IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

Bank Locker with Three Layer Protection System

K Chiranjeevi[1], D Divya[2], E Ajay[3], M Sravani[4], G Vinay[5]
Assistant Professor, Dept. of Electronics & Communication Engineering[1]
UG Students, Dept. of Electronics & Communication Engineering[2,3,4,5]
Christu Jyothi Institute of Technology & Science, Jangaon, Telangana, India
chiranjeevikutikanti@gmail.com ,divyaduasari@gmail.com, ajaerla014@gmail.com,
sravanimathangi22@gmail.com,vinaygandla003@gmail.com

Abstract: *This project proposes a smart Bank Locker Security System using fingerprint authentication, camera surveillance, GSM alerts, keypad access, and IoT monitoring, all controlled by an Arduino. The fingerprint scanner ensures only authorized users gain access, while the camera captures activity during access attempts. The GSM module sends real-time alerts to security personnel. The keypad offers an extra security layer, and IoT integration enables remote monitoring and control. This system offers a low-cost, reliable, and scalable solution for enhancing bank security*

Keywords: Bank Locker Security, Multi-layer Authentication, Fingerprint, Password, OTP, Arduino, GSM, Biometric, Access Control

I. INTRODUCTION

This project introduces a multi-layered bank security system that uses fingerprint authentication as the primary method for verifying authorized access. If unauthorized access is attempted, the system instantly sends an alert message to the bank authorities or security personnel using the GSM module. The keypad adds an extra security layer by requiring a personal identification number (PIN) for access. Moreover, the camera captures real-time images of any suspicious activity, helping in monitoring and recording evidence for future investigation.

By connecting these technologies through the **Arduino Uno**, the system offers real-time responses, continuous monitoring, and stronger protection compared to traditional security methods like manual checking and CCTV alone. Bank officials can be alerted immediately, even if they are not physically present, ensuring quick action against potential threats. This smart and affordable security solution demonstrates how modern embedded systems and communication technologies can be combined to create safer environments, and it paves the way for more intelligent security infrastructures in the future.

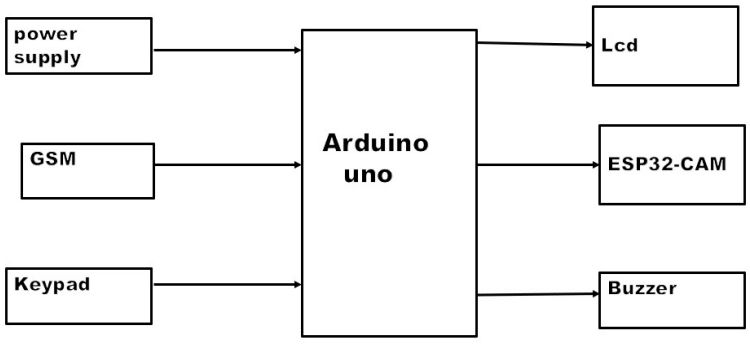

Fig 1:Block diagram of Bank locker

II. INTERNET OF THINGS (IOT)

The Internet of Things (IoT) refers to the network of physical devices, Banks, home appliances, and other items embedded with sensors, software, and connectivity which enables them to connect and exchange data. In Bank locker

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

security system, IoT technology is utilized to create a network of interconnected devices (sensors, microcontrollers, and display units) that gather, process, and transmit appliances related data in real-time. However, the proliferation of connected devices also brings challenges, especially in areas like **datasecurity** and **privacy**. Since IoT devices collect vast amounts of personal and sensitive data, ensuring that this information is protected from unauthorized access is critical. Additionally, interoperability between different IoT devices and platforms is a concern, as the lack of standardized protocols can hinder seamless integration. Despite these challenges, the continued evolution of IoT holds the promise of creating more intelligent and efficient systems across homes, industries, healthcare, cities, and beyond.

III. BANK LOCKER SECURITY SYSTEM

The 3-Layer Bank Locker Security System is a microcontroller-based security project designed to provide a high level of protection for valuables stored in lockers, such as those found in banks or private vaults. It incorporates three layers of authentication to ensure that only authorized users can access the locker.

The system works in a sequential manner. First, the user must successfully scan a pre-enrolled fingerprint using a fingerprint sensor module. If the fingerprint is matched, the user is prompted to enter a PIN using a 4x4 keypad. Once the correct PIN is entered, the final layer involves receiving a randomly generated OTP on a registered mobile number through a GSM module. Only after entering this correct OTP will the locker be unlocked. Each step must be completed accurately; otherwise, the system will deny access and send a warning message through the GSM module, providing real-time alerts.

This project uses an Arduino Uno microcontroller as the brain of the system, which coordinates the interaction between the fingerprint sensor, keypad, GSM module, and LCD display. The LCD provides user interface feedback by showing instructions or access results. The fingerprint module stores and verifies biometric data, while the keypad allows secure numeric input. The GSM module plays a crucial role by handling mobile communication and sending OTPs or alert messages. Power is supplied through a battery or adapter, and the entire system is compact, affordable, and easy to integrate into locker mechanisms.

This layered security system addresses the growing need for better protection of sensitive items in financial institutions and high-security areas. Unlike traditional key or card-based systems, this project introduces biometric and real-time digital authentication, which significantly reduces the risk of theft or unauthorized access. It can also be adapted for home safes, secure doors, or digital vaults. The use of commonly available components and open-source software makes this project a cost-effective and customizable solution for enhancing physical security.

IV. EXISTING SYSTEM

Existing security systems used in banks and high-security facilities involve a mix of traditional methods and modern technologies to prevent unauthorized access, theft, and criminal activities. These systems often combine physical security measures like strong locks and CCTV cameras with electronic monitoring solutions such as biometric authentication, alarm systems, and GSM-based alerting mechanisms. Many existing solutions aim to improve real-time responsiveness, automate threat detection, and provide remote notifications to security personnel. However, older systems may still rely heavily on manual monitoring, increasing the risk of delayed responses to unauthorized access.

V. PROPOSED METHOD

The proposed Bank Security System is a smart and multi-layered security solution that uses the latest microcontroller and IoT technologies to enhance security in banks. By combining Arduino Uno, fingerprint sensors, keypads, LCD displays, GSM modules, buzzers, and the ESP32-CAM module, the system ensures both local and remote security monitoring. It is designed to offer stronger protection, faster alerts, and easier control compared to traditional security setups.

The system's primary access control is based on biometric fingerprintauthentication. Only registered fingerprints are allowed access to secure areas. This ensures that access is restricted to authorized personnel only, reducing the risk of unauthorized entry through stolen keys, PINs, or fake identities. Biometric security is harder to bypass compared to traditional methods.

DOI: 10.48175/IJARSCT-28157

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

In addition to biometric verification, a keypad PIN entry system is included to add a second layer of security. Even if an authorized fingerprint is used, the correct PIN must still be entered to gain full access. This two-factor authentication greatly improves security, as it requires possession (fingerprint) and knowledge (PIN) together for entry.

The system is also cost-effective and easily expandable. As it uses commonly available and affordable components like Arduino and GSM modules, the overall cost remains low. Furthermore, the modular design allows future upgrades, such as adding cloud storage for captured images, connecting to mobile apps for remote access control, or integrating with smart bank management systems.

VI. SOFTWARE EMPLOYED

In this 3-layer bank locker security system project, the primary software employed is the Arduino IDE, which is used for writing, compiling, and uploading the program code to the Arduino Uno microcontroller. The code is written in a simplified version of C/C++, and the IDE also provides a built-in Serial Monitor to view system messages, debug outputs, and test the behavior of the sensors and modules in real-time. Additionally, simulation software such as Proteus can be used during the design phase to visualize and verify the circuit connections and component interactions before physical implementation. In some cases, CoolTerm or similar serial communication tools may also be utilized to monitor communication between the Arduino and modules like the GSM. For projects that involve GSM modules, AT Command testing tools can be helpful to independently test and troubleshoot SMS functionality. Together, these software tools support the smooth development, debugging, and testing of the entire security system.

The GSM module (typically SIM800 or SIM900) is programmed to send SMS alerts to the owner containing GPS coordinates when unauthorized access is detected. A relay module is controlled digitally to cut off the motor or ignition system, effectively immobilizing the vehicle. A buzzer is triggered using simple digital output commands to raise a local alarm. In addition, optional use of the EEPROM library allows the system to store GPS history or system states in non-volatile memory.

The GSM module (typically SIM800 or SIM900) is programmed to send SMS alerts to the owner containing GPS coordinates when unauthorized access is detected. A relay module is controlled digitally to cut off the motor or ignition system, effectively immobilizing the vehicle. A buzzer is triggered using simple digital output commands to raise a local alarm. In addition, optional use of the EEPROM library allows the system to store GPS history or system states in non-volatile memory.

VII. RESULTS AND DISCUSSIONS

The 3-layer bank locker security system was designed to incorporate three sequential layers of authentication—fingerprint recognition, keypad-based password entry, and OTP verification via GSM. Each component was tested individually and then as an integrated system. The fingerprint sensor module was found to be quick and accurate in identifying enrolled fingerprints, rejecting unregistered attempts with high precision. The keypad reliably accepted password inputs, and the system only proceeded to the next stage when the correct password was entered.

The OTP mechanism was implemented using a GSM module, which sends a randomly generated OTP to the user's registered mobile number. During testing, OTP delivery occurred within a few seconds, and the system effectively verified it within a preset timeout period. The GSM module also sent SMS alerts during unauthorized access attempts, enhancing the security notification system. This functionality proves crucial for real-time monitoring and response, especially in sensitive environments like bank vaults.

The LCD display played a vital role in guiding the user through each layer of authentication. Clear and timely instructions were displayed, reducing user confusion and enhancing usability. From prompting for fingerprint placement to password input and OTP entry, the system ensured smooth interaction. This user-friendly design is essential in real-world scenarios where clarity and ease of use are as important as security.

Overall, the combined use of biometric, password, and OTP authentication significantly improved the security level of the locker system. Even if one layer is bypassed or compromised, the remaining layers act as safeguards. This layered approach reduces the chances of unauthorized access, making it more robust than single-layer systems. The results support the effectiveness of multi-factor authentication in securing sensitive systems like bank lockers.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

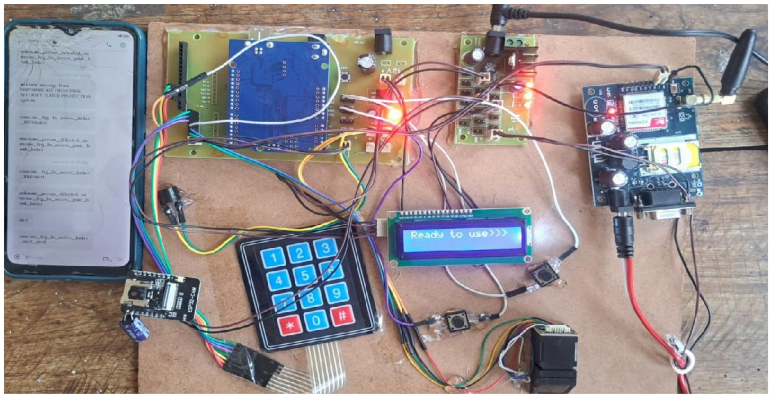

Fig 2 : Output of bank locker security system

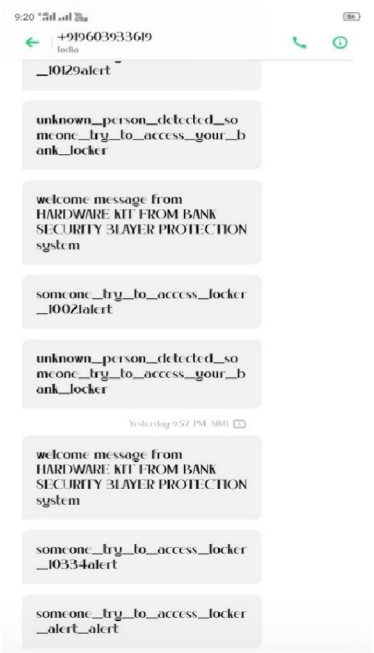

Fig 3 : locker alert

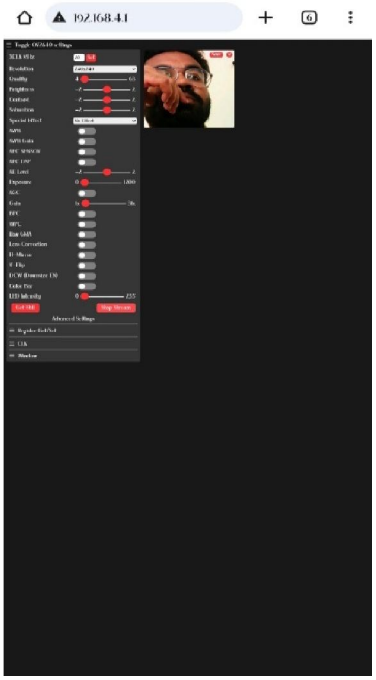

Fig 4 : livestream

VII. CONCLUSION

This project presents an efficient and multi-layered security system for bank lockers using an Arduino Uno. The combination of fingerprint authentication, password verification, and OTP-based GSM confirmation provides a strong defense against unauthorized access. Each layer adds an extra level of security, ensuring that even if one is compromised, the system remains protected by the others.

Through the integration of various components such as a fingerprint sensor, keypad, GSM module, and LCD display, the system effectively demonstrates the real-world application of embedded systems. The project also highlights the importance of combining both hardware and software in designing a secure and responsive system. The use of serial communication and conditional logic allowed for seamless interaction between components, providing a user-friendly interface.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 8, June 2025
Impact Factor: 7.67

REFERENCES

[1]. A bank locker equipped with fingerprint recognition technology and image capturing features was developed by Ambrish Kumar1, Anish Kumar2, Kushagra Gohil3, Laxit Porwal4, Manish Cheepa5, and Ankit Vijayvargiya6 from the Department of Electrical Engineering at SKIT in Jaipur, India (302033).

[2]. In 2017, Divya R.Spresented a paper titled "Super Secure Door Lock System for Critical Zone"at the International Conference on Network and Advances in Computational Technology.

[3]. In 2014, Srinivatsan Sridharan from the Department of Computer Science at the International Institute of Technology in Bangalore, India, developed a system for authenticated and secure biometric- based access to bank safety lockers.

[4]. Amit Verma fromthe Departmentof ElectronicsandCommunicationEngineering(ECE) at Amity University in Noida, Uttar Pradesh, India, authored an IEEE paper in 2014 on the development of an intelligent system for bank security

[5]. In 2016, Pradeep Kumar from the Department of Electronics and Communication Engineering (ECE) at Amity University developed an efficient multi-stage security system for user authentication.

[6]. In 2015, Sanal Malhotra from the Department of Electronics and Communication Engineering (ECE) at AmityUniversityin Uttar Pradesh, India, developed a bankingsecuritysystem that utilizes hand gesture recognition