Iot-Enabled Multi-Layered Security Framework For Intelligent Bank Locker Protection

[1]Dr. A. Swetha,[2]Rangappa Gari Vishnu Kumar,[3]Shaik Hussain Basha,[4]Shaik Mohammad Tanveer,[5]Bandaru Kalyan,[6]Eladi Vikas
[1]Professor, Department of Electronics and Communication Engineering, Dr. K.V. Subba Reddy Institute of Technology
[2,3,4,5,6]B. Tech Student, Department of Electronics and Communication Engineering, Dr. K.V. Subba Reddy Institute of Technology

ABSTRACT

Bank locker security demands highly reliable and tamper-proof authentication mechanisms due to increasing theft attempts, unauthorized access, and cyber-physical intrusions. Traditional locker systems rely on a single level of authentication—such as a physical key or PIN—which is susceptible to duplication, hacking, or brute force attacks. This research proposes an IoT-enabled three-layer security system for bank lockers that integrates RFID authentication, biometric verification (fingerprint/face recognition), and OTP-based access control transmitted through secure IoT platforms. Additional features include real-time intrusion detection using sensors and automatic alert generation to bank authorities and customers. The system leverages microcontrollers such as ESP32 or Raspberry Pi for network connectivity, cloud synchronization, and data logging. By implementing multi-level authentication, the security of bank lockers is significantly enhanced, reducing the risk of unauthorized access. The proposed model is cost-effective, scalable, and future-ready for integration with smart banking environments. Results demonstrate improved security reliability, greater user accountability, and rapid response mechanisms.

Keywords: Internet of Things (IoT), Bank Locker Security, Multi-Layer Authentication, RFID Authentication, Biometric Verification, One-Time Password (OTP), ESP32, Raspberry Pi, Intrusion Detection System, Smart Banking Security.

I. INTRODUCTION

Bank locker systems are critical assets that require robust protection against unauthorized access, physical break-ins, and internal misuse. Traditionally, lockers depend on mechanical keys, manual supervision, or basic PIN systems that can easily be compromised. With advancements in IoT and embedded technologies, it is now possible to design intelligent, multi-layered authentication systems capable of verifying user identity with high accuracy. IoT-based security allows real-time monitoring, remote alerting, and data logging, which enhances transparency and traceability in banking operations. A three-layer security system, combining RFID, biometrics, and OTP verification, ensures that even if one layer is compromised, unauthorized access is still prevented. This study explores the design and implementation of a multi-layer IoT security architecture tailored for bank lockers, ensuring maximum protection and user accountability. The integration of IoT enhances reliability through continuous monitoring, making the system suitable for modern financial institutions.

II. Related Words

Recent advancements in Internet of Things (IoT) technologies have significantly improved the design of secure authentication mechanisms for smart systems. Multi-factor authentication (MFA) has become an important approach for strengthening IoT security by combining multiple verification methods such as passwords, biometrics, and hardware tokens. Ahmed proposed an effective MFA mechanism for IoT devices that enhances authentication reliability while protecting systems from unauthorized access and cyber-attacks [1]. Similarly, Bamashmos et al. introduced a two-layered authentication framework integrated with blockchain technology to improve data integrity and security for IoT environments [2]. These approaches demonstrate that combining multiple authentication factors significantly increases system security compared to traditional single-layer authentication systems.

Several studies have focused on authentication frameworks and their role in securing interconnected IoT devices. Suleski et al. analyzed different multi-factor authentication approaches used in IoT-based

healthcare systems and emphasized the importance of combining biometric authentication with secure communication protocols [3]. In addition, Yalli et al. presented a comprehensive survey of authentication schemes designed for IoT networks, highlighting challenges such as scalability, resource constraints, and secure key management [5]. Ometov et al. further discussed the challenges associated with implementing multi-factor authentication in advanced IoT applications, including computational limitations and secure identity management [9]. These studies indicate that efficient authentication frameworks are essential for maintaining secure access control in IoT-enabled systems.

RFID technology has also been widely used in secure identification and access control systems. El Gaabouri et al. conducted a systematic review on RFID authentication security approaches and emphasized that secure RFID protocols can significantly improve access control mechanisms in smart systems [4]. Earlier work by Tripathi demonstrated the effectiveness of RFID-based digital security systems for door lock applications, showing how RFID tags can be used to uniquely identify authorized users [13]. These studies highlight the advantages of RFID technology in implementing secure and efficient access control solutions.

Recent research has also explored smart locker systems and intelligent security mechanisms using IoT technologies. Alzhrani designed an IoT-integrated smart locker security system that combines embedded systems and network connectivity to enable secure monitoring and remote access control [6]. Parab proposed an IoT-based biometric locker system that integrates fingerprint authentication to enhance the security of locker systems [14]. Similarly, Chandrappa and Prithviraj introduced a smart locker architecture leveraging IoT and machine learning techniques to improve security and monitoring capabilities [15]. These systems demonstrate how integrating IoT technologies with authentication mechanisms can significantly enhance the security of physical storage systems.

Furthermore, recent frameworks have explored advanced authentication techniques and system architectures for IoT devices. Höfener et al. proposed a requirements framework for IoT authentication mechanisms that addresses security, scalability, and device interoperability challenges [7]. Mehta reviewed various authentication approaches for IoT networks and emphasized the importance of combining cryptographic techniques with multi-factor authentication methods [8]. Additionally, AlJanah et al. introduced multi-factor and multi-level authentication frameworks that utilize encryption and secure communication protocols to protect IoT devices from cyber threats [10], [11]. Saideh et al. also investigated sensor-based authentication techniques that utilize environmental data to strengthen IoT security systems [12].

Overall, the reviewed literature indicates that integrating multi-factor authentication, RFID identification, biometric verification, and IoT connectivity can significantly improve the security of intelligent systems. However, many existing systems focus on limited authentication layers or lack real-time monitoring and alert mechanisms. Therefore, the proposed IoT-Enabled Multi-Layered Security Framework for Intelligent Bank Locker Protection aims to address these limitations by implementing a comprehensive three-layer authentication mechanism combined with real-time intrusion detection and automated alert systems.

III. PROPOSED MODEL

The proposed IoT-Enabled Multi-Layered Security Framework for Intelligent Bank Locker Protection is designed to enhance the security of traditional bank locker systems by implementing a three-layer authentication mechanism combined with IoT-based monitoring and alert systems. The model integrates RFID authentication, biometric verification, and One-Time Password (OTP) validation to ensure that only authorized users can access the locker. By combining multiple authentication layers, the system significantly reduces the risk of unauthorized access, duplication of keys, and brute-force attacks commonly associated with conventional locker security systems.

In the first layer of authentication, RFID technology

is used to identify authorized users. Each customer is provided with a unique RFID card that contains a secure identification code. When the card is scanned using an RFID reader connected to the microcontroller (ESP32 or Raspberry Pi), the system verifies the card's ID with the stored database. If the RFID credentials match the registered data, the system allows the user to proceed to the next authentication stage. If the card is invalid, the system denies access and triggers an alert notification to the bank's monitoring system.

The second layer of authentication involves biometric verification, such as fingerprint recognition or facial recognition. Biometric sensors capture the user's unique physiological characteristics and compare them with the stored biometric data in the system database. This step ensures that even if an RFID card is lost or stolen, unauthorized individuals cannot access the locker without the correct biometric identity. The biometric verification module is connected to the microcontroller, which processes and validates the captured biometric data before granting further access.

The third authentication layer uses an OTP-based verification system to provide an additional level of security. Once RFID and biometric authentication are successfully completed, the system generates a unique one-time password that is sent to the registered mobile number or email of the locker owner through an IoT communication platform. The user must enter this OTP using a keypad or mobile interface connected to the system. If the entered OTP matches the generated code within the specified time limit, the locker mechanism is unlocked. Otherwise, access is denied and a security alert is generated.

In addition to multi-layer authentication, the proposed model incorporates real-time intrusion detection and monitoring mechanisms. Sensors such as vibration sensors, magnetic door sensors, or motion detectors continuously monitor the locker environment for suspicious activities. If unauthorized tampering, forced entry, or abnormal movement is detected, the system immediately sends alerts to bank authorities and the locker owner through IoT platforms such as cloud servers or mobile applications. The system also logs all access events, authentication attempts, and sensor activities for auditing and security analysis.

The entire system is controlled by an ESP32 or Raspberry Pi microcontroller, which acts as the central processing unit of the security framework. These controllers enable Wi-Fi connectivity, allowing the system to communicate with cloud databases, send notifications, and maintain secure data records. The IoT-based architecture also enables remote monitoring and real-time system updates. As a result, the proposed model provides a scalable, cost-effective, and highly secure solution for modern banking environments, ensuring improved protection of bank lockers and enhanced customer trust.

IV. PROPOSED SYSTEM

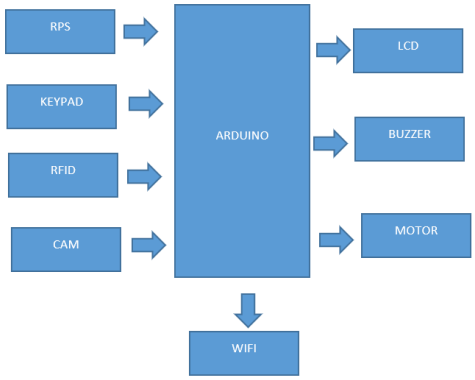

Fig.1.Block diagram

The block diagram represents the architecture of the IoT-Enabled Multi-Layered Security Framework for Intelligent Bank Locker Protection. In this system, the Arduino microcontroller acts as the central processing unit that coordinates all input devices, authentication modules, and output components. Various sensors and authentication modules such as RPS, keypad, RFID reader, and camera module provide input signals to the Arduino. Based on these inputs, the controller processes authentication requests and controls the output devices such as the LCD display, buzzer, and motor mechanism responsible for locker operation. The integration of Wi-Fi connectivity enables the system to communicate with IoT platforms for remote monitoring and alert notifications.

The RFID module serves as the first layer of

authentication. Each authorized user possesses an RFID card that contains a unique identification code. When the user places the RFID card near the RFID reader, the module transmits the card ID to the Arduino controller. The controller verifies the received ID with the stored database. If the card matches the registered credentials, the system proceeds to the next authentication stage. If the card is invalid or unauthorized, the system denies access and activates the security alert mechanism.

The keypad module provides an interface for entering security credentials such as a PIN or an OTP. After successful RFID verification, the user is required to enter a password or OTP through the keypad. The Arduino compares the entered code with the stored or generated authentication value. If the entered code is correct, the authentication process continues; otherwise, the system activates the buzzer and denies access to the locker. This step adds an additional layer of security by ensuring that only authorized users can proceed.

The camera module (CAM) acts as a biometric or visual verification system. It captures the user's image during the authentication process and can be used for facial recognition or for recording the access event. This feature improves accountability and provides evidence in case of unauthorized access attempts. The captured data can also be transmitted through the IoT network for remote monitoring by bank authorities.

The LCD display provides real-time feedback to the user during the authentication process. It displays system messages such as "Scan RFID Card," "Enter Password," "Access Granted," or "Access Denied." The buzzer functions as an alert device that generates an audible alarm whenever an incorrect authentication attempt or suspicious activity is detected. This immediate alert helps prevent unauthorized access and notifies nearby security personnel.

The motor module represents the mechanical locking mechanism of the bank locker. Once all authentication stages are successfully completed, the Arduino activates the motor to unlock the locker door. After a specific period or when the door is closed, the motor returns to the locked position to secure the locker again. This automated mechanism ensures reliable and controlled locker access.

Finally, the Wi-Fi module enables IoT connectivity for the entire system. Through Wi-Fi communication, the Arduino can send alerts, authentication logs, and system status updates to cloud platforms or mobile applications. This allows bank authorities and locker owners to monitor locker access in real time and receive immediate notifications in case of suspicious activity. The integration of IoT technology therefore enhances both security monitoring and remote management capabilities of the bank locker system.

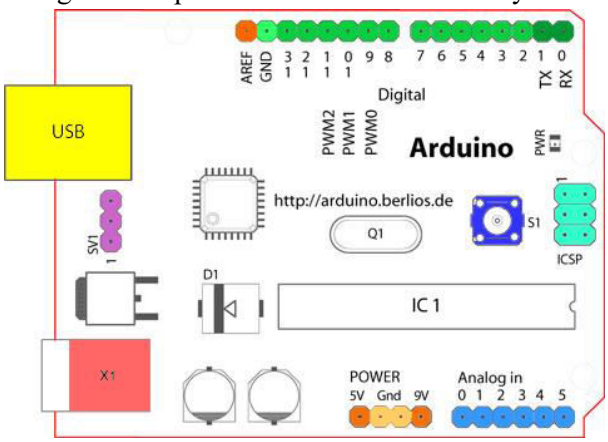

Fig.2. Structure of Arduino Board

V. RESULTS AND DESCUSSIONS

The proposed IoT-Enabled Multi-Layered Security Framework for Intelligent Bank Locker Protection improves bank locker security and access control by integrating authentication technologies, embedded processing, IoT communication, and automated alert mechanisms. The system continuously monitors locker access using authentication modules connected to the Arduino microcontroller. Components such as the RFID reader, keypad module, camera module, and RPS sensor provide multiple levels of authentication and monitoring. These modules collect real-time authentication and security data and transmit the information to the Arduino controller for processing. The controller analyzes the authentication inputs and determines whether the user is authorized to access the locker. When unauthorized attempts or suspicious activities are detected, the system activates alert mechanisms and sends notifications through IoT communication networks. This automated security approach significantly reduces the chances of unauthorized

access and enhances the protection of bank locker systems.

The specifications of the components used in the proposed system are presented in **Table 1**. The Arduino microcontroller acts as the central processing unit responsible for collecting authentication data, processing security parameters, and controlling output devices. The RFID reader is used to identify authorized users by reading unique RFID card IDs. The keypad module allows users to enter a password or OTP as an additional authentication layer. The camera module captures images during the authentication process for visual verification and monitoring. The RPS sensor monitors locker door movement or mechanical activity and helps detect abnormal tampering or forced entry attempts. The Wi-Fi module enables IoT communication for sending alerts and monitoring system activities remotely. The LCD display provides real-time system status and authentication messages, while the buzzer generates an audible alarm when unauthorized access attempts are detected.

TABLE 1: SYSTEM COMPONENT SPECIFICATION

SI.NO	Components	Specifications
1	Arduino	Operating Voltage: 5V microcontroller used for system control
2	RFID Reader	Reads unique RFID card identification for user authentication
3	Keypad	Allows password or OTP entry for secure access
4	Camera Module	Captures user images for monitoring and verification
5	RPS Sensor	Detects movement or tampering of the locker mechanism
6	Wi-Fi Module	Enables IoT communication and remote monitoring
7	LCD Display	Displays authentication status and system messages
8	Buzzer	Generates audible alert during unauthorized access attempts
9	Motor	Controls the automatic locking and unlocking of the locker
10	Power Supply	Provides stable power to all system components

The hardware implementation integrates the Arduino controller with multiple authentication modules and output devices to achieve secure locker access control. During system operation, the RFID reader first scans the user's RFID card to verify identity. Once the RFID authentication is successful, the system prompts the user to enter a password or OTP through the keypad. Simultaneously, the camera module captures the user's image for monitoring and verification purposes. The RPS sensor continuously monitors locker movement to detect any abnormal mechanical activity or tampering attempts. All collected authentication data is transmitted to the Arduino controller, which processes the inputs and compares them with predefined security parameters.

The Wi-Fi communication capability of the system enables the locker monitoring device to transmit authentication data and security alerts to cloud platforms or mobile applications. Through this connectivity, bank authorities and locker owners can monitor locker activity remotely and receive instant notifications whenever access attempts occur. The LCD display provides real-time system feedback by displaying authentication instructions and status messages such as "Scan RFID Card," "Enter Password," or "Access Granted." In situations where unauthorized access is attempted, the system immediately activates the buzzer alarm to alert nearby security personnel and prevent possible security breaches.

The experimental results demonstrate that the proposed IoT-based bank locker security system successfully authenticates authorized users and detects unauthorized access attempts in real time. The authentication modules operate accurately and

transmit verification data to the Arduino controller without significant delay. The Wi-Fi communication module reliably sends alert notifications to remote monitoring platforms, allowing effective security monitoring. The LCD display continuously updates system status, while the buzzer provides immediate alerts during security violations. The integrated hardware components operate efficiently and maintain stable system performance during continuous monitoring.

Overall, the implementation of the proposed system enhances bank locker security by providing an intelligent, automated, and multi-layered authentication framework. The integration of RFID identification, password authentication, biometric monitoring, and IoT communication enables strong protection against unauthorized access. The system demonstrates reliable performance, real-time monitoring capability, and user-friendly operation, making it suitable for applications in banks, financial institutions, secure storage facilities, and smart security environments.

VI. CONCLUSION AND FUTURE SCOPE

Conclusion:

The IoT-enabled three-layer bank locker security system offers a highly secure, reliable, and scalable solution for modern banking environments. By integrating RFID authentication, biometric verification, and OTP-based access control, the system significantly reduces vulnerabilities associated with traditional locker security. Literature findings support the effectiveness of multi-layer authentication and highlight IoT's role in improving real-time monitoring, alerting, and transparency. The proposed system ensures enhanced protection, immediate response to unauthorized activity, and improved user accountability. As bank security demands continue to grow, future improvements may include AI-based threat detection, blockchain-based access logs, and RFID anti-cloning technologies to further strengthen the system.

Future Scope:

The proposed IoT-Enabled Multi-Layered Security Framework for Intelligent Bank Locker Protection can be further enhanced by integrating advanced biometric authentication technologies such as iris recognition, facial recognition using deep learning, and palm vein scanning. These biometric techniques provide higher accuracy and stronger identity verification compared to conventional fingerprint systems. By combining multiple biometric methods with existing RFID and OTP authentication mechanisms, the overall reliability and security level of the bank locker system can be significantly improved. Future implementations can also utilize AI-based facial recognition algorithms to automatically detect and verify authorized users with higher precision and faster response times.

Another important future enhancement involves the integration of blockchain technology and advanced encryption methods for secure data storage and authentication record management. Blockchain can provide a decentralized and tamper-proof database for storing locker access logs, authentication records, and transaction histories. This would ensure that all locker access events are securely recorded and cannot be altered, thereby improving transparency and accountability within banking security systems. Additionally, implementing end-to-end encryption and secure communication protocols will further protect sensitive authentication data transmitted through IoT networks.

The system can also be expanded by incorporating advanced IoT cloud platforms and mobile applications for improved remote monitoring and management. Future versions of the system could provide real-time dashboards for bank administrators and locker owners, allowing them to monitor locker usage, receive instant notifications, and manage authentication permissions through mobile devices. Integration with smart banking systems and centralized security networks would allow banks to manage multiple lockers simultaneously and perform automated security analysis to detect suspicious patterns of access.

Furthermore, the proposed model can be enhanced by integrating additional intrusion detection sensors such as vibration sensors, magnetic sensors, and pressure sensors to detect forced entry or tampering attempts. These sensors can work alongside machine

learning algorithms to analyze abnormal patterns and predict potential security threats. The system can also incorporate backup power systems and fail-safe mechanisms to ensure continuous operation even during power failures or network interruptions. Such improvements would increase the reliability and robustness of the security framework.

Finally, future developments may focus on developing a fully automated smart locker management system integrated with digital banking services and biometric identity verification platforms. This would enable secure locker access through mobile-based authentication, digital identity systems, and cloud-based access control mechanisms. With the rapid advancement of IoT, artificial intelligence, and smart banking technologies, the proposed system has the potential to evolve into a highly intelligent and scalable security infrastructure capable of protecting financial assets and sensitive storage facilities in modern banking environments.

VII. REFERENCES

[1]. A. A. Ahmed, "An effective multifactor authentication mechanism for IoT devices," *Sensors*, vol. 19, no. 17, 2019.
DOI: https://doi.org/10.3390/s19173663

[2]. S. Bamashmos et al., "Two-layered multi-factor authentication using blockchain for IoT devices," *Sensors*, vol. 24, no. 11, 2024.
DOI: https://doi.org/10.3390/s24113575

[3]. T. Suleski et al., "A review of multi-factor authentication in the Internet of Healthcare Things," *Healthcare*, vol. 11, 2023.
DOI: https://doi.org/10.3390/healthcare11010063

[4]. I. El Gaabouri et al., "A systematic literature review on RFID authentication security approaches," *Future Internet*, vol. 15, no. 11, 2023.
DOI: https://doi.org/10.3390/fi15110354

[5]. J. S. Yalli et al., "Authentication schemes for Internet of Things networks: A survey," *Array*, vol. 22, 2024.
DOI: https://doi.org/10.1016/j.array.2024.100318

[6]. A. A. Alzhrani, "Design and implementation of an IoT-integrated smart locker security system," *Engineering, Technology & Applied Science Research*, 2024.
DOI: https://doi.org/10.48084/etasr.7737

[7]. O. Höfener et al., "Requirements framework for IoT device authentication mechanisms," *Computers & Security*, 2025.
DOI: https://doi.org/10.1016/j.cose.2025.103891

[8]. M. Mehta, "Authentication approaches in Internet of Things," *Recent Trends in Applied Sciences*, 2025.
DOI: https://doi.org/10.5281/zenodo.11250466

[9]. A. Ometov et al., "Challenges of multi-factor authentication for securing advanced IoT applications," *IEEE Communications Surveys & Tutorials*, 2019.
DOI: https://doi.org/10.1109/COMST.2019.2894362

[10]. S. AlJanah, N. Zhang, and S. W. Tay, "Multi-factor multi-level authentication framework for IoT applications," 2022.
DOI: https://doi.org/10.48550/arXiv.2201.07323

[11]. S. AlJanah, N. Zhang, and S. W. Tay, "Multi-factor homomorphic encryption method for authenticated access to IoT devices," 2023.
DOI: https://doi.org/10.48550/arXiv.2307.03291

[12]. M. Saideh, J. Jamont, and L. Vercouter, "Opportunistic sensor-based authentication factors in IoT," 2024.
DOI: https://doi.org/10.48550/arXiv.2404.07675

[13]. P. Tripathi, "A digital security system with door lock using RFID technology," *International Journal of Computer Applications*, 2010.
DOI: https://doi.org/10.5120/ijca2010914580

[14]. J. Parab, "IoT-based smart biometric locker security system," *SSRN Electronic Journal*, 2022.
DOI: https://doi.org/10.2139/ssrn.4304562

[15]. A. Chandrappa and P. Prithviraj, "Smart locker 2.0: Leveraging IoT and machine learning for secure locker systems," 2023.
DOI: https://doi.org/10.48550/arXiv.2304.01987