Security system for bank lockers using GSM, fingerprints, and passwords

[1]E. Srividya , [2]Gersham Mercy Joyce, [3]Peyyalamitta Sahithi, [4]N.Vimala, [5] O.Saritha

[1]Assistant Professor, Department of ECE, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad,
[2]Assistant Professor, Department of ECE, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad,
[3]Lecturer, Department of ECE, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad,
[4]Assistant Professor, Department of ECE, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad,
[5]Assistant Professor, Department of ECE, Sree Dattha Institute of Engineering and Science, Sheriguda, Ibrahimpatnam, Hyderabad,

Abstract: Designing and implementing a highly safe and dependable smart bank locker security system based on network-based password, biometric fingerprint, and OTP-based GSM technology is the primary objective of this research. This can be set up in households, schools, treasury offices, and banks. According to this technique, only the legitimate owner is able to unlock the locker and retrieve valuables like cash, jewels, or documents. This security solution makes use of GSM technologies, biometric fingerprints, and network-based passwords. Ensuring the protection of assets and information is crucial in the field of banking security. Although they can be somewhat effective, traditional security mechanisms like password-based systems are vulnerable to hacking. Therefore, this study suggests a sophisticated bank lock security system that incorporates several authentication methods, such as fingerprint, password, and GSM (Global System for Mobile Communications) technology. This multi-tiered strategy seeks to greatly improve security levels while providing authorized users with accessibility and convenience. In order for the suggested system to work, users must first connect the device to the approved mobile device via a Wi-Fi network and enter a secure password. After the device has successfully connected to the mobile, users are asked to verify their identity using fingerprint recognition technology, which provides a very dependable biometric authentication method. After that, users must input the OTP that the mobile device has received via GSM technology.

Key words: OTP, GSM, biometric fingerprint, password, Wi-Fi network etc.

I. Introduction

A major change in guaranteeing strong security measures is seen in the development of bank locker security systems that use password, fingerprint, and GSM (Global System for Mobile Communications) technology. Peer-to-peer mode allows Wi-Fi Direct-capable devices to connect to one another. In our implementation, a single device creates a mobile hotspot with a unique name and password, acting as the host. The other device finds the hotspot that the host device has generated and searches for Wi-Fi networks that are available. The devices link directly after detection, allowing for smooth communication. A huge step forward in safety was the introduction of biometric authentication, especially fingerprint recognition. As a more trustworthy and secure means of verifying identity, fingerprint technology rose to popularity in the latter half of the twentieth and early first century. Using this technique, a person's fingertip can have its unique ridge and valley patterns highlighted for easier access. Because each fingerprint is distinct and difficult to replicate, fingerprint scanners are an added layer of security for bank lockers.

GSM technology, prevalent in mobile communications, was incorporated into security systems to deliver real-time notifications and monitoring functionalities. Integrating GSM modules into bank locker systems enables the transmission of notifications to authorized workers or clients through SMS or calls in the event of suspicious activity, unauthorized access attempts, or emergencies. This facilitated immediate response even in the absence of individuals at the bank.

The integration of password-based access, biometric authentication, and GSM technology has created a multi-layered security approach. Customers use their password or PIN as the first authentication step, followed by scanning biometric data like fingerprints. GSM technology alerts concerned parties in case of security breaches. Banks face increasing anti-social activities, necessitating a re-evaluation of security measures. Personal identification technology is gaining interest to distinguish between legitimate users and imposters. Bank lockers are considered safe storage options, but are vulnerable to hacker attacks, thefts, and forgotten passwords.

II. LITERATURE SURVEY

a) Manual Key Based Locker System

Local banks' manual key-based locker system lacks robust security due to key loss or theft. To enhance security, measures like advanced key materials, biometric authentication, surveillance cameras, and regular staff training can be implemented. Insurance coverage for locker contents and electronic identification options like bank lockers and ATMs can also help mitigate vulnerabilities.

b) Smart Bank locker with RFID technology

The Smart Bank locker system uses RFID technology for user access and locker retrieval. However, it's vulnerable to hacking, necessitating additional security measures like encryption, secure authentication protocols, and regular system updates. RFID-based automated systems automate locker access using unique RFID cards for customer identification, allowing for secure and convenient access to lockers.

c) Bank locker using Fingerprint Technology

anks use fingerprint technology for locker access, where users enter their fingerprints in a database. If they match, access is granted. However, this method has potential for unauthorized extraction or theft. Additional security measures are needed to protect against these risks. Fingerprint-based door locking systems store users' fingerprints and validate their access. Passive RFID and GSM technologies offer heightened security, making these systems more secure than existing systems.

Shankar, A.A., et.al [2015] explained about Fingerprint-based door locking systems prevent unauthorized access by storing authorized users' fingerprints, which are validated by sensors. If matching, the door opens automatically, or a buzzer alerts nearby people.

The study by R. Ramani et.al [2012], introduces a methodology for implementing a secure bank locker system utilizing RFID and GSM technologies, with a particular emphasis on the heightened security afforded using passive RFID and GSM compared to other existing systems [3].

III. PROPOSED SYSTEM

Bank locker systems use OTP-based GSM technology to secure access, but it is susceptible to hacking and unauthorized forwarding. To mitigate this risk, banks should implement robust encryption algorithms and secure transmission protocols. This research aims to develop a secure bank locker system with multi-factor authentication, involving hardware and software components. The system requires a fingerprint scanner to open lockers, and a Wi-Fi network connection to an authorized mobile device. The system then sends an OTP through GSM technology, ensuring the system's effectiveness in providing secure and reliable access.

Furthermore, to enhance security during OTP delivery, the system may employ end-to-end encryption techniques, ensuring that the OTP remains confidential during transmission over the GSM network. This helps mitigate the risk of interception or eavesdropping by unauthorized entities, maintaining the integrity and confidentiality of the OTP delivery process.

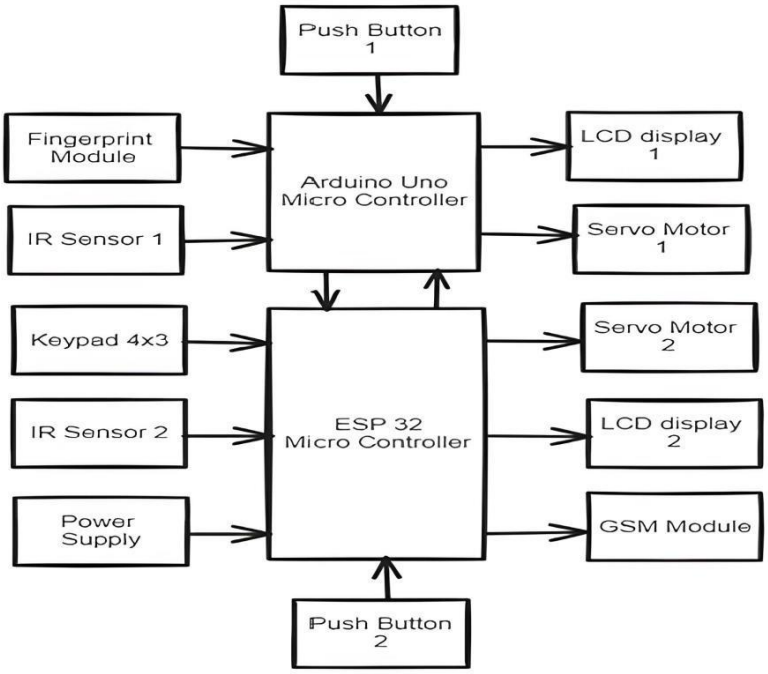

Fig1: Block Diagram

The authentication procedure commences when the user presses the button at Gate One, therefore illuminating the LED on the fingerprint scanner. This action instructs the scanner to request the user to position their finger on the scanning surface for biometric authentication. The

scanner acquires fingerprint data, which is subsequently analyzed using advanced techniques like minutiae matching or pattern recognition. Successful authentication occurs when the acquired fingerprint corresponds with an authorized template stored in the system, hence enabling access to the Locker.

The fingerprint-based security system for bank lockers uses a flowchart to ensure secure access. Users place their finger on a scanner, and the system compares the fingerprint with stored templates in the database. If a match is found, access is granted, and security personnel may be alerted. The system has a limited number of attempts before temporarily locking out further attempts.

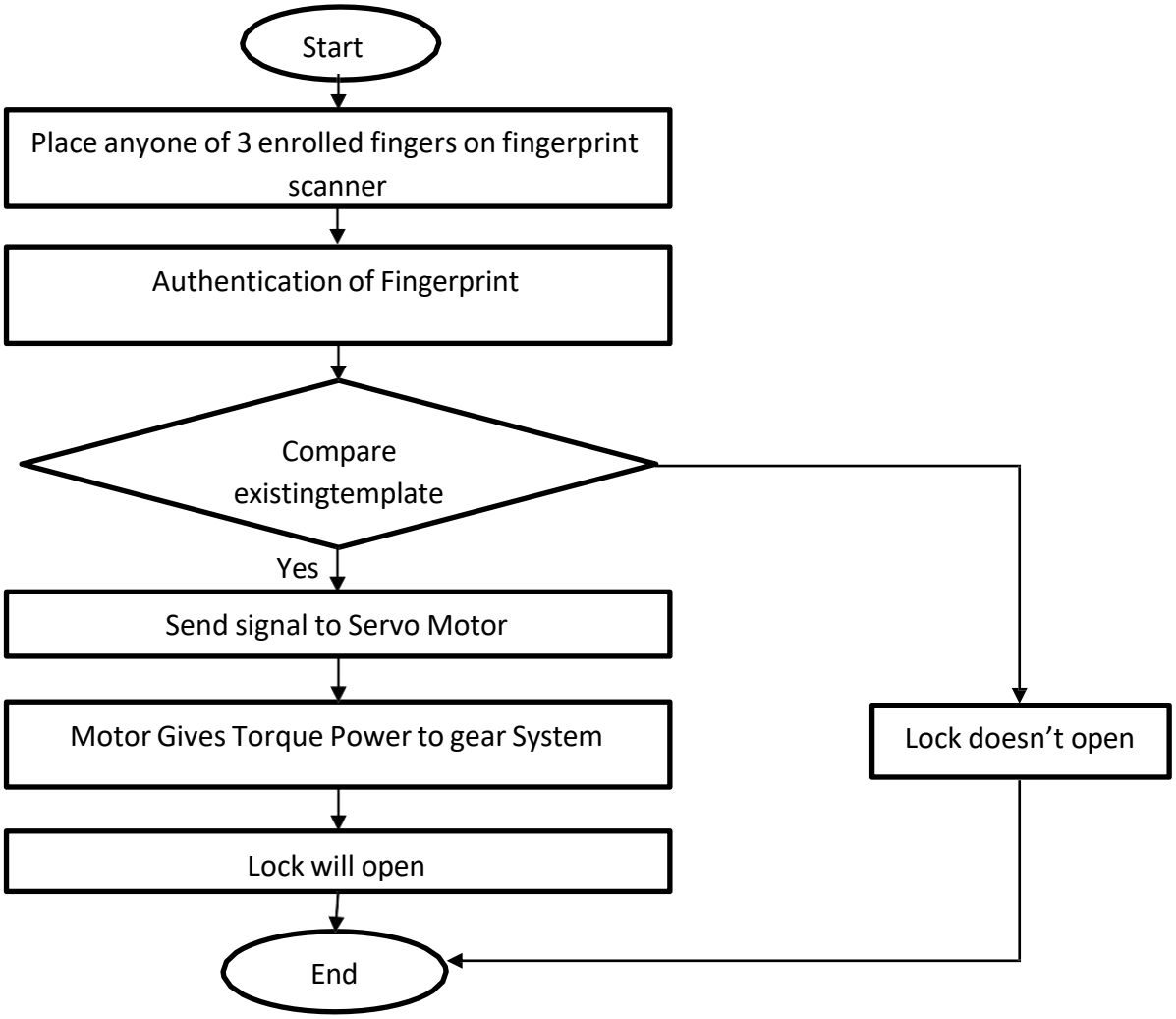

Fig2: Flowchart of Fingerprint Sensor

Cryptographic algorithms like HMAC-SHA1 or HMAC-SHA256 are commonly utilized to compute the OTP based on a shared secret key and a counter or timestamp value. This ensures that each OTP generated is unique and valid only for a limited duration, thereby enhancing security against replay attacks and unauthorized access attempts.

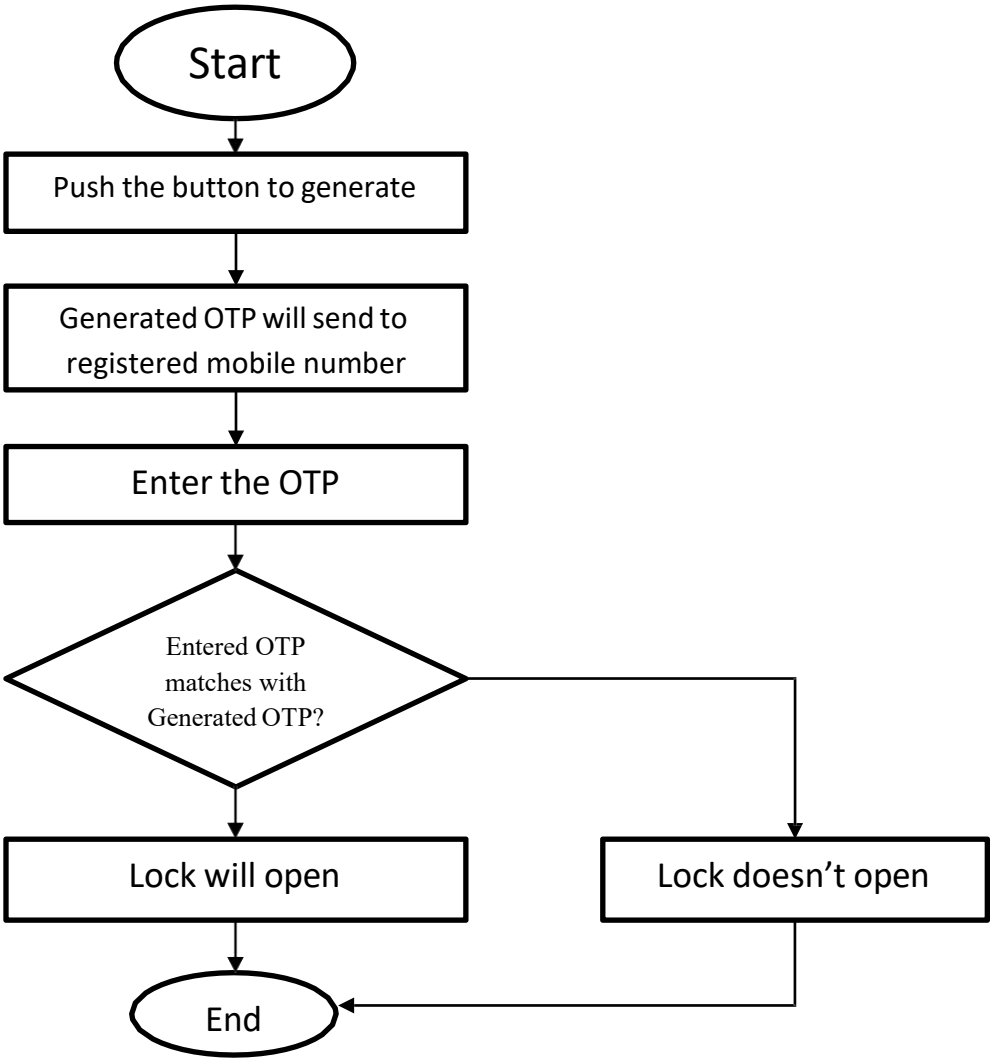

Fig3: Flow chart of OTP Using GSM Module

The system uses GSM technology to securely transmit OTP to the bank locker's registered mobile number. GSM protocols, such as SMS and USSD, offer robust encryption and authentication mechanisms for data transmission. SMS-based delivery encodes the OTP into a text, while USSD-based delivery facilitates real-time communication.

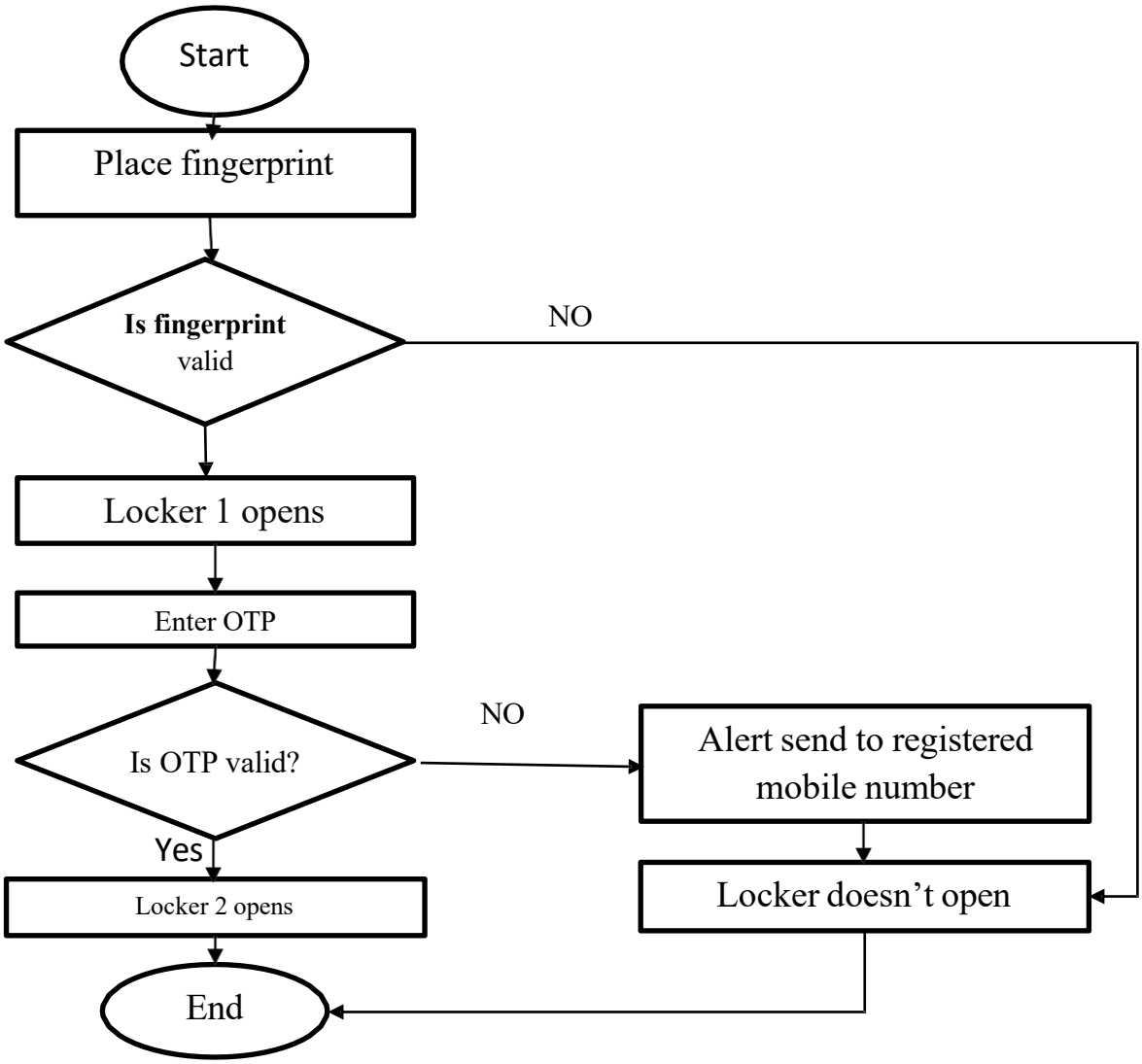

Fig4: Flow chart of Bank locker

IV. RESULTS

The fingerprint-based security system for bank lockers adheres to a defined flowchart to guarantee secure access. Upon approaching the locker, the user commences the process by positioning their finger on a fingerprint scanner. The Initial Fingerprint Authentication procedure integrates cutting-edge biometric technology with sophisticated algorithms to ensure a dependable and secure method of user identification verification, hence guaranteeing access to Locker One and protecting precious items contained within. The scanner acquires the fingerprint image and transmits it to the processing unit. The processing unit subsequently contrasts the acquired fingerprint with the stored templates in the database. Upon verification of a match, signifying the authorised user, the system permits access to the locker. Nevertheless, in the absence of a match, access is prohibited, and an alert may be activated to inform security staff. The system may impose a finite number of attempts before temporarily restricting further

access for security reasons. This flowchart guarantees a smooth and secure procedure for accessing bank lockers, improving overall security and minimizing the danger of unauthorized access.

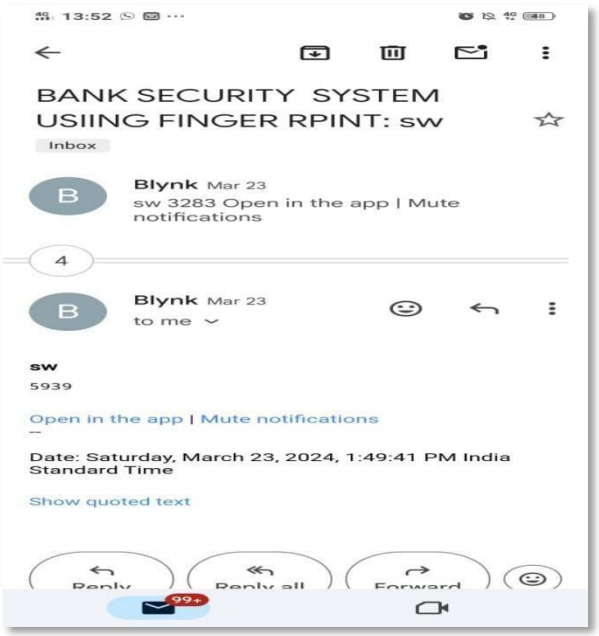

Fig 5. OTP Received by Email

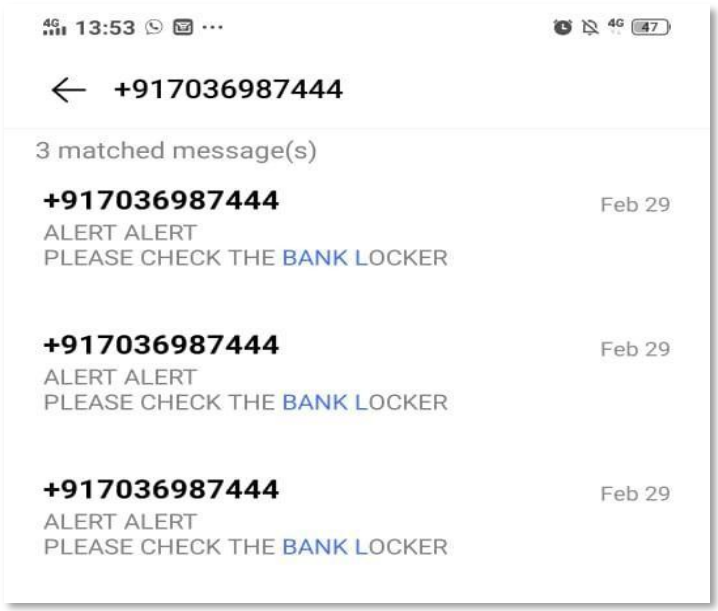

Fig 6: Alert message received by Registered Mobile

Moving on to the third step, the user proceeds to Gate two. By pressing the button at Gate two, an OTP is promptly dispatched to the registered mobile number via GSM technology. The user then inputs the received OTP using a keypad provided. If the entered OTP matches the one sent, Locker Two unlocks, allowing access to its contents.

V. CONCLUSION

The Smart Bank locker security system project uses network-based password, fingerprint, and GSM technology to ensure the safety of valuable materials stored in bank lockers. This low-cost, low-power, compact, and highly secure system streamlines the process for authorized individuals. Future developments may include IoT-based systems and biometric sensors. The system also incorporates digital signature, IRIS, and Retina scanning for visual identification. This innovative approach represents a significant advancement in bank locker security, enhancing security and efficiency for officials.

REFERENCES

1. Swetha, J., 2014. RFID based automated bank locker system. *International Journal of Research in Engineering and Technology*, *3*(5).
2. Shankar, A.A., Sastry, P.R.K., Ram, A.V. and Vamsidhar, A., 2015. Finger print based door locking system. *International Journal Of Engineering And Computer Science*, *4*(3), pp.10810-10814.
3. R. Ramani , S. Selvaraju , S. Valarmathy, P. Niranjan , “Bank Locker Security System based on RFID and GSM Technology ’’, International Journal of Computer Applications (0975 – 8887) Volume 57– No.18, November 2012
4. M. Gayathri, P. Selvakumari, R. Brindha “Fingerprint and GSM based Security System” International Journal of Engineering Sciences & Research Technology, ISSN: 2277- 9655, Gayathri et al.3(4): April, 2014.
5. Sanal Malhotra, “Banking Locker System with Odor Identification & Security Question Using RFID GSM Technology”. International Journal of Advances in Electronics Engineering – IJAEE Volume 4: Issue 3
6. Abhilasha A Sayar1, Dr. Sunil N Pawar2, “Review of Bank Locker System Using Embedded System”, International Journal of Advanced Research in Computer and

Communication Engineering Vol. 5, Issue 2, February 2016.

7. Hugh Wimberly, Lorie M. Liebrock, “Using Fingerprint Authentication to Reduce System Security: An Empirical Study”, 2011 IEEE Symposium on Security and Privacy.
8. Mary Lourde R and Dushyant Khosla, “Fingerprint Identification in Biometric Security Systems,” International Journal of Computer and Electrical Engineering, Vol. 2, No. 5, October, 2010.
9. Sandip Dutta, Nitin Pandey, Sunil Kumar Khatri, “Microcontroller Based Bank Locker Security System Using IRIS Scanner and Vein Scanner”, International Conference on Inventive Research in Computing Applications (ICIRCA), 2018, DOI: 10.1109/ICIRCA.2018.8597215 Publisher: IEEE.
10. Pramila D Kamble and Dr. Bharti W. Gawali "Fingerprint Verification of ATM Security System by Using Biometric and Hybridization" International Journal of Scientific and Research Publications, Volume 2, Issue 11, November 2012.
11. Archana C. Lomte, “Biometric fingerprint authentication with minutiae using ridge feature extraction”, International Conference on Pervasive Computing (ICPC), DOI: 10.1109/PERVASIVE.2015.7087178, Publisher: IEEE, 2015.
12. Manjunath, Ram Kumar, Pradeep Kumar, Nalajala Gopinath, Ms. Haripriya M.E, “NFC Based Bank Locker System”, International Journal of Engineering Trends and Technology (IJETT) – Volume23 Number 1- May 2015.
13. Vaijanath R. Shintre1, Mukesh D. Patil, “Banking Security System Using PSoC”, International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 7, July 2015.