International Journal for Modern Trends in Science and Technology
Volume 12, Issue 03, pages 443-449.
ISSN: 2455-3778 online
Available online at: http://www.ijmtst.com/vol12issue03.html
DOI: https://doi.org/10.5281/zenodo.19142832

Internet of Things for Bank Locker Security System

Kurakula Prasanth Reddy | Konda Tharun | Parikela Gopichand | Mukkala Jaya Surya Teja | Mudraboyina Abhishek

Department of ECE, NRI Institution of Technology, Vijayawada, Andhra Prasad, India.

To Cite this Article
Kurakula Prasanth Reddy, Konda Tharun, Parikela Gopichand, Mukkala Jaya Surya Teja & Mudraboyina Abhishek (2026). Internet of Things for Bank Locker Security System. International Journal for Modern Trends in Science and Technology, 12(03), 443-449. https://doi.org/10.5281/zenodo.19142832

Article Info
Received: 17 February 2026; Revised: 16 March 2026; Accepted: 18 March 2026.

KEYWORDS

RFID, embedded systems, ESP32-CAM, Multi-Level Security System for Bank Locker.

ABSTRACT

This project presents a Multi-Level Security System for Bank Locker that integrates embedded systems, biometric authentication, and image processing to ensure a highly secure and reliable access control mechanism. The system is built around a Raspberry Pi Pico as the central controller and incorporates multiple authentication layers including RFID card verification, OTP entry through a 4×3 keypad, fingerprint recognition, and iris recognition using a laptop camera. When an RFID card is scanned, the system prompts the user to enter a one-time password (OTP), whereas fingerprint and iris authentication provide direct biometric verification. An LCD is used to guide the user through each authentication step, while a buzzer provides audio alerts for invalid attempts.

To enhance security further, the system integrates real-time monitoring and alert mechanisms. For every unauthorized or failed authentication attempt, the system captures a live image using an ESP32-CAM module and sends an alert message along with the image to a Telegram bot. The generated OTP is also securely shared via Telegram to authorized users. Upon successful multi-factor authentication, a servo motor is activated to unlock the bank locker and automatically relock it after access. By combining multi-factor authentication, biometric verification, and real-time alerting, this project provides a robust, intelligent, and tamper- resistant security solution suitable for modern banking environments.

INTRODUCTION

The rapid advancement of digital technologies has significantly transformed modern banking systems, leading to the adoption of automated locker facilities for safeguarding valuable assets and confidential documents. Traditional bank locker systems primarily rely on mechanical keys or single authentication mechanisms, which are vulnerable to theft, duplication,

and unauthorized access. As security threats continue to evolve, it has become essential to develop intelligent locker security solutions that provide stronger protection through multiple layers of authentication and real-time monitoring.

The Internet of Things (IoT) has emerged as a powerful technology that enables interconnected devices to communicate and exchange data over the internet. IoT-based security systems allow real-time monitoring, remote alerts, and automated control, making them suitable for high-security environments such as banking institutions. Several recent studies have explored the use of IoT technologies to improve locker security systems. For example, a two-layer IoT locker security system integrating RFID and OTP authentication was proposed to enhance access control reliability and reduce unauthorized entry attempts [1]. Similarly, smart locker systems using fingerprint authentication combined with OTP verification have demonstrated improved identity validation compared to traditional access methods [2].

In addition to RFID and OTP-based systems, biometric technologies have gained significant attention due to their ability to uniquely identify individuals based on physiological characteristics. Biometric authentication methods such as fingerprint and iris recognition provide higher accuracy and security because these traits are difficult to replicate or forge. Research on multimodal biometric systems combining iris and fingerprint recognition has shown improved robustness and reliability compared to single biometric systems [6]. Furthermore, the integration of biometric authentication with embedded platforms such as Raspberry Pi enables the development of cost-effective and scalable smart security systems for banking applications [4].

Recent advancements also emphasize the role of intelligent authentication frameworks that combine multiple security layers to prevent unauthorized access. Multi-factor authentication systems integrate knowledge-based, possession-based, and biometric verification techniques to ensure a highly secure access control mechanism [5]. Additionally, IoT-enabled monitoring systems using devices such as the ESP32-CAM module allow real-time image capture and remote alert transmission, enabling immediate action in the event of suspicious activities [9].

Motivated by these developments, this project proposes an **IoT-based multi-level bank locker security system** that integrates RFID authentication, OTP verification through a keypad, fingerprint recognition, and iris recognition using a laptop camera. The system is controlled by a Raspberry Pi Pico microcontroller that coordinates all authentication modules and security operations. In case of unauthorized access attempts, the system captures images using an ESP32-CAM module and sends alerts to authorized users via a Telegram bot. This multi-layer authentication approach significantly enhances the reliability and safety of bank locker access while providing real-time monitoring capabilities.

The overall architecture of the proposed IoT-based bank locker security system is illustrated in **Figure 1**, which shows the interaction between authentication modules, the central controller, and the IoT-based alert mechanism.

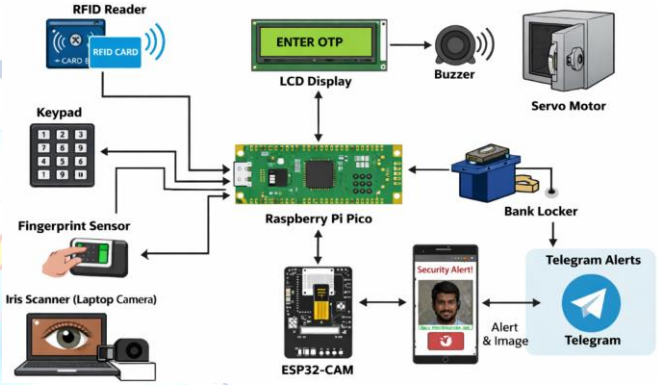

Figure 1 Conceptual architecture of the proposed system with IoT monitoring.

In this architecture, the Raspberry Pi Pico acts as the central controller that manages authentication processes and system operations. RFID verification initiates the access request, followed by OTP entry through a keypad, while biometric modules such as fingerprint and iris recognition provide additional identity validation. An LCD display guides the user through the authentication process, and a buzzer provides alerts for incorrect attempts. When unauthorized access is detected, the ESP32-CAM captures an image and sends it along with an alert message to a Telegram bot. Upon successful authentication, a servo motor unlocks the locker and automatically relocks it after a predefined duration.

By combining IoT communication, biometric authentication, and real-time alert mechanisms, the proposed system provides a robust and intelligent security framework suitable for modern banking environments.

RELATED WORK

Bank locker security has been an important research area due to increasing concerns regarding unauthorized access, theft, and security breaches in financial institutions. Traditional locker systems mainly rely on mechanical locks and keys, which are vulnerable to duplication and loss. To overcome these limitations, researchers have proposed several smart locker systems that incorporate IoT technologies, biometric authentication, and multi-factor verification mechanisms to enhance security and monitoring.

Handasah et al. [1] proposed a two-layer IoT-based locker security system that integrates RFID authentication with a One-Time Password (OTP) verification mechanism. In their system, the RFID card is used as the first level of authentication, while OTP provides an additional verification layer to ensure that only authorized users can access the locker. The system demonstrated improved security compared to traditional locker systems by reducing the chances of unauthorized access through duplicated RFID cards.

Nair et al. [2] developed a smart locker security system using fingerprint authentication combined with OTP verification. Their approach uses biometric fingerprint identification as the primary authentication method, while OTP acts as a secondary verification step. This method significantly improves reliability because biometric characteristics are unique to each individual and difficult to forge. The authors demonstrated that combining biometric authentication with OTP provides stronger access control compared to single-factor authentication systems.

Sen et al. [3] presented a three-layer bank locker authentication system based on GSM communication technology. The system integrates password verification, OTP authentication, and GSM-based alerts to enhance security. Whenever an unauthorized attempt is detected, the system sends a notification message to the authorized user through a GSM module. This real-time alerting mechanism improves monitoring and enables quick response to potential security threats.

Joshi et al. [4] proposed a smart bank locker system implemented using a Raspberry Pi platform with biometric authentication. Their system incorporates fingerprint recognition to identify authorized users and allows secure locker access through an embedded computing platform. The use of Raspberry Pi enables efficient integration of sensors, biometric modules, and communication interfaces, making the system flexible and scalable for real-world banking applications.

In addition to hardware-based authentication approaches, several studies have explored multi-factor authentication frameworks to strengthen security. Ganmati et al. [5] conducted a comprehensive survey on deep learning-based multi-factor authentication systems and highlighted the importance of combining multiple verification methods such as biometric recognition, tokens, and passwords to reduce security vulnerabilities. Their findings emphasize that integrating multiple authentication techniques significantly improves the robustness and reliability of security systems.

Biometric fusion techniques have also been explored to enhance authentication accuracy. Sridevi and Shobana [6] proposed a multimodal biometric security system combining iris and fingerprint recognition using Bloom filter techniques. Their work demonstrated that integrating multiple biometric traits improves recognition performance and reduces false acceptance rates compared to single biometric systems.

Machine learning methods have also contributed to the development of intelligent authentication and security systems. Breiman [7] introduced the Random Forest algorithm, a powerful ensemble learning technique widely used in classification and prediction tasks. Random Forest models have been applied in various security-related applications, including biometric recognition and anomaly detection, due to their ability to handle complex data patterns and improve prediction accuracy.

Open-source implementations have further facilitated the development of biometric recognition systems. The IrisRecognition Python project developed by mvjq [8] provides an implementation of iris detection and recognition algorithms using image processing techniques. Such frameworks allow researchers and developers to implement iris-based authentication systems efficiently in embedded or IoT environments.

IoT hardware platforms also play an important role in modern security systems. The ESP32-CAM module, documented by Espressif Systems [9], integrates a microcontroller with a camera and Wi-Fi capabilities, enabling real-time image capture and remote data transmission. This module is widely used in IoT-based

surveillance and monitoring systems due to its compact design and low power consumption.

Although several studies have proposed different authentication methods such as RFID verification, OTP authentication, biometric recognition, and GSM-based alert systems, many existing solutions rely on limited security layers or lack real-time monitoring features. Therefore, integrating multi-factor authentication, biometric verification, IoT-based communication, and real-time alert mechanisms can significantly improve the overall reliability and effectiveness of bank locker security systems. The proposed system addresses these challenges by combining RFID authentication, OTP verification, fingerprint recognition, iris recognition, and IoT-based monitoring using ESP32-CAM and Telegram alerts to provide a comprehensive and intelligent security solution.

PROPOSED SYSTEM

The proposed system presents an IoT-based multi-level security architecture for bank locker systems designed to ensure highly reliable authentication and real-time monitoring. The system integrates multiple authentication techniques including RFID verification, OTP entry through a keypad, fingerprint recognition, and iris recognition. These authentication mechanisms are coordinated by a Raspberry Pi Pico, which acts as the central controller responsible for processing user inputs, validating credentials, and controlling the locker mechanism.

In the proposed architecture, the authentication process begins when a user scans an RFID card near the RFID reader. The RFID reader reads the card's unique identification number and sends it to the Raspberry Pi Pico for verification. If the RFID card is valid, the system proceeds to the second layer of authentication where the user is prompted to enter a One-Time Password (OTP) through a 4×3 keypad. The OTP is generated by the system and securely transmitted to authorized users via a Telegram bot.

Apart from RFID-based authentication, the system also supports biometric authentication methods such as fingerprint recognition and iris recognition. The fingerprint sensor captures the user's fingerprint and compares it with the stored fingerprint templates in the system database. Similarly, iris recognition is performed using a laptop camera, where an image processing algorithm analyzes the iris pattern to verify the user's identity. These biometric techniques provide highly secure and unique identification because physiological characteristics are difficult to duplicate.

An LCD display is used to provide user instructions and system status messages during the authentication process. It guides the user through each step such as scanning the RFID card, entering OTP, or performing biometric verification. A buzzer is also integrated to provide immediate audible alerts whenever invalid authentication attempts occur.

For enhanced security and monitoring, the system incorporates an ESP32-CAM module that captures real-time images during unauthorized or failed authentication attempts. These captured images, along with alert messages, are transmitted to authorized personnel using a Telegram bot. This IoT-based alert system enables real-time monitoring and allows immediate action if suspicious activity is detected.

Once all authentication layers are successfully verified, the Raspberry Pi Pico activates a servo motor that unlocks the bank locker. The servo motor rotates to open the locker door and automatically returns to the locked position after a predefined time interval. This automated locking mechanism ensures that the locker remains secure even if the user forgets to relock it manually.

The overall architecture of the proposed multi-level bank locker security system is illustrated in Figure 1, which shows the interaction between authentication modules, the central controller, and the IoT communication components.

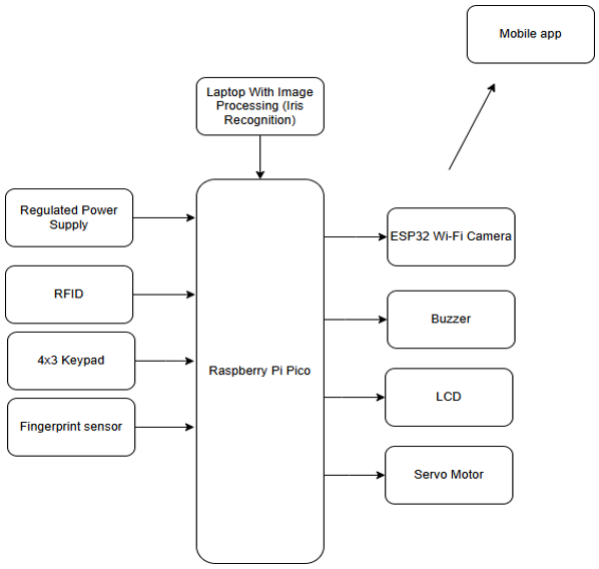

Figure 2 Block diagram of the proposed system with feedback and IoT.

As shown in Figure 1, the **Raspberry Pi Pico acts as the central processing unit** that manages all authentication modules and controls system operations. The RFID reader, keypad, fingerprint sensor, and camera provide multiple authentication inputs, while the LCD and buzzer provide user interaction and alert feedback. The ESP32-CAM module enables remote monitoring by capturing images and sending alerts through the Telegram network. Finally, the servo motor controls the mechanical locking and unlocking of the bank locker.

By integrating **multi-factor authentication, biometric verification, and IoT-based monitoring**, the proposed system significantly improves the security and reliability of bank locker access. The architecture ensures that unauthorized users cannot gain access even if one authentication layer is compromised, thereby providing a robust and intelligent security solution suitable for modern banking environments.

METHODOLOGY

The proposed IoT-based multi-level bank locker security system operates through a sequence of authentication and monitoring stages to ensure secure access to the locker. The methodology integrates embedded hardware components, biometric verification, and IoT communication to create a reliable security framework. The system is controlled by a Raspberry Pi Pico, which coordinates all authentication modules and system operations.

The operation begins when a user initiates a locker access request. The system first verifies the user through RFID authentication. If the RFID card is recognized as valid, the system proceeds to the OTP verification stage, where the user enters a One-Time Password through a 4×3 keypad. The OTP is generated and securely sent to the authorized user through a Telegram bot.

In addition to RFID-based authentication, the system supports biometric verification methods such as fingerprint and iris recognition. The fingerprint sensor scans the user's fingerprint and compares it with stored fingerprint templates. Similarly, the iris recognition process uses a laptop camera to capture the iris image and perform pattern matching with stored iris data.

If the authentication process fails at any stage, the system triggers a security alert mechanism. The ESP32-CAM module captures a real-time image of the person attempting access and sends it to authorized personnel through Telegram. At the same time, a buzzer alert is activated and the locker remains locked.

When all authentication layers are successfully verified, the Raspberry Pi Pico activates a servo motor to unlock the locker door. The locker remains open for a predefined duration and automatically locks again after the user completes access. This automated process ensures secure locker operation without requiring manual locking.

The overall methodology ensures that multiple authentication layers work together to prevent unauthorized access while also providing real-time monitoring and alert notifications.

```
Algorithm: Multi-Level Bank Locker Security Authentication
Step 1: Start the system and initialize all hardware modules
(RFID reader, keypad, fingerprint sensor, camera, LCD, buzzer, and servo motor).
Step 2: Display a welcome message on the LCD: "Scan RFID Card".
Step 3: Wait for the user to scan the RFID card.
Step 4:
If RFID is valid → Proceed to OTP verification.
Else → Activate buzzer and deny access.
Step 5: Generate a One-Time Password (OTP) and send it to the authorized user through the Telegram bot.
Step 6: Display message on LCD: "Enter OTP".
Step 7:
If entered OTP matches the generated OTP → Proceed to biometric verification.
Else → Trigger security alert and deny access.
Step 8: Capture fingerprint using the fingerprint sensor.
Step 9:
If fingerprint matches stored template → Proceed to iris verification.
Else → Capture image using ESP32-CAM and send alert to Telegram.
Step 10: Capture iris image using laptop camera and perform iris pattern matching.
Step 11:
If iris is verified → Grant access.
Else → Capture image and send alert to Telegram.
Step 12: Activate servo motor to unlock the bank locker.
Step 13: Display message on LCD: "Locker Opened".
Step 14: Wait for predefined time (e.g., 10–15 seconds).
Step 15: Rotate servo motor to lock the locker again.
Step 16: Display message on LCD: "Locker Locked".
Step 17: End process and return to standby mode.
```

RESULTS AND DISCUSSIONS

The Multi-Level Bank Locker Security System was successfully implemented and tested with multiple authentication methods including RFID + OTP, fingerprint, and iris recognition. The system effectively integrates embedded hardware, biometric authentication, and IoT-based real-time alerts to secure the bank locker. The Raspberry Pi Pico successfully managed all modules, and the ESP32-CAM provided live images for monitoring unauthorized access attempts.

During testing, RFID card scans required OTP verification. OTPs were securely shared via Telegram, ensuring only authorized users could proceed. Fingerprint and iris recognition provided direct authentication and demonstrated high accuracy in matching stored templates. The LCD guided the user through each step, and the buzzer provided immediate feedback in case of failed authentication attempts. The servo motor successfully controlled locker unlocking and automatic relocking, ensuring physical security.

Unauthorized attempts were effectively detected. The ESP32-CAM captured live images, which were transmitted to the registered Telegram bot along with an alert message, allowing real-time monitoring. The system handled multiple consecutive failed attempts, demonstrating the reliability of the alert mechanism and the robustness of the multi-layer authentication approach. Overall, the results indicate that combining multiple authentication layers with real- time IoT alerts and biometric verification provides a highly secure and reliable system for sensitive bank locker applications.

Figure 3 Multi-Level Security System for Bank Locker

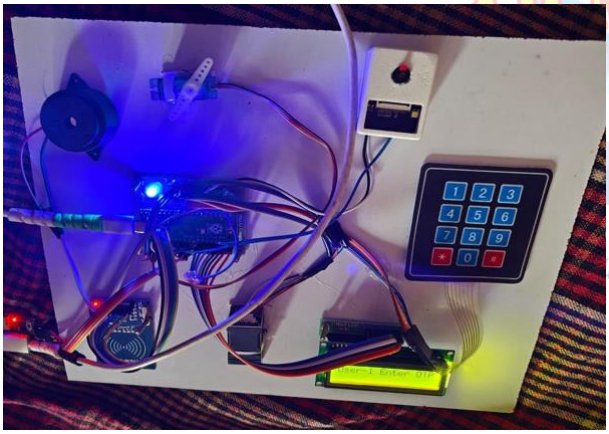

Figure 3 Using Keypad Entering the code

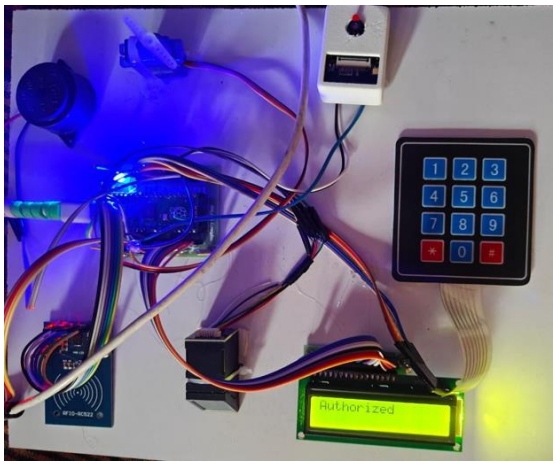

Figure 4 Authorization has been done

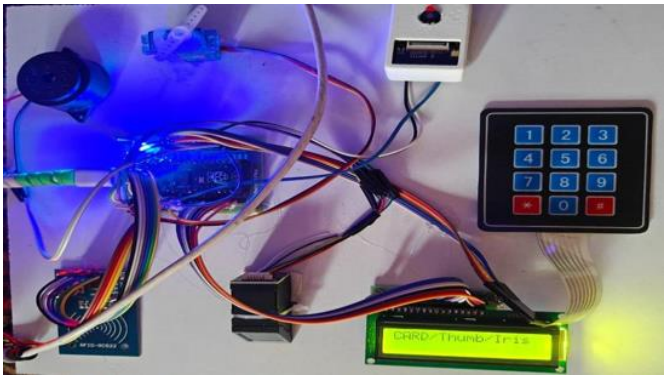

Figure 4 Using Iris Method

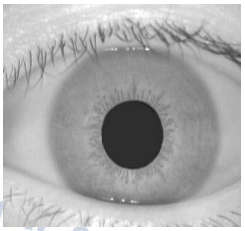

Figure 5 Normal Eye

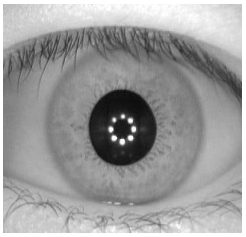

Figure 6 During IRIS Detection

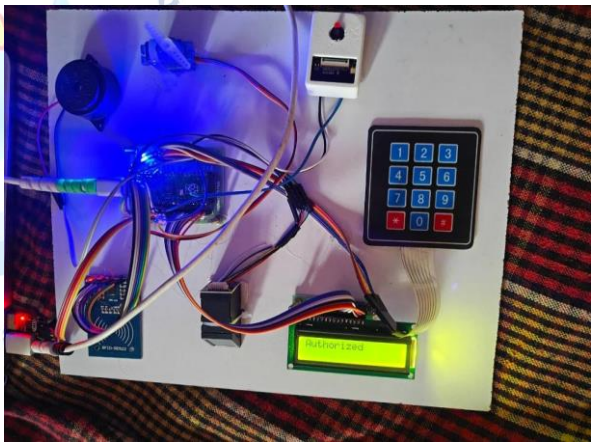

Figure 7 Authorization has been done

CONCLUSION

The Multi-Level Bank Locker Security System successfully demonstrates an intelligent, multi-factor authentication approach for securing sensitive access points. By combining RFID card verification, OTP entry, fingerprint recognition, and iris recognition, the system ensures that only authorized users can gain access to the bank locker. The integration of IoT-enabled real-time alerts via an ESP32-CAM and Telegram bot adds an additional layer of security, allowing administrators to monitor and respond to unauthorized access attempts immediately.

The Raspberry Pi Pico effectively coordinates all sensors and actuators, while the servo motor reliably controls locker unlocking and relocking. The LCD and buzzer provide user-friendly feedback during the authentication process. Testing demonstrated high accuracy and reliability across all authentication methods, and the system successfully captured and transmitted images of unauthorized attempts. Overall, this project provides a robust, scalable, and modern approach to bank locker security, illustrating the potential of combining embedded systems, biometric verification, image processing, and IoT technologies for critical security applications.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Handasah, U., et al., "Two-Layer IoT Locker Security System Using RFID and OTP," Scientific Reports, Nature, 2025.

[2] Nair, R. R., et al., "Smart Locker Security with Fingerprint and OTP Verification," International Journal of Engineering and Technology, 2025.

[3] Sen, S., et al., "GSM-Based 3-Layer Bank Locker Authentication System," International Journal of Recent Technology and Engineering (IJRTE), 2025.

[4] Joshi, R., et al., "Smart Bank Locker Using Raspberry Pi and Biometric Authentication," Journal of Emerging Technologies and Innovative Research, 2025.

[5] Ganmati, A., et al., "Survey on Deep Learning-Based Multi-Factor Authentication Systems," arXiv preprint, 2025.

[6] Sridevi, R., & Shobana, P., "Multimodal Iris and Fingerprint Security Using Bloom Filters," arXiv preprint, 2024.

[7] Breiman, L., "Random Forests," Machine Learning Journal, vol. 45, pp. 5–32, 2001.

[8] mvjq, "IrisRecognition: Python Iris Recognition Project," GitHub Repository, 2024, https://github.com/mvjq/IrisRecognition

[9] ESP32 Documentation, "ESP32-CAM Module for IoT Applications," Espressif Systems, 2024.