INTERNATIONAL JOURNAL OF ELECTRONICS AND COMPUTER APPLICATIONS

ORIGINAL ARTICLE

Article access online

OPEN ACCESS

Received: 29.03.2025

Accepted: 03.07.2025

Published: 19.07.2025

Citation: Dabewar S, Gupta A, Ajgonkar S, Laturkar A. (2025). Multi-level Secure Bank Locker . International Journal of Electronics and Computer Applications. 2(1): 60-64. https://doi.org/10.70968/ijeaca.v2i1.E1018

* **Corresponding author**.

aparna.laturkar@moderncoe.edu.in

Funding: None

Competing Interests: None

ISSN
Print: XXXX-XXXX
Electronic: 3048-8257

Multi-level Secure Bank Locker

Sachin Dabewar[1], Anuj Gupta[1], Shubham Ajgonkar[1], Aparna Laturkar[1]*

1 Department of Electronics and Telecommunication, Progressive Education Society's Modern college of Engineering, Pune, Maharashtra, India

Abstract

In today's world, the security of bank lockers is paramount due to increasing instances of theft and unauthorized access. This project addresses the challenge of enhancing locker security by developing a Multi-level Secure Bank Locker System. The system integrates several advanced technologies, including RFID for user authentication, a sound sensor to detect tampering attempts, and a SIM800L GSM module for real-time alert notification Additionally, a fingerprint sensor is used to ensure biometric security, while a keypad matrix allows for PIN verification, further safeguarding access. The novelty of the system lies in its multi-layered security approach that combines hardware components and communication technologies. The ESP32 Micro-controller serves as the central processing unit, managing data flow and communication between the modules. In case of unauthorized access or tampering, the system triggers a buzzer for an immediate alarm and sends an alert via SMS to the owner's registered mobile number or Telegram app. Initial tests of the system demonstrated its robustness in preventing unauthorized access and responding effectively to tampering attempts. The results highlight the practicality of employing multiple security layers, which significantly improves the reliability and safety of traditional bank lockers.

Introduction

In recent years, there has been a notable rise in sophisticated burglary methods, including wall tampering near banks, where intruders attempt to bypass security by physically breaching walls or adjacent structures to access vaults and lockers. Such incidents highlight the growing inadequacy of traditional security systems in protecting valuable assets. Conventional lockers are increasingly vulnerable to security threats, including theft, simple PIN and key-based vulnerabilities, and the absence of real-time alerts. As theft techniques and unauthorized access methods evolve, securing personal and institutional assets particularly in banking environments has become critically important.

Bank lockers, which have traditionally relied on mechanical locks and minimal authentication methods, are often susceptible to breaches. These outdated systems, often dependent on a single form of entry such as a key or PIN, are no longer sufficient to meet modern security standards.

Fortunately, advancements in technology offer new opportunities to significantly enhance locker security through multi-layered authentication and real-time alert mechanisms.

This project introduces a Multi-Level Secure Bank Locker System that integrates several advanced technologies to ensure the safety and integrity of locker contents. The system utilizes Radio Frequency Identification (RFID) for primary user authentication ,fingerprint scanning for biometric verification, sound sensors to detect physical tampering, and a SIM800L GSM module to send real-time alerts to the locker owner during unauthorized access attempts. The ESP32 micro-controller serves as the system's central processing unit, managing communication and coordination between components. By combining RFID, biometric, sensor, and communication technologies, the system provides a robust and intelligent multi-layered defense against intrusion. This approach effectively addresses common vulnerabilities in traditional locker systems, offering a secure, reliable, and cost-effective solution for modern banking environments.

Literature survey

- Smith et al. (2020) explored the integration of various authentication methods like RFID, biometric fingerprinting, and OTP based systems in enhancing the security of physical assets. Their study concludes that combining these layers not only reduces the likelihood of unauthorized access but also significantly increases the complexity for potential attackers, making systems like bank lockers more secure.
- Johnson and Lee (2019) analyze the effectiveness of biometric systems, particularly fingerprint sensors, in secure environments. They argue that fingerprint recognition provides a highly reliable and secure form of access control due to the uniqueness of individual fingerprints, which are nearly impossible to duplicate, making it a strong candidate for applications requiring high levels of security, such as bank vaults and lockers.
- Kumar Chaturvedi et al. (2018) conducted research on tamper detection using sound and vibration sensors in high-security environments. They found that these sensors are highly effective in detecting unauthorized physical attempts to breach security systems. Their implementation in lockers provides an immediate alert mechanism that can thwart break-in attempts before they lead to a full breach.
- Patel and Sharma (2021) focused on the use of GSM technology for real-time notifications in security systems. They demonstrated that integrating GSM modules allows immediate communication between the security system and the user, enabling SMS alerts in case of unauthorized access attempts. This remote monitoring feature enhances user response time and reduces the potential for loss or damage in sensitive systems such as bank lockers.
- Varma and K. Kapoor (2018) conducted research on Cloud-integrated locker systems with GSM alerts. They found that these cloud-integrated locker systems are highly effective in detecting unauthorized physical attempts to breach security systems. Their implementation in lockers provides an immediate alert mechanism that can thwart break-in attempts before they lead to a full breach.
- S. Rao, M. Deshmukh (2017) suggested that "Fingerprint recognition systems provide a highly reliable and precise means of identity verification, capitalizing on the distinctive nature of each individual's fingerprint pattern to deliver a strong and secure access control solution.
- P. Singh, R. Mishra et al. (2022) analyzed that "Real-world applications, such as bank lockers, can benefit from the integration of RFID, biometric fingerprinting, and OTP based authentication. This layered approach creates a robust security system.

Methodology: Proposed System

A. Introduction

The Multilevel Secure Bank Locker System is designed to provide robust security using a four-layered authentication process, significantly enhancing the protection of valuable assets. The first layer involves RFID Scanning, where each authorized user is issued a unique RFID card containing a pre-registered identification code verified by an RFID reader. Upon successful card verification, the user must enter a Personal Identification Number (PIN), adding a secondary layer of security to confirm the cardholder's authenticity.

The third level involves Aadhaar Number Verification, utilizing the 12-digit unique identification number issued by the Government of India, providing a government-backed layer of identity confirmation. The final and most critical stage is Fingerprint Scanning, employing biometric technology to validate the user's identity based on their unique fingerprint patterns. This integrated approach, combining RFID, PIN, Aadhaar, and biometric verification, ensures only legitimate users can access the locker, significantly reducing the risk of unauthorized access.

B. System Overview

Here given a brief overview of Multi-level Secure Bank Locker with the help of block diagram along with detailed explanation of each block defined in Figure 1.

1. Power Supply

Provides power to all the components connected to the system. Delivers appropriate voltage (likely 3.3V or 5V) to the microcontroller and peripherals. Ensures consistent

operation of the entire system.

2. ESP-32

Acts as the central control unit, managing input and output signals from various components. Receives data from the RFID module, fingerprint sensor, keypad matrix, and sound/PIR sensor. Controls the operation of the motor driver, GSM module, buzzer, and display (LCD).

3. RFID Reader Module

Used for the initial authentication of the user by scanning an RFID card or tag. Sends identification data to the micro-controller for processing.

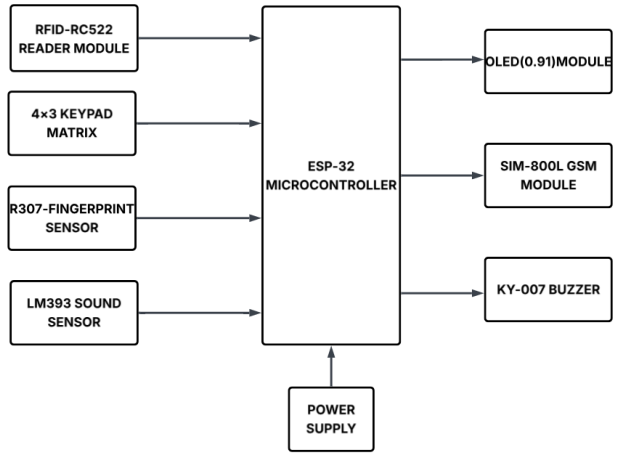

Fig 1. Block Diagram: Multi-level Secure Bank Locker

4. 4x3 Keypad Matrix

Allows users to enter an OTP (One-Time Password) or PIN for secure authentication. The entered data is sent to the microcontroller for validation.

5. Fingerprint Sensor

Provides biometric authentication by scanning the user's fingerprint. Ensures that only authorized individuals can access the locker.

6. Sound Sensor

The sound sensor detects unusual sounds, such as those caused by tampering, while the PIR sensor detects motion. Any unusual activity triggers an alert, sending a signal to the microcontroller.

7. OLED Display 0 96"(128x64)

Displays system status messages, prompts for user input, or alerts regarding access. Connected to the microcontroller to show real-time data.

8. Buzzer

Generates an audible alert in case of unauthorized access or system tampering. Activated by the micro-controller when a security breach is detected.

C. Functional Overview

a. Flowchart:

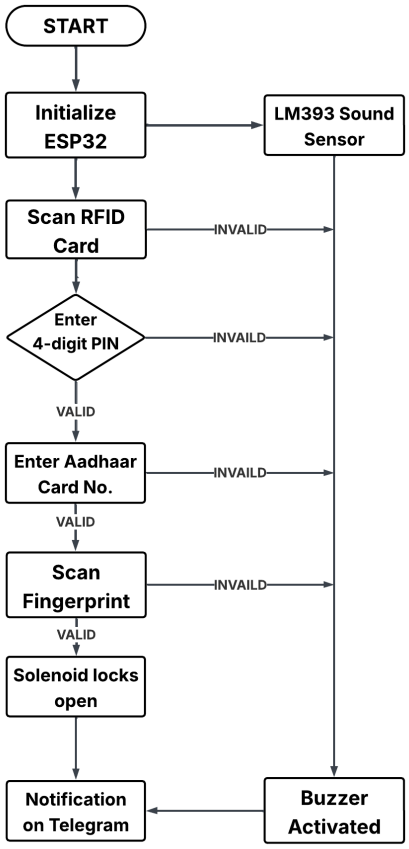

Fig 2. Flowchart: Multi-level Secure Bank Locker

b. Algorithm:

1. Start

The system is powered on, initiating the ESP32 microcontroller.

2. Initialize Sound Sensor

The sound sensor is activated to detect any tampering or unauthorized access attempts.

3. Initialize RFID Module

The RFID reader is powered on and ready to scan any RFID card presented to the system.

4. Card Matching Check

The system checks whether the RFID card presented matches the authorized card stored in the database.

Yes: If the card matches, the system proceeds to the next step.

No: If the card doesn't match, the buzzer is activated to indicate an unauthorized access attempt along with alert notification to the user via Telegram App/SMS.

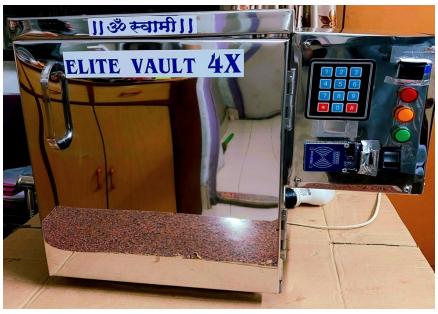

Fig 3. Structure of Multi-level Secure Bank Locker

Fig 4. For every Input

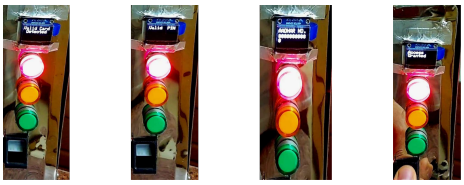

Fig 5. For every Valid Input

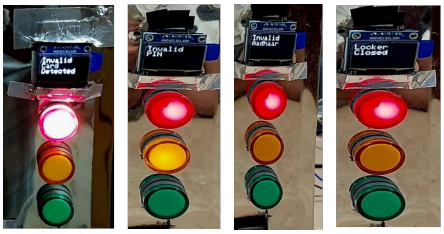

Fig 6. For every Invalid Input

5. PIN Verification

After a valid RFID card, the user is prompted to enter a valid 4- digit PIN.

Yes: If PIN is valid then the system proceeds to the next step.

No: If PIN is valid then buzzer is activated to indicate an unauthorised access.

6. Aadhar Card No Verification

After valid PIN entry, the user is prompted to enter valid 12-digit Aadhar Card No.

Yes: If Aadhar Card No. is valid then the system proceeds to the next step.

No: If Aadhar Card No. is not valid then buzzer is activated to indicate an unauthorized access along with alert notification to user via Telegram App/SMS.

7. Fingerprint Verification Check

After valid Aadhar No, the user is prompted to scan his /her fingerprints. The system compares the scanned fingerprint with the stored fingerprint data.

Yes: If the fingerprint matches, the lock is activated, and the locker is opened.

No: If the fingerprint does not match, the locker remains locked, and alerts are sent to the user and bank control room etc. via Telegram App/SMS.

8. Lock Operation

If all the previous steps are verified successfully, the lock is activated & locker door gets opened also user is notified for locker activation via Telegram App

Result

- The system successfully prevents unauthorized access by integrating multiple layers of security: RFID card, PIN + Aadhar Verification, and fingerprint authentication. Any unauthorized attempts trigger the buzzer for alert.
- The system sends real-time alerts via Telegram for invalid access attempts, ensuring security monitoring.
- The solenoid lock operates efficiently based on valid authentication, with manual override using the keypad.
- OLED display and keypad interaction ensure smooth user experience for PIN setup and authentication.
- The fingerprint sensor accurately verifies the user's identity, allowing access only if the scanned fingerprint matches the stored fingerprint, ensuring a high level of security and user authentication.

Conclusion

The **Multi-Level Secure Bank Locker** System effectively enhances the security of high-value assets by integrating multiple layers of authentication, including RFID, PIN, Aadhaar number, and fingerprint recognition. With real-time tamper detection and instant notifications via the GSM module, the system ensures robust protection against unauthorized access. The successful implementation of this project highlights its practical applications in banks, residential security, and other high-security environments. Looking ahead, the system can be further strengthened through the integration of iris recognition and facial detection technologies, offering even more precise biometric security. Additionally, advancements such as AI-based behavior analysis, blockchain for secure activity logs, and mobile app-based remote access and monitoring could significantly enhance its intelligence, scalability, and user convenience. These improvements would make the system a versatile, future-ready, and highly reliable solution for modern security challenges.

References

1) Ponnammal A, Natarajan S. Transport phenomena of SmSe1-x Asx . *Pramana - Journal of Physics*. 1994;42(5):421–425. Available from: https://www.ias.ac.in/article/fulltext/pram/042/05/0421-0425.
2) Barnard RW, Kellogg C. Applications of convolution operators to problems in univalent function theory. *Michigan Mathematical Journal*. 1980;27(1):81–94. Available from: https://dx.doi.org/10.1307/mmj/1029002312.
3) Shin KG, Mckay ND. Open Loop Minimum Time Control of Mechanical Manipulations and its Applications. In: Proc .Amer. Contr. Conf. 1984;p. 1231–1236.
4) Rao AS, Deshmukh M. Biometric-Based Security System for Bank Lockers. *Journal of Emerging Technologies*. 2019;21(1):15–19.
5) Patel V. Bank Locker with GSM and RFID. *International Journal of Security Systems*. 2019;10(2):50–55.
6) Kumar R. Enhancing Security and Flexibility in Smart Locker Systems. *International Journal of Smart Systems*. 2023;18(5):70–75.
7) Sharma MD, Gupta AK. A Review of Intelligent Locking Systems. *Journal of Internet of Things*. 2022;25(8):200–205.
8) Lee H, Park S. Secure Smart Lockers Using Blockchain Technology. *International Journal of Blockchain Security*. 2021;6(3):118–124.
9) Doe J, Smith M. Advanced Access Control Systems for Lockers. *Security and Privacy Journal*. 2020;12(4):80–85.
10) Khan A, Sharma M. IoT-Based Smart Bank Locker. *International Journal of Trend in Research and Development*. 2022;10(3):59–63.