STM JOURNALS

Journal of
Microcontroller Engineering and Applications

ISSN: 2455-197X
Volume 13, Issue 2, 2026
May—August
DOI (Journal): 10.37591/JoMEA

https://journals.stmjournals.com/jomea

Review JoMEA

GSM-Based OTP Security Locker Using Arduino

K. Siva Ranjini[1,*], J. Keerthi[2], I. Anushka[3], B. Syam[4]

Abstract

This work presents a microcontroller-driven secure locker system that leverages GSM-based communication for dynamic user authentication. Unlike conventional locking mechanisms that depend on static credentials or physical keys, the proposed system utilizes a time-sensitive one-time password (OTP) transmitted to a pre-authorized mobile number. The authentication workflow is managed using an Arduino-based embedded platform integrated with a SIM A7670C GSM module The system coordinates OTP generation, transmission, and validation in real time, ensuring that access is granted only upon successful verification within a defined time window. Hardware modules including a relay-controlled solenoid lock, infrared-based trigger unit, and LCD interface are employed to enable automated and interactive operation. This architecture eliminates dependency on manual input devices such as keypads, thereby minimizing attack surfaces Experimental validation confirms stable operation under varying signal conditions, demonstrating consistent OTP delivery and response handling. Additionally, to improve defence against unwanted access attempts, the system includes retry limiting, automated OTP expiration, and alarm notification functions. Additionally, low-power operation and flexible hardware integration are supported by the suggested architecture, making deployment in residential, commercial, financial, and institutional security contexts easier. The proposed model offers a scalable and cost-efficient approach to access control, making it suitable for decentralized security applications.

Keywords: GSM module, IR sensor, relay, solenoid lock, and LCD

INTRODUCTION

The increasing demand for secure and adaptive access control systems has exposed the limitations of traditional locking systems. Physical keys are prone to duplication and loss, whereas static password systems suffer from predictability and unauthorized sharing. These vulnerabilities necessitate a shift toward dynamic authentication models that can provide context-aware and time-bound access [1].

This project implements a GSM-enabled OTP authentication system that integrates embedded control with a mobile communication infrastructure. Instead of relying on locally stored credentials, the system dynamically generates a unique access code for each authentication attempt and transmits it via cellular networks [2]. This ensures that access credentials are transient and resistant to reuse attacks.

The design is centered around an Arduino microcontroller, which orchestrates the sensor input processing, OTP generation logic, and communication protocols. By removing the need for Internet connectivity and leveraging GSM coverage, the system ensures wider deployability, particularly in resource-constrained or remote environments.

***Author for Correspondence**
K Siva Ranjini
E-mail: ranjanikankala@gmail.com

[1]Assistant Professor, Department of ECE, BVC Engineering College (Autonomous), Odalarevu, Andhra Pradesh, India
[2,3,4]Student, Department of ECE, BVC Engineering College (Autonomous), Odalarevu, Andhra Pradesh, India

Received Date: April 08, 2026
Accepted Date: May 04, 2026
Published Date: June 01, 2026

Citation: K Siva Ranjini, J. Keerthi, I. Anushka, B. Syam. GSM Based OTP Security Locker Using Arduino. Journal of Microcontroller Engineering and Applications. 2026; 13(2): 8–15p.

The proposed solution is designed to offer a dependable and intelligent security mechanism for settings that require constant monitoring and restricted access. The Arduino microcontroller automatically initiates the authentication routine when it receives input signals from an infrared sensing device. The registered mobile number of the authorized user receives a one-time password that is created randomly via the GSM module [3]. The danger of password reuse, credential leakage, and unauthorized copying is significantly decreased because the created password is only valid for a brief period. This time-dependent authentication technique strengthens the defence against intrusion attempts and increases the overall system dependability.

The system includes an LCD module for user interaction and status monitoring, as well as a relay-driven solenoid lock to ensure effective operation. After a successful OTP verification, the relay unit permits safe locking and unlocking operations, and the display module continually sends operating signals regarding system replies and authentication status. Because the system does not rely on the Internet, it may operate efficiently in areas with limited infrastructure or distant locations where reliable wireless access may not be available [4]. Furthermore, the modular design of the hardware configuration simplifies maintenance and facilitates future connections with cloud-based monitoring platforms, alarm systems, and biometric sensors.

The suggested design provides a viable option for homes, workplaces, laboratories, banks, and institutional security applications that require improved access control because of its affordable implementation, low power consumption, and reliable communication capacity.

By automating the entire verification and locking process, the system also reduces human intervention, which lowers operational errors and accelerates reaction times. Under various network settings, experimental observations have shown reliable authentication performance and stable OTP transmission [5]. Therefore, without adding undue implementation complexity or maintenance requirements for users in various residential and commercial environments, the proposed architecture can function as an efficient basis for next-generation embedded security solutions that require flexibility, scalability, and reliable real-time communication.

SYSTEM ARCHITECTURE

The GSM-based OTP Security Locker system was built using Arduino as the main control unit, which connects all components, such as the GSM module, IR sensor, relay, solenoid lock, and LCD. This ensures proper communication and control between all parts of the system [6].

The input section detects user access using an IR sensor. The Arduino then generates a one-time password (OTP) and sends it to the user's mobile number using the GSM module. The system verifies the OTP within a limited time period for authentication.

The output section controls the relay and solenoid lock. If the OTP is correct, the locker opens; otherwise, access is denied to the user. The LCD shows system messages, making the system secure and user friendly.

For dependable real-time operation, the entire architecture was designed to facilitate effective coordination between the hardware and communication units. Without the need for human interaction, the Arduino controller continually tracks the sensor activity and oversees the entire verification process. The GSM module makes it possible to transmit authentication data securely via cellular networks, guaranteeing consistent communication even in remote locations [7]. Through time-sensitive password validation, the system maintains restricted access and limits repeated invalid attempts to increase operational safety of the system. By separating the high-power locking mechanism from the low-power control section, the relay driver circuit improves the system stability and electrical protection.

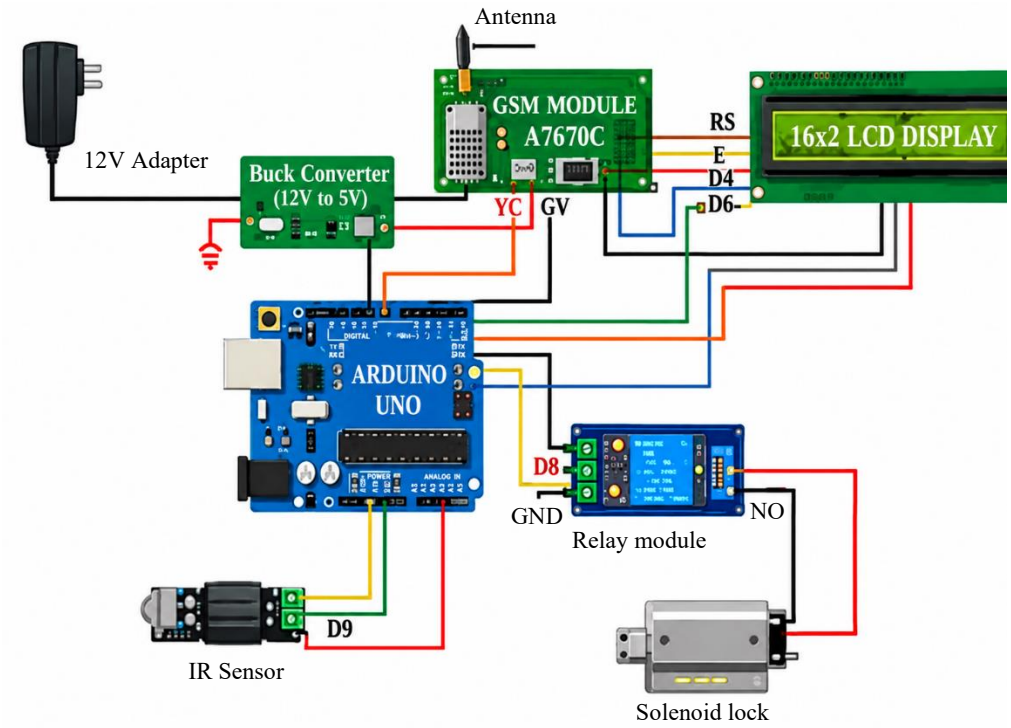

Figure 1. System architecture.

Furthermore, the modular design of the architecture, as shown in Figure 1, enables simple maintenance, component replacement, and future extension with cutting-edge technologies such as alarm systems, biometric authentication, or remote monitoring interfaces for enhanced security management and intelligent access control applications [8].

Input Signals

- *Power supply*: Provides required voltage to all components of the system.
- *Reset (RST):* Initializes the system and clears previous operations.
- *Access trigger*: Detects user request using IR sensor or switch.
- *GSM signal input*: Receives network signal for sending OTP messages.
- *OTP input*: Used for entering or verifying the received one-time password.
- *System control signals*: Manage operations such as OTP generation, verification, and lock control.

Output Signals

The design produces several output control signals:

- *GSM message signal*: Sends OTP to the user's registered mobile number
- *LCD Signal:* Displays the system status, such as OTP sent, access granted, or denied
- *Relay activation signal*: Controls the relay module for lock operation
- *Solenoid lock signal*: Activates or deactivates the locking mechanism
- *Buzzer/alert signal*: Indicates wrong OTP or unauthorized access attempt
- *Access granted signal*: Indicates successful OTP verification and locker opening
- *Access denied signal*: Indicates failure in OTP verification

The GSM-based OTP security locker system was designed as a modular embedded system consisting of several functional units. The system operates through coordinated interactions between hardware components and software programming to ensure secure access control, as shown in Figure 2.

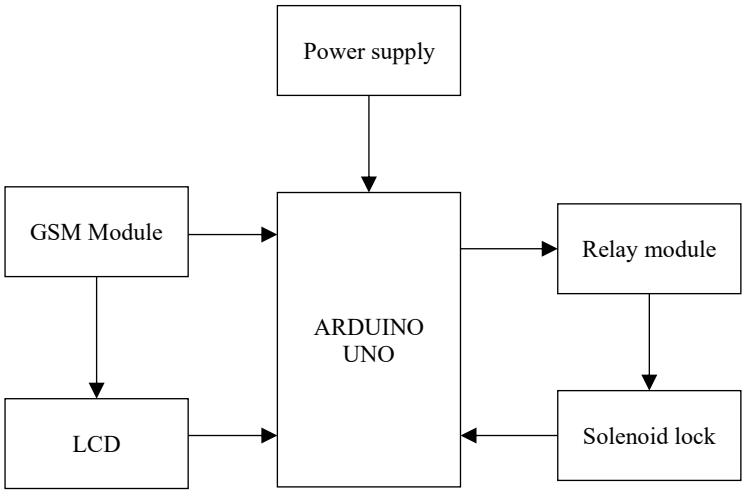

Figure 2. Block diagram.

HARDWARE COMPONENTS

The hardware implementation of the GSM-based OTP Security Locker system comprises a few interconnected parts that cooperate to offer safe and automated access control. As the central processing unit, the Arduino UNO, as shown in Figure 3, controls all the attached modules and facilitates communication [9]. The authentication procedure was initiated by the IR sensor, as shown in Figure 4, which also detected user interaction. Real-time status messages, such as OTP verification updates and system answers, are provided by a 16×2 LCD, as shown in Figure 5, which enhances user engagement and operational clarity. By sending one-time passwords to approved mobile numbers, the GSM Module A7670C, as shown in Figure 6, facilitates wireless communication while guaranteeing safe and dependable authentication via cellular network access. Table 1 illustrates the hardware specifications summary.

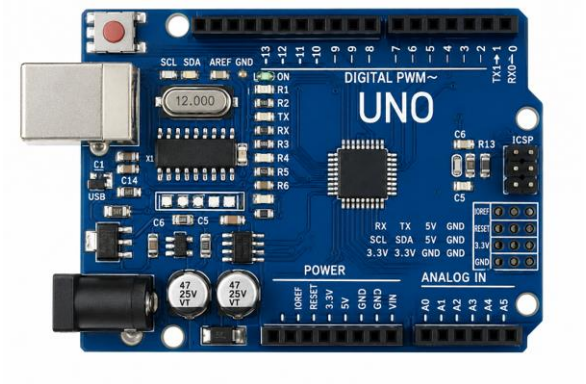

Figure 3. Arduino UNO.

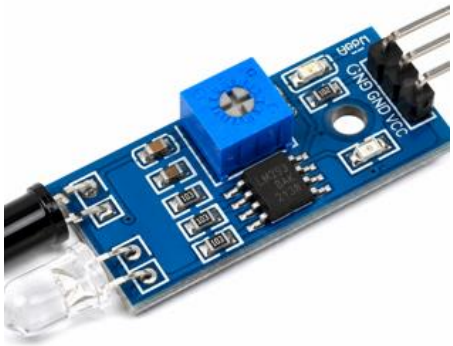

Figure 4. R Sensor.

Figure 5. LCD (16×2).

Figure 6. GSM Module A7670C.

Table 1. Hardware specifications summary.

Component	Key specification	Component	Key specification
Arduino UNO	ATmega328, 16MHz, 14 Digital I/O, 6 Analog I/O	IR Sensor	Voltage: 3.3–5V
LCD	16*2 ,3.7V-4.2V	GSM Module	A7670C, 4G LTE Cat-1, UART, AT cmd
Buck converter	LM2596, 4–40V in, 1.25–35V out, 3A		

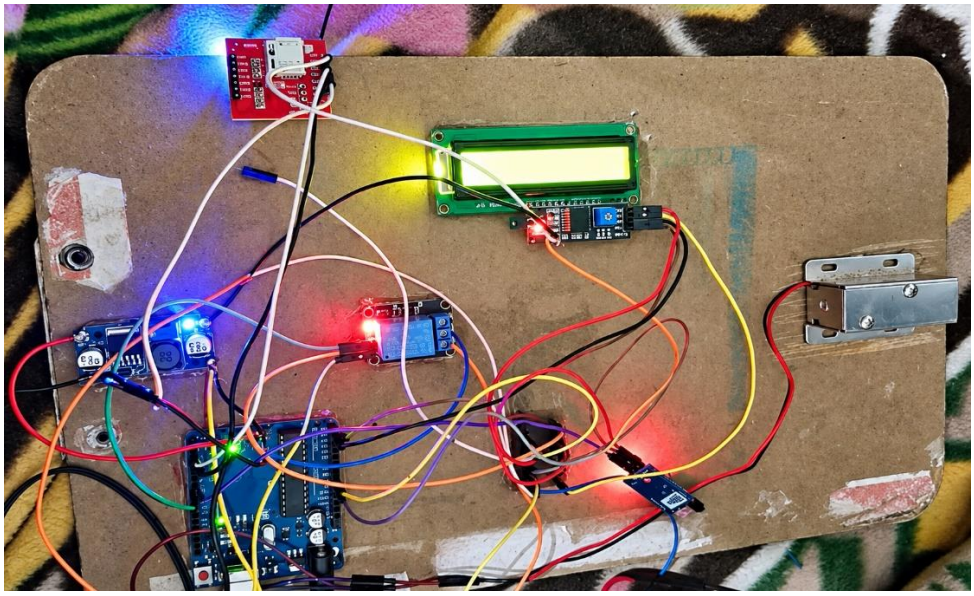

Figure 7. Hardware setup.

COMPLETE HARDWARE SETUP

The complete hardware setup, as shown in Figure 7, of the GSM-based OTP Security Locker system integrates all essential modules into a unified security platform. The Arduino UNO served as the primary controller, coordinating communication between the GSM module, IR sensor, LCD, relay circuit, and solenoid lock. The IR sensor detects access attempts and triggers the authentication process, whereas the GSM module sends the generated OTP to the authorized user [10]. The LCD continuously provides the system status and verification messages for user convenience. After successful OTP validation, the relay activates the solenoid lock to allow access to the door. The arrangement ensures secure, efficient, and automated locker operation.

RESULT

The GSM-based OTP Security Locker system was implemented using Arduino as the main controller along with a GSM SIM A7670C module, relay module, solenoid lock, IR sensor, and LCD. The hardware components were properly interfaced, and the system was programmed using Embedded C in Arduino.

Figure 8 illustrates the OTP authentication and access verification processes. AT commands are used to establish communication between the Arduino and GSM module to send OTP messages to the user's mobile number.

During implementation, the system was designed to generate a random OTP whenever an access request was detected. The generated OTP was successfully transmitted via the GSM network, and the system waited for verification. The relay and solenoid lock are connected such that the locker opens only when the correct OTP is verified. The LCD provides real-time status updates, such as OTP sent, verification in progress, and access granted or denied. Figure 9 shows the notification that SMS alert received.

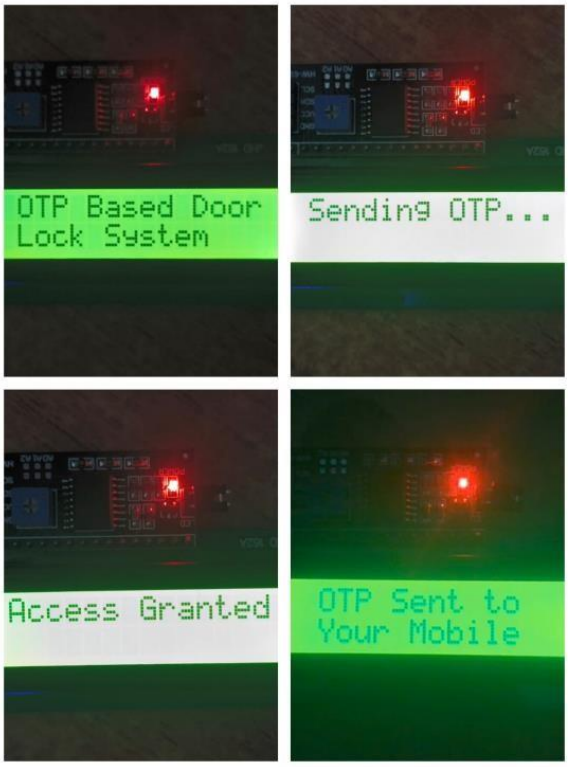

Figure 8. OTP Authentication and access verification process.

Figure 9. SMS alert received.

APPLICATIONS

The proposed system can be deployed in environments requiring controlled and traceable access without relying on network infrastructure. Typical use cases include distributed locker systems in financial institutions, controlled storage units in industrial facilities, and personal security installations in residential setups.

Additionally, the architecture can support temporary access provisioning scenarios, such as logistics delivery lockers or shared workspace storage. By associating authentication with a registered mobile identity, the system introduces a layer of accountability that is absent in conventional locking methods.

Residential security systems, where homeowners may employ OTP-based authentication to protect valuable assets and personal belongings, are another significant application of the proposed concept. Additionally, the design is appropriate for offices, libraries, laboratories, and educational institutions when access to particular storage units is restricted. The solution can facilitate temporary access authorization for parcel lockers in logistics and delivery services, allowing safe package pickup via time-limited OTP verification. Similarly, co-working spaces and shared workplaces may profit from granting authorized users temporary locker access for a set amount of time.

Compared to traditional locking techniques, this solution improves accountability, traceability, and user verification by connecting authentication with a registered cell phone number. For wider implementation across decentralized security applications, its scalable and modular architecture further facilitates integration with upcoming smart-security technologies.

CONCLUSION

The GSM-based OTP Security Locker system provides a secure and reliable solution for protecting valuable items using mobile-based authentication. By creating a one-time password (OTP) and transmitting it via the GSM module, the system allows access only to verified and authorized users. The integration of Arduino, relay, solenoid lock, IR sensor, and LCD makes the system efficient, user friendly, and cost effective. This system addresses the drawbacks of conventional locking methods by removing the need for physical keys and fixed passwords. This study presents a smart security locker system based on GSM communication and dynamic OTP authentication for improved access protection. The proposed model is designed to enhance security by replacing traditional locking approaches that depend on mechanical keys or fixed passwords. An embedded Arduino controller was employed to manage the complete authentication and locking process in real time. Whenever an access request is detected, the system generates a unique one-time password and sends it to a registered mobile number using a GSM communication module. Access is granted only after successful OTP verification within the specified period. The hardware implementation integrates multiple components, including a GSM module, infrared sensing unit, relay driver circuit, solenoid locking mechanism, and LCD interface. The infrared sensor initiates the authentication procedure, and the LCD module provides operational updates and verification status to the user. The relay-controlled solenoid lock ensures secure automated access after a successful validation. The proposed architecture offers reliable performance, low implementation cost, and simplified operation, making it suitable for both residential and commercial security applications. Because the system operates using GSM connectivity rather than Internet-based communication, it can function effectively in remote locations with limited network infrastructure. Experimental evaluation demonstrated stable OTP delivery, accurate authentication, and dependable real-time operation under varying communication conditions.

REFERENCES

1. Deva SV, Akashe S. Implementation of GSM based security system with IoT applications. Int J Comput Netw Inf Secur. 2017;14(6):13.
2. Hemalatha A, Gandhimathi G. RFID, password and OTP based door lock system using 8051 microcontroller. Int J Eng Res Technol. 2019;7(11):1-6.
3. Murthy BR, Jagadish O, Alam KT, Dada VM, Gandhi KP. Development of GSM based advanced alert home locker safety security system using Arduino Uno. Int J Sci Res Sci Technol. 2018;4(2):1154-60.
4. Arun A, Raj TA, Selvan RK, Balan SS, Lavanya S. OTP-based smart wireless locking system. In: Proceedings of the 2024 International Conference on Communication, Computing, Smart Materials and Devices (ICCCSMD); 2024 Dec 19. p. 1-6.
5. Singh A, Pal A, Rai B. GSM based home automation, safety and security system using Android mobile phone. Int J Eng Res Technol. 2015;4(5).
6. Gudadhe H, Govardhane A, Gupta S, Gurav Y, Bhaganagare R, Gujar S, et al. Auto power cutoff and load monitoring system using Arduino. In: Proceedings of the 2025 12th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO); 2025 Sep 18. p. 1-6.

7. Magar JT, Rajbamshi S, Nakarmi B. Frequency-dependent energy comparison between sleep mode and MOSFET power gating for low-duty GSM SIM modules in IoT data loggers. In: Proceedings of the 2026 International Conference on ICT and Photonics (ICTP); 2026 Feb 11. Vol. 1. p. 1-4.
8. Qian K, Den Haring D, Cao L. 8051 microcontroller. In: Embedded Software Development with C. Boston (MA): Springer US; 2009. p. 73-96.
9. Eseosa O, Promise E. GSM based intelligent home security system for intrusion detection. Int J Eng Technol. 2014;4(10):595-605.
10. Sachan A. GSM based automated embedded system for monitoring and controlling of smart grid. Int J Electr Robot Electron Commun Eng. 2013;7(12):1273-7.

