TriGuard Bank Locker Authentication

[1]Aditi Joshi, [2]Sai Joshi, [3]Mrunmayee Joshi, [4]Rajasi Moratkar, [5]Rashi Bhavik,
[6]Dr. Jaya Raut, [7]Sandeep Sonaskar
[1,2,3,4,5]UG Students, Department of Electronics and Telecommunication Engineering, MKSSS Cummins College of Engineering for Women, Nagpur, Maharashtra, India - 441110
[6]Assistant Professor, Department of Electronics and Telecommunication Engineering,
MKSSS Cummins College of Engineering for Women, Nagpur, Maharashtra(State), India – 441110
[7]Industrial Guide, Director VS Informatics Pvt. Ltd., Nagpur, Maharashtra(State), India – 440022

Abstract—**TriGuard Bank Locker Authentication system developed specially as a robust security system for the enhancement of bank locker security. Security keys deployed in a lock system are most vulnerable to intrusion and thus unauthorized access is easily attained. Unlike earlier systems, which were primarily dependent on an intelligent chip to accomplish biometric authentication and multi-factor security, the present system uses a highly reliable access control method with a combination of biometric authentication and multi-factor security to implement access control. It is ESP microcontroller CPU-based, ESP32-CAM for face recognition, and biometric authentication via a fingerprint sensor, OTP entry keypad, and LCD display for live status update.**

The access process has different authentication levels for security and flexibility. The locker may be accessed by the account holder directly through face recognition alone. In the absence of the account holder, the access is granted to a registered relative through fingerprint authentication and subsequent OTP verification is provided. An automated OTP is sent to the account holder's registered mobile number. The account holder must forward it to the relative for the last authentication process via the keypad. If an intruder attempts to access, the system denies authentication and protected against any potential security breach. With the integration of facial recognition for the account holder and fingerprint scan along with OTP authentication under a single system, TriGuard Bank Locker Authentication merges the aspects of both higher security and the capability for greater optimization and completely minimizes attacks from conventional locking mechanisms.

***Keywords*—IoT, biometric authentication, real-time monitoring, fingerprint recognition, facial recognition, OTP verification, security framework, access control, secure bank locker system, embedded systems, ESP32, encryption, tamper detection, prevention of unauthorized access, resource optimization, secure storage, multi-factor authentication.**

I. Introduction

The security system assaults directed towards protection of financial assets have led to sophisticated types of authentication processes that reverse the associated threats of traditional security. Security systems have been transformed over the years, away from traditional methods like key locks, PIN codes, and identification cards. These were easier to manipulate or circumvent, so they are being phased out in favor of more advanced and secure technologies. Embedding identity parameters like facial recognition and fingerprint scanning has the potential to enrich security in access control systems. The TriGuard-Bank Locker Authentication System, in essence, stands on Face ID, fingerprint authentication, and OTP-based authentication.

The whole system is managed via an ESP microcontroller to authenticate multi-layered authentication. As indicated by its name, the ESP32-CAM module is integrated to capture a picture of the account holder's face and access it upon successful authentication. If the account holder is not present, an authorized relative can access the locker through fingerprint identification. Such fingerprint recognition will result in sending an OTP to the registered mobile number of the account holder, who sends the OTP to the relative, who enters it using a keypad to access. All unauthorized access attempts by unregistered fingerprint inputs as well as wrong OTP entries are automatically dropped to achieve strong security. While biometric systems have acceptable performance in most applications, ongoing efforts are required to enhance their convenience, security, and privacy.

The hardware topology of the TriGuard system comprises an ESP microcontroller to control, ESP32-CAM for facial recognition, fingerprint sensor for biometric verification, keypad for OTP input, and an LCD display to provide system status feedback. This biometric and OTP-based access control system thus fulfills the needs of real-time security monitoring, cyber threat protection, and user convenience. Certainly, the TriGuard system offers a highly secure, scalable, user-friendly solution for the protection of financial assets in Bank Locker Systems using biometric authentication and brought-in security technologies.

II. Objective

Increased Security by Using Multi-Tier Authentication
The system implements three tiers of authentication via Face ID identification, fingerprint recognition, and OTP-based entry. Thus, only the authorized person can open the bank locker, and three-tier authentication provides no opportunity for unauthorized users.

Biometric And OTP Relative Access
In cases where the main owner is unavailable, access may be granted to a family member through fingerprint identification and an OTP, allowing secondary access to be determined and secured.

Real-Time Monitoring and Instant Alerts

The system empowers GSM-based real-time communication in sending immediate alerts to the administrator after a successful login, a failed login, an unauthorized usage attempt, which allows active monitoring of security.

Protection Against Unauthorized Access

The highest protection against abuse is ensured through restrictions against locker access without a valid Face ID, fingerprint, and OTP verification, which are all considered to be malfunctions.

Management Interface with Operational Facility for Participants

The system is equipped with an LCD screen and push-button interface, thus guiding users in a user-friendly manner through the various authentication stages, allowing the administrators and authorized personnel to operate the system easily.

Strong Power Supply

To ensure the system operates continuously and does not lose functionalities during power failure, thereby ensuring uninterrupted security operations.

Scalability And Flexibility for Future Expansion

Designed for scaling and extension for further development purposes to integrate extra security options, integration with bank systems, and flexibility of application in different secure access control functions.

III. Literature Survey

H. S. Detroja, P. J. Vasoya, D. D. Kotadiya, and C. B. Bambhroliya suggested a very secure locker system based on RFID, fingerprint biometric authentication, password and GSM technology. The system registers users using a username, password and fingerprint. While logging time the user scans an RFID tag, fingers and then enters a password like three step authentications. If all the authentication steps fail, then the alarm buzz at that time and sends out an alert message to users registered mobile number. Successful verification allows the microcontroller to capture user data and unlock the locker while recording user's check-ins and check-outs.

S. S. Palsodkar and S. B. Patil suggested a biometric locker system in which banks are advancing their system by automating their system where they must store the biometric details for accessing lockers as authorized user's information has to be saved in the bank's data or server. Only authorized users can be granted the access to the locker and only they can open locker, providing better security with biometric and GSM verification.

G. Chavan, S. Dabke, A. Ghandghe and K. A. Musale created a sophisticated banking security system that provides authenticated user's access to the locker with a multiple authentication process. It provides a unique password and OTP to verify authentication. When entering the first door, an OTP is sent through an Android application, which deactivates the IR sensor and provides entry to the second door. Unauthorized attempt at access, e.g., crossing the IR sensor without OTP authentication, generates an alarm. Access to the locker is only permitted fully after clearing all three levels of authentication.

Marco's research (2023) examined the role of facial recognition in safe mobile banking. The research was successful in addressing the lack of biometric authentication among existing mobile banking apps and highlighted the advantages of facial recognition along with OTP verification. The research made facial recognition a safe mode of authentication and proposed integration approaches to facilitate effective and secure user authentication.

Golatkar et al. (2022) investigated multifactor authentication for bank staff in web banking security. The research incorporated user registration, OTP verification and fingerprint scanning for safe access. The system was designed to avoid fraud and unauthorized transactions using biometric and OTP-based authentication, thus enhancing customer confidence and providing multi-layered security.

Pooja et al. (2018) suggested a fingerprint-based bank locker security system that combines OTP validation. The system necessitates users to register with biometric credentials for easy access in a secure manner. Identification is performed using fingerprint scanning and OTP verification through Bluetooth. Biometric security was the focus of the study as a primary aspect.

IV. Methodology

Typical bank security systems are mechanical key systems in which users get one key, and the other is held by the bank or in previous systems, RFID cards were assigned unique ID numbers for authentication. However, they lacked strong security measures, making them vulnerable to theft or duplication. An unauthorized person could easily misuse a stolen RFID card to gain access, posing a significant security risk. The tri-guard bank locker authentication system is a combination of many multi-factor authentication methods, like photo ID for the account holder, finger scanning, and OTP-verification for the relatives to eliminate the discredit caused by the conventional methods. This security system allows access only after validating and authenticating the identity of the user: thereby making their security very high and denying unauthorized entries. The TriGuard Bank Locker Authentication system provides improved security with a multilayered authentication process. The system comprises hardware modules such as an ESP32 microcontroller, which is the main part of the project, as the central processing unit, an ESP32-CAM module for facial recognition, a fingerprint sensor for biometric authentication, a keypad to enter OTP, LCD display for displaying the required content and a power supply module for uninterrupted and smooth operation.

The implementation is done using Embedded C/C++ for ESP32 processing, OTP generation, and incorporating a face recognition library for verification. The verification starts with face recognition for owner access to the bank; if not available, a registered relative verifies through fingerprint scan, creating an OTP sent to the owner's mobile phone. OTP authentication via the keypad, entry is permitted. Unlimited attempts to enter the correct OTP are provided by the system, which is active until the correct OTP is entered. With a constant power supply, the system provides high security and robust protection against unauthorized entry. When an unregistered user tries to unlock the locker, all the authentication procedures such as fingerprint scanning and OTP verification will be rejected, and the system will be inactive without showing any data or performing any action.

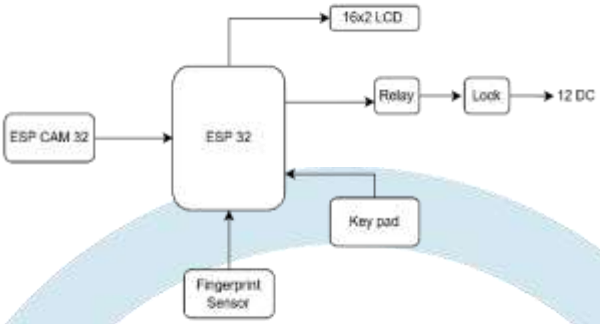

Fig 1: Block Diagram of Bank Locker System

V. Proposed System

This safety precaution of TriGuard Bank Locker Authentication System has a multi-layer defense against unauthorized entry, duplication of keys, and forced opening. Adding biometric authentication with Face ID, Fingerprint scanning, and OTP authentication adds a layer of security and transparency with heavier and secure integration of a robust security system. A biometric system is an extraction and pattern or feature authentication with information being stored in the microcontroller and matched with input for the purpose of verification. The operation of this system is based on a dual mode: verification and identification. Identification is the matching of collected biometric information with information stored, while verification matches both for confirming authenticity.

The entire authentication method is controlled by the ESP32 microcontroller whereby Face ID authentication using the ESP32-CAM module and fingerprint biometric authentication is done using the fingerprint sensor. OTP authentication is done through the GSM SIM800L module, which sends one-time passwords OTP to the mobile number stored in the module. The OTP is then entered through the 4x4 matrix keypad to confirm two-factor authentication. The LED of the GSM module is delayed for 3 seconds for stabilization before being connected for stable communication. A 16x2 LCD display is used for real-time status information.

The storage of authentication information is done in the onboard memory of the ESP32, and fingerprint templates are stored in the fingerprint module. The power supply unit for the system works with DC-to-DC supplies, the solenoid valve is fed by a 12V battery supply, while the rest of the circuit is powered by 5V, ensuring efficacy and steadiness.

The process of authentication is supported by primary and secondary access mechanisms. The first one allows the account owner to unlock the locker via Face ID authentication. If the account owner is unavailable, the second one allows the authorized family member to open the locker by fingerprint scanning, followed by OTP sent to the account holder's registered mobile. The OTP is then entered via the keypad for authentication to be complete. Absence of a response in case of unauthorized access means that the system would not recognize the fingerprint scan, therefore no OTP would be created while the unlocking operation would be shut down. The TriGuard Bank Locker Authentication System is very flexible and can be used in corporate vaults, secure storerooms, and even domestic safes. This is both an automated and expandable system, which gives more security and ease of convenience.

By negating human involvement in its setup, it also provides a low-cost, effective means of securing valuables. As its biometric authentications are unique to all, it safeguards against unauthorized access. The users do not have to remember any passwords or carry any physical tokens provided by the system which makes this system very secure and easy to work with.

Table 1: Components and Specification

Sr. No.	Component Name	Specification
1	**ESP32 Microcontroller**	Dual-core processor, Wi-Fi +Bluetooth,240 MHz, 4MB Flash
2	**ESP32-CAM Module**	2MP camera, WiFi + Bluetooth, supports face detection and recognition
3	**Fingerprint Sensor**	Optical sensor; supports template creation, storage, and matching; UART interface
4	**GSM SIM800L Module**	Quad-band GSM; UART interface; supports AT commands; operates at 3.7V– 4.2V
5	**Keypad(4x4 Matrix)**	16-key matrix layout for manual PIN/OTP entry

6	**LCD Display**	16x2 LCD for real-time user interaction and authentication status
7	**LED Indicator**	Provides real-time authentication status
8	**Power Supply**	12V DC battery for continuous operation

VI. SYSTEM EXPLANATION

TriGuard Bank Locker Authentication System is a multi-layer security solution designed to protect bank lockers using biometric and OTP authentication. It is built on the ESP32 microcontroller, which is the master control unit and interfaces with multiple authentication modules, including the ESP32-CAM for facial recognition, a biometric fingerprint reader, a keypad for entering the OTP and LCD display for user feedback. Access control is ensured regarding authorized users that can open the locker against undesired access. The authentication process starts when an individual tries to open the locker. The main method of authentication is facial recognition carried out by the ESP32-CAM module, which scans the account holder's face and compares it with stored data. The locker opens upon successful authentication. In case the account holder is not present, an alternative process of verification is made available to an authorized relative.

For relative access, the user initially scans his or her fingerprint through the biometric fingerprint sensor. Once the fingerprint is authenticated, the GSM SIM800L module sends an OTP to the mobile number of the registered account holder. The account holder sends the OTP to the relative, who enters the same via the 4x4 keypad. OTP does not expire until the right one is entered. There are no attempts restricted; the system merely waits for an accurate input, and the relative may access the locker without time limitations. The locker is governed by a relay module, locking the solenoid solely for proper fingerprint readings. There is no unlocking either without a fingerprint scan or on detection of an invalid fingerprint. The solenoid valve that is part of the locking system needs 12V power to be triggered and open the locker upon successful authentication. Although the solenoid valve is energized by the 12V power, the entire circuit runs at 5V. A DC-to-DC converter makes the 12V supply at 5V to power the ESP32, fingerprint reader, keypad, and GSM module. An LED indicator in a GSM module operates on the concept of adding a 3-second delay to capture longstanding OTP transmission as the network is being connected.

In case of Account-holder it has some steps under it to enroll the face. ESP32-CAM, it runs through different steps. First, the laptop hotspot is activated, and the bank locker is turned on. When both systems are done connecting, the laptop displays an 11-digit identification number. Copy this ID and paste it into a new Chrome tab to open a page that has provisions for Start Streaming and Enroll Face. On clicking the Enroll Face option, the face will be scanned for enrollment by the ESP32-CAM. When the laptop enrolls the face properly, the account holder can gain access to the account by face recognition. After the face has been enrolled, the relay is activated to give further access to the system.

The outcome is that the TriGuard Bank Locker Authentication System becomes an advanced promising secure, efficient, and expandable method due to biometric authentication, IoT integration, and secure access control mechanisms, which are at present required in bank security for free and unencumbered access to the use.

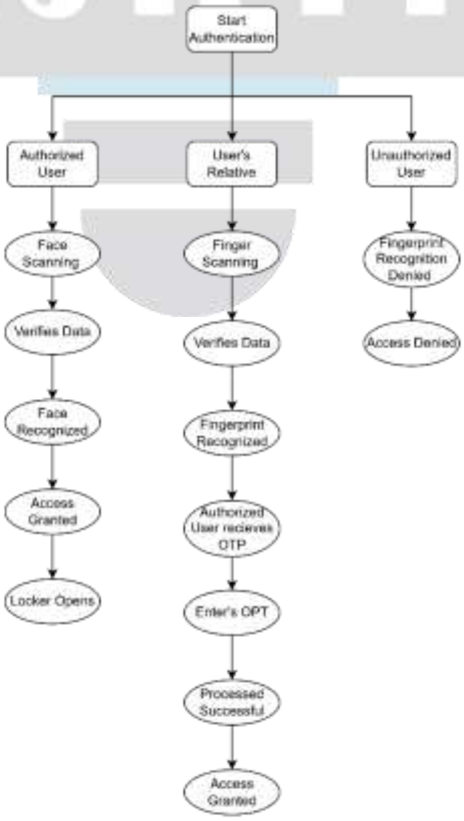

Fig 2: Flow Chart of Bank Locker System

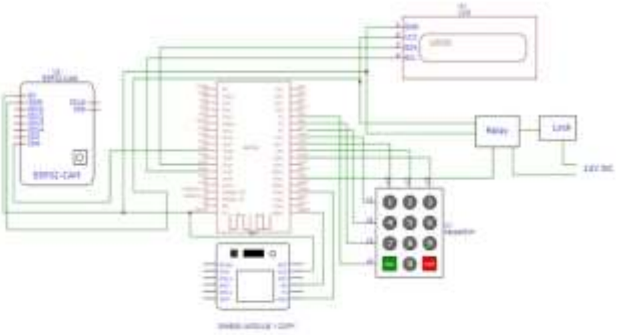

Fig 3: Circuit Diagram of Bank Locker System

VII. Performance Analysis

TriGuard Bank Locker Authentication System is a secure and effective method of authenticating your bank locker using Face ID, fingerprint verification, and OTPs for authentication. Biometric fingerprint verification is quite responsive and has a low false acceptance or false rejection rate, thus restricting the attempts of unauthorized entry. Authentication requests will be handled with minimal delay by an ESP32 microcontroller, maintaining smooth user experience. The LCD interface and keypad interface are intended towards end users and administrators for accessible and most efficient authentication process.

A GSM SIM800L module is a second layer of security with dynamic OTPs delivered to registered users for security. With uninterruptible power supply (UPS), the machine fully functions in future even during blackouts. Since immediate signals of LED indicator immediately notify the users feedback about authentication, it enhances system integrity.

The TriGuard System has demonstrated its value over the years in securing bank lockers; additional improvements in the future could include multi-factor authentication, advanced algorithms for encryption. Providing configurability for larger banking institutions would also definitely make the system an incredibly reliable and tamper-proof security solution of choice for modern financial applications.

VIII. Result

The successful installation and testing of the TriGuard Bank Locker Authentication System proved to be effective in securing bank lockers via multi-layer authentication. The system accurately authenticated the account holder, ensuring smooth and secure access through Face ID recognition. Under scenarios in which the account holder would not be available, approved relatives of the account holder are given entry to the locker via fingerprint scan with subsequent secure OTP verification sent to the account holder's phone. Thus, the convenience of the system does not compromise on security. Attempts at unauthorized access were denied by the system because entry was not allowed to the unregistered persons proved its solid security system. Automated OTP under notifications improved monitoring and accountability. It enabled dynamic processing and faster user authentication through an integration of the ESP microcontroller and ESP32-CAM. Overall, the system was reliable, scalable, and user-friendly, making it very feasible for financial institutions and high-end storage units and promising a considerable level of safety against unauthorized access.

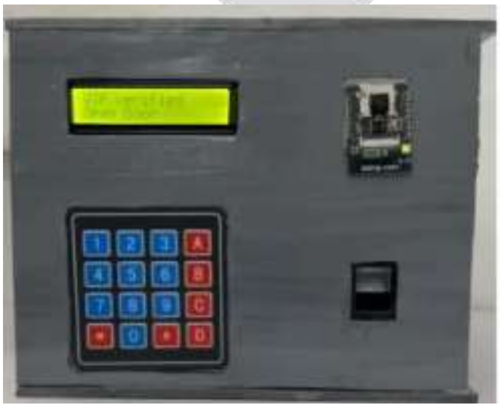

Fig 4: Final Output

IX. Conclusion

The TriGuard Bank Locker Authentication System is a contemporary security system with many layers which are immune to the cons of old-password-based authentication. Face ID recognition, fingerprint scanning, and OTP authentication at once make it secure from unauthorized access. Moreover, there are live SMS notifications, making it an even more reliable security system because it ensures 24/7 monitoring and accountability.

All of it comes in a cost-effective, low energy, compact, and independent mode and is a highly efficient in-built solution for security. So modular and space-efficient, they can well be configured to their firewalls, banks, and corporate houses or warehouses for valuable commodities.

The system has a very bright future in the application as the security needs change, and enhancements can be made through AI-enabled fraud detection, advanced multi-factor authentication, stronger encryption methods, and would be more tampered-proof and future-proof. Proper backup integration facilitates smooth operations, making the security close at any time and as demands of banking and financial security continue to explode, it follows that the TriGuard System is going to be the whole, up-to-date answer for tough, secure access to authorized users.

X. Future Scope

The TriGuard Bank Locker Authentication System is a sophisticated security system designed for multi-factor authentication businesses to secure valuables. Using Face ID recognition, fingerprint scanning, and one-time password (OTP) verification, it has ensured that only authentic individuals can gain access to its secured valuables. This system can be well utilized by the banking and financial institutions to avoid fraud and illegal entry, while corporate houses will utilize it to safeguard valuable documents and material from unauthorized individuals. Additionally, it can be utilized by jewellery stores and precious storage warehouses with such capabilities as tampering detection and real-time alerting to improved security conditions. First, Government and defence agencies may utilize TriGuard for confidential documents and sensitive files for access by only authorized officials. Further, domestic applications are now poised to enjoy IoT-based cloud security alerts, remote management of access, and real-time SMS alerts, thereby filling out the picture of a complete security solution for commercial and personal purposes. Its scalability and flexibility make this system a security system worthy of a dynamic high-security application in future-proof designs. In the future years, the TriGuard System will revolutionize the face of security with next-generation biometric authentication technologies, which will encompass innovations such as palm vein verification and iris scanning. These will be used to enhance the access control features provided by TriGuard.

It will integrate the two: With that, AI capabilities provide behavioural analysis such that the system can tailor authentication based on per-user behaviour and their risk rating. Among the most groundbreaking innovations would be the use of blockchain technology, providing hack-proof and auditable security logs through which banking security could be improved with greater transparency and trust. Furthermore, there are other features like the use of voice as access control, automatic lockdowns of the systems under unauthorized attempts detection, and AI-based anomaly detection in the times real-time threats identification and response systems in the scenarios that are highly thick with security threat. Along with the introduction of the Machine Learning algorithms, the authentication sensitivity will be automatically modified according to the patterns of behaviour of users facilitating higher security and convenience to the consumer. The banking security will be increased even more by introducing the TriGuard System with a Graphical User Interface (GUI) and cloud-based banking transactions, where customers can engage in banking operations remotely with extremely low branch office visits. A cloud storage platform will store user credentials like face photos, fingerprints, and unique IDs which may easily be verified in real-time. The combination of AI, cloud computing, and GUI-based remote access will optimize scalability, accessibility, and security, rendering the system highly effective for financial institutions and opening more opportunities for gains in improving operational and other efficiencies.

References

[1] A. Chikara, P. Choudekar, R. Asija, and D. Asija, “Smart Bank Locker Using Fingerprint Scanning and Image Processing,” in *Proc. 6th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, 2020, pp. 725–728, doi: 10.1109/ICACCS48705.2020.9074482.

[2] S. Dutta, N. Pandey, and S. K. Khatri, “Microcontroller-Based Bank Locker Security System Using IRIS Scanner and Vein Scanner,” in *Proc. Int. Conf. Invent. Res. Comput. Appl. (ICIRCA)*, 2018, IEEE Xplore Compliant Part No. CFP18N67-ART, ISBN: 978-1-5386-2456-2.

[3] R. Gusain, H. Jain, and S. Pratap, “Enhancing Bank Security System Using Face Recognition, Iris Scanner, and Palm Vein Technology,” in *Proc. 3rd Int. Conf. Internet Things: Smart Innov. Usages (IoT-SIU)*, 2018, pp. 1–5, doi: 10.1109/IoT-SIU.2018.8519850.

[4] S. Hossain, M. I. Ahmed, and M. N. Mostakim, “A Prototype of Automated Vault Locker Solution for Industrial Application,” in *Proc. 1st Int. Conf. Adv. Sci. Eng. Robot. Technol. (ICASERT)*, 2019, pp. 1–6, doi: 10.1109/ICASERT.2019.8934754.

[5] M. P. Pavithra, V. Adari, V. K. Sha, K. B. Rao, K. Nikhil, and K. Surendra, “Enhanced Security for ATMs with Facial Recognition Features and OTP,” *J. Nonlinear Anal. Optim.*, vol. 15, no. 1, pp. 1–7, 2024.

[6] H. Patil, V. Mahandule, L. Khachane, and S. Narkhede, “Multi-Banking ATM System Services Using Biometrics,” *Manage. Sci. Lett.*, vol. 14, no. 4, pp. 219–226, 2024.

[7] A. N. Reddy and S. B., “Locker Security System Using Facial Recognition and One-Time Password (OTP),” *Int. J. Comput. Sci. Mobile Comput.*, vol. 11, no. 2, pp. 45–50, 2022.

[8] A. Kumar, P. Sood, and U. Gupta, “Internet of Things (IoT) for Bank Locker Security System,” in *Proc. 6th Int. Conf. Signal Process. Commun. (ICSC)*, 2020, pp. 315–318, doi: 10.1109/ICSC48311.2020.9182713.

[9] P. Kavitha, P. Usha Rani, S. Karkuzhali, V. Karkuzhali, and J. Sumithra, “Triple stage security for bank lockers using biometric authentication system,” *AIP Conference Proceedings*, vol. 2966, no. 1, pp. 030009-1–030009-6, 2024. [Online]. Available: https://doi.org/10.1063/5.0190725

[10] S. Lunawat, V. S. Kumbhar, M. Badole, and M. S. Andhare, “3-Level authentication for bank locker security,” *International Journal of Scientific Research in Multidisciplinary Studies*, vol. 5, no. 6, pp. 44–47, Jun. 2019.

[11] S. Sridharan, "Authenticated Secure Biometric Based Access to the Bank Safety Lockers," 2014 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2014, pp. 1-5. https://ieeexplore.ieee.org/document/7034063