IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

IoT-AI BASED SMART SECURE LOCKER MULTI-LEVEL BANK SECURITY WITH INSTANT ALERTS

[1]M.Padma Sree,[2]G.Srinivasarao,[3]G.Estheru Rani, [4]A.Tanusha, [5]E.Chandana

[1]Assistant Professor,[2]Professor,[3,4,5]UG Student

[1]Department of Electronics and Communication Engineering,

[1]Bapatla Women's Engineering College, Bapatla, A.P,India-522101

[2]Department of Electronics and Communication Engineering,

[2]Bapatla Women's Engineering College, Bapatla, A.P, India-522101

[3,4,5]Department of Electronics and Communication Engineering,

[3,4,5]Bapatla Women's Engineering College, Bapatla, A.P, India-522101

Abstract: The Smart Secure Locker is a multilevel bank security system that uses face recognition via SVM, fingerprint scanning, and password verification for robust access control. It starts with face authentication on a laptop, followed by fingerprint and password checks through Arduino. If all steps are successful, the locker unlocks with an indicator. Any failure triggers a buzzer alarm and alerts bank authorities. This system ensures real-time monitoring and protection against cyber threats, biometric spoofing, and password breaches. By combining machine learning and hardware, it offers tamper-proof, automated, and highly secure locker access.

Index Terms **- Bank Locker Muti-level Security, Face Recognition, Fingerprint Authentication, Password, Buzzer, SVM Algorithm**

I. INTRODUCTION

In today's digital era, the demand for advanced and reliable security solutions has become more critical than ever, particularly in sectors where safety and confidentiality are paramount, such as banking. Conventional locker systems that rely solely on passwords, PINs, or physical keys are increasingly vulnerable to breaches, theft, and unauthorized access. These traditional methods lack adaptability and fail to provide real-time responses during security threats.

This paper presents a Smart Secure Locker System that incorporates multilevel authentication, including face recognition using a Support Vector Machine (SVM) algorithm executed on a laptop, fingerprint verification, RFID-based access control, and PIN-based keypad input. The proposed system is designed for deployment in bank lockers and other sensitive security zones, providing a robust defence against unauthorized access. Additionally, Buzzer is employed to send real-time alerts to bank authorities, enhancing surveillance and responsiveness in critical scenarios.

The face recognition module acts as the first layer of verification, where a webcam integrated with the laptop captures the user's image and processes it using the SVM classification technique for identity verification. Once the facial identity is confirmed, the user proceeds to the embedded system stage, which utilizes an Arduino Uno, biometric fingerprint sensor, keypad, and LCD display for subsequent authentication steps.

II. RESEARCH METHODOLOGY

In [1], a multi-factor bank locker security system was proposed using fingerprint authentication, password verification via Wi-Fi, and GSM-based OTP delivery. This layered system enhances security by combining biometric, network, and mobile communication technologies. It also provides real-time alerts and restricts access after failed attempts, ensuring robust protection of valuable assets.

In [2], an intelligent SMS-based remote water metering system was developed to monitor and bill water usage remotely without human involvement. This system enabled fast and accurate billing but did not incorporate any physical security or user authentication mechanisms.

In [3], a bank vault security system was developed using multiple sensors, fingerprint scanners, GSM modules, and IP cameras for secure access. The system aimed to provide full automation and prevent unauthorized entry, but it faced challenges such as slow performance, complex circuit design, and time-consuming processes during real-time alert generation.

In [4], a digital door lock system using RFID was developed to allow secure access through RFID tags. While it improved manual key systems, it lacked real-time monitoring, centralized control, or environmental sensors for intrusion detection.

In [5], an intelligent security system based on IoT was proposed to enhance traditional security setups in offices and banks. The system uses motion sensors, speech sensors, LTE/Wi-Fi modules, and surveillance cameras integrated with a central processing unit. Although the system supports real-time monitoring and communication, it does not offer multi-factor authentication for restricted access.

In [6], a GSM-based embedded system was proposed for remote laboratory safety monitoring, aiming to alert and prevent hazardous events through wireless GSM communication. It highlighted the advantages of real-time alert systems in safety-critical environments but did not include any biometric authentication for personalized access control.

In [7], a Locker Security System using Internet of Things (IoT) was developed to monitor locker conditions through an ESP32 microcontroller, PIR sensor, and magnetic switch. The system detects unauthorized access and uploads the status to Firebase, triggering a mobile alert via Twilio cloud and activating a buzzer. Whie the system ensures real-time intrusion alerts, it lacks biometric verification or voice-based authentication.

In [8], a multi-layer bank security system was proposed using RFID, fingerprint, and iris authentication, along with PIR sensors for motion detection. It provides dual-level access control and alerts security via alarms and emailed snapshots. The system enhances physical security but lacks IoT-based remote monitoring.

III. EXISTING AND PROPOSED METHOD

Traditional bank lockers use basic methods like GSM, fingerprint, and password, but in the existed method they lack AI and real-time monitoring, making them vulnerable. Modern IoT-based systems enhance security with two-level authentication using sensors, keypads, and buzzers, ensuring safer access and alerts for unauthorized attempts.

The proposed Smart Secure Locker system introduces a multi-level authentication approach to enhance bank locker security. It integrates three authentication methods: face recognition using an SVM algorithm, fingerprint verification, and password authentication. Face recognition is performed on a laptop, and if verified, it sends a serial command to Arduino to proceed with fingerprint authentication. Upon a successful fingerprint scan, the user must enter the correct password. If all three verifications are successful, the locker unlocks with an indicator light turning on. If any authentication fails at any stage, an Arduino-controlled buzzer is triggered to alert bank officials immediately. This real-time threat detection system prevents unauthorized access attempts. Unlike existing systems, this model ensures stronger security, automated monitoring, and instant alerts, reducing the risks of hacking, biometric spoofing, and forced access. The proposed system is cost-effective, scalable, and adaptable for modern banking infrastructures, providing a tamper-proof and highly secure locker protection solution. The figure 1 shows the block diagram of smart secure locker.

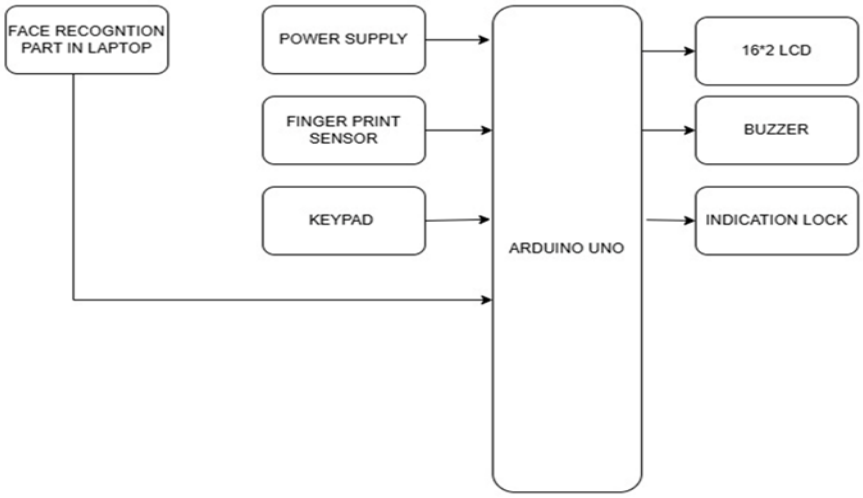

Fig 1: Block diagram Smart secure locker

3.1 System Operation

- The authentication process begins with face recognition using a webcam connected to a laptop, where a Support Vector Machine (SVM) algorithm captures and compares the user's live facial image with a pre-trained dataset to determine authorization.
- If the face is recognized, indicating the user is authorized, the system proceeds to the next level; otherwise, access is denied and no further action is taken.
- Upon successful face recognition, control is transferred to the embedded system, which is powered by a regulated power supply for stable operation.
- The user is then prompted to provide a fingerprint, which is captured by a fingerprint sensor and compared with the stored fingerprint templates in the system.
- If the fingerprint matches the stored data, the system advances to the final authentication level; otherwise, a buzzer alert is triggered to indicate a failed attempt.
- At this stage, the user must input a secure personal PIN using the keypad, which the Arduino checks against the stored credentials for verification.
- The Arduino Uno functions as the central controller, handling all authentication inputs and coordinating outputs based on the verification results.
- If all three authentication steps: face recognition, fingerprint match, and correct PIN entry are successful, a message is displayed on the 16x2 LCD, the lock mechanism is activated to grant access, and a buzzer may sound to indicate success or failure.

IV. HARDWARE COMPONENTS

- **Arduini UNO:** The Arduino UNO is a microcontroller board powered by the ATmega328P microchip. It is part of the Arduino family, an open-source platform used for building electronics projects. The UNO is one of the most commonly used Arduino boards due to its simplicity, ease of use, and strong community support. The below figure 2 shows Arduini UNO.
  - **Microcontroller:** ATmega328P
  - **Operating Voltage:** 5V
  - **Input Voltage:** 7–12V
  - **Digital I/O Pins:** 14 (of which 6 can provide PWM output)
  - **Analog Input Pins:** 6
  - **Flash Memory:** 32 KB (0.5 KB used by bootloader)
  - **SRAM:** 2 KB
  - **Clock Speed:** 16 MHz
  - **USB Interface:** Used for programming and serial communication
  - **Power Supply Options:** USB or external barrel jack or Vin pin

Fig no 2: Arduino UNO

- **Fingerprint Sensor:** The R307 is a fingerprint sensor module specifically designed for biometric identification and verification tasks. It includes an optical sensor, built-in processor, and onboard memory to store fingerprint templates. It communicates via UART serial and is commonly used in security systems, door locks, and Arduino-based projects for secure access control. The figure 3 shows fingerprint sensor.

Fig no 3: Fingerprint Sensor

- **Keypad:** An IoT keypad is a digital input device connected to a microcontroller and integrated with the Internet of Things for secure PIN entry in bank systems. It allows real-time monitoring, logging of access attempts, and remote alerts. Often used with Arduino or other controllers, it enhances security by combining local input with cloud-based surveillance and data storage. The below figure 4 shows keypad.

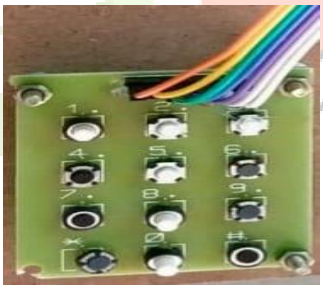

Fig no 4: Keypad

- **LCD Display:** A 16x2 LCD display is a straightforward alphanumeric screen that can present up to 16 characters on each of its two lines. It runs on 5V, uses the HD44780 controller, and can operate in 4-bit or 8-bit mode to communicate with microcontrollers like Arduino. Each character is displayed using a 5x8 pixel matrix, and a built-in LED backlight ensures visibility. It's widely used in embedded systems, IoT, and security projects to display text and user feedback. The figure 5 shows 16x2 LCD.

Fig no 5: 16x2 LCD

V. SOFTWARE IMPLIMENTATION

5.1 Python-IDLE:

IDLE (Integrated Development and Learning Environment) is Python's default editor used to write and execute Python code. In the Smart Secure Locker system, IDLE is used to run the face recognition program developed using the Support Vector Machine (SVM) algorithm. It captures the user's face through a webcam, compares it with stored data, and if matched, sends a serial signal to the Arduino to proceed with fingerprint verification. IDLE enables easy development and testing of Python scripts, making it ideal for integrating AI features into embedded systems.

5.2 Arduino IDE:

Arduino IDE is an open-source platform used to write, compile, and upload code to Arduino microcontroller boards. In the Smart Secure Locker system, it is used to control hardware components like the fingerprint sensor, password keypad, buzzer, and electronic lock. The IDE receives serial input from the Python-based face recognition system and manages the subsequent authentication steps. Its simple interface and cross-platform compatibility make it ideal for developing embedded applications with real-time control and response.

VI. CONCLUSION AND FUTURE SCOPE

The Smart Secure Locker system ensures high security using face recognition (SVM), fingerprint scanning, and password verification, all controlled by Arduino. It offers real-time alerts for unauthorized access and reduces breach risks through multi-level authentication. Integration of machine learning and embedded systems improves accuracy and automation. Future upgrades like iris or voice recognition, RFID, IoT-based remote access, mobile apps, blockchain for access logs, and cloud storage can enhance scalability and make it suitable for broader applications like banking, defence, and smart homes.

VII. RESULTS AND DISCUSSION

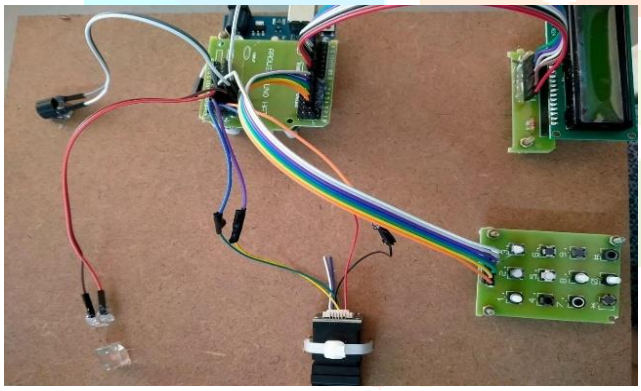

Fig 6: Setup for secure locker

Fig 7: Recognizing face

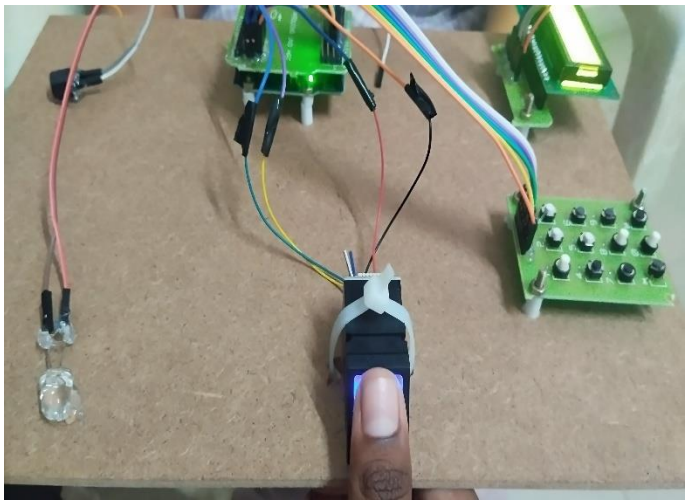

Fig 8: Placing finger

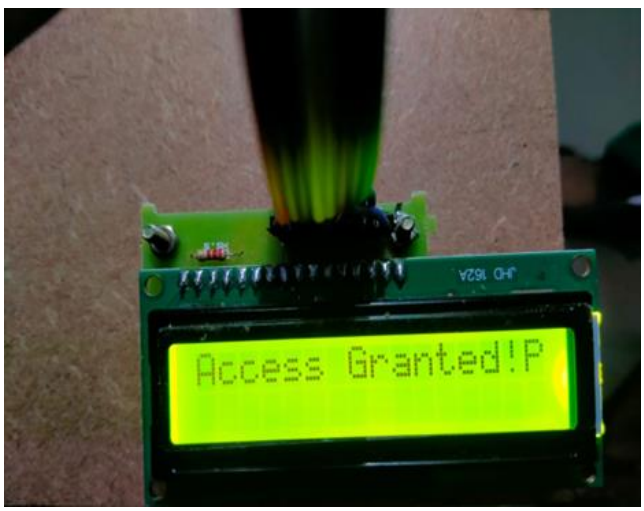

Fig 9: Granted message to access locker

As shown in above figures smart secure locker system recognizes the face and furtherly sends command to IoT in which fingerprint sensor present through the code. After placing finger as shown in figure 8 it asks for password. When you enter password, upon the successful authentication it gives access to open the locker.

REFERENCES

[1] Mr.G.Narendra, Y.Shiva Kumar, Ch. Akshaya, N. Koushika presented "*Bank Locker Security System using Password, Fingerprint and GSM Technology*" at International Journal of Computational Engineering Research (IJCER). The paper can be found in ISSN (e): 2250 – 3005 Volume, 14 Issue, 5 Sep. - Oct. – 2024

[2] Vasudevan, M., Suriyan, K. T. V., Prasanth, S. T., & Vignesh, K. (2023). "*Smart Bank Security System using Embedded System and IoT"*. *International Journal of Creative Research Thoughts (IJCRT)*, 11(4). Retrieved from http://www.ijcrt.org/

[3] Chaithanya, K., Vienala, S., & Korukonda, H. (2022). "*IoT-enabled multi-layered security solutions for bank locker access management"*. NeuroQuantology, 20(22), 5553–5565. https://doi.org/10.48047/nq.2022.20.22.NQ10574

[4] Islam, M. A., Sarder, M. S., Mamun, M. H., Ahmed, F., Sarkar, S. K., Mridul, A. H., Ahmed, M. T., & Khatun, T. (2022). "*Multi-level bank locker security system with digital signature authentication and Internet of Things"*. Research Square. https://doi.org/10.21203/rs.3.rs-2173423/v1

[5] Shrinidhi Gindi, naiyetr Shaikh, Kashif Beig, Abdeali Sabuwala. *"Smart Lock System Using RFID"* published in International Research Journal of Engineering and Technology (IJRET), Volume-07 issue on 07 July 2020, 2853-2858.

[6] Gogineni, S., Marimuthu, K., & Sheik, S. A. (2018). "*IOT Based Centralized Bank Security System for Monitoring and Auto Arresting"*. *Advances in Wireless and Mobile Communications*, 11(1), 1–9. Research India Publications. Retrieved from http://www.ripublication.com

[7] Shinde, N. P., & Nelwade, S. (2017). "*Multi-Level Secured Bank Locker System"*. International Journal for Scientific Research & Development (IJSRD), 5(10), 125–128. Retrieved from http://www.ijsrd.com

[8] Gayathri, M., Selvakumari, P., & Brindha, R. (2014). "*Fingerprint and GSM based security system"*. International Journal of Engineering Sciences & Research Technology, 3(4), 4024–4029. Retrieved from http://www.ijesrt.com

[9] Anusooya Vadukanathan, Gnanakumar Duraikannu, Venkatamuthukumar Jaganathan, Srividhya Sridhar, Gobalakrishnan Suyambrakasam (2024). "*Enhanced Bank Locker Security System Utilizing RFID for Dual-Layer Protection"* published in IEEE Journal.

[10] Singh, A., & Kaur, R. (2022). *AI-integrated secure locker system with facial recognition and multi-factor authentication*. International Journal of Scientific & Engineering Research, 13(7), 101–107. https://www.ijser.org/researchpaper/AI-Integrated-Secure-Locker-System-with-Facial-Recognition.pdf