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 6, Issue 6, May 2026
Impact Factor: 8.2

Secure Fingerprint Bank Locker with Image Capture

Salave Sagar Vasant, Narsale Suraj Vishnu, Sabale Pratik Vilas, Prof. Shaikh T . N
Dept. of Electronics and Telecommunication Engineering
Rajiv Gandhi College of Engineering, Karjule Harya, Parner, India
salvesagar686@gmail.com, 01surajnarsale@gmail.com
sabalepratik7744@gmail.com, email@gmail.com

Abstract: *Physical security systems for financial institutions and personal vaults are rapidly evolving beyond traditional mechanical locks, which are highly susceptible to picking, duplication, and theft. This paper details the design and implementation of a highly secure, multi-factor authentication bank locker system powered by an ESP32 microcontroller and an auxiliary ESP32-CAM module. The proposed framework establishes a dual-layer authentication protocol utilizing an R307 fingerprint scanner as the primary access method, complemented by a 4x4 matrix keypad for secondary PIN-based verification. To provide an immutable audit trail, the system integrates an ESP32-CAM module capable of capturing photographic evidence of both successful access events and unauthorized breaches. These images, alongside status alerts, are transmitted in real-time to the owner or security personnel via the Telegram messaging API over a Wi-Fi network. Furthermore, the system employs an automated lockout mechanism and an audible buzzer alarm triggered after three consecutive failed attempts. By combining biometric verification, cryptographic PINs, physical actuation (via a servo motor), and IoT-enabled visual logging, this framework delivers a comprehensive, edge-based security solution for high-value asset protection.*

Keywords: Biometric Security, ESP32, ESP32-CAM, IoT Locker, Two-Factor Authentication, Telegram Bot API, Physical Access Control

I. INTRODUCTION

The protection of highly sensitive documents, currency, and physical assets requires access control systems that are both resilient against brute-force attacks and capable of real-time monitoring. Traditional locking mechanisms rely on "what you have" (a key) or "what you know" (a combination). These paradigms are fundamentally flawed, as keys can be stolen and combinations can be observed or guessed.

Modern security engineering dictates a shift toward "who you are" — biometric authentication. Fingerprint recognition offers a high degree of uniqueness and is exceedingly difficult to spoof. However, biometrics alone do not provide a complete security narrative. If a breach does occur, or if an authorized user accesses the vault under duress, traditional systems fail to provide actionable, real-time intelligence to external security forces.

To address these vulnerabilities, this project introduces an Internet of Things (IoT) augmented security locker. The system utilizes the powerful ESP32 SoC as the central logic unit, managing a state machine that handles user inputs, biometric matching, and electromechanical unlocking. Crucially, the system bridges the gap between physical security and digital auditing by employing an ESP32-CAM module. This allows the locker to act not just as a barrier, but as an active surveillance node, capturing photographic evidence of the operator and pushing these images directly to a secure Telegram channel. This dual-layered physical and digital security architecture drastically reduces the window of opportunity for theft while ensuring comprehensive access logging.

DOI: 10.48175/568

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 6, Issue 6, May 2026
Impact Factor: 8.2

II. SYSTEM ARCHITECTURE

The hardware architecture is designed around a master-slave microcontroller configuration to ensure that the computationally intensive task of image processing does not interrupt the real-time security logic.

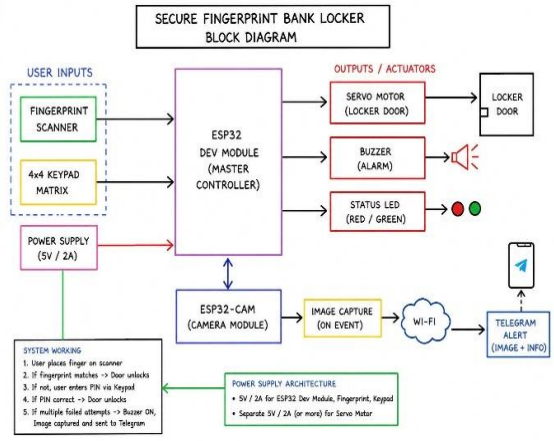


Fig. 1. Comprehensive Block Diagram illustrating the master ESP32 Dev Module routing inputs from the Fingerprint Scanner and Keypad, controlling actuators, and triggering the auxiliary ESP32-CAM for Wi-Fi telemetry.

As detailed in Fig. 1, the system's core is the ESP32 Dev Module. It draws power from a 5V / 2A supply, which features a split architecture to ensure the Servo Motor's current spikes during locker door actuation do not cause brownouts on the logic board. The primary user inputs are the Fingerprint Scanner (R307) and a 4x4 Keypad Matrix. The outputs include the Servo Motor, a Piezoelectric Buzzer for alarms, and Red/Green Status LEDs to indicate locked/unlocked states. A secondary ESP32-CAM module is interfaced with the master controller to handle image capture and Wi-Fi transmission to the Telegram API.

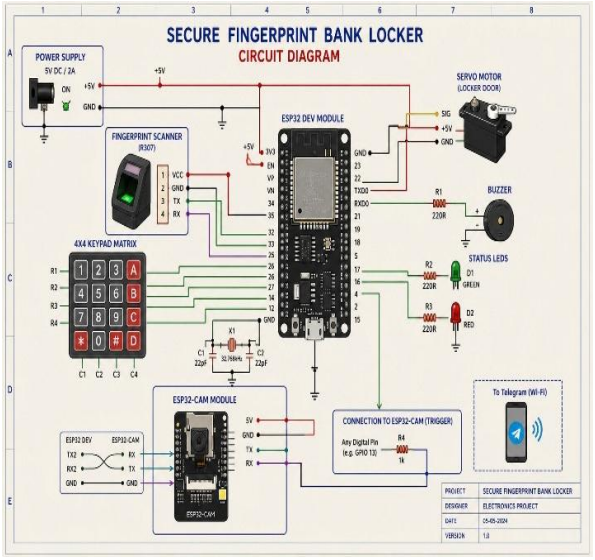


Fig. 2. Circuit schematic demonstrating the pin mapping: the R307 communicates via UART, the Keypad via standard GPIOs, and a dedicated digital trigger pin connects the Master ESP32 to the ESP32-CAM.

Fig. 2 outlines the electrical connectivity. The R307 fingerprint sensor communicates with the master ESP32 via a hardware serial UART connection (TX/RX). The 4x4 keypad utilizes 8 digital GPIO pins to scan for row/column button presses. To initiate an image capture, the master ESP32 uses a single digital trigger pin (e.g., GPIO 13) protected

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 6, Issue 6, May 2026
Impact Factor: 8.2

by a 1kΩ resistor (R4) to signal the ESP32-CAM. The ESP32-CAM, operating on its own processing thread, then captures the frame and executes the HTTPS POST request to Telegram.

III. METHODOLOGY

The system's operational logic is governed by a strictly defined state machine that prioritizes security and fault tolerance.

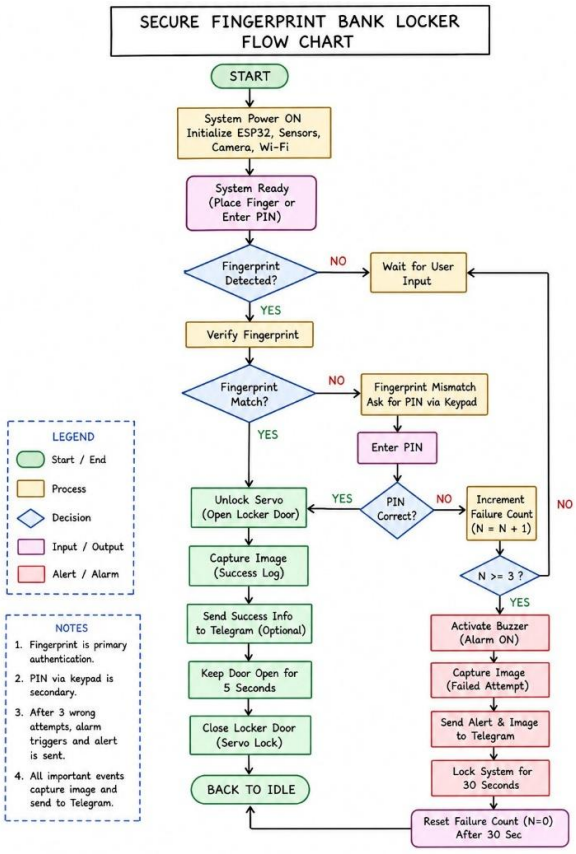


Fig. 3. System Flowchart detailing the dual-layer authentication logic, the 3-strike failure protocol, and the IoT-based image logging mechanism.

As mapped in the flowchart (**Fig. 3**), the firmware execution follows these sequential stages:

Initialization: Upon power-up, the ESP32 initializes all sensors, connects to the local Wi-Fi network, and enters the 'System Ready' idle state.

Primary Authentication: The user places a finger on the scanner. If a match is found in the R307's local database, the system jumps to the unlock sequence.

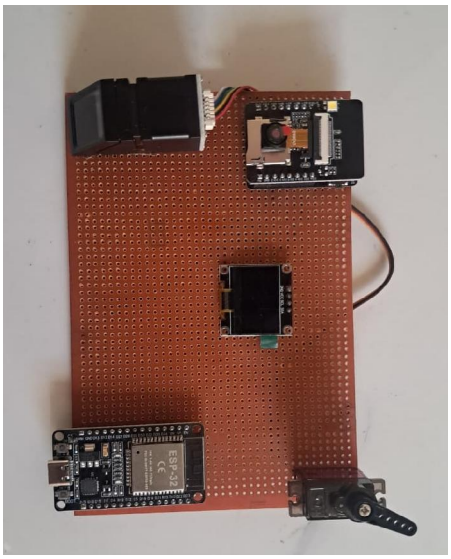
Secondary Authentication (Fallback): If the fingerprint does not match (or the scanner fails to read properly), the system prompts for a PIN via the 4x4 keypad.

Access Granted Protocol: If either the fingerprint or PIN is valid, the master ESP32 commands the servo motor to unlock the door, turns on the Green LED, triggers the ESP32-CAM to capture a "Success Log" image, and sends this information to Telegram. The door remains unlocked for 5 seconds before automatically re-locking.

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 6, Issue 6, May 2026
Impact Factor: 8.2

Security Threat Protocol: If an incorrect PIN is entered, a failure counter (N) increments. If $N \ge 3$, the system registers a security breach. It activates the Buzzer alarm, triggers the ESP32-CAM to capture a "Failed Attempt" image, and sends a high-priority alert to Telegram. The system then enters a hard lockout state for 30 seconds, refusing all inputs, before resetting the failure count to zero and returning to the idle state.

IV. RESULTS AND DISCUSSION



The prototype was successfully tested under various simulated access scenarios. The R307 fingerprint sensor demonstrated a high True Accept Rate (TAR) and successfully rejected unauthorized prints. In the event of primary biometric failure, the fallback keypad allowed legitimate users to gain access seamlessly.

The master-slave architecture between the ESP32 and ESP32-CAM proved highly effective. Offloading the image processing and TLS/SSL encryption required by the Telegram API to the ESP32-CAM ensured that the master ESP32's loop was never blocked. When a breach was simulated, the system successfully captured an image of the unauthorized user and delivered it to the designated Telegram chat within 3 to 5 seconds, depending on local network latency. The 30-second lockout and audible alarm effectively simulated a deterrent against sustained brute-force PIN guessing.

V. CONCLUSION AND FUTURE WORK

The developed Secure Fingerprint Bank Locker framework presents a robust, edge-computed solution to physical asset security. By blending biometric verification with an automated, IoT-driven photographic audit trail, the system provides both preventative security and reactive intelligence. The integration of the Telegram API allows for real-time monitoring without the need for a dedicated, expensive central server architecture.

Future iterations of this project will focus on integrating a Battery Management System (BMS) with lithium-ion cells to provide an Uninterruptible Power Supply (UPS) in the event of grid failure. Additionally, the ESP32-CAM's capabilities could be expanded to include local facial recognition (using Edge Impulse or similar lightweight ML frameworks) to achieve true dual-biometric (Face + Fingerprint) authentication before the servo lock is ever disengaged.

REFERENCES

[1]. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, 2004.

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 6, Issue 6, May 2026
Impact Factor: 8.2

[2]. K. A. A. Nazeer, et al., "IoT based smart security and home automation system," *International Conference on Computing, Communication and Automation (ICCCA)*, 2017.
[3]. R. Want, "An introduction to RFID technology," *IEEE Pervasive Computing*, vol. 5, no. 1, pp. 25-33, 2006.
[4]. M. Abomhara and G. M. Køien, "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks," *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65-88, 2015.
[5]. Espressif Systems, "ESP32-CAM Video Streaming and Face Recognition," 2021. [Online].
[6]. Espressif Systems, "ESP32 Series Datasheet," 2023. [Online].
[7]. P. P. Ray, "A survey on Internet of Things architectures," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 291-319, 2018.
[8]. S. S. S. A. Rizvi, et al., "Biometric authentication for smart home security systems using IoT," *IEEE International Conference on Smart Cloud*, 2019.
[9]. J. P. A. Yaacoub, et al., "Securing internet of medical things systems: Limitations, issues and recommendations," *Future Generation Computer Systems*, vol. 105, pp. 581-606, 2020.
[10]. T. N. R. Kumar, et al., "Bank locker security system based on RFID and GSM technology," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 10, 2013.
[11]. H. Arasteh, et al., "IoT-based smart cities: A survey," *IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, 2016.
[12]. S. R. Safavian and M. Mahdavi, "Security of IoT: A review," *International Conference on Web Research (ICWR)*, 2019.
[13]. R. H. Weber, "Internet of Things–New security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23-30, 2010.
[14]. U. Rehman, et al., "A smart locker system based on IoT," *International Conference on Electrical, Communication, and Computer Engineering (ICECCE)*, 2019.
[15]. M. U. Farooq, et al., "A critical analysis on the security concerns of internet of things (IoT)," *International Journal of Computer Applications*, vol. 111, no. 7, 2015.
[16]. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
[17]. Telegram Messenger Inc., "Telegram Bot API Documentation," 2023. [Online].
[18]. V. V. N. S. Madhav, et al., "IoT based anti-theft banking security system," *International Journal of Innovative Technology and Exploring Engineering*, vol. 8, no. 6, 2019.
[19]. D. Singh, G. Tripathi, and A. J. Jara, "A multidisciplinary model and architecture for the internet of things," *IEEE International Conference on Emerging Data and Industry 4.0*, 2014.
[20]. M. A. A. Dawood, "Two factor authentication system for bank lockers using fingerprint and GSM," *IEEE International Conference on Communication, Control and Information Sciences (ICCISc)*, 2021.