Enhancing Bank Locker Security through MultiLayered Authentication and IoT Integration

J.Jayapriya
PG scholar, EEE
Rajalakshmi Engineering college
Chennai, India
230911004@rajalakshmi.edu.in

M.Arulmozhi
Assistant Profossor(SS), ECE
Rajalakshmi Engineering college
Chennai, India
arulmozhi.m@rajalakshmi.edu.in

V.Jagadeesh
PG scholar, EEE
Rajalakshmi Engineering college
Chennai,India
230911003@rajalakshmi.edu.in

M.Sandhiya
PG scholar, EEE
Rajalakshmi Engineering college
Chennai,India
230911005@rajalakshmi.edu.in

Dr.A.Nazar Ali
Professor, EEE
Rajalakshmi Engineering college
Chennai,India
nazaeali.a@rajalakshmi.edu.in

G.Bathri Prasath
PG scholar, EEE
Rajalakshmi Engineering college
Chennai,India
230911002@rajalakshmi.edu.in

***Abstract*— In the face of evolving security threats, financial institutions continuously seek innovative solutions to fortify the protection of valuable assets stored in bank lockers. This research explores a comprehensive approach to enhance bank locker security by integrating multiple layers of authentication and leveraging the Internet of Things (IoT). The proposed system incorporates fingerprint recognition, keypad password entry, one-time password (OTP) verification, and real-time image capture of unauthorized access attempts. Fingerprint recognition ensures biometric uniqueness, offering a secure and convenient means of locker access. The inclusion of keypad password entry adds an additional layer of security, requiring users to input a personalized code. OTP verification further strengthens the authentication process by dynamically generating time-sensitive codes, minimizing the risk of unauthorized access. The integration of IoT plays a pivotal role in augmenting security measures. In the event of an unauthorized access attempt, the system captures and transmits an image of the intruder to a designated manager's bot. This proactive alert system enables timely response and intervention. Additionally, the system maintains an access history log, providing an audit trail for security administrators to monitor and analyze locker usage patterns. The proposed multi-layered authentication system with IoT integration not only fortifies bank locker security but also offers a robust defence against emerging threats. This research contributes to the on-going efforts in developing advanced security frameworks for safeguarding financial assets, ultimately fostering greater confidence among customers in the banking sector.**

Keywords—Bank locker Security System , Multi-layered authentication, OTP verification, IOT, Proactive alert system.

I. INTRODUCTION

The bank lockers are the most secure place to keep valuable things. But banks are frequently targets of criminal activity, the rise in threats against banks is concerning. The modern methods that are accessible in our banks are not very effective, they may easily be easily fabricated or faked by the cunning and bad minds of our society. In the current system, a person needs two keys for their locker in order to unlock a bank locker.

The person who opens the bank locker will acquire one key, and the bank will keep the other key. The biggest disadvantage is that in the event of losing the key the individual will be penalized and charged for the replacement. In order to address these issues, the papers present several keyless techniques. A password- protected door locking system for bank lockers is developed with the ability to activate, authenticate, and validate the user in real time while also unlocking the door for secure entry to the bank locker. Passwords have the basic advantage of being more secure than other systems [1]. The password for this system is entered via a keypad. The intruder alarm warns the wrong accessing individual if the user enters the incorrect password [2]. The one-time password (OTP) is dynamic and is only good for one login session. Traditional or static password- based authentication is improved by using OTP [3]. But, the password might occasionally be forgotten, in which case there will be another discussion about using RFID cards. The use of a passive kind of RFID in a digital security system allows it to activate, verify users in real time, and open doors for secure access [4]. If the ID number read by the RFID reader tag is accurate, an SMS is sent to a legalized person using GSM. If the entered password is valid, the locker opens [5-6]. Each and every person cannot afford the higher cost of using an RFID tag, and we risk forgetting the RFID tag.

Latest innovations in security system development leverage the biometric approach. Every individual has a unique set of biometrics, which can be used to authenticate a

person’s identity and prove their uniqueness. The fingerprintbased lock provides a great solution to the problems that are frequently experienced. Fingerprints are pre-stored in the memory can access a system using fingerprint recognition technology [7]. If the fingerprints don’t match, the authorized individual gets a alert message and activates the buzzer [8-10]. The security system has four layers. The combination different authentication provides more security for the locker. The four levels Voice Authentication, Password Authentication, and Facial Authentication. The user gains entry to the secured area after successfully unlocking all four security layers [11]. The method allows the documents or money to be retrieved from the locker only by the authenticated person using fingerprint sensor and data is read and entered into the AVR microcon-troller.[12] It is impossible to identify the person accessing the

979-8-3503-8168-9/24/$31.00 ©2024 IEEE

locker by using just an alert message or buzzer. So, The implementation of Internet of Things (IoT) has been done to allow only authorized people to enter securely by taking pictures using a Raspberry Pi, sending them to the user's email address via mail [13]. ESP32-cam, a camera sensor with a good reputation, is employed for both live broadcasting and person photography. The system can recognize the face of the individual in front of the door using AI-Thinker in the esp32-cam. [14].All activities are recorded by the IoT device, which is deployed and will be saved on Cloud. The IoT- based security system contributes to increased user client property protection [15]. To provide high level security, the system proposes various authentication methods.

II. Requirements

A. Arduino UNO

A popular microcontroller board meant for ease of use and variety in electronics projects is the Arduino Uno. Powered by the Atmega328P microcontroller, it operates at an operating voltage of 5V, with a recommended input voltage range of 7-12V. The board features 14 digital I/O pins, six of which provide PWM output, and six analog input pins. Each digital I/O pin can handle a maximum current of 20 mA, while the 3.3V pin can handle up to 50 mA. With 32 KB of flash memory, 2 KB of SRAM, and 1 KB of EEPROM, the Arduino Uno provides sufficient memory for storing code and data.The Arduino Uno operates at a clock speed of 16 MH.

B. LCD Display

A Liquid Crystal Display (LCD) is a versatile output device commonly used in electronic projects, featuring various specifications that define its performance and usability. The resolution, expressed in pixels, determines the display's clarity and detail, with higher resolutions providing sharper images.LED backlights are prevalent due to their brightness, power efficiency, and longer lifespan. Interface compatibility is another crucial aspect, and LCDs may support various interfaces like I2C, SPI, or parallel communication.

C. Buzzer

A buzzer, often referred to as a piezo buzzer, is a compact and commonly used audio output device in electronic circuits. Operating at low voltages, typically around 5V DC, it produces sound through the vibration of a piezoelectric element when an electrical signal is applied. Sound levels, measured in decibels (dB), indicate the loudness, and buzzers can range from 70 dB to 120 dB.. Buzzers find widespread use in electronic projects, providing audible alerts, notifications, or alarms.

D. Node MCU

The Node MCU is an open-source IoT (Internet of Things) platform based on the ESP8266 WiFi module. It features a Tensilica L106 32-bit microcontroller, clocked at 80MHz or 160MHz, with integrated WiFi connectivity. The Node MCU supports IEEE 802.11 b/g/n standards, enabling seamless wireless communication. It has GPIO pins for digital input/output, PWM, I2C, and more, offering flexibility in interfacing with various sensors and actuators.

E. GSM Module

GSM modules are integral components in communication systems, offering a range of features for wireless connectivity. Typically, these modules support multiple frequency bands, ensuring compatibility with various cellular networks globally. They incorporate SIM card slots for subscriber identity and authentication, employing AT commands for interfacing with microcontrollers or other devices. GSM modules often feature UART interfaces for seamless communication and integration. Security is a crucial aspect, with encryption and authentication protocols to safeguard data transmission. These modules operate on low power, facilitating efficient energy use, and they support functions like SMS (Short Message Service) and GPRS (General Packet Radio
Service) for data transmission.

F. Servo Motor

Servo motors are specialized motors designed for precise control of angular or linear position. They consist of a DC motor, gears, and a feedback mechanism. The feedback, often in the form of a potentiometer, enables the servo to continuously adjust and maintain its position. Servo motors are known for their high precision and accuracy, making them suitable for applications requiring controlled movement. They typically operate on low voltage and are available in various sizes and power ratings. Servo motors can rotate over a limited range, commonly around 180 degrees, and can be controlled with pulse-width modulation (PWM) signals.

G. ESP32- CAM

The ESP32-CAM is a versatile development board integrating the ESP32 microcontroller and a camera module, making it a powerful platform for IoT and image-related projects. It features the ESP32-S chip, providing dual-core processing and built-in WiFi and Bluetooth connectivity. The OV2640 camera module captures still images or video with a resolution of up to 2 megapixels. The board supports microSD card storage for saving images or videos locally. With GPIO pins, UART, I2C, and other interfaces, the ESP32-CAM facilitates seamless integration with various sensors and devices.

H. Finger print Sensor

Fingerprint sensors are biometric devices designed to capture and authenticate unique fingerprint patterns for security applications. These sensors typically utilize capacitive or optical scanning technology to capture highresolution images of fingerprints. The specifications of a fingerprint sensor include its resolution, expressed in dots per inch (DPI), determining the level of detail in fingerprint images. The sensor's accuracy is often measured by its False Acceptance Rate (FAR) and False Rejection Rate (FRR)..

III. System Architecture

A. Proposed System

Fig 1 shows the block diagram consisting of all the components of the proposed system.

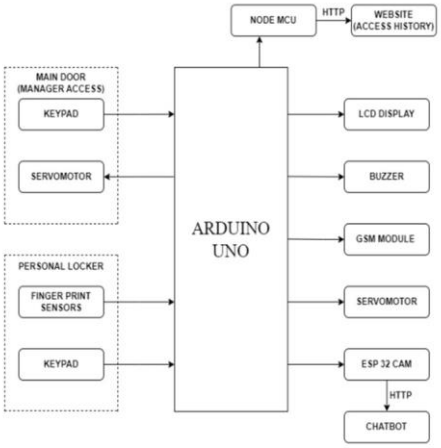

Fig. 1. Block Diagram

B. Process model specification

Fig 2 shows the process model specification which defines the modes of operation of the proposed system.

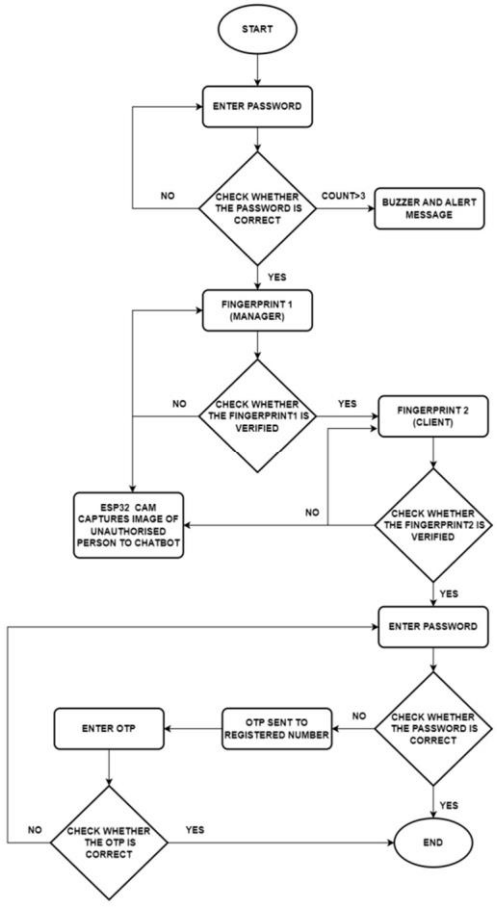

Fig. 2. Flow Chart

IV. Proposed Work

A. Overview

Security is paramount in the financial sector, particularly concerning the safeguarding of valuable assets stored in bank lockers. This research presents a cutting-edge approach to bolstering bank locker security by incorporating multiple layers of authentication and harnessing the capabilities of the Internet of Things (IoT). The proposed system combines fingerprint recognition, keypad password entry, one-time password (OTP) verification, and real-time image capture to create a robust defense against evolving security threats.

B. Multi-Layered Authentication System

The Multi-Layered Authentication System incorporates multiple layers creates a multi-faceted authentication system. Their functionalities and modules are as follows:

1) Fingerprint Recognition: Fingerprint recognition relies on capturing and analyzing the unique features of an individual's fingerprint. In our proposed bank locker security system, the Adafruit Fingerprint Sensor (GT521F32), designed to be compatible with Arduino Uno, interfaces seamlessly with the microcontroller. The Arduino Uno effectively manages communication between the fingerprint sensor and the broader system. The captured fingerprint data undergoes meticulous processing via the Arduino Uno's embedded algorithms, which identify and extract minutiae points for the creation of a unique fingerprint template. During the authentication process, the Arduino Uno intelligently compares the captured fingerprint to stored templates, granting or denying access based on the established identification. Furthermore, the microcontroller ensures the secure storage of fingerprint templates, employing robust encryption mechanisms to safeguard sensitive biometric data. This integrated solution not only bolsters security but also provides a reliable, unique, and convenient authentication method for the bank locker system.

2) keypad password authentication: In our enhanced bank locker security system, Keypad Password Entry serves as an additional layer of authentication following the initial fingerprint recognition. Once users have their fingerprints successfully verified, they input a personalized code via the keypad. The Arduino Uno, acting as the system's microcontroller, manages seamless communication between the keypad and the security system. The entered password is validated against stored credentials, allowing authorized users with the correct code to proceed to the next level of security. As an added layer, a servo motor is employed to physically control the locker's lock mechanism. Upon successful completion of the dual-layered authentication process, the Arduino Uno triggers the servo motor to either unlock or lock the bank locker, providing tangible and secure access. This integration of a servo motor ensures a robust physical barrier, enhancing the overall security of the bank locker system. In summary, the combination of biometric fingerprint recognition, keypad password entry, and servo motor activation establishes a comprehensive multi-layered authentication system for securing valuable assets in the bank locker.

3) OPT generation: In our proposed bank locker security system, an error-handling mechanism enhances security and user experience. In the event of an incorrect keypad password entry, the system promptly sends an alert message to the client's registered mobile number, notifying them of the unauthorized attempt to access their personal locker. Simultaneously, a one-time password (OTP) is dynamically generated and dispatched to the client's mobile device via SMS. This OTP serves as an alternative password, adding an extra layer of security. To facilitate seamless interaction, an LCD display acts as the interface, presenting

pertinent information such as alert notifications and OTP prompts. Upon receiving the alert and OTP, the user is prompted on the LCD display to enter the received code using the keypad. If the entered OTP matches and is still valid, access to the personal locker is granted. This dynamic scenario not only strengthens security through multi-factor authentication but also ensures user convenience and swift resolution in the case of an incorrect keypad entry, contributing to a secure and user-friendly bank locker system.

C. IOT integration

1) Real-time image capturing: In the proposed system aimed at enhancing bank locker security through multilayered authentication and IoT integration, a pivotal feature has been seamlessly integrated to address potential security breaches. Specifically, the system diligently monitors password entry attempts, and upon detecting three consecutive incorrect passwords, triggers a comprehensive security response. This trigger initiates the activation of an ESP32-CAM, an IoT-enabled camera strategically placed within the bank locker facility. The ESP32-CAM promptly captures real-time images of the individual attempting unauthorized access. Leveraging the HTTP communication protocol, these images are expeditiously transmitted to a designated manager's Telegram chat bot. This carefully orchestrated process allows for timely visual verification by the designated manager, empowering them to swiftly intervene and investigate any suspicious activity. By aligning the image capturing mechanism with the occurrence of multiple incorrect password attempts, this integrated security measure reinforces the robustness of the overall system, providing a proactive defense against potential threats to valuable assets stored in bank lockers.

2) Comprehensive access history log: In our cuttingedge bank locker security system, Arduino Uno plays a pivotal role as the central control unit, overseeing the entire security framework. The system seamlessly integrates a fingerprint scanner for user authentication, NodeMCU for IoT communication via HTTP, and dual access history logs displayed on a dedicated website.When a user attempts access, the Arduino Uno interfaces with the fingerprint scanner, verifying their identity through biometric data. The unique fingerprint signature triggers the recording of the entry in the respective access log, either for managers or clients. This biometric authentication adds a robust layer to the multi-faceted security approach.

Arduino Uno communicates with NodeMCU via HTTP, ensuring swift updates to the website interface and providing real-time visibility into access history logs. The main door log showcases manager entries, allowing administrators to monitor authorized access, while the client door log offers clients immediate insight into their locker usage patterns.

V. Results and Discussion

The successful implementation of the proposed multilayered authentication system with IoT integration is complemented by a well-executed hardware setup, as depicted in the figures below. Each hardware component plays a crucial role in fortifying bank locker security and contributes to the overall robustness of the system.

The hardware setup, as illustrated in Fig 3, includes the integration of the Adafruit Fingerprint Sensor (GT-521F32), Arduino Uno, keypad, servo motor, NodeMCU, LCD display, and ESP32-CAM. The seamless integration of these components forms the foundation for the multi-layered authentication system and IoT capabilities. Fig 4 illustrates the fingerprint recognition process using the Adafruit Fingerprint Sensor (GT-521F32) and Arduino Uno. The system accurately captures and processes fingerprint data for reliable user authentication. The user-friendly and nontransferable nature of fingerprints enhances the overall convenience and reliability of the authentication process.

Fig 5 demonstrates the keypad password entry process, where users input a personalized code following successful fingerprint recognition. The Arduino Uno manages communication with the keypad and triggers the servo motor for tangible access. Fig 6 showcases the OTP generation process, triggered by incorrect keypad password entries. The system promptly sends alerts to the user's registered mobile number and generates dynamic OTPs for additional authentication. The dynamic nature of OTPs and real-time alerts contribute to both security and user convenience. Fig 7 displays the ESP32-CAM capturing realtime images upon detecting multiple incorrect password attempts. These images are transmitted to a designated manager's Telegram chatbot via the HTTP communication protocol. The integration of IoT for real-time image capturing introduces a proactive security measure. The rapid transmission of images allows for immediate visual verification and intervention, enhancing the system's overall security posture. Fig 8 showcases the manager's main door access log displayed on a dedicated website. The Arduino Uno communicates with NodeMCU via HTTP, ensuring real-time updates to the website interface.

Fig 9 illustrates the client access log displayed on the dedicated website. Arduino Uno facilitates communication with NodeMCU, ensuring swift updates and real-time visibility into locker usage patterns for clients.The client access log empowers users to monitor and analyze their locker usage patterns. This transparency enhances user confidence and contributes to the overall effectiveness of the security system.

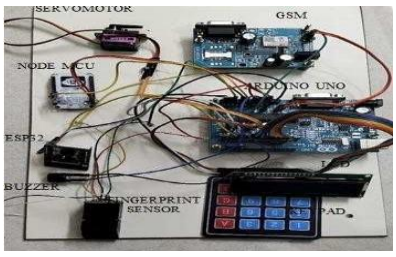

Fig. 3. Proposed system Hardware Setup


Fig. 4. Keypad authentication

Fig. 5. Fingerprint authentication

Fig. 6. OTP generation

Fig. 7. ESP32-CAM image captured and sent to chatbot

io.adafruit.com/E0807/

Created at	Value
2023/03/13 05:46:28PM	RECE...
2023/03/08 10:00:42AM	RECE...
2023/03/08 09:56:27AM	RECE...
2023/03/08 09:56:06AM	RECE...
2023/03/07 09:56:55AM	RECE...
2023/03/07 09:52:03AM	RECE...
2023/03/07 09:26:24AM	RECE...
2023/03/07 09:22:54AM	RECE...
2023/03/07 09:20:06AM	RECE...
2023/03/07 09:16:28AM	RECE...
2023/03/07 09:13:13AM	RECE...
2023/03/07 09:10:51AM	RECE...
2023/03/07 09:08:48AM	RECE...
2023/03/07 08:59:49AM	RECE...

Fig. 8. Access history log of main door (Manager)

2023/03/08 10:01:08AM	JAISH...	×
2023/03/08 10:01:00AM	MANA...	×
2023/03/08 09:56:09AM	View...	×
2023/03/07 09:58:39AM	JAISH...	×
2023/03/07 09:58:30AM	MANA...	×
2023/03/07 09:52:40AM	JAISH...	×
2023/03/07 09:52:32AM	MANA...	×
2023/03/07 09:28:37AM	JAISH...	×
2023/03/07 09:28:14AM	JAISH...	×
2023/03/07 09:27:30AM	JAISH...	×
2023/03/07 09:26:51AM	JAISH...	×
2023/03/07 09:26:42AM	MANA...	×
2023/03/07 09:24:23AM	JAISH...	×
2023/03/07 09:24:14AM	MANA...	×
2023/03/07 09:20:38AM	JAISH...	×
2023/03/07 09:20:14AM	MANA...	×

Fig. 9. Access history log of personal locker (Manager and client)

VI. Conclusion

The proposed multi-layered authentication system with IoT integration represents a significant advancement in bank locker security. By combining various authentication methods and leveraging real-time monitoring through IoT, the system not only fortifies the defense against evolving security threats but also provides a proactive alert system for timely intervention. The inclusion of fingerprint recognition, keypad password entry, and OTP verification ensures a robust and layered approach to authentication, enhancing the overall security posture of bank lockers. The real-time image capture and transmission feature through IoT contributes to a swift response mechanism, enabling security managers to address potential breaches promptly. The maintenance of an access history log further facilitates ongoing monitoring and analysis, aiding in the identification of patterns and potential vulnerabilities. Ultimately, this research contributes to the ongoing efforts in developing advanced security frameworks for safeguarding financial assets, fostering increased confidence among customers in the banking sector.

VII. References

[1] A.Y. Prabhakar et al., "Password Based Door Lock System" *International Research Journal of Engineering and Technology (IRJET)*, Vol. 06 Issue:02, e-ISSN: 2395-0056, 2019.

[2] J Baikerikar et al., "Smart Door Locking Mechanism" *4th Biennial International Conference on Nascent Technologies in Engineering (INCTE),* DOI:10.1109/ICNTE51185.2021.9487704,2021.

[3] Arpit Sharma et al., "Smart Locker System" International Research journal of Modernization in Engineering Technology and Science (IRJMETS), Vol.02,Issue:04, e-ISSN: 2582-5208, 2020.

[4] M P L Chandanshive et al., "Bank Locker Security System based on GSM and RFID", *International Journalof Research in Engineering and Science (IJRES),* Vol.09, pp.30-33, 2021.

[5] M Shresta et al., "Bank Locker Security System with 2 Step

Verification Using GSM" *International Journal for Advanced Research In Science & Technology*, Vol.12, Issue 11, ISSN: 2457-0362, 2022

[6] S H. Jadhav et al., "Smart Bank Locker Security System Using Biometric Fingerprint and GSM Technology" *International Journal of Science and Research (IJSR)*, Vol.05 Issue 10, ISSN: 2319-7064, 2016.

[7] N Meenakshi et al., "Arduino Based Smart Fingerprint Authentication System" 1st*International Conference on Innovations in Information and Communication Technology (ICIICT)*, DOI: 10.1109/ICIICT1. 2019.B741459, 2019.

[8] Pooja K M et al., "Finger Print Based Bank Locker Security System*" International Journal of Engineering Research & Technology (IJERT),* Vol.06, Issue 13, ISSN: 2278-0181, 2018.

[9] L J A Marcilin et al., "Biometric Finger Vein Based Bank Security System Using ARDUINO and GSM Technology" *International Journal of Applied Engineering Research (IJAER),*Vol.13, pp.8774-8777, 2018.

[10] N.Y.L. Venkata et al., "Intelligent Secure Smart Lock System Using Face Biometrics" *International Conference on Recent Trends on Electronics, Information,Communication Technology (RTEICT),*Vol XIV, Issue II, ISSN : 0022-1945,2021.

[11] Akash Thomas et al., "Fingerprint Based Bank Locker Security System" *International Research Journal of Engineering and Technology (IRJET)*, vol.08, Issue :07, e-ISSN: 2395-0056, 2021.

[12] Saifali Shaikh et al., "Bank Locker System Using IOT Concept*" International Journal of Scientific Research & Engineering Trends,* Vol.07 Issue 02, ISSN: 2395-566X, 2021.

[13] Mohan Kumar et al., "Intelligent Security System for Banking Using Internet of Things" Journal *of Computational and Theoretical Nanoscience*, DOI: 10.166/jctn.2019.8180,2019.

[14] Mhaskar et al., "A Survey on IOT Based Secure Bank Locker System" *International Journal of Research Publication and Reviews (IJRPR)*, Vol.02, Issue 12, pp 1143-1146, 2021.

[15] Mohan Kumar et al., Intelligent Security System for Banking Using Internet of Things" *Journal of Computational and Theoretical Nanoscience*, pp 3296-3299, 2019.