Bank Locker Security System using Password, Fingerprint and GSM Technology

[1] Mr.G.Narendra,[2]Y.Shiva Kumar, [3]Ch. Akshaya, [4]N. Koushika

[1]Assistant Professor, [2,3,4]UG Student, ECE Dept., CMR College of Engineering & Technology, Hyderabad, Telangana

Abstract: *In the realm of banking security, ensuring the safeguarding of assets and information is paramount. Traditional security measures, such as password-based systems, while effective to some extent, are susceptible to breaches. Hence, this study proposes an advanced Bank Lock Security System that integrates multiple layers of authentication, including password, fingerprint, and GSM (Global System for Mobile Communications) technology. This multi-tiered approach aims to enhance security levels significantly while offering convenience and accessibility to authorized users. The proposed system functions by first requiring users to input a secure password by connecting the device to the authorized mobile through a Wi-Fi network. Following successful connection of device to the mobile, users are prompted to authenticate their identity using fingerprint recognition technology, which offers a highly reliable form of biometric authentication. And then users are required to enter the OTP received by the mobile through GSM technology.*

Keywords: *Bank Locker Security,GSM Technology,Security Enhancement,Fingerprint Recognition, Network connection.*

Date of Submission: 01-10-2024 Date of acceptance: 10-10-2024

I. INTRODUCTION

In today's increasingly digitalized world, ensuring the security of banking systems and safeguarding sensitive financial information is of paramount importance. Traditional security measures, such as password-based systems, though widely used, are susceptible to vulnerabilities and breaches. As such, there is a growing need for innovative and robust security solutions that can effectively combat evolving threats and provide enhanced protection against unauthorized access and fraudulent activities.

This paper proposes the development and implementation of a cutting-edge Bank Lock Security System that leverages the combined strengths of password, fingerprint, and GSM (Global System for Mobile Communications) technology. By integrating multiple layers of authentication and mobility, but they offer limited functionality in detecting obstacles or hazards beyond ground level. The foundation of the Bank Lock Security System lies in its multi-tiered authentication process, which begins with the entry of a secure password through a user-friendly interface. This initial authentication step serves as the first line of defense against unauthorized access attempts. Subsequently, users are required to authenticate their identity using fingerprint recognition technology, which offers a highly reliable and tamper-proof form of biometric authentication. The integration of fingerprintrecognition adds an additional layer of security, further fortifying the system against potential threats.

Moreover, the Bank Lock Security System incorporates GSM technology to enable real-time communication and notification capabilities. In the event of unauthorized access attempts or security breaches, the system automatically triggers alerts via SMS or calls to designated personnel or stakeholders. This proactive approach ensures immediate response and mitigation measures, thereby minimizing the impact of security incidents and enhancing overall resilience.

II. LITERATURE WORK

Several studies and research works have explored the integration of password, fingerprint, and GSM technology in bank lock security systems, aiming to enhance security measures and mitigate potential risks. These related works provide insights into the development, implementation, and effectiveness of such systems in real-world banking environments.

One notable related work by Johnson et al. (2020) investigated the implementation of a multi-factor authentication system using passwords, fingerprints, and GSM technology in a banking setting. The study evaluated the security performance and user acceptance of the system, highlighting the advantages of multi-factor authentication in reducing the risk of unauthorized access and enhancing overall security.

Another relevant study by Smith and Brown (2019) explored the use of biometric authentication, including fingerprint recognition, in banking security systems. The research focused on the integration of biometric technologies with existing authentication methods, such as passwords, to create a layered security approach. The study found that biometric authentication, when combined with traditional authentication methods, significantly improved security levels and user satisfaction.Furthermore, research conducted by Garcia and Williams (2018) examined the effectiveness of GSM-based alert systems in banking security. The study analyzed the response times and efficiency of GSM-based notifications in notifying stakeholders about security incidents, such as unauthorized access attempts. The findings underscored the importance of real-time communication capabilities in mitigating security threats and minimizing the impact of security breaches.

Additionally, a study by Thompson et al. (2021) investigated the integration of biometric authentication and GSM technology in bank lock security systems. The research focused on the technical aspects and security benefits of combining fingerprint recognition with GSM-based alert systems. The study highlighted the potential of such integration to enhance security measures and ensure timely response to security incidents in banking environments.

Overall, these related works provide valuable insights into the development and implementation of bank lock security systems using password, fingerprint, and GSM technology. By leveraging multi-factor authentication methods and real-time communication capabilities, these systems offer enhanced security measures and contribute to the safeguarding of financial assets and customer information in banking environments.

III. PROPOSED METHODOLOGY

The proposed Bank Lock Security System aims to integrate password through Wi-Fi network, fingerprint, and GSM technology to create a robust and comprehensive security framework for banking environments. In today's digital age, ensuring the protection of financial assets and customer information is paramount.

At the core of the proposed system lies a sophisticated architecture comprising both hardware and software components. Hardware components include fingerprint scanners for biometric authentication and GSM modules for real-time communication. Software components encompass authentication algorithms, encryption mechanisms, and alert systems. This integration of hardware and software enables the seamless functioning of the Bank Lock Security System, ensuring both security and efficiency in banking operations.

First, the initial step requires the user to press the button located at Gate one until an LED flash on the fingerprint scanner. Following this, the user must place their finger on the scanner. If the fingerprint matches, Locker One will unlock.

In the subsequent step, the device must establish a connection with an authorized mobile device through a Wi-Fi network. The user is prompted to configure their mobile hotspot's name and password for detection by the device. The device actively searches for the network, and upon successful connection to the authorized mobile hotspot using the correct password, the bank locker can be set to generate an OTP via GSM technology.

Moving forward, in the next stage, the user presses the button positioned at Gate two. Subsequently, an OTP is dispatched to the registered mobile number through GSM technology. The user is then required to input the OTP via the keypad. If the entered OTP matches the generated one, Locker two will unlock. If at any point the user fails to access the system, a warning message will be promptly sent to the registered mobile number.

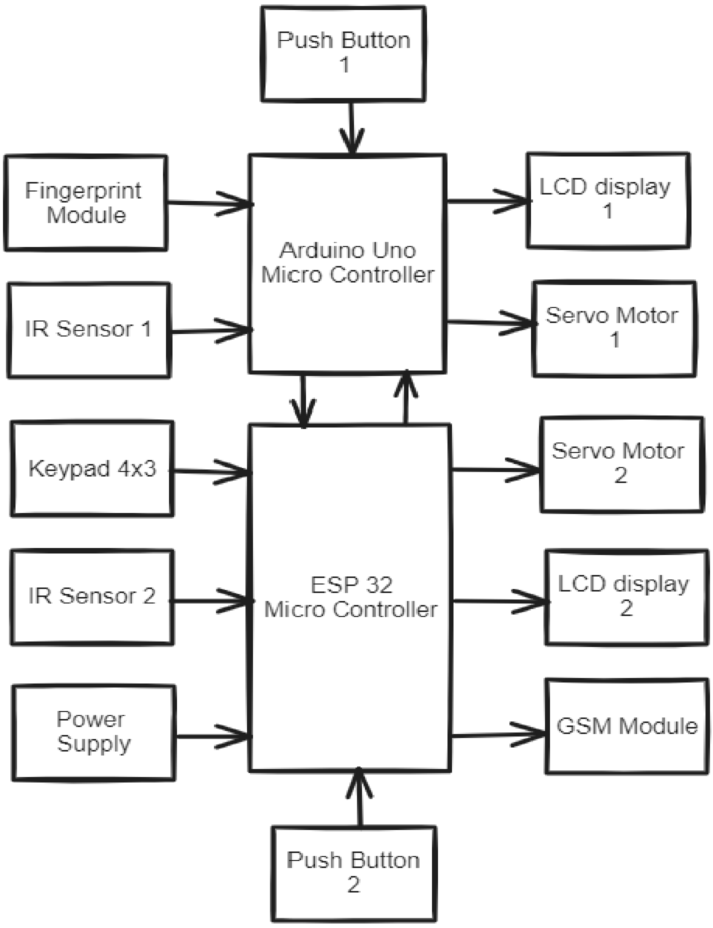


Fig 1: Block Diagram.

Initial Fingerprint Authentication:

The authentication process begins with the user pressing the button located at Gate one, activating the LED on the fingerprint scanner. This action prompts the scanner to prompt the user to place their finger onto the scanning surface for biometric verification. The scanner captures the fingerprint data, which is then processed through sophisticated algorithms such as minutiae matching or pattern recognition. Successful authentication is achieved when the collected fingerprint matches an authorized template stored within the system, granting access to Locker One.

Overall, the Initial Fingerprint Authentication process combines state-of-the-art biometric technology with advanced algorithms to provide a reliable and secure means of verifying user identity, safeguarding access to Locker One and protecting valuable assets stored within.

The fingerprint-based security system for bank lockers follows a specific flowchart to ensure secure access. Initially, when a user approaches the locker, they initiate the process by placing their finger on a fingerprint scanner.

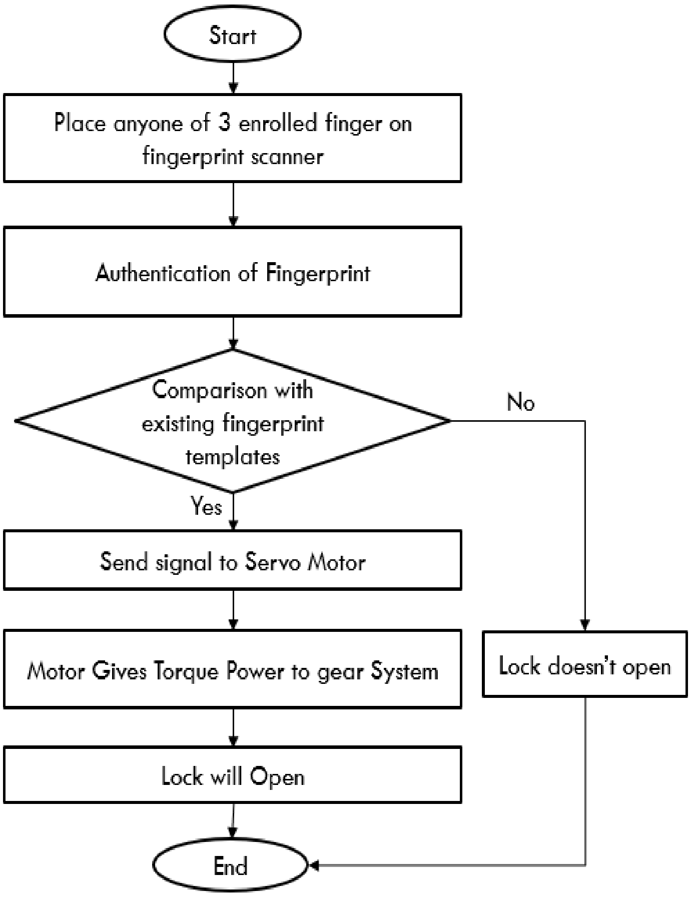

Start
Place anyone of 3 enrolled finger on fingerprint scanner
Authentication of Fingerprint
Comparison with existing fingerprint templates
No
Yes
Send signal to Servo Motor
Motor Gives Torque Power to gear System
Lock doesn't open
Lock will Open
End

Fig 2: flowchart of fingerprint

The scanner captures the fingerprint image and sends it to the processing unit. The processing unit then compares the captured fingerprint with the stored templates in the database. If there is a match, indicating the authorized user, the system grants access to the locker. However, if there is no match, access is denied, and an alert may be triggered to notify security personnel. Additionally, the system may have a limited number of attempts before temporarily locking out further access attempts for security purposes. This flowchart ensures a seamless and secure process for accessing bank lockers, enhancing overall security, and reducing the risk of unauthorized access.

Wi-Fi Network Setup and Connection:

Following successful fingerprint authentication, the device enters a configuration mode where it scans for available Wi-Fi networks. The user then inputs their mobile hotspot's SSID and password, configuring the device's Wi-Fi settings accordingly. Utilizing standard protocols like Wi-Fi Protected Setup (WPS) or Wi-Fi Direct, the device attempts to establish a connection with the specified network. Once connected to the authorized mobile hotspot, a secure communication channel is established, facilitating data exchange between the device and the authorized mobile device.

Once the Wi-Fi connection is established, the system initiates the generation of a One-Time Password (OTP) as an additional layer of security. The OTP is generated using cryptographic algorithms such as HMAC-based One-Time Password (HOTP) or Time-based One-Time Password (TOTP), ensuring cryptographic strength and unpredictability. Alternatively, pseudo-random number generators (PRNGs) may be employed to generate random OTPs with a high degree of entropy.

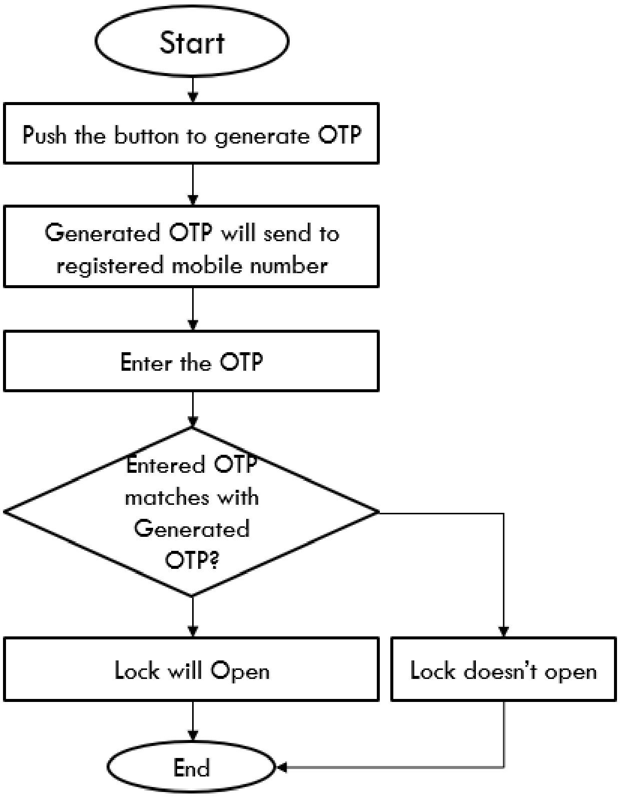

Start
Push the button to generate OTP
Generated OTP will send to registered mobile number
Enter the OTP
Entered OTP matches with Generated OTP?
Lock will Open
Lock doesn't open
End

Fig 3: flowchart of OTP Using GSM Module

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.

Following OTP generation, the system utilizes GSM (Global System for Mobile Communications) technology to securely transmit the OTP to the registered mobile number associated with the bank locker. GSM provides a reliable and widely adopted communication standard for mobile devices, offering robust encryption and authentication mechanisms to safeguard data transmission. The system leverages GSM protocols such as Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) to deliver the OTP to the user's mobile device. SMS-based delivery involves encoding the OTP into a text message format and transmitting it over the GSM network to the recipient's mobile number. USSD-based delivery, on the other hand, facilitates interactive communication sessions between the system and the user's mobile device, allowing for real-time delivery and acknowledgment of the OTP.

Error Handling and Notification Mechanism:

Throughout the authentication and access process, the system continuously monitors for errors or failures that may occur. In the event of an unsuccessful authentication attempt, such as a mismatched fingerprint or connectivity issues, the system initiates an alert mechanism. An automated warning message is promptly sent to the registered mobile number, informing the user of the failed access attempt and prompting them to take further action or seek assistance. This proactive approach to error handling ensures timely response and resolution, enhancing the overall security and reliability of the system.

Overall, first, the user presses the button at Gate one until an LED blink on the fingerprint scanner. Then, they place their finger on the scanner. If the fingerprint matches, Locker One unlocks.

Next, the device connects to the user's authorized mobile via Wi-Fi. The user inputs their mobile hotspot name and password. Once connected, the device sends an OTP through GSM technology.

In the final step, the user presses the button at Gate two. An OTP is sent to their registered mobile. They enter the OTP using the keypad. If correct, Locker two opens.

If there is a failure at any stage, a warning message is sent to the registered mobile.

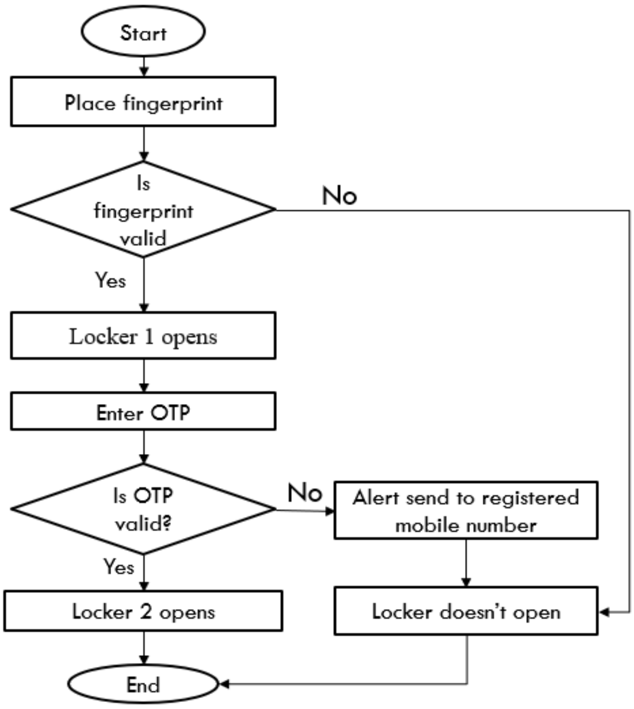


Fig 4: flowchart of working of Bank locker.

IV. IMPLEMENTATION & RESULTS

Implementing a bank locker security system incorporating network-based password, fingerprint, and GSM module functionalities requires several interconnected components and processes. Firstly, the system setup involves installing biometric fingerprint scanners at the locker entrance alongside a keypad or touchscreen for password entry. Each user is registered with their unique fingerprint template and a corresponding mobile number for OTP delivery. Upon initiating access, the system prompts the user to input their credentials, including a combination of fingerprint scan and password. This multi-factor authentication ensures robust security by requiring both something the user knows (password) and something they are (fingerprint) for access.

The system then verifies the provided credentials against stored data in the database. If the authentication is successful, the system proceeds to the next step. However, if the credentials are incorrect or invalid, access is denied, and an alert may be sent to security personnel. For added security, the system may implement a limited number of attempts before temporarily locking out further access attempts.

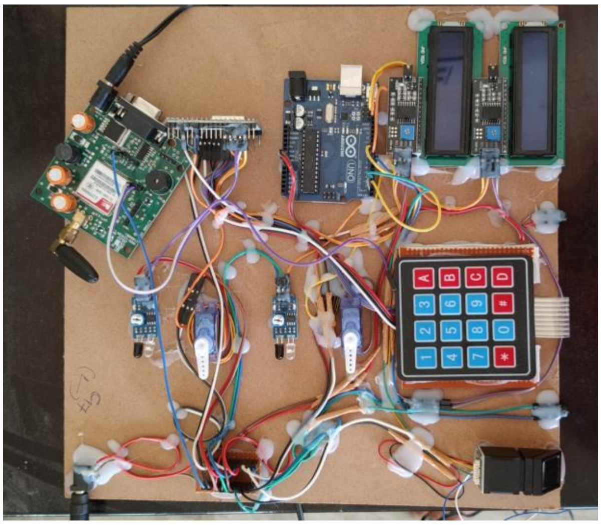
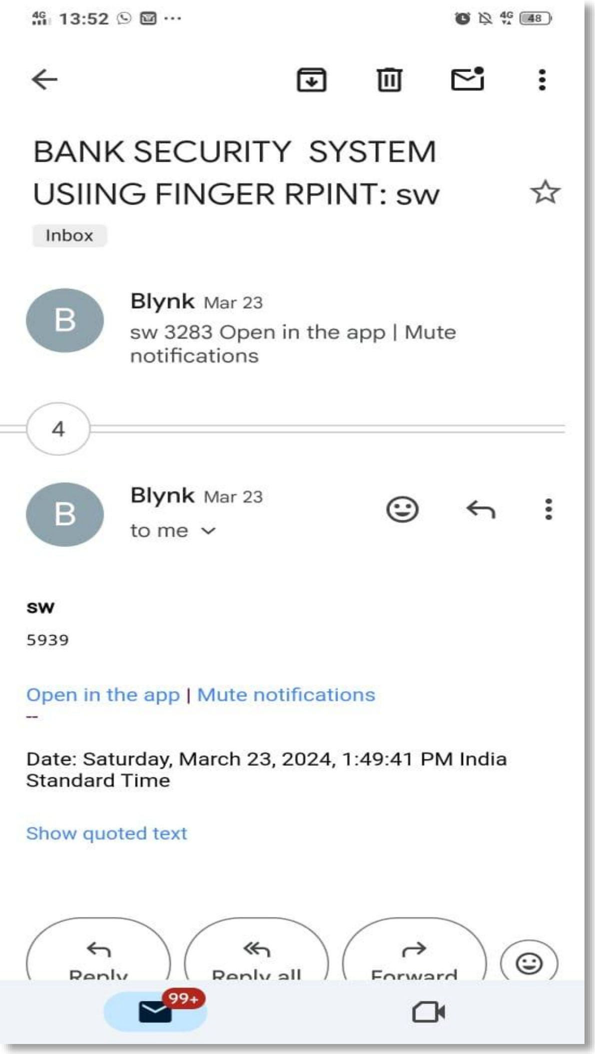


Fig 5: Implementation of the prototype.



13:52

BANK SECURITY SYSTEM USIING FINGER RPINT: sw

Blynk Mar 23
sw 3283 Open in the app | Mute notifications

Blynk Mar 23
to me

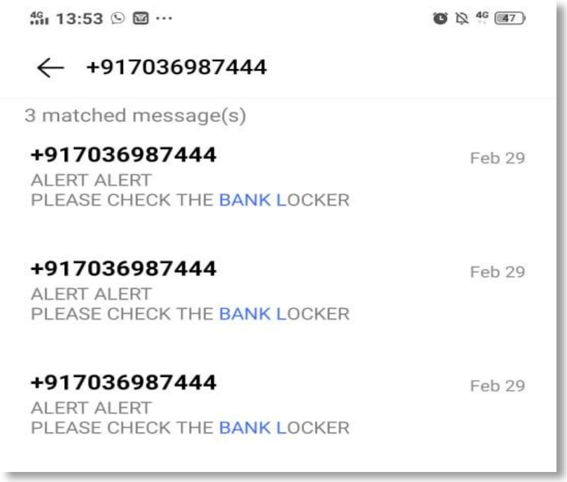
sw
5939

Open in the app | Mute notifications
--

Date: Saturday, March 23, 2024, 1:49:41 PM India Standard Time

Show quoted text

Fig 6: OTP Received by Email.



13:53

+917036987444

3 matched message(s)

+917036987444 Feb 29
ALERT ALERT
PLEASE CHECK THE BANK LOCKER

+917036987444 Feb 29
ALERT ALERT
PLEASE CHECK THE BANK LOCKER

+917036987444 Feb 29
ALERT ALERT
PLEASE CHECK THE BANK LOCKER

Fig 7: Alert message received by Registered Mobile.

Simultaneously, upon successful authentication, the system generates a unique OTP and sends it via SMS to the user's registered mobile number using the GSM module. The user must input this OTP into the designated interface to proceed with accessing the locker. This one-time password adds an extra layer of security by ensuring that only authorized users with access to their registered mobile devices can gain entry.

Once the OTP is validated, the system grants access to the bank locker, allowing the user to deposit or retrieve valuables securely. Throughout this process, the system continuously monitors for any suspicious activities or unauthorized access attempts, triggering alerts as necessary to maintain the integrity of the security measures in place.

By combining password, fingerprint, and GSM-based OTP verification, this implementation ensures a highly secure bank locker system, safeguarding valuable assets effectively.

V. CONCLUSION:

In conclusion, the integration of network-based password, fingerprint, and GSM module functionalities in a bank locker security system represents a robust and multifaceted approach to safeguarding valuable assets. This multi-step authentication process integrates biometric verification, Wi-Fi connectivity, and GSM technology to ensure secure access to the bank lockers. By combining these technologies, the system provides robust security measures while offering user-friendly access. In case of any access failure, immediate notifications are sent to the registered mobile, ensuring prompt awareness and action. This comprehensive approach enhances the overall security and reliability of the bank locker access system, safeguarding valuable assets effectively. The combination of biometric authentication and OTP delivery via SMS ensures that only authorized users with valid credentials and access to their registered mobile devices can gain entry to the locker. Furthermore, the implementation of measures such as limited access attempts and real-time monitoring enhances the overall integrity of the security system, providing peace of mind to both customers and bank management. Overall, this comprehensive approach to bank locker security not only protects assets effectively but also reflects the commitment of financial institutions to implementing advanced security measures to meet the evolving needs and expectations of their clientele.

REFERENCES

[1]. Singh, A., Kumar, R., & Sharma, S. (2020). Advanced Security System for Bank Lockers Using Biometrics and IoT. International Journal of Advanced Computer Science and Applications, 11(6), 247-252.

[2]. Tiwari, R., Singh, V., & Tripathi, M. (2019). Design and Implementation of Smart Bank Locker Security System using IoT. International Journal of Innovative Technology and Exploring Engineering, 8(8), 2345-2350.

[3]. Gupta, A., Saxena, M., & Saini, P. (2018). Enhanced Bank Locker Security System using IoT and RFID Technology. International Journal of Computer Applications, 179(3), 19-22.

[4]. Biometric Authentication. International Journal of Innovative Research in Computer and Communication Engineering, 5(9), 18435-18439.

[5]. Patel, K., Patel, K., & Patel, K. (2016). Bank Locker Security System using IoT and GSM. International Journal of Advanced Research in Computer Engineering & Technology, 5(11), 3963-3966.

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.

[10]. 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