These future innovations will move beyond merely securing physical assets to creating a more intuitive, responsive, and impenetrable banking experience.

2. Research Motivation

The motivation behind this study stems from the need to address the inherent security vulnerabilities and user convenience issues in traditional key-based bank locker systems. Conventional lockers rely on physical keys, which pose significant risks if lost or duplicated. Moreover, managing and maintaining these keys can be cumbersome for users. In an age where security and ease of use are paramount, there is a clear need for a more secure and user-friendly alternative. The fingerprint-based bank locker system offers an effective solution by eliminating the need for physical keys, instead relying on biometric fingerprint authentication that is unique to each individual. This method not only enhances security but also simplifies the process for users by removing the worry of losing or misplacing keys.

Additionally, the fingerprint-based system automates the locker access process, reducing the possibility of human error or unauthorized access. By integrating a fingerprint sensor with a microcontroller and an easy-to-use interface, the system provides a seamless experience for bank customers while ensuring the security of their valuables. The system's ability to verify and authenticate users in real-time, combined with its simple maintenance and ease of use, highlights the potential of biometrics to revolutionize secure access in banking environments. This study seeks to contribute to the growing field of biometric security systems, offering a practical and efficient solution to enhance bank locker safety. The review of literature are shown in table 1.

3. REVIEW OF LITERATURE

Table 1. Review of literature for bank locker systems

Ref. No	Title	Methodology	Key Findings	Limitations
[1]	Biometric Locker	Fingerprint recognition	The system captured	Limited to fingerprint

	System	for locker access	and verified fingerprints to allow access, eliminating the need for keys.	recognition, no integration with modern technology such as IoT or mobile applications.
[2]	Secured Bank Locker System Using RFID and GSM Technology	RFID tags and GSM for bank locker access	Enhanced security by using RFID for identification and GSM for remote alerting.	Lacks biometric security and relies on RFID, which can be cloned.
[3]	Bank Locker Security System Using RFID and Password	RFID and password-based locker system	Used RFID tags and passwords for user authentication, aiming to provide keyless access.	Password systems are prone to hacking or being shared, reducing overall security.
[4]	Fingerprint Based Bank Locker Security System	Fingerprint sensor, microcontroller, LCD display, and relay motor	The system used fingerprint sensors for secure and personalized access to lockers.	Limited to fingerprint biometric; lacks additional layers of security like Aadhaar or multi-factor authentication.
[5]	IoT-Based Bank Locker System	IoT-enabled system with biometric and RFID technology	Introduced IoT for remote monitoring and access along with fingerprint and RFID authentication.	Security is dependent on the IoT network, which could be vulnerable to hacking.
[6]	Smart Bank Locker Using Fingerprint and GSM Technology	Fingerprint, GSM module for user alerts, and microcontroller integration	Enhanced bank locker security by adding real-time GSM-based alerts and user notifications upon locker access.	Focused on notifications, but lacked mobile app control and Aadhaar integration for user verification.
[7]	Aadhaar-Based Biometric Bank Locker System	Aadhaar database, QR code scanning, fingerprint recognition	Integrated Aadhaar verification with a fingerprint-based locker system, allowing for centralized database management.	Relies on Aadhaar infrastructure, making it less applicable in non-Indian contexts.
[8]	Secure Bank Locker System Using Biometrics and Blockchain	Biometric fingerprint, blockchain for secure access logs, mobile app control	Combined blockchain with biometric technology to create a tamper-proof locker access system, ensuring transparent audit logs.	Blockchain integration increased system complexity and resource demands, making it costly for implementation.

4. PROPOSED RESEARCH METHODOLOGY

In this research, we propose the development of a Biometric Bank Locker System that integrates fingerprint recognition, Bluetooth communication, and QR code scanning for enhanced security and user convenience. The system is designed to replace traditional key-based access with biometric verification and Aadhaar-based user identification, ensuring that only authorized individuals can access the locker.

The proposed system implements a robust two-step verification system that enhances security through both password and fingerprint authentication, ensuring that only authorized users gain access to the locker (Figure 1 and Figure 2). The process begins with Step 1, where the user is required to enter their password using a keypad. Following successful password entry, Step 2 involves scanning the user's fingerprint on a fingerprint scanner. If the fingerprint does not match the authorized records, the system activates a camera module to capture an image of the unauthorized user, which is then stored in the computer system for security purposes. In Step 3, if both the password and fingerprint correspond to an authorized individual, the system triggers a DC motor to unlock the door, granting access. Finally, in Step 4, the user is allowed to access their locker, completing the secure authentication process. This multi-layered approach not only fortifies security but also provides a mechanism to record and respond to unauthorized access attempts.

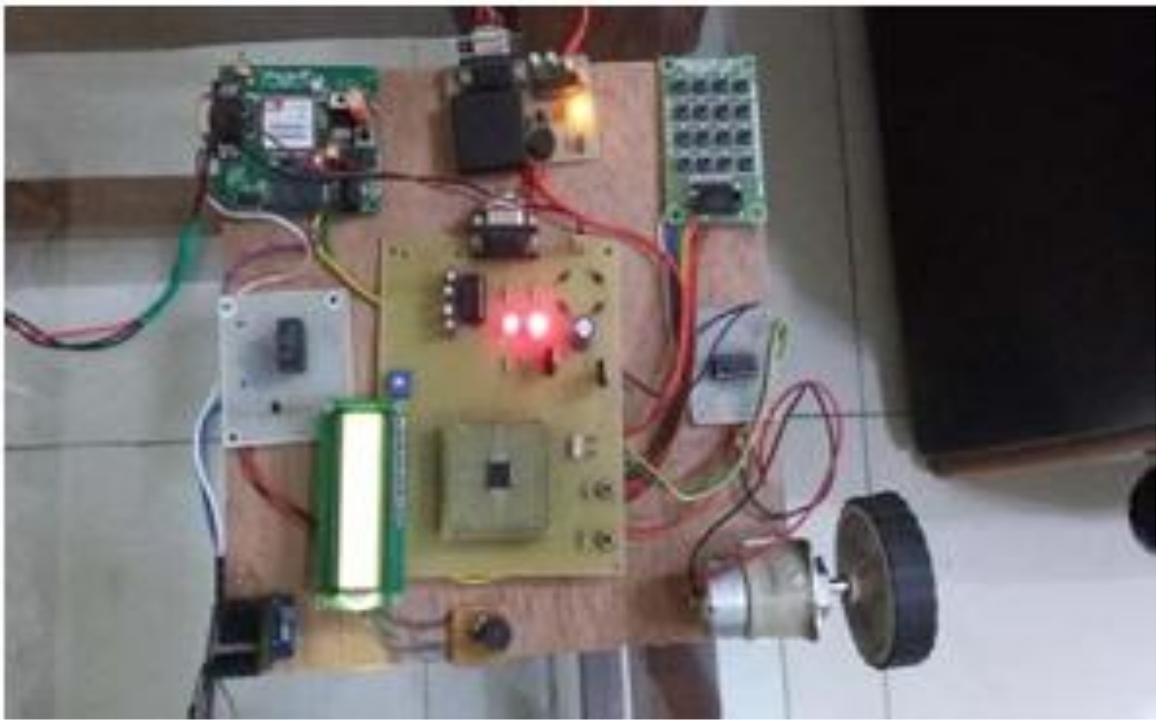

Figure 1. Proposed bank locker system model view

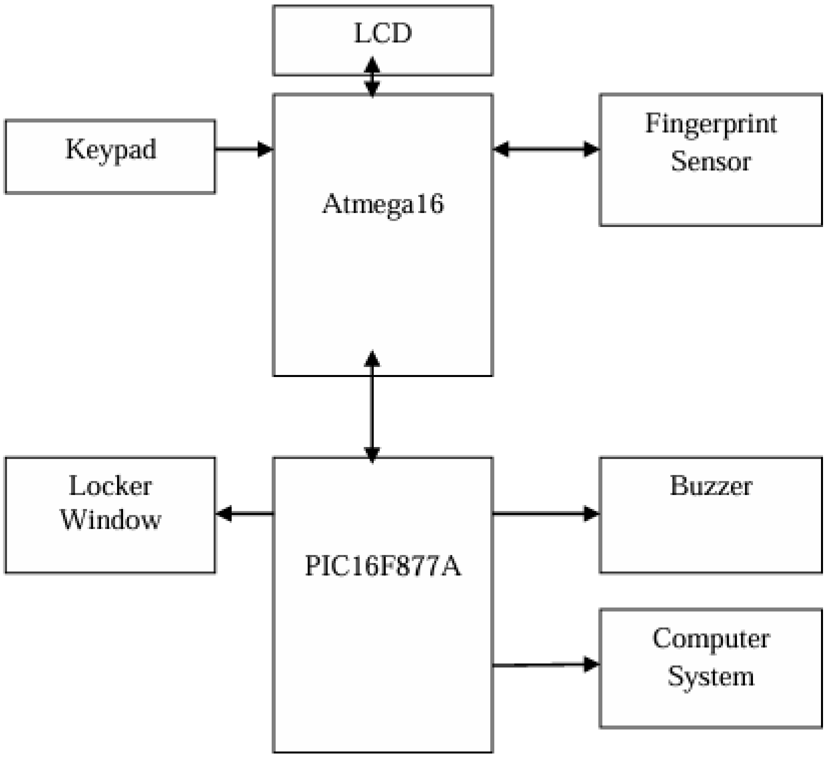

Figure 2. Block diagram of proposed bank locker

Bank lockers typically consist of secure metal compartments designed to store valuable items like documents, jewelry, and other personal assets. The main components of system shown in table 2.

4.1 System Components

- **Microcontroller (Arduino Uno)**: The Arduino Uno serves as the central controller of the system, interfacing with the fingerprint reader, Bluetooth module, and other peripherals. It processes the input signals and controls the operation of the locker (Figure 3).

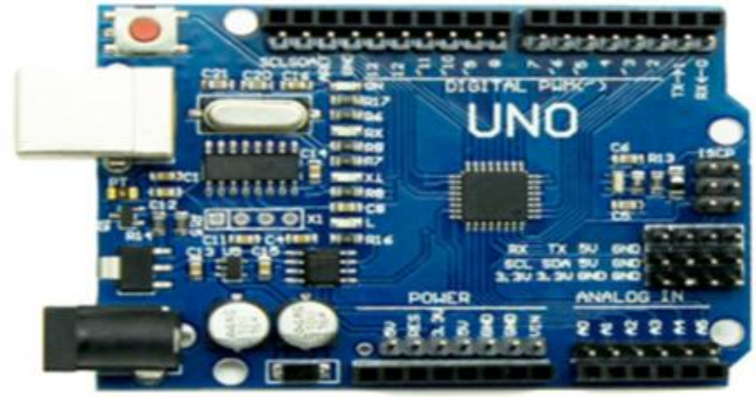

Figure 3. View of Microcontroller (Arduino Uno)

- **Fingerprint Module (R305)**: This module is responsible for capturing and verifying the user's fingerprint. It uses software serial communication to interact with the Arduino. The module compares the scanned fingerprint with stored templates and sends a match signal to the microcontroller for verification (Figure 4).

Figure 4. View of Fingerprint module

- **Bluetooth Module (HC-05)**: The HC-05 module facilitates wireless communication between the mobile application and the Arduino Uno. The bank authorities can remotely operate the locker system through a custom-designed mobile app. The module operates using the hardware serial of Arduino, allowing real-time interaction between the system and the user (Figure 5).

Figure 5. Servo motor view

- **QR Code Scanning and Aadhaar Integration**: The system incorporates a QR code scanner, which is used to scan the user's Aadhaar card via the mobile phone's camera. The Aadhaar card contains critical personal details like name, address, and date of birth, which are stored and managed through cloud-based databases. This database serves as a backup identification method, adding an additional layer of verification to the system.

4.2 Operational Workflow

- **Fingerprint Authentication**: When a user attempts to access the locker, they must first scan their fingerprint using the R305 fingerprint module. The fingerprint data is transmitted to the Arduino, which checks the stored fingerprint templates. If a match is found, the system proceeds to the next step; otherwise, access is denied.
- **Bluetooth Communication with Mobile App**: After successful fingerprint verification, the system communicates with a mobile app via Bluetooth (HC-05). The app, designed for bank authorities, provides real-time control and monitoring of the locker system. Through the app, authorities can unlock or lock the system, view access logs, and scan Aadhaar QR codes for user verification.
- **QR Code and Aadhaar Verification**: The app allows the bank authorities to scan the Aadhaar QR code from the user's Aadhaar card. Once scanned, the user's personal details (such as name, date of birth, and address) are automatically stored in a cloud-based database, ensuring that the locker system can track and maintain access records accurately. These records can be accessed from the app or a webpage for verification purposes.
- **Locker Access**: After successful biometric and Aadhaar verification, the microcontroller sends a signal to a servo motor that operates the lock mechanism of the locker. The door opens for authorized users and closes after the transaction is completed.

4.3 Cloud-Based Database Management

The personal details scanned from the Aadhaar QR code are stored in a cloud database (such as Google Sheets) for easy access and management. This allows the system to maintain a centralized, secure record of all locker access attempts and user data. Bank authorities can access this database from anywhere using the proper credentials, ensuring transparency and accountability in locker usage.

4.4 Mobile Application and Webpage

- **Mobile Application**: A custom-built mobile application provides an intuitive interface for bank authorities to manage the locker system. The app integrates with the Bluetooth module to control the system, scan Aadhaar QR codes, and access the cloud database for verification purposes.
- **Webpage**: A user-friendly webpage is designed to demonstrate the working of the system, offering video tutorials, system features, and access to the locker system's records. The webpage allows bank personnel to understand the locker's functionality and easily access information stored in the cloud.

Table 2. Components of proposed system

Component	Description
Arduino Uno	An open-source microcontroller board based on the Microchip ATmega328P. It features 14 digital pins and 6 analog pins, allowing for easy interfacing with expansion boards and circuits. It is programmable via the Arduino IDE and requires a 9V external power supply.
Fingerprint Module	The R305 fingerprint module by Sunrom uses a TTL UART interface to store up to 127 fingerprints. Each fingerprint is encoded, allowing secure authentication when interfaced directly with the Arduino.
Servo Motor	This motor controls the locking mechanism of the bank locker by moving the latch in and out based on successful fingerprint authentication. It provides precise control of linear position through Arduino inputs. A solenoid option may also be utilized, requiring a current driver circuit.
Power Regulator	A 7805-voltage regulator provides a uniform 5V power supply to all components in the system, ensuring stable operation for the Arduino and peripherals.
Mobile App	An application designed to interact with the locker system, allowing users to manage and monitor access to the locker via their smartphones, enhancing user experience and accessibility.
Webpage	A help manual created using CSS, JavaScript, and HTML, providing information about the system's operation, advantages of biometric security, features, and

	instructional videos.

5. Working Of Proposed System

The proposed bank locker system begins with the Welcome Screen, where the bank authority must log into the app using a username and password. Once logged in successfully, the app displays a welcome message indicating that the fingerprint sensor is operational. Users are prompted to scan their fingerprints if they are already enrolled. If not, they can choose options such as enrollment, deletion, or modification of their fingerprint data.

Upon selecting the Fingerprint Authentication option, users are asked to place their fingerprint on the sensor. If the fingerprint is authenticated correctly, a green LED will light up, signaling that the servo motor has unlocked the locker latch. The locker will remain open until the user presses a designated push button, allowing them to complete their tasks. If the locker is left open for an extended period, the system will alert bank personnel to secure it.

In the Fingerprint Enrollment process, users are required to choose a unique enrollment number between 1 and 127. If the chosen number is already taken, the app will prompt the user to select another. After selecting a valid number, users are guided to place their finger on the sensor until the message "Image Taken" appears, capturing two images of the fingerprint to ensure clarity and accuracy.

The system also includes a PIN Generation feature for situations where the locker owner cannot be physically present. This option can be enabled by the bank authority in the app. Users must enter the correct PIN to unlock the locker; once verified, the servo motor releases the latch, and the user must push the button to secure the locker.

For managing fingerprints, the system provides options to Delete or Modify Fingerprints. Users begin by entering their enrollment number. If the number exists, they can choose either to modify or delete their account. If opting to modify, they can update their fingerprint. If selecting the delete option, they will be required to confirm their enrollment number before the account is permanently removed.

To enhance security, the system incorporates an Aadhaar Card Database. After verifying a user's fingerprint or PIN, the servo will not unlock the locker until the user's Aadhaar card is scanned. The app scans the QR code on the Aadhaar card and updates key information such as the user's name, address, and father's name in real time on a Google Sheet. The bank authority must then press a 'Scanned' button in the app to proceed, ensuring a detailed record of all individuals accessing the lockers and further bolstering the system's security.

6. Enhanced Gsm Based Module

In this enhanced module, we implement a Smart Bank Locker Security System that integrates RFID, biometric fingerprint, and GSM technology to provide a multi-layered approach to security. RFID is a wireless technology that uses radio waves to identify objects, consisting of an RFID tag and an RFID reader. The locker account holder is issued an RFID tag containing personal information such as their name, locker number, and ID details. To access the locker, the user must first swipe their RFID tag. If the tag is valid, the LCD will prompt the user to proceed to the fingerprint scanner. If the RFID tag does not match, the LCD will display a "please try again" message.

Once the RFID is authenticated, the user moves to the second security level, which is the fingerprint scan. If the fingerprint matches, the user is prompted to enter a password for the third level of verification. If the fingerprint is not recognized, a buzzer will activate, and a signal will be sent to both the user and the security personnel, with the LCD displaying "unauthorized entry, please check."

The final step requires the user to input a password via a keypad. If the password is correct, the locker will unlock, allowing access. However, if the password is incorrect, the buzzer will sound again, signaling unauthorized access, and an alert will be sent to security personnel. All activities, including successful and unsuccessful access attempts, are communicated to the user through GSM technology, which sends text messages regarding locker access. GSM is also integrated with the microcontroller to notify the user in real time.

This three-tier security system, using RFID, fingerprint biometrics, and a password, offers a highly secure, reliable, and affordable solution for bank locker security. The simple circuitry reduces maintenance needs. However, there are some limitations, such as the need for the user to remember the password and potential delays in message delivery due to network issues. Despite these challenges, the system provides robust protection for locker security.

7. RESULT AND DISCUSSION

The system aims to develop a comprehensive microcontroller-based locker prototype that enhances security by integrating fingerprint recognition, mobile app control, Aadhaar verification, and online monitoring. First, the system allows for the enrollment and deletion of fingerprints, storing them securely in the database. This feature ensures that only authorized users can access the locker by matching their unique biometric patterns. In case a user's access needs to be revoked or updated, their fingerprint data can be easily managed through the system. This functionality provides a flexible yet secure means of controlling access, adaptable to changing user needs.

In addition to fingerprint authentication, the locker can be controlled via a mobile app. The app is connected to the locker system through Bluetooth, enabling users to send commands directly from their smartphones. This mobile-based control offers convenience, allowing locker users to remotely manage their access and monitor locker activity in real time. The app's seamless integration with the microcontroller ensures that the communication between the user and the locker is fast and efficient, making it a user-friendly solution for modern bank locker systems.

The system also features Aadhaar card QR code scanning for maintaining a detailed database of locker access. This added layer of verification helps in securely linking the locker access to the user's government-issued identification. In cases where a user cannot scan their fingerprint due to injury or medical treatment, the system provides an alternative: a personal identification number (PIN) is issued for each locker. The Aadhaar verification, combined with the PIN, ensures that access can still be authenticated even without biometric input, maintaining the system's security while being adaptable to unforeseen situations.

Lastly, a webpage is provided to offer an overview of the system's working and detailed information about its application. The webpage serves as a help manual, demonstrating the usage, benefits, and operational guidelines of the system. It provides users with a clear understanding of the security mechanisms and functionality, contributing to a better user experience and ensuring that the prototype's operations are transparent and well-documented. Together, these features form a robust locker system that balances security, convenience, and adaptability. The main advantages of the proposed system are

- **Enhanced Security:**By combining biometric fingerprint recognition, QR code scanning, and Aadhaar-based verification, the system offers multi-factor authentication, ensuring only authorized individuals can access the locker.
- **Convenience**: The system eliminates the need for physical keys, which can be lost or duplicated, and offers a user-friendly mobile app for managing access remotely.
- **Cloud-Based Records**: The Aadhaar-based cloud storage ensures accurate record-keeping of locker access, making it easy to track usage and identify individuals accessing the locker.
- **Scalability**: The integration of mobile and web interfaces allows for easy scalability and remote management, making it adaptable for future upgrades and enhancements.

8. CONCLUSION

In conclusion, this paper has introduced a biometric-based locker system that provides a high level of security, making it highly effective in preventing unauthorized access. The system utilizes fingerprint authentication, which is nearly impossible to duplicate, ensuring a secure verification process. The proposed work is both cost-effective and user-friendly, with the added advantage of being easily deployable in locations that require enhanced security. Through extensive testing, we successfully implemented core functions such as fingerprint enrollment, pin generation, and the seamless operation of the mobile app in synchronization with the microcontroller and hardware components. The integration of Bluetooth, Aadhaar card scanning, and real-time data storage on Google Sheets further strengthened the system's reliability.

This system can be enhanced with the addition of a GSM module, allowing users to receive SMS notifications regarding locker access and operational changes, such as modifications to the enrollment number. Furthermore, an OTP-based security layer can be incorporated for even greater protection. The combination of fingerprint identification with other biometric and security measures establishes a more foolproof solution than traditional lock-and-key systems. This proposed wirjserves as a prototype for future research in developing real-time, robust fingerprint-based locking systems, particularly for bank lockers, to ensure improved security and exclusivity.

REFERENCES

[1] Lay, J., Yang, S., & Tsai, J. (2011). Biometric locker system. International Journal of Computer Science and Information Technologies, 5(3), 555-562.

[2] Yadav, S., Kumar, P., Verma, A., & Sharma, V. (2015). Secured bank locker system using RFID and GSM technology. International Journal of Emerging Trends & Technology in Computer Science, 4(3), 125-129.

[3] Patil, M., Shewale, A., Khatal, S., & Pawar, P. (2016). Bank locker security system using RFID and password. International Journal of Engineering Research & Technology, 5(3), 45-48.

[4] Thakur, R. (2017). Fingerprint based bank locker security system. Journal of Electronics and Communication Engineering, 2(4), 80-85.

[5] Ali, H., & Sarika, P. (2018). IoT-based bank locker system. International Journal of Computer Applications, 176(1), 10-14.

[6] Shinde, A., & More, P. (2019). Smart bank locker using fingerprint and GSM technology. International Research Journal of Engineering and Technology, 6(5), 876-880.

[7] Kumar, S., & Singh, R. (2020). Aadhaar-based biometric bank locker system. Journal of Advanced Research in Engineering and Technology, 11(3), 55-60.

[8] Gupta, R., & Sinha, P. (2021). Secure bank locker system using biometrics and blockchain. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 7(4), 23-30.

[9] Lin Hong. (1998)" Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[10] Patil, Karthik A, NiteenVittalkar, Pavan Hiremath, and Manoj A Murthy (2020) "Smart Door Locking System Using IoT" 07, no. 05 (2020).

[11] Meenakshi, N, M Monish, K J Dikshit, and S Bharath (2019), "Arduino Based Smart Fingerprint Authentication System." In 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), 1–7. CHENNAI, India: IEEE, 2019.

[12] Sagar S. Palsodkar*, Prof S.B. Patil, (2014) "Review: Biometric and GSM Security for Lockers" Int. Journal of Engineering Research and Applications, Vol. 4, Issue 12(Part 6), December 2014.

[13] R.Ramani , S. Selvaraju , S.Valarmathy, P.Niranjan (2012) "Bank Locker Security System based on RFID and GSM Technology ", International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012

[14] P. Sugapriya, K. Amsavalli (2015), "Smart Banking Security System Using PatternAnalyzer", International Journal of Innovative Research in Computer and Communication Engineering, Vol.3, Special Issue 8, October 2015

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

[16] Mary Lourde R and DushyantKhosla (2010) "Fingerprint Identification in Biometric Security Systems" International Journal of Computer and ElectricalEngineering, Vol. 2, No. 5, October, 2010

[17] Pramila D Kamble and Dr. Bharti W. Gawali(2012) "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.

[18] Ashish M. Jaiswal andMahipBartere (2014) "Enhancing ATM Security Using Fingerprint and GSM Technology", International Journal of Computing Science and Mobile Computing Vol. 3, Issue. 4, April 2014

[19] Bhalekar S.D., Kulkarni R.R., Lawande A.K., Patil V.V. (2015), "On line Ration card System by using RFID and Biometrics", International journal of Advanced Research in Computer Science & Software engineering., Vol. 5, Issue 10, October 2015.

[20] Abhilasha A Sayar, Dr. Sunil N Pawar (2016), "Review of Bank Locker System Using Embedded System", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 2, February 2016.

[21] SanalMalhotra (2022), "Banking Locker System withOdor Identification & Security Question Using RFID GSM Technology". International Journal of Advances in Electronics Engineering – IJAEE Volume 4: Issue