ISSN: 2454-9940

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

E-Mail :
editor.ijasem@gmail.com
editor@ijasem.org

www.ijasem.org

INTERNATIONAL JOURNAL OF APPLIED SCIENCE ENGINEERING AND MANAGEMENT

ISSN:2454-9940 www.ijsem.org
Vol 20, Issuse.2 April 2026

Enhancing Bank Locker Security through Multi-Layered Authentication and IoT Integration

[1]Gorre Nagendra Kumar,[2]Lingala Suchitha Reddy,[3]Chatla Sairam,[4]Kandhukuri Maheshwara Chary, [5]Dr.G.Nagajyothi Sree,

[1,2,3,4] Student,Department of ECE,Narsimha Reddy Engineering College,Misammaguda(V), Kompally-500100, Telangana State,India.
[5] Associate Professor,Department of ECE,Narsimha Reddy Engineering College,Misammaguda(V), Kompally-500100, Telangana State,India.

Abstract

Financial organizations are always looking for new ways to secure the precious valuables kept in bank lockers from new security threats. This study delves into a thorough strategy to strengthen the security of bank lockers by using the Internet of Things (IoT) and including various levels of verification. The suggested system includes features like as fingerprint scanning, a keypad for entering passwords, one-time password (OTP) verification, and the ability to collect images of intrusion attempts in real-time. Fingerprint recognition provides a safe and easy way to enter lockers by ensuring biometric uniqueness. Keypad password entry is an extra security feature that asks users to enter a unique code. One-time password (OTP) verification is an additional layer of protection against unauthorised access as it generates time-sensitive codes dynamically. Improving safety precautions is largely dependent on the use of IoT. When a bot belonging to a certain management detects an attempt at illegal access, the system snaps a picture of the invader and sends it to that manager. This early warning system allows for prompt action. In order to help security managers keep tabs on how often users enter certain lockers, the system keeps a record of all accesses. The security of bank lockers is enhanced and new threats are effectively countered by the proposed multi-layered authentication system that incorporates the internet of things. The ongoing efforts to establish sophisticated security frameworks for securing financial assets are enhanced by this study, which eventually fosters more trust among banking consumers.

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

INTRODUCTION

The safest place to store valuables is in a bank locker. However, criminals often target banks, thus the recent uptick in threats against these institutions is cause for alarm. Accessible current procedures in our banks are not very effective, and they can be simply falsified or produced by the crafty and evil brains in our society. Currently, in order to open a bank locker, one requires both the key and the keypad. One key will be given to the individual who unlocks the bank locker, while the other key will be retained by the bank. The most significant drawback is that there is a penalty and replacement payment for when the key is lost. Several keyless strategies are presented in the articles to tackle these issues. Secure access to the bank locker may be achieved with the help of a password-protected door lock that simultaneously activates, authenticates, and validates the user in real time. than begin with, passwords are superior than alternative methods in terms of security [1]. This method requires the use of a keypad for password entry. When the user inputs the wrong password, the intruder alert notifies the wrong person that they are trying to access the system [2]. A one-time password (OTP) is a temporary security code that changes with each login. Using one-time passwords (OTPs) improves the security of static password-based authentication [3]. Unfortunately, forgetting the password does happen from time to time; in such a scenario, we will have to revisit the

topic of RFID cards. Digital security systems that use a passive kind of RFID are able to activate, authenticate people in real-time, and unlock doors for protected access [4]. An SMS is sent to a person with legal status via GSM if the ID number received by the RFID reader tag is correct. The safe will open [5-6] if the password is correct. Due to the increased expense and the possibility of losing the RFID tag, not everyone can afford to use one.

The most recent advancements in the field of security system development have made use of biometric methods. It is possible to verify an individual's identification and distinguish them from others by using their distinct biometrics. A fantastic answer to the challenges that are often encountered is the fingerprint-based lock. One way to get access to a system that uses fingerprint recognition technology is to have one's fingerprints saved in memory beforehand [7]. The authorized person receives a notification and presses the buzzer if the fingerprints don't match [8-10]. There are four tiers to the security system. The locker is more secure with the combination of several authentication methods. A four-tiered authentication system that uses voice, password, and facial recognition. After a person has unlocked all four levels of protection, they are granted access to the protected area [11]. The system reads data from the fingerprint sensor and inputs it into the AVR microcontroller, ensuring that only the authorized user may access the locker and recover the papers or money.[12] Using a simple alert message or buzzer to identify who is accessing the locker is not going to work. Thus, the Internet of Things (IoT) has been put into place so that only authorized individuals may enter safely. A Raspberry Pi is used for this purpose, and the photos are sent to the user's email address via mail [13]. For both live streaming and portrait photography, the ESP32-cam camera sensor is used. It has a high reputation. This system is able to identify the person standing in front of the door thanks to the AI-Thinker in the esp32 camera. cited as [14]. The installed IoT gadget records all activity and stores them on the cloud. Users' and clients' property is better protected thanks to the Internet of Things (IoT) security system [15]. The system presents a number of authentication mechanisms to offer high-level security.

REQUIREMENTS

The Uno board for Arduino Among those interested in electrical projects, the Arduino Uno is a well-liked microcontroller board due to its versatility and user-friendliness. It is designed to work with an input voltage range of 7-12V and is powered by the Atmega328P microprocessor, which works at 5V. In addition to six analog input pins and fourteen digital I/O pins, six of these pins may output pulse width modulation. The maximum current that can be handled by each digital I/O pin is 20 mA, with the exception of the 3.3V pin, which can manage 50 mA. There is more than enough memory on the Arduino Uno—32 KB of flash, 2 KB of SRAM, and 1 KB of EEPROM—to store data and code. A clock speed of 16 MH is what the Arduino Uno uses to function. B. Liquid Crystal Displays (LCDs) Liquid crystal displays (LCDs) are a typical kind of output device in electronic projects; their performance and usability are defined by a number of requirements. Display clarity and detail are dictated by the resolution, which is measured in pixels. Images with higher resolutions are sharper. Because of its longevity, low power consumption, and high brightness, LED backlights are widely used. An additional important consideration is the compatibility of the interface; LCDs may support many interfaces, such as I2C, SPI, or parallel communication.
Buzzer (C) A buzzer, often called a piezo buzzer, is a small and ubiquitous component of many electrical circuits that produces audible sound. It uses low voltages (usually around 5V DC) to generate sound by vibrating a piezoelectric element in response to an applied electrical signal. Buzzers typically have a volume level between 70 and 120 decibels (dB), the standard unit of measurement for sound volume. For the purpose of giving auditory warnings, notifications, or alarms, buzzers are extensively used in electronic projects.

D. MCU Node One such open-source IoT (Internet of Things) platform is the Node MCU, which uses the ESP8266 WIFI module as its foundation. A Tensilica L106 32-bit microprocessor with built-in WIFI and clock speeds of 80 MHz or 160 MHz is shown. Wireless connectivity is a breeze with the Node MCU since it is compatible with IEEE 802.11 b/g/n standards. With its general-purpose input/output (GPIO) pins, it's easy to connect to a wide range of sensors and actuators.
E. GSM Module: GSM modules provide many functions for wireless connection and are hence essential parts of communication systems. In most cases, these modules are compatible with a wide range of cellular networks throughout the world since they support numerous frequency bands. They use AT instructions to interface with microcontrollers or other devices, and they include SIM card slots for subscriber authentication and identification. For easy connection and integration, GSM modules commonly provide UART ports. The use of authentication and

ISSN:2454-9940 www.ijsem.org
Vol 20, Issuse.2 April 2026

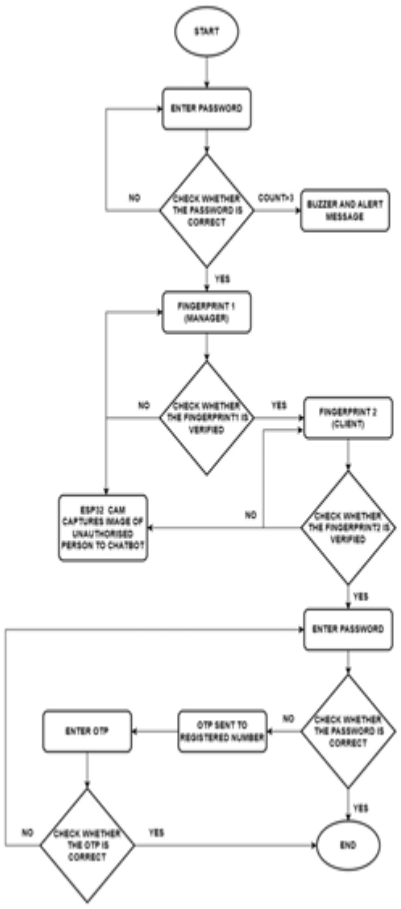
encryption algorithms to protect data transfer is an important part of the security measures. These modules are compatible with data transmission protocols including GPRS (General Packet Radio Service) and SMS (Short Message Service) and run on low power, allowing for efficient energy use. F. Servo Motor: These are specialty motors made for linear or angular position control. A direct current motor, gears, and a system for providing feedback make them up. The servo can continually fine-tune and hold its position thanks to the feedback, which is often a potentiometer. When controlled movement is required, servo motors are the way to go because of their reputation for precision and accuracy. You may get them in a range of sizes and power levels, and they usually run on low voltage. Servo motors are controlled by pulse-width modulation (PWM) impulses and have a restricted range of rotation, usually about 180 degrees. H. ESP32-CAM A strong foundation for Internet of Things (IoT) and image-related applications, the ESP32-CAM is an adaptable development board that combines the ESP32 microcontroller with a camera module. It has WIFI and Bluetooth integrated right in, and the ESP32-S processor gives it dual-core computing power. Up to 2 megapixels of resolution may be captured with the OV2640 camera module, whether it's still photos or video. You may save media files locally on the board via the microSD card slot. A wide variety of sensors and devices may be easily integrated with the ESP32-CAM because to its many interfaces, including GPIO pins, UART, and I2C. H. Fingerprint Sensors Security applications may benefit from fingerprint sensors, which are biometric devices that can record and verify distinct fingerprint patterns. These fingerprint scanners usually take high-resolution pictures using capacitive or optical scanning technologies. The degree of detail of fingerprint pictures is determined on the resolution of the fingerprint sensor, which is specified in dots per inch (DPI). The False Acceptance Rate (FAR) and the False Rejection Rate (FRR) are common metrics for gauging the precision of the sensor.

SYSTEM ARCHITECTURE

The whole suggested system is shown in Fig. 1, which is a block diagram. Fingerprint recognition, keypad password input, one-time password verification, and real-time picture capturing of unlawful access attempts are all ways the suggested system improves the security of bank lockers. Keypad password input provides an additional degree of protection, while fingerprint recognition guarantees safe and easy access. One-time password (OTP) verification reduces the likelihood of unwanted access by creating time-sensitive codes. IoT integration captures and transmits images of unauthorized attempts to a manager's bot for timely intervention.

Block Diagram B. Process model specification Fig 2 shows the process model specification which defines the modes of operation of the proposed system.

ISSN:2454-9940 www.ijsem.org
Vol 20, Issuse.2 April 2026



Flow chart

PROPOSED WORK

Keeping clients' money and other valuables secure in bank vaults is an area of critical importance for the banking industry. This study introduces a state-of-the-art method for strengthening the security of bank lockers via the use of the Internet of Things (IoT) and various levels of authentication. A strong defense against ever-changing security risks is created by the suggested system, which integrates fingerprint recognition, keypad password input, one-time password (OTP) verification, and real-time picture capture.

A complex authentication system with several levels is the Multi-Layer Authentication System. These are the features and components that they include: The First: Fingerprint Identification: The process of fingerprint identification is based on taking a picture of a person's fingerprint and studying its distinct characteristics. The Adafruit Fingerprint Sensor (GT 521F32), which is compatible with Arduino Uno, integrates well with the microcontroller in our suggested solution for bank locker security. The Arduino Uno does a good job of coordinating the fingerprint sensor's interactions with the rest of the system.

The inbuilt algorithms in the Arduino Uno carefully examine the collected fingerprint data, finding and extracting minute details to generate a one-of-a-kind fingerprint template. In order to verify the user's identity, the Arduino Uno cleverly checks the recorded fingerprint against pre-existing templates and then either authorizes or denies access accordingly. In addition, strong encryption measures are used by the microcontroller to preserve sensitive biometric data, ensuring that fingerprint templates are stored securely. With this unified system, the bank locker system is protected and users have access to a trustworthy, one-of-a-kind, and hassle-free authentication mechanism. Keypad Password Entry: Our upgraded bank locker security system incorporates Keypad Password Entry as a secondary authentication layer, supplementing the original fingerprint identification. Users enter a unique code using the keypad once their fingerprints have been satisfactorily authenticated. The microprocessor of the system, the Arduino Uno, ensures that the keypad and security system communicate without a hitch. Approved users who have the relevant code may go on to the next security level once the password is checked against stored credentials. A servo motor is used as an additional layer to physically operate the lock mechanism of the locker. After the two-factor authentication is finished, the servo motor is activated by the Arduino Uno to lock or open the bank locker, giving a physical and secure way to enter. An additional layer of protection for the bank locker system is provided by the use of a servo motor, which guarantees a strong physical barrier. To summarize, a thorough multi-layered authentication system is set up to secure important valuables in the bank locker via the combination of biometric fingerprint identification, keypad password input, and servo motor activation. creation of OPTs: Our suggested method for protecting bank lockers includes an error-handling mechanism that improves both security and usability. When the client enters the wrong password on the keypad, the system immediately notifies them via their registered cellphone number that someone has tried to access their personal locker without their permission. At the same time, a client's mobile device receives an SMS with a randomly created one-time password (OTP). This one-time password (OTP) acts as a backup password, increasing safety.

ISSN:2454-9940 www.ijsem.org
Vol 20, Issuse.2 April 2026

The interface is an LCD display that shows important information including alert messages and one-time password prompts, allowing for easy interaction. The user is shown on the LCD screen to input the code that they got via the keypad after getting the alert and one-time password. You will be allowed access to your personal locker if the provided one-time password (OTP) is genuine and matches. In addition to bolstering security via multi-factor authentication, this dynamic scenario guarantees user ease and quick resolution in the event of an incorrect keypad input, all of which contribute to a bank locker system that is both safe and easy to use. Part C. Internet of Things Integration 1) Capturing images in real-time: to prevent security breaches, a crucial component has been added into the suggested system to increase the safety of bank lockers using multi-layered authentication and the Internet of Things. If the system detects three consecutive wrong passwords, it will initiate a thorough security response, which is why it continuously watches password entering attempts. This event sets off an ESP32-CAM, an Internet of Things (IoT) camera that is carefully positioned within the bank's locker room. Quickly snapping photos of the intruder in real time, the ESP32-CAM records their every move. Using the Hypertext Transfer Protocol (HTTP), these pictures are quickly sent to a manager's Telegram chatbot.

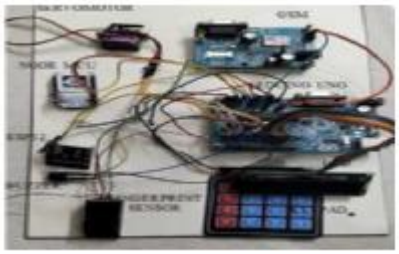
This well planned procedure enables the designated manager to visually verify any questionable behavior in a timely manner, enabling them to intervene and investigate any issue with lightning speed. This integrated security solution strengthens the whole system and provides proactive protection against possible threats to precious assets housed in bank lockers by matching the picture capture process with the occurrence of many failed password attempts. Detailed record of all accesses: Arduino Uno is the brains behind our state-of-the-art bank locker security system, acting as a master controller that keeps an eye on everything. The fingerprint scanner, the NodeMCU, and the dual access history logs are all part of the system that works together to authenticate users and communicate with the internet of things (IoT) using HTTP.In order to confirm the user's identification using biometric data, the Arduino Uno communicates with the fingerprint scanner whenever they try to get access. When a manager or client's unique fingerprint is scanned, it automatically adds the entry to the appropriate access log. Incorporating biometric authentication into the multi-pronged security strategy strengthens it. The lightning-fast website interface changes and real-time insight into access history logs are both made possible by the HTTP communication between Arduino Uno and NodeMCU. Administrators may keep tabs on permitted access in the main door log, which displays entries made by managers, and customers can see how often they use their lockers in the client door log.

RESULTS AND DISCUSSION

A well-executed hardware configuration is essential for the effective deployment of the proposed multi-layered authentication system with IoT integration, as shown in the figures below. Strengthening the security of bank lockers and the system as a whole is the responsibility of each individual hardware component. Figure 3 shows the hardware configuration, which contains the following components: ESP32-CAM, an LCD display, an Adafruit Fingerprint Sensor (GT-521F32), an Arduino Uno, a keypad, a servo motor, and NodeMCU. The capabilities of the Internet of Things (IoT) and the multi-layered authentication system are built upon the smooth integration of various components. In Figure 4, we can see how the Adafruit Fingerprint Sensor (GT-521F32) and the Arduino Uno work together to recognize fingerprints. In order to authenticate users reliably, the system takes and analyzes fingerprint data precisely. Fingerprints improve the authentication procedure in general due to their user-friendliness and non-transferability. After fingerprint recognition is successful, users enter a customized code using the keypad, as shown in Fig. 5. When a user presses a key, the Arduino Uno controls a servo motor to make physical access possible. When a user enters an incorrect password on the keypad, the process of generating an OTP is shown in Figure 6. Quick notifications are sent to the user's registered cellphone number and dynamic one-time passwords (OTPs) are generated for further security. Optimal Time Passwords (OTPs) and real-time notifications are convenient and secure because of their dynamic nature. Upon detecting several erroneous password attempts, the ESP32-CAM captures real-time photos (Fig. 7). Using the HTTP communication protocol, these photos are sent to a manager's chosen Telegram chatbot. Internet of Things (IoT) integration for real-time picture capture brings a preventative security precaution. Immediate visual verification and action are made possible by the quick transmission of pictures, which improves the system's overall security posture. The primary door access record kept by the management is shown on a specific website (Fig. 8). Thanks to the HTTP connection between the Arduino Uno and NodeMCU, the web interface may receive

ISSN:2454-9940 www.ijsem.org
Vol 20, Issuse.2 April 2026

changes in real time. Figure 9 shows the dedicated website's customer access record. Clients may see use trends in real time and get fast updates thanks to Arduino Uno's connectivity with NodeMCU.Customers may keep tabs on how often they use their lockers by looking at the client access record. The security system as a whole benefits from this openness, which boosts user trust.



Proposed system Hardware Setup

Fig. 5. Fingerprint authentication

OTP generation

ESP32-CAM image captured and sent to chatbot

CONCLUSION

The security of bank lockers would be greatly enhanced by the suggested multi-layered authentication system that incorporates the Internet of Things. The solution strengthens the protection against developing security threats and offers a proactive alarm system for timely action by integrating several authentication methods and using real-time monitoring via the Internet of Things. The security of bank lockers is enhanced by including several layers of authentication, such as fingerprint recognition, keypad password input, and one-time password verification. With the help of the Internet of Things (IoT), security administrators may quickly respond to any breaches thanks to the real-time picture capture and transfer capability. Ongoing monitoring and analysis is made much easier with the help of an access history record, which may help identify trends and possible risks. Customers will have more faith in banks as a result of this study,

which adds to the continuing efforts to create sophisticated security systems to protect financial assets.

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), vol02, issue:04, e-ISSN: 2582-5208, 2020. [4] [5] [6] [7] [8] [9]

[4]. M. P. L. Chandanshive et al., "Bank Locker Security System based on GSM and RFID", International Journal of 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 S. H.

[6]. 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. N.

[7]. Meenakshi et al., "Arduino Based Smart Fingerprint Authentication System" 1stInternational Conference on Innovations in Information and Communication Technology (ICIICT), DOI: 10.1109/ICIICT1. 2019.B741459, 2019. K. M. Pooja et al., "Finger Print Based Bank Locker Security System" International Journal of Engineering Research & Technology (IJERT), vol.06, issue: 13, ISSN: 2278-0181, 2018. L. J. A.

[8]. 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.

[9]. 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.

[10]. 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.

[11]. 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.

[12]. 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.

[13]. 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.

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