iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: VII Month of publication: July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73215

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
*ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538*
*Volume 13 Issue VII July 2025- Available at www.ijraset.com*

# GSM Based Bank Locker Security System with 3-Layer Authentication

Sagnik Sen[1], Aditi Dutta[2], Anirudhha Hazari[3], Subhankar Bhattacharjee[4]
*[1, 2, 3]UG Scholar, [4]Professor, Department of ECE, Techno International New Town, Kolkata, India*

***Abstract: This paper introduces the design and development of a GSM-based banking locker security system that incorporates multilayered authentication to improve financial asset security. The system uses SIM900A GSM module to implement a three-level security mechanism: a masked 6-digit Personal Identification Number (PIN), a one-time password (OTP) as SMS to the registered mobile number through the SIM900A GSM module with a one min lockout feature for wrong OTP input, and a final key combination of special characters for final verification. Our system uses Arduino UNO to process inputs and control along with peripherals such as a keypad, LCD, buzzer, and motor driver, for secure interaction and physical access control. Our system provides instant system feedback along with real-time alerting via the GSM Module enabling proper access authorization and intrusion detection. Test results further validate the robustness of the system against unauthorized access and its efficiency in providing multi-layer authentication. Our model offers a scalable and cost-effective solutions for the secure banking infrastructure, providing potential applications in private lockers, vaults and ATM machines.***

***Keywords: Three-level security mechanism, Lockout feature, Physical access control, Real time alert via SMS, Robustness of system against unauthorized access.***

## I. INTRODUCTION

The security of the financial assets has become a primary concern in the rapidly evolving digital landscape. Traditional Bank Locker systems rely on manual supervision of the 2-key mechanical locks, which fully works on trust. Incidents of unauthorized access, key duplication and insider breaches exhibit vulnerabilities. To address this short-comings we have tried to implement an intelligent, automated, multi-layered authentication system with real-time monitoring capabilities.

This paper proposes a GSM-based bank locker security system designed to offer enhanced protection using a three-layer authentication mechanism. The system utilizes a 6-digit masked Personal Identification Number (PIN), a One-Time Password (OTP) that is dynamically generated and sent through GSM by the use of the SIM900A module, which also has a one-minute lock-out feature for wrong OTP input, and an additional verification from a special key combination. The system also incorporates features like a user feedback LCD, alert buzzer, and motor-driven locker mechanism, all managed through a central microcontroller.

With the use of telecommunication, the given model presents a cost-effective, user-friendly, and scalable security solution. The system presented here shows strong access control and rapid intrusion response, making it an effective option for banks, individual lockers, and other high-security applications.

## II. LITERATURE REVIEW

### *A. GSM and Iot Enabled Bank Locker Security System*

The authors proposed a GSM-enabled locker security model using an ATmega8 microcontroller, a 4x4 keypad, and an LCD. The system grants access upon correct PIN entry, while incorrect attempts trigger an SMS alert to a registered number. Although it addresses basic authentication and intrusion alerts, it relies solely on static password verification without any additional security layers such as OTP or hardware-based validation, leaving it vulnerable to password theft.

### *B. High Accuracy Bank Locker System using GSM and GPS*

The authors introduced a dual authentication system that uses both PIN and OTP verification over the GSM channel. The model integrates GPS tracking and tamper detection, along with encrypted communication for enhanced data security. Although this approach significantly strengthens security and enables real-time monitoring, the added complexity and cost make it better suited for high-security institutional environments rather than low-cost personal locker systems.

### *C. Advanced GSM and IoT Enabled Bank Locker Security with Multi-layer Authentication*

The authors developed a two-stage authentication system involving a password input via both SMS and keypad, controlled by a PIC16F877A microcontroller. A PIR sensor adds a basic level of motion detection for intrusion alerts. However, this system lacks dynamic OTP generation and multi-factor authentication, which limits its robustness in critical security applications.

### *D. Comparison with Proposed System*

The proposed GSM-based locker system advances existing solutions by implementing a three-layer security protocol—a masked 6-digit PIN, a GSM-delivered OTP, and a final key combination input. This layered approach improves resistance against brute force and credential theft while maintaining low system complexity and cost, making it suitable for both personal and institutional use.

## III. SYSTEM ARCHITECTURE AND COMPONENTS

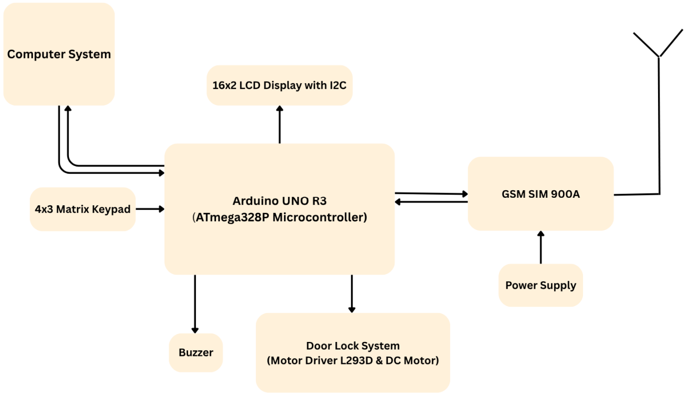


Fig. 1 System Block Diagram

### *A. Input Unit: 4x3 Keypad*

The main input device is the 4x3 matrix keypad. This keypad allows users to enter their PIN and last key combination. The Arduino UNO is directly connected to the keypad. It reads key presses in real time and checks them against logic that has already been set up.

### *B. Output Units: Lock Mechanism, LCD, and Buzzer*

The Arduino UNO is connected to a 16x2 LCD with an I2C interface to show system status, masked PIN inputs, OTP requests, and notifications such as “Access Granted” or “Incorrect PIN.” In the event of invalid attempts or unauthorized access, a buzzer is used to produce audible alerts. A DC motor and an L293D motor driver operate the locking mechanism and they are only triggered upon successful completion of the three-stage authentication process.

### *C. Communication Module: GSM SIM 900A*

It also supports wireless communication, through the SIM900A module. It sends the OTPs and reminder messages to the user’s registered mobile number. The status check and verification is in real-time utilizing a two-way communication between Arduino UNO and GSM module. A separate power supply is used for the GSM module.

### *D. Computer System Interfacing*

Arduino UNO is connected to a computer system to upload the code and for serial monitoring and debugging. The interface additionally supports live system testing during development and integration.

### *E. Power Supply*

A dedicated power supply provides regulated voltage to GSM module for continuous communication. The rest of the components, such as Arduino, motor driver, and peripherals, are powered either through USB or shared regulated supply based on system configuration.

## IV. MULTI-LAYER SECURITY MECHANISM

### *A. Three Layer Authentication: PIN, OTP Key Combination*

The system offers a strong three-level authentication mechanism to protect the bank locker.

1) *Step 1: The first layer:* We enter the six-digit PIN code through the4x3 matrix keyboard. At the LCD display this PIN is masked and is covered against a view from other people. If a correct 6-digit pin is entered, the data is moved onto the second level.
2) *Step 2: The second layer*: Here the one-time password (OTP) will be generated immediately and sent to the registered mobile number using the GSM SIM900A module. The OTP will expire after a certain amount of time and will need to be entered correctly within the time limit.
3) *Step 3: The third layer:* It contains a key-combination input of specific special characters like ‘’ which acts as an additional layer of security to prevent from brute-force or shoulder-surfing attacks.

### *B. Logical flow of access control*

The access control logic is sequential and fail safe. If any mistake is made by the user in feeding the PIN, the system rejects the entry and sounds buzzer. Otherwise, user is also denied from access if PIN is right but OTP entered wrong or entered at different time is not in the valid lists. The Arduino UNO activates the motor driver to open the locker only when the PIN, OTP, and the key combination are authentic. In case of all failed attempts, denial SMS is dispatched to the user’s mobile number for instant knowledge.

### *C. Advantages over Single-layer System*

Such a multifactor system substantially improves a security level compared to traditional single-layer systems, which can often be penetrated by only a password or a biometric identifier. By combining what the user knows (PIN), what the system has issued (OTP), and what the user does (keying in a sequence), the solution combats stolen passwords, identity fraud, and unauthorized physical entry. Particularly appropriate for sensitive environments such as bank lockers, layered authentication is required for trust and tamper resistance.

TABLE I
AUTHENTICATION FLOW TABLE

| Step | Input | Valid? | Action |
|---|---|---|---|
| 1 | PIN | No | Buzzer + SMS Alert |
| 2 | OTP | No | Lockout 60s + Alert |
| 3 | Key Combo | No | Access Denied |
| All Correct | – | Yes | Unlock Locker |

## V. GSM COMMUNICATION PROTOCOL

### *A. GSM Working Principle and AT Command Interface*

The GSM module used in this project is SIM900A that can be attached to the controller to remain connected to the device whenever required. It works on standard 2G network, it’s an easy to deploy and cost-effective module. It can communicate with Arduino UNO via AT commands using a serial interface (UART). These commands help the microcontroller to configure message format, set the recipient numbers, compose the SMS content, and further initiate the message. The typical AT command sequence includes GSM module uses AT commands:

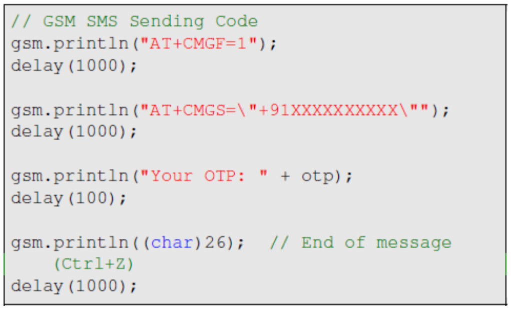
- AT - Check connectivity
- AT+CMGF=1 - Set SMS to text mode
- AT+CMGS="number" - Send SMS
- OTP message → send content
- CTRL+Z (ASCII 26) →indicate the end of data or end of message

This serial communication is two-way, meaning the Arduino can send and receive data from the GSM module, which is then displayed as real-time notifications.

### *B. OTP Generation and SMS Transmission*

By Random Number we mean that the password output given by the Arduino will be generated via a 6-digit random numeric code. After being generated, the OTP is formatted as a string and sent as an SMS message over AT command protocol. SIM900A module is used to connect the system and the mobile network to send OTP to registered mobile number. The system then generates a code and awaits the user for an input to validate the OTP code within a certain time-out period. If the OTP validates, then the system progresses to the last stage of authentication.

### *C. AT Command Sequence*



```
// GSM SMS Sending Code
gsm.println("AT+CMGF=1");
delay(1000);

gsm.println("AT+CMGS=\"+91XXXXXXXXXX\"");
delay(1000);

gsm.println("Your OTP: " + otp);
delay(100);

gsm.println((char)26);  // End of message
    (Ctrl+Z)
delay(1000);
```

## VI. HARDWARE IMPLEMENTATION

The GSM-based bank locker security system combines several hardware components to provide a safe, multi-layer authentication process. The design is centred on stable interfacing, component optimization, and synchronized response management.

### *A. Circuit Diagram*

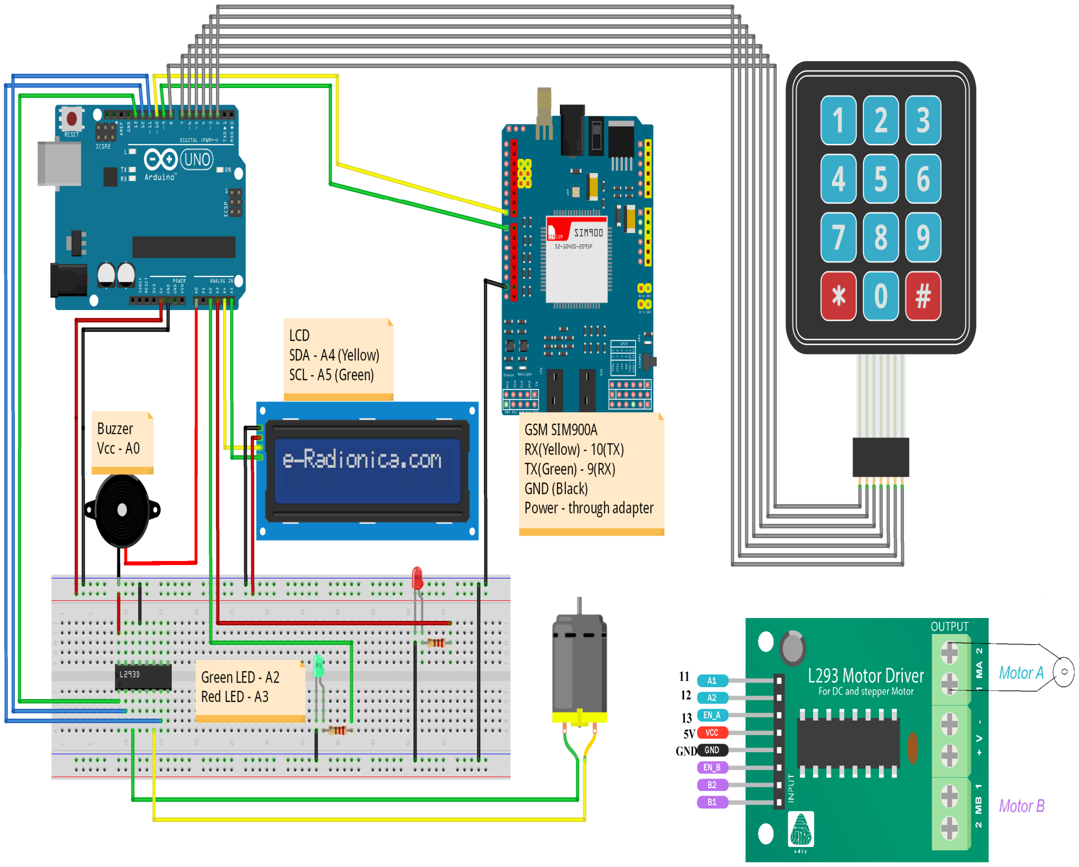


Fig. 2 Circuit Diagram showing connections for all components

### *B. Components Connections with Description*

TABLE II
COMPONENT CONNECTIONS

| Component | Pins | Description |
|---|---|---|
| Arduino Uno | – | Microcontroller to control all system operations |
| 4x3 Keypad | D2–D8 | User Input (PIN and Key combination) |
| 16x2 LCD (I2C) | SDA=A4, SCL=A5 | Displays messages to the user |
| GSM SIM900A Module | RX=D10(TX UNO) TX=D9(RX UNO)<br>Power=12V Adapter | Sends OTP and alerts via SMS. External power supply required. |
| L293D Motor Driver | A1=D11,<br>A2=D12,<br>En- A=13 | Drives DC motor for locking and unlocking mechanism |
| DC Motor | Output Terminals MA1 and MA2 of L293D | Opens/closes the locker |
| Buzzer | A0 | Alert tone on error or access |
| Power Supply | 12V Adapter | Provides power to system components |

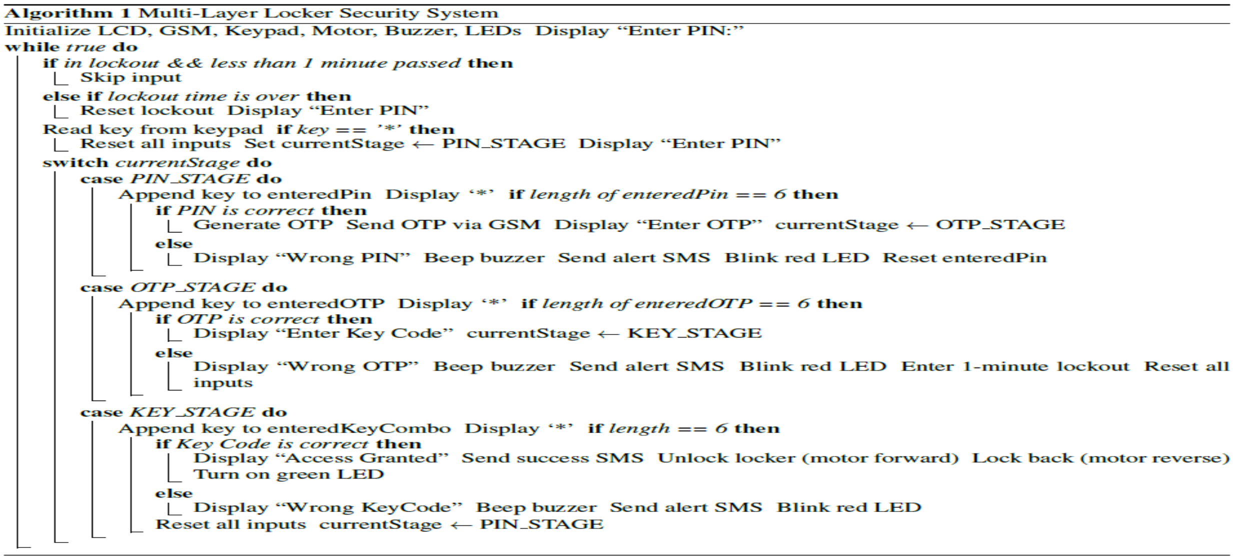
### *C. Working Flow*

- At the start of the system, the LCD asks the user to enter PIN through the keypad.
- On valid PIN, Arduino initiates GSM to send OTP on mobile.
- User inputs OTP; on match, final key sequence is asked.
- Successful input initiates motor through L293D to open locker.
- Incorrect attempts trigger buzzer and do not allow access.
- This hardware arrangement provides both security and efficiency of operation.

## VII. SOFTWARE ARCHITECTURE AND FLOW DIAGRAM

This part describes the software-level design of this multi-layer bank locker security system. It gives the structured pseudocode that controls the sequential execution of PIN, OTP, and keycode verification. The accompanying flow diagram of execution shows the visual form of logical sequence from user input to ultimate actuation.

### *A. Pseudocode: Core Logic*



```
Algorithm 1 Multi-Layer Locker Security System
Initialize LCD, GSM, Keypad, Motor, Buzzer, LEDs  Display "Enter PIN:"
while true do
    if in lockout && less than 1 minute passed then
        Skip input
    else if lockout time is over then
        Reset lockout  Display "Enter PIN"
    Read key from keypad  if key == '*' then
        Reset all inputs  Set currentStage ← PIN_STAGE  Display "Enter PIN"
    switch currentStage do
        case PIN_STAGE do
            Append key to enteredPin  Display '*'  if length of enteredPin == 6 then
                if PIN is correct then
                    Generate OTP  Send OTP via GSM  Display "Enter OTP"  currentStage ← OTP_STAGE
                else
                    Display "Wrong PIN"  Beep buzzer  Send alert SMS  Blink red LED  Reset enteredPin
        case OTP_STAGE do
            Append key to enteredOTP  Display '*'  if length of enteredOTP == 6 then
                if OTP is correct then
                    Display "Enter Key Code"  currentStage ← KEY_STAGE
                else
                    Display "Wrong OTP"  Beep buzzer  Send alert SMS  Blink red LED  Enter 1-minute lockout  Reset all
                    inputs
        case KEY_STAGE do
            Append key to enteredKeyCombo  Display '*'  if length == 6 then
                if Key Code is correct then
                    Display "Access Granted"  Send success SMS  Unlock locker (motor forward)  Lock back (motor reverse)
                    Turn on green LED
                else
                    Display "Wrong KeyCode"  Beep buzzer  Send alert SMS  Blink red LED
                Reset all inputs  currentStage ← PIN_STAGE
```

### B. *Execution Flow*

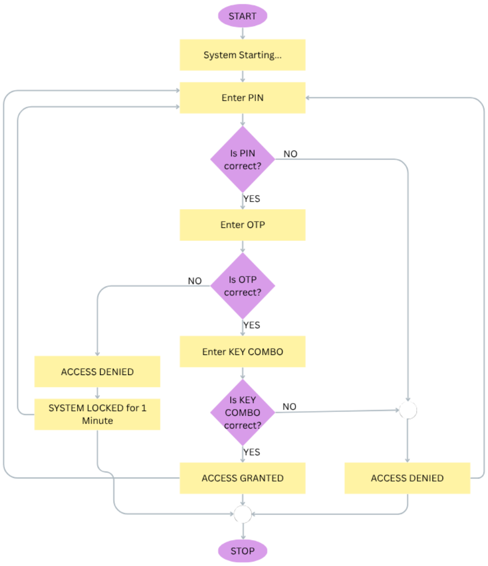


Fig. 2 System Execution Flow

### C. *Error Handling and Fallback Security Measures*

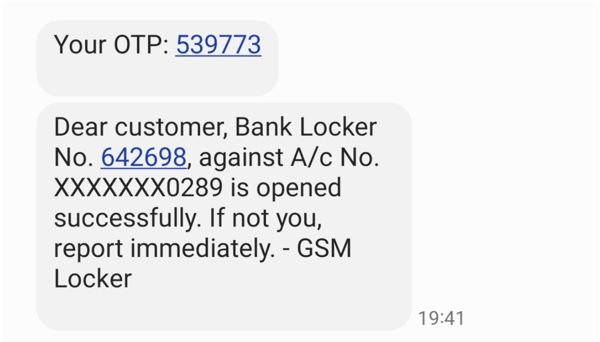
The system features error management with lockout on wrong OTP attempts, disabling the input for 60 seconds. Warning is triggered through SMS on wrong PIN, OTP, or keycode. Red LED and buzzer alert failed access. The fallback security feature keeps the locker locked unless all three levels of authentication are completed successfully, inhibiting unauthorized access.

## VIII. RESULTS AND PERFORMANCE ANALYSIS

The GSM-based bank locker security system was tested for accuracy, response time, and reliability with a three-layer authentication scheme—PIN, OTP over GSM, and key code. Four test cases were considered:

### A. *Case 1: Correct PIN, OTP, and Key Code*

Access authenticated; locker opened and closed without any issues.



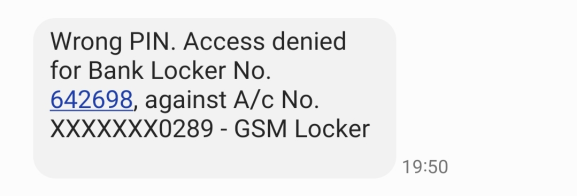
Your OTP: 539773

Dear customer, Bank Locker No. 642698, against A/c No. XXXXXXX0289 is opened successfully. If not you, report immediately. - GSM Locker

19:41

### B. *Case 2: Incorrect PIN*

System rejected access promptly with buzzer alarm and SMS alert.

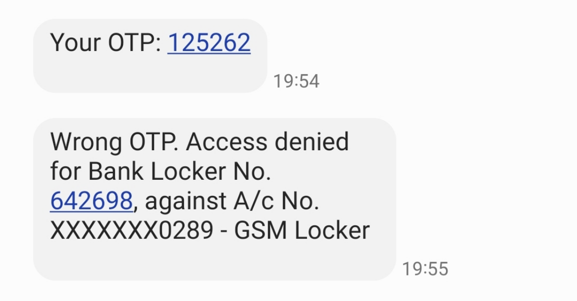


Wrong PIN. Access denied for Bank Locker No. 642698, against A/c No. XXXXXXX0289 - GSM Locker

19:50

### *C. Case 3: Right PIN, Wrong OTP*

OTP mismatch initiated lockout for 60 seconds and alert SMS.

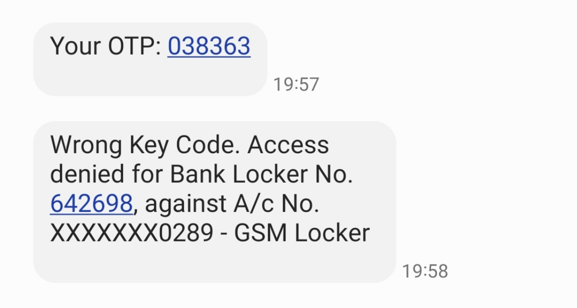


Your OTP: 125262
19:54

Wrong OTP. Access denied for Bank Locker No. 642698, against A/c No. XXXXXXX0289 - GSM Locker
19:55

### *D.* Case 4: Right PIN, Right OTP, Wrong Key Code –

Access denied; buzzer and SMS notification triggered.



Your OTP: 038363
19:57

Wrong Key Code. Access denied for Bank Locker No. 642698, against A/c No. XXXXXXX0289 - GSM Locker
19:58

The GSM module responded in about 5–7 seconds to provide the OTP. Motor operation for locking/unlocking averaged 4 seconds per cycle. The system responded consistently within acceptable limits with high accuracy in making decisions at each level. The security layer and fallback measures were effective in protecting locker entry from unauthorized attempts.

## IX. OBSERVATIONS AND IMPROVEMENTS

The prototype was found to work consistently within normal test conditions. The three-step authentication system (PIN → OTP → Key Combo) successfully blocked unauthorized access. The LCD display gave clear prompts, and the GSM module succeeded in sending OTPs within 5–7 seconds. Motor control for actuating the locker performed as expected, and SMS alerts were received in time for any incorrect attempt.

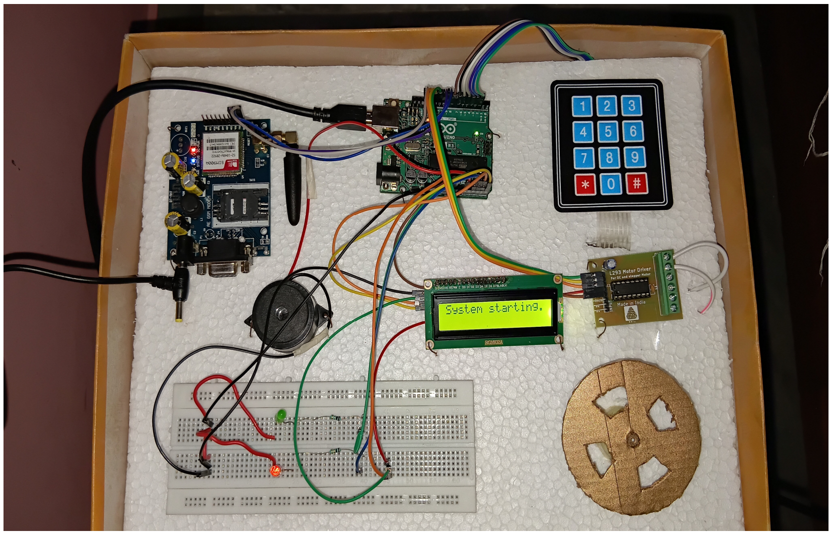


Fig. 4 Depicts the prototype designed using the hardware components

### *E. Limitations*

In spite of secure logic, the system has certain weaknesses. SIM Spoofing is an option for intercepting or simulating GSM messages, which poses a threat. Brute-force can be executed due to constrained keypad inputs, particularly when users do not reset credentials from time to time. Insufficient cloud monitoring restricts real-time incident logging and audit trails.

### *F. Future Enhancements*

1) *Cloud Logging:* Incorporating IoT cloud platforms (i.e., Firebase, AWS IoT) to log all attempted accesses, timestamps, and alerts. Biometric.
2) *Add-On:* Adding a fingerprint module or face recognition for enhanced physical security.
3) *GSM to IoT Upgrade:* Substituting GSM with Wi-Fi or LoRa-based modules to improve speed, connectivity, and enable real-time mobile app integration.
4) *Tamper Detection:* Incorporating sensors to identify physical attacks or power tampering.

These upgrades can materially improve reliability, scalability, and security of the system.

## X. CONCLUSION

The system is designed to overcome the various constraints of existing locker mechanism in bank such as manpower, its inefficient service, low security level etc. The system significantly reduces the risk of unauthorized access, as well as trans- action time, with a secure combination of PIN entry, OTP verification through GSM, and a final key combination. Based on an Arduino UNO and interfaced to the SIM900A, keypad, LCD, buzzer, motor driver, this system is compact, low cost and user friendly. Its capability to instantaneously notify users on failed access attempts, and run without continuous human monitoring, makes this smart certified system an ideal choice, especially for new age banks that want to strengthen locker security through smart and trusted technology.

## REFERENCES

[1] M. A. Naqi, V. Bhanu, S. Nikitha, and T. Shravani, “High Accuracy Bank Locker Security System Using GSM and GPS,” International Journal for Research in Applied Science & Engineering Technology (IJRASET), vol. 12, no. IV, pp. 2620–2626, Apr. 2024.

[2] M. R. Joshi and V. R. Bhagat, “GSM Based Door Locking and Unlocking System Using Arduino,” International Journal of Innovative Research in Science, Engineering and Technology, vol. 9, no. 3, pp. 1778–1783, Mar. 2020.

[3] H. Ali, M. A. Khan, and S. Saeed, “IoT-Based Smart Lock System Using GSM and RFID Technology,” International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 5, pp. 450–457, May 2021.

[4] A. Patil, S. Deshmukh, and R. Jadhav, “GSM and IoT Enabled Bank Locker Security System,” International Research Journal of Engineering and Technology (IRJET), vol. 8, no. 7, pp. 548–552, July 2021.

[5] R. Singh and N. Sharma, “Design of GSM and OTP Based Electronic Locker System,” Journal of Emerging Technologies and Innovative Research (JETIR), vol. 9, no. 2, pp. 101–106, Feb. 2022.

[6] R. Kumar and A. Gupta, “GSM and IoT Based Advanced Bank Locker Security System with Real-Time Notification,” International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 4, no. 6, pp. 35–41, June 2020.

[7] P. Verma and R. Srivastava, “Smart Door Locking System Using GSM and Face Recognition,” International Journal of Engineering Research & Technology (IJERT), vol. 12, no. 4, pp. 98–102, Apr. 2023.

[8] M. Abdullah and R. Patel, “Implementation of GSM and Fingerprint Based Locker Security System,” International Journal of Computer Applications Technology and Research (IJCATR), vol. 11, no. 3, pp. 57–62, Mar. 2022.

[9] A. Rahman and N. Banu, “IoT Enabled Bank Locker Security Using RFID and GSM Module,” International Journal of Engineering and Advanced Technology (IJEAT), vol. 9, no. 3, pp. 2125–2129, Feb. 2020.

[10] Y. Zhang and K. Li, “Design and Implementation of GSM-Based Smart Lock System for Secure Access Control,” International Journal of Recent Technology and Engineering (IJRTE), vol. 9, no. 6, pp. 95–101, June 2021.

[11] V. Patidar and A. Meena, “GSM Based Digital Security System with OTP and Fingerprint Verification,” International Journal of Research in Engineering and Technology (IJRET), vol. 11, no. 5, pp. 50–55, May 2022.

[12] K. Sharma and M. Goyal, “Advanced GSM and IoT Enabled Bank Locker Security with Multi-layer Authentication,” International Journal of Electronics and Communication Engineering & Technology (IJECET), vol. 15, no. 2, pp. 112–118, Feb. 2024.