IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, April 2026
Impact Factor: 8.2

Smart Security Door Lock System using Password and OTP

Yash Harish Sonawane, Rehan Ajit Mulani, Aditya Yogesh Raut
Jayawantrao Sawant Polytechnic, Hadapsar, Pune, India

Abstract: *The increasing demand for secure access control systems has led to the development of intelligent locking mechanisms that combine multiple authentication techniques. This paper presents a Smart Security Door Lock System that integrates password-based authentication with One-Time Password (OTP) verification using a GSM module. The system is built using a microcontroller (Arduino), keypad, LCD display, relay module, and solenoid lock. The system enhances security by implementing dual-layer authentication, where the user must first enter a valid password and then verify an OTP received on a registered mobile number. This significantly reduces the risk of unauthorized access. The system is designed to be cost-effective, reliable, and suitable for real- world deployment in homes, offices, and restricted areas.*

Keywords: Smart Lock, OTP Authentication, Arduino, GSM Module, Keypad Security, Embedded System IoT Security

I. INTRODUCTION

In today's rapidly evolving world, ensuring security has become a fundamental requirement across residential, commercial, and industrial environments. Traditional locking systems that rely on mechanical keys are increasingly proving to be inadequate due to their susceptibility to key duplication, loss, and unauthorized access. With advancements in embedded systems and communication technologies, there is a growing shift toward smart security solutions that offer enhanced protection and convenience.

Electronic locking systems introduced password-based access control, which improved security to some extent. However, such systems still face limitations, including vulnerability to password theft, guessing attacks, and lack of dynamic authentication. To address these issues, modern security systems are moving toward multi-factor authentication methods that combine different verification techniques.

This project proposes a Smart Security Door Lock System using Password and One-Time Password (OTP), which integrates embedded system design with GSM communication technology. By combining static password authentication with dynamic OTP verification, the system ensures a higher level of security and reduces the risk of unauthorized access. The use of readily available components such as microcontrollers, GSM modules, and user interfaces makes the system both practical and cost-effective.

II. LITERATURE SURVEY

A review of existing research and technologies in the field of smart security systems reveals a wide range of approaches aimed at improving access control. Early systems primarily relied on mechanical locks, which were simple but highly insecure. With technological advancements, electronic systems such as keypad-based locks and RFID-based access control were introduced. While these systems improved usability, they still lacked sufficient security due to static authentication methods.

Recent developments have focused on biometric systems, including fingerprint and facial recognition technologies, which provide higher accuracy and security. However, these systems are often expensive, complex to implement, and may face reliability issues under certain conditions such as poor lighting or sensor errors.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, April 2026 Impact Factor: 8.2

Another significant advancement in security systems is the use of One-Time Password (OTP) mechanisms, which provide dynamic authentication by generating a unique code for each access attempt. OTP-based systems have been widely used in banking and online security due to their effectiveness in preventing unauthorized access.

Research also highlights the integration of GSM modules in embedded systems to enable real-time communication and remote authentication. Combining password-based systems with OTP verification has been identified as an effective approach to enhance security while maintaining cost efficiency and ease of implementation.

III. PROBLEM STATEMENT

In recent years, the need for secure and reliable access control systems has increased significantly due to rising security concerns in residential, commercial, and industrial environments. Traditional locking mechanisms that rely on physical keys are highly vulnerable to issues such as key duplication, loss, and unauthorized access. Even existing electronic locking systems that use only passwords suffer from major limitations, including the risk of password guessing, hacking, and lack of dynamic security features.

Furthermore, most conventional systems do not provide real-time verification or remote authentication, making them less effective in preventing unauthorized entry. In many cases, once a password is known or compromised, the entire system becomes insecure. Additionally, there is a lack of cost-effective solutions that offer high-level security without increasing system complexity or implementation cost.

Therefore, there is a need to develop a smart and efficient door locking system that overcomes these limitations by incorporating multi-layer authentication. The system should provide enhanced security through dynamic verification methods such as One-Time Password (OTP), ensure real-time communication, and remain affordable and easy to implement. This project aims to address these challenges by designing a dual-authentication-based smart door lock system using password and OTP verification.

IV. AIM AND OBJECTIVES

The aim of this project is to design and develop a smart and secure door locking system that uses both password and One-Time Password (OTP) authentication to provide enhanced access control. The system focuses on improving security by implementing a dual-layer verification mechanism, thereby reducing the chances of unauthorized entry while maintaining simplicity, reliability, and cost-effectiveness. It is intended to serve as a practical solution for modern security requirements in homes, offices, and other restricted areas.

To achieve this aim, the project sets several key objectives. The first objective is to implement a password-based authentication system using a keypad, enabling users to securely enter credentials. The second objective is to integrate a GSM module to generate and send OTPs to a registered mobile number, ensuring dynamic and real-time verification. Another objective is to develop a microcontroller-based control system that manages all operations efficiently, including input processing and decision-making.

Additionally, the project aims to design a relay-based mechanism to control the solenoid door lock for reliable physical access. Providing real-time feedback through an LCD display is also an important objective to enhance user interaction. Finally, the system is designed with flexibility for future upgrades such as IoT integration, biometric authentication, and remote monitoring capabilities.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, April 2026
Impact Factor: 8.2

V. SYSTEM ARCHITECTURE

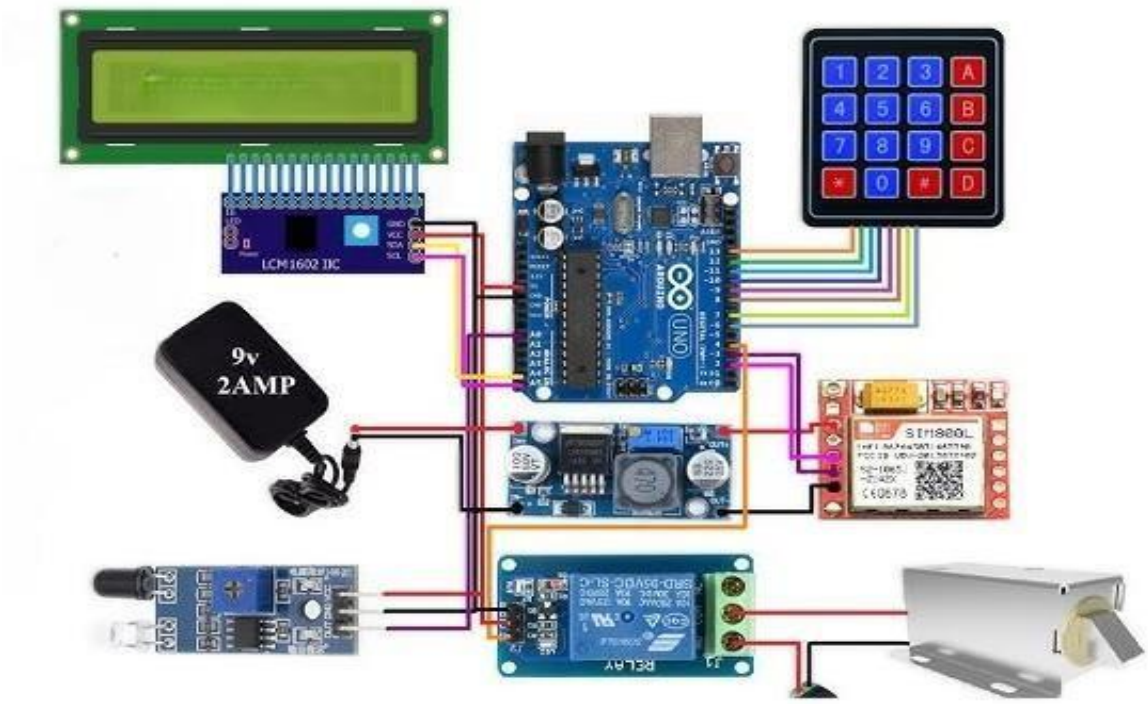

Fig. 1 System Architecture of Smart Security Door Lock System using Password and OTP

VI. CIRCUIT DESIGN AND HARDWARE DESCRIPTION

1. Arduino UNO
Acts as the main controller
Processes inputs and controls outputs
2. Keypad (4x4)
Used for entering password and OTP Connected to digital I/O pins
3. GSM Module (SIM800L)
Sends OTP via SMS Communicates using UART
4. LCD Display (16x2)
Displays instructions and status
5. Relay Module
Acts as a switch for lock control
6. Solenoid Door Lock
Opens/closes door based on relay
7. Power Supply
9V/12V regulated supply

VII. SOFTWARE DESIGN

The software design of the Smart Security Door Lock System is responsible for controlling the overall operation of the system, including user authentication, OTP generation, communication with the GSM module, and control of the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, April 2026 Impact Factor: 8.2

locking mechanism. The system is programmed using embedded C/C++ in the Arduino IDE, where the microcontroller acts as the central processing unit to execute all logical operations.

The program begins with system initialization, where all input and output devices such as the keypad, LCD display, GSM module, and relay are configured. Once initialized, the system enters a continuous loop where it waits for user input. The user is prompted to enter a password through the keypad, which is then captured and compared with the predefined password stored in the system memory.

If the password entered is correct, the software generates a random One-Time Password (OTP). This OTP is transmitted to the user's registered mobile number using AT commands through the GSM module. The system then prompts the user to enter the received OTP. The entered OTP is read and verified against the generated OTP.

If both the password and OTP are verified successfully, the microcontroller sends a signal to the relay module, activating the solenoid lock to open the door. The LCD display shows a success message. If either the password or OTP is incorrect, the system denies access and displays an error message.

The software also includes delay handling, input validation, and basic security features such as limited attempts and system reset to ensure stable and secure operation.

VIII. WORKING PRINCIPLE

The Smart Security Door Lock System using Password and OTP operates on a dual-layer authentication mechanism to ensure secure access control. The process begins when the user inputs a password through the keypad interface. This input is read by the microcontroller, which compares it with the pre-stored password in its memory. If the entered password is incorrect, the system immediately denies access and prompts the user to try again. However, if the password is verified successfully, the system proceeds to the second level of authentication.

At this stage, the microcontroller generates a One-Time Password (OTP) and sends it to the user's registered mobile number using the GSM module. This ensures that only the authorized user, who has access to the registered mobile device, can proceed further. The user then enters the received OTP using the keypad. The system verifies the entered OTP with the generated one in real time.

If the OTP matches correctly, the microcontroller activates the relay module, which in turn energizes the solenoid lock mechanism to unlock the door. Simultaneously, the LCD display provides feedback such as "Access Granted." If the OTP is incorrect, the system denies access and displays an appropriate message like "Access Denied."

Throughout the process, the system continuously monitors inputs and ensures secure, accurate, and reliable operation, thereby preventing unauthorized access and enhancing overall security

IX. ADVANTAGES & APPLICATIONS

The Smart Security Door Lock System using Password and OTP offers a combination of enhanced security and practical usability, making it suitable for a wide range of applications. One of the key advantages of this system is its dual-layer authentication mechanism, which significantly improves security by requiring both a correct password and a valid OTP. This ensures that even if the password is compromised, unauthorized access is still prevented without the OTP. The use of real-time OTP generation adds a dynamic layer of protection, making the system more secure than conventional electronic locks.

Another important advantage is its cost-effectiveness, as it is built using readily available components such as Arduino, GSM module, keypad, and relay. The system is easy to install and operate, requiring minimal technical expertise. It also provides quick response time and reliable performance, making it suitable for continuous operation. Additionally, the design is scalable, allowing future integration with advanced technologies like IoT, biometric authentication, and remote monitoring systems.

Due to these advantages, the system can be applied in various domains. It is highly suitable for smart homes, where enhanced security is essential. It can also be used in office environments to restrict unauthorized access, as well as in bank lockers and secure storage areas. Furthermore, it is applicable in hostels, paying guest accommodations

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 3, April 2026
Impact Factor: 8.2

X. LIMITATIONS

While the Smart Security Door Lock System using Password and OTP offers enhanced security and reliability, it also has certain limitations that need to be considered. One of the primary limitations is its dependence on the GSM network for OTP transmission. In areas with weak or unstable network coverage, there may be delays in receiving the OTP, which can affect the user experience and system efficiency.

Another limitation is related to the keypad-based password entry. Since the password is entered manually, it may be exposed to risks such as shoulder surfing or observation by unauthorized individuals. This can compromise the first layer of security if proper precautions are not taken.

The system also relies on a continuous power supply for operation. In case of power failure, the system may become non-functional unless supported by a backup power source. Additionally, the hardware components such as the GSM module and relay may require proper maintenance to ensure long-term reliability.

Furthermore, the system currently supports a basic level of security and may not include advanced encryption or intrusion detection mechanisms. It is also limited in scalability for very large or enterprise-level applications without further upgrades.

Despite these limitations, the system remains effective for small to medium-scale security applications and can be improved through future enhancements.

XI. FUTURE SCOPE

The Smart Security Door Lock System using Password and OTP has significant potential for future enhancements as technology continues to advance. One of the major areas of improvement is the integration of Internet of Things (IoT) technology, which would allow users to control and monitor the door lock remotely through a mobile application. This would enable features such as remote unlocking, real-time notifications, and access logs, thereby increasing convenience and security.

Another important development is the addition of biometric authentication methods such as fingerprint recognition or facial recognition. Combining biometrics with OTP verification would create a multi-factor authentication system with an even higher level of security. The system can also be upgraded to use Wi-Fi or cloud-based services instead of GSM, which would reduce dependency on network signal strength and improve OTP delivery speed.

Furthermore, cloud integration can allow data storage for entry logs, user activity tracking, and security alerts, making the system suitable for large-scale applications. Advanced encryption techniques can also be implemented to secure communication between devices. In addition, features like voice control, integration with smart home systems, and AI-based threat detection can be explored.

Overall, the system can evolve into a fully automated, intelligent security solution aligned with modern smart home and industrial security requirements.

XII. CONCLUSION

The Smart Security Door Lock System using Password and OTP provides a reliable and efficient solution for modern access control by implementing dual-layer authentication. By combining password verification with OTP- based validation, the system significantly enhances security compared to traditional locks and single-factor electronic systems. Even if the password is compromised, unauthorized access is prevented without the OTP, ensuring a higher level of protection.

The system is built using cost-effective and easily available components such as Arduino, GSM module, keypad, LCD, relay, and solenoid lock, making it practical for real-world applications. It demonstrates stable performance, quick response time, and accurate authentication under normal conditions. The integration of GSM technology enables real-time OTP delivery, adding a dynamic security feature.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 3, April 2026 Impact Factor: 8.2

Although the system depends on network availability for OTP transmission, its overall reliability remains strong due to the primary password layer. The design is modular and can be easily upgraded with advanced technologies like IoT, biometrics, or mobile app control.

In conclusion, this project offers a secure, scalable, and user-friendly access control system suitable for homes, offices, and industrial environments, with strong potential for future enhancements.

XIII. ACKNOWLEDGMENT

I would like to express my sincere gratitude to all those who have supported and guided me throughout the development of this project, "Smart Security Door Lock System using Password and OTP."

First and foremost, I would like to thank my project guide for their valuable guidance, continuous encouragement, and insightful suggestions, which greatly contributed to the successful completion of this project. Their technical expertise and support helped me understand the concepts clearly and implement them effectively.

I would also like to thank the faculty members of the Electronics and Telecommunication Engineering department for providing the necessary resources, knowledge, and motivation during the course of this project. Their support played an important role in enhancing my technical skills.

I am grateful to my institution for providing the infrastructure and facilities required to carry out this work. I would also like to thank my friends and classmates for their support, cooperation, and constructive feedback throughout the project development.

Finally, I express my heartfelt thanks to my family for their constant encouragement, patience, and moral support, which motivated me to complete this project successfully.

REFERENCES

[1]. IEEE, Research Papers on Smart Security and Access Control Systems, IEEE Publications.
[2]. Arduino, Arduino UNO Technical Documentation and Programming Guide, Official Arduino Website.
[3]. SIMCom, SIM800L GSM Module Datasheet and AT Command Manual, SIMCom Wireless Solutions.
[4]. K. Ogata, Modern Control Engineering, Prentice Hall.
[5]. Raj Kamal, Embedded Systems: Architecture, Programming and Design, McGraw Hill Education.
[6]. International Journal of Advanced Research in Science and Technology, Papers on Embedded Security Systems.
[7]. MDPI Journals, IoT-Based Smart Security and Automation Systems.
[8]. Elsevier, Research Articles on Smart Home and Security Technologies.
[9]. IEEE Xplore Digital Library, Papers on OTP Authentication and GSM Communication Systems.
[10]. Electronics Tutorials, Relay Modules, Keypad Interfacing, and LCD Display Techniques.