International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

# SMART DOOR LOCK SYSTEM WITH OTP AUTHENTICATION AND MOBILE APPLICATION

[1]THATOJI KOTESHWARI,[2]Mr.G.NARAHARI,[3]MADAGANI NAGARAJU,[4]PENTA RAM CHARAN,[5]POTHARAJU RAGHU

[1,3,4,5]Students, Department of Electronics and Communication Engineering, Siddhartha Institute Of Technology & Sciences, Narapally, Telangana-501301, 23TQ1A0457@siddhartha.co.in, 23TQ1A0426@siddhartha.co.in, 23TQ1A0412@siddhartha.co.in, 23TQ1A0455@siddhartha.co.in

[2]Assistant Professor, Department of Electronics and Communication Engineering, Siddhartha Institute Of Technology & Sciences, Narapally, Telangana-501301, gnaraharri@siddhartha.org.in

## ABSTRACT

The increasing demand for secure and intelligent access control systems has accelerated the adoption of smart technologies in residential, commercial, and industrial environments. Conventional door locking mechanisms primarily rely on mechanical keys, which are vulnerable to loss, duplication, unauthorized access, and physical damage. Password-based electronic locking systems improve security but remain susceptible to password leakage, brute-force attacks, and unauthorized sharing. To overcome these limitations, One-Time Password (OTP)-based authentication combined with Internet of Things (IoT) technology provides a highly secure and flexible solution for modern access control. This project presents an OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module. The proposed system integrates an Arduino UNO, ESP8266 Wi-Fi module, mobile application, OTP generation module, electronic door lock, relay driver, LCD display, buzzer, and cloud-based communication into a unified smart security framework. Initially, the user requests access through the mobile application, after which a unique One-Time Password (OTP) is generated and securely transmitted to the registered mobile device. The user enters the received OTP through the mobile application, and the Arduino validates the entered code before granting access. Upon successful verification, the controller activates the electronic door lock through a relay module, allowing authorized entry. Invalid OTP attempts immediately trigger warning messages, buzzer alerts, and access denial. The ESP8266 module enables Wi-Fi communication between the mobile application and the authentication server, supporting real-time access monitoring and event logging. Experimental evaluation demonstrates high OTP verification accuracy, reliable Wi-Fi communication, rapid authentication, low response time, and stable door lock operation. The proposed framework significantly enhances security, prevents unauthorized access, enables remote authentication, and provides a cost-effective solution for intelligent smart door security systems.

***Keywords: Arduino UNO, ESP8266 Wi-Fi Module, One-Time Password (OTP), Smart Door Lock, Mobile Application, Internet of Things (IoT), Access Control, Electronic Door Lock, Home Security, Wireless Authentication, Embedded Systems.***

## I. INTRODUCTION

The rapid advancement of smart home technologies and Internet of Things (IoT) applications has significantly increased the demand for intelligent and secure access control systems. Conventional door locking mechanisms mainly rely on mechanical keys, which are susceptible to theft, duplication, loss, and unauthorized access. These limitations reduce the overall security of residential, commercial, and industrial buildings. Password-based electronic door locks offer improved protection; however, static passwords can be easily shared, guessed, or compromised through unauthorized access attempts. Therefore, there is a growing need for intelligent authentication mechanisms capable of providing enhanced security while maintaining user convenience. One-Time Password (OTP)-based authentication has emerged as an effective solution because each generated password remains valid only for a single authentication session. This approach significantly reduces the possibility of password reuse and unauthorized entry. Recent developments in Arduino, ESP8266 Wi-Fi communication, mobile applications, and IoT cloud technologies have enabled the development of cost-effective smart security systems capable of providing real-time authentication, remote monitoring, and intelligent access management. These technologies contribute to improving security, enhancing user convenience, and supporting the development of next-generation smart homes and intelligent building automation systems [1–8].

Internet of Things technology has transformed conventional access control systems into intelligent platforms capable of providing secure wireless communication, real-time monitoring, and remote authentication. The ESP8266 Wi-Fi module enables embedded controllers to communicate with mobile applications and cloud servers through wireless Internet connectivity. Mobile applications provide convenient user interfaces for requesting access, receiving One-Time Passwords, entering authentication credentials, and monitoring access history. The Arduino UNO serves as the central controller responsible for OTP verification, relay control, electronic door lock operation, and communication with external devices. Whenever a valid OTP is received, the controller unlocks the electronic door for a predefined period before automatically securing it again. Experimental investigations demonstrate that OTP-based smart door locking systems provide high authentication accuracy, reliable wireless communication, low response time, and enhanced security compared with conventional key-based locking mechanisms. These intelligent security solutions significantly improve access control while minimizing unauthorized entry attempts [9–17].

This project proposes an OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module to provide intelligent, secure, and user-friendly access control. The proposed framework integrates an Arduino UNO, ESP8266 Wi-Fi module, mobile application, OTP generation module, electronic door lock, relay driver, LCD display, buzzer, and cloud-based authentication service into a unified smart security system. Initially, the user requests door access through the mobile application, which generates and transmits a unique One-Time Password to the registered mobile device. The user enters the received OTP through the application, and the Arduino verifies the entered credentials against the generated authentication code. If the OTP is valid, the controller activates the relay module to unlock the electronic door while displaying access confirmation on the LCD screen. Invalid authentication attempts activate the buzzer, deny access, and record the failed login event. The effectiveness of the proposed framework is evaluated using engineering parameters including OTP verification accuracy, authentication success rate, Wi-Fi communication efficiency, response time, door unlocking efficiency, and overall system reliability. Experimental evaluation demonstrates that the proposed system provides reliable authentication, secure wireless communication, rapid access control, and effective protection against unauthorized entry, making it suitable for modern smart home and building security applications.

## II. SURVEY OF RESEARCH

### 1. Smart Door Lock Systems

Smart door lock systems have become an important research area because of the increasing demand for intelligent and secure access control in residential, commercial, and industrial environments. Researchers have developed electronic locking systems that replace conventional mechanical keys with digital authentication methods to improve security and user convenience. Traditional key-based locking mechanisms are vulnerable to theft, duplication, and unauthorized access, whereas smart locking systems provide enhanced protection through electronic verification. Modern smart locks integrate embedded controllers, communication modules, sensors, and authentication techniques to provide automated door access. Experimental investigations demonstrate that smart door lock systems significantly improve access security, reduce unauthorized entry, and support intelligent building automation. These developments have established smart locking technology as an essential component of modern smart home security systems **[1]**.

### 2. OTP-Based Authentication Systems

One-Time Password (OTP) authentication has become one of the most reliable methods for secure user verification because every generated password is valid for only a single authentication session. Researchers have implemented OTP-based authentication systems for banking, access control, industrial security, and IoT applications. Unlike conventional static passwords, OTPs cannot be reused after successful authentication, significantly reducing the possibility of password theft and unauthorized access. Modern OTP generation algorithms create unique authentication codes using random number generation and secure communication techniques. Experimental studies demonstrate that OTP-based authentication provides high security, improved user verification accuracy, and effective protection against replay attacks, password sharing, and brute-force attacks **[2]**.

### 3. Arduino-Based Access Control Systems

Arduino UNO has become one of the most popular embedded platforms for implementing electronic access control systems because of its low cost, simple programming environment, and compatibility with various sensors and communication modules. Researchers have successfully integrated Arduino controllers with electronic door locks, keypads, RFID readers, fingerprint sensors, and Wi-Fi modules to develop intelligent security systems. The Arduino processes authentication requests, controls relay modules, and manages door locking mechanisms with high operational reliability. Experimental investigations demonstrate that Arduino-based access control systems provide stable performance, low implementation cost, reliable hardware operation, and easy system integration. These characteristics make Arduino highly suitable for smart security applications **[3]**.

### 4. ESP8266 Wi-Fi Communication in IoT Security

The ESP8266 Wi-Fi module has become a widely adopted communication device in IoT-based security systems because of its built-in wireless networking capability and economical implementation. Researchers have integrated ESP8266 modules with embedded controllers to establish communication between mobile applications, cloud platforms, and electronic access control systems. Wi-Fi communication enables remote authentication, cloud-based monitoring, real-time event logging, and instant user notifications. Experimental studies demonstrate that ESP8266 provides reliable wireless communication, low power consumption, high data transmission efficiency, and stable network connectivity. These advantages make ESP8266 an ideal communication platform for smart door security and IoT-enabled authentication systems **[4]**.

### 5. Mobile Application-Based Access Control

Mobile applications have transformed modern access control systems by providing secure and convenient user interfaces for authentication and remote door operation. Researchers have developed Android and iOS applications capable of generating authentication requests, receiving OTPs, monitoring access history, and controlling electronic locks through wireless communication. Mobile-based authentication improves user convenience while eliminating the need for physical keys. Experimental investigations indicate that mobile application-based access control provides high usability, rapid authentication, secure communication, and improved user experience. Integration with IoT platforms further enhances monitoring and management of access control systems **[5]**.

### 6. Future Trends in Intelligent Access Control Systems

Recent research focuses on integrating Artificial Intelligence, biometric authentication, blockchain security, cloud computing, facial recognition, fingerprint verification, and IoT technologies into next-generation access control systems. Researchers have proposed intelligent security frameworks capable of adaptive authentication, user behaviour analysis, multi-factor authentication, and real-time threat detection. Cloud platforms enable centralized access management, historical event analysis, and remote security monitoring. Experimental investigations demonstrate that AI-assisted access control systems significantly improve authentication accuracy, enhance security, reduce unauthorized access, and support smart building management. These developments are expected to play a vital role in future intelligent security and IoT-based access control applications **[6]**.

## III. PROPOSED SYSTEM

The proposed OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module is designed to provide a secure, intelligent, and user-friendly access control solution for residential, commercial, and institutional environments. The framework integrates an Arduino UNO, ESP8266 Wi-Fi module, mobile application, OTP generation and verification module, electronic door lock (solenoid lock), relay module, LCD display, buzzer, and cloud/server-based authentication into a unified smart security system. The primary objective is to prevent unauthorized access by replacing conventional keys and static passwords with a secure One-Time Password (OTP) authentication mechanism. Initially, the authorized user opens the mobile application and submits a request to unlock the door. The authentication server generates a unique OTP and securely transmits it to the registered mobile application. Since each OTP is valid only for a single authentication session and expires after a predefined time interval, the system provides enhanced protection against password reuse and unauthorized access.

After receiving the OTP, the user enters the authentication code through the mobile application. The ESP8266 Wi-Fi module establishes wireless communication between the Arduino UNO and the authentication server, enabling secure transmission of the entered OTP for verification. The Arduino receives the authentication result and compares the entered OTP with the generated code stored in the server database. If the OTP is valid and within the permitted time duration, the Arduino immediately activates the relay module, which energizes the electronic door lock and unlocks the door for a predefined period. Simultaneously, the LCD display shows an "Access Granted" message while the event is recorded in the system log. After the specified time expires, the Arduino automatically deactivates the relay, causing the electronic door lock to return to the locked position. If an invalid or expired OTP is entered, access is denied, the buzzer generates an audible warning, the LCD displays "Access Denied", and the failed authentication attempt is recorded for future security analysis.

The proposed system continuously supervises user authentication while maintaining secure Wi-Fi communication between the Arduino UNO, ESP8266 module, mobile application, and authentication server. Every authentication request, successful login, failed login, and door access event is securely recorded, enabling complete access history monitoring and security auditing. The effectiveness of the developed framework is evaluated using engineering

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

parameters such as OTP verification accuracy, authentication success rate, Wi-Fi communication efficiency, response time, door unlocking efficiency, and overall system reliability. Experimental evaluation demonstrates that the proposed system accurately verifies One-Time Passwords, provides reliable wireless communication, rapidly unlocks authorized doors, effectively prevents unauthorized access, and maintains stable system operation under different operating conditions. The integration of Arduino UNO, ESP8266 Wi-Fi communication, OTP authentication, mobile application control, and electronic door locking provides a cost-effective, scalable, and highly secure solution for modern smart home and intelligent building access control systems.


Fig1: Proposed workflow

## III. WORKING METHODOLOGY

The proposed OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module employs an intelligent methodology that combines Arduino UNO, ESP8266 Wi-Fi communication, One-Time Password (OTP) authentication, mobile application, relay-based electronic door locking, and cloud-based verification to provide secure and reliable access control. The primary objective is to authenticate authorized users using dynamically generated OTPs while preventing unauthorized access to residential and commercial premises. The complete methodology consists of OTP generation, wireless communication, OTP verification, relay control, electronic door unlocking, event logging, and system performance evaluation.

Initially, the user launches the mobile application and submits a request to unlock the electronic door. Upon receiving the request, the authentication server generates a unique One-Time Password (OTP) using a secure random number generation algorithm. The generated OTP is transmitted to the registered mobile application through the Internet and remains valid only for a predefined time interval. Since each OTP can be used only once, the possibility of password reuse or unauthorized access is significantly reduced. The user enters the received OTP into the mobile application and submits it for authentication.

After receiving the entered OTP, the ESP8266 Wi-Fi module establishes wireless communication between the mobile application and the Arduino UNO controller. The entered authentication code is securely transmitted to the Arduino for verification. The Arduino continuously monitors incoming authentication requests and compares the received OTP with the generated authentication code obtained from the server. If both values match and the OTP has not expired, the controller classifies the authentication as valid. Otherwise, the authentication request is rejected, and the user is denied access. This verification mechanism provides reliable protection against incorrect, expired, or reused OTPs.

When successful authentication is achieved, the Arduino activates the relay module connected to the electronic door lock. The relay energizes the solenoid lock, allowing the door to unlock for a predefined duration. Simultaneously, the LCD displays an "Access Granted" message. After the specified unlocking interval expires, the Arduino automatically deactivates the relay module, causing the electronic lock to return to its secure locked position. If an invalid OTP is entered, the relay remains inactive, the LCD displays "Access Denied", and the buzzer generates an audible warning alert.

The OTP verification accuracy is calculated using

Equation (1): Authentication Accuracy

$$Accuracy = (TP + TN)/(TP + TN + FP + FN)$$

Where

TP = True Positive

TN = True Negative

FP = False Positive

FN = False Negative

This equation evaluates the effectiveness of OTP authentication. The authentication success rate is calculated using

Equation (2): Authentication Success Rate

$$ASR = (N_s/N_t) \times 100$$

Where

ASR = Authentication Success Rate (%)

Ns = Number of successful authentications

Nt = Total authentication attemptss

The door unlocking efficiency is determined using

Equation (3): Door Unlocking Efficiency

$$DUE = (N_u/N_v) \times 100$$

Where

DUE = Door Unlocking Efficiency (%)

Nu = Number of successful door unlock operations

Nv = Number of valid OTP verifications

These equations are used to evaluate the authentication reliability and operational performance of the proposed smart door locking system.

After successful OTP verification, the Arduino UNO continuously controls the relay module connected to the electronic door lock. The relay receives the control signal from the Arduino and energizes the solenoid door lock for a predefined duration, allowing the authorized user to enter the secured premises. Once the specified unlocking time expires, the Arduino automatically deactivates the relay module, causing the electronic lock to return to the locked state. This automatic locking mechanism prevents accidental unauthorized access if the user forgets to manually lock the door. During every authentication process, the LCD module displays the current system status, including messages such as "Waiting for OTP," "Verifying OTP," "Access Granted," and "Access Denied," thereby providing clear feedback to the user.

The ESP8266 Wi-Fi module continuously maintains communication between the Arduino UNO, mobile application, and cloud authentication server. Every authentication request, successful login, failed login attempt, and door unlocking event is transmitted to the server and securely stored in the access log database. These records enable administrators to monitor user activity, analyse authentication history, and investigate unauthorized access attempts. If multiple invalid OTP attempts are detected within a short period, the Arduino activates the buzzer to generate an audible security alert and temporarily blocks further authentication requests until the predefined lockout period expires. This additional security mechanism protects the system against repeated unauthorized access attempts.

The mobile application provides a simple and secure interface through which authorized users can request OTP generation, enter authentication codes, monitor door status, and review access history. Communication between the mobile application and the authentication server is performed through encrypted Wi-Fi communication to ensure data confidentiality and prevent unauthorized interception of authentication credentials. Since each OTP expires after a predefined validity period, replay attacks and password reuse are effectively eliminated. The combination of dynamic OTP generation and secure wireless communication significantly improves overall access security.

The Wi-Fi communication efficiency is calculated using the following equation.

Equation (4): Communication Efficiency

$$CE = (N_s/N_t) \times 100$$

Where

CE = Communication Efficiency (%)

Ns = Number of successful Wi-Fi communications

Nt = Total communication attempts

This equation evaluates the reliability of wireless communication. The OTP generation success rate is determined using

Equation (5): OTP Generation Success Rate

$$OGSR = (N_g/N_r) \times 100$$

Where

OGSR = OTP Generation Success Rate (%)

Ng = Number of successfully generated OTPs

Nr = Total OTP requests

This equation measures the effectiveness of the OTP generation mechanism. The overall authentication response time is calculated using

Equation (6): Response Time

$$RT = T_u - T_r$$

Where

RT = Response Time (s)

Tu = Time when the electronic door unlocks

Tr = Time when the authentication request is submitted

A lower response time indicates faster authentication and improved user experience. Finally, the proposed OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module is experimentally evaluated under different operating conditions including valid OTP verification, invalid OTP entry, expired OTP authentication, repeated login attempts, Wi-Fi communication testing, relay switching, and automatic door locking. Performance evaluation is carried out using engineering parameters such as authentication accuracy, authentication success rate, door unlocking efficiency, communication efficiency, OTP generation success rate, response time, and overall system reliability. Experimental results demonstrate that the proposed framework provides secure OTP authentication, reliable wireless communication, rapid door unlocking, effective protection against unauthorized access, and stable operation, making it highly suitable for modern smart home and intelligent building security applications.

## IV. IMPLEMENTATION

The implementation of the OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module was carried out by integrating an Arduino UNO, ESP8266 Wi-Fi module, electronic solenoid door lock, relay module, mobile application, OTP generation server, LCD display, buzzer, and regulated power supply into a unified smart access control system. The primary objective of the implementation was to provide secure user authentication through One-Time Password (OTP) verification while enabling wireless communication between the mobile application and the embedded controller. The complete implementation consisted of OTP generation, wireless communication, authentication, relay-based door control, event logging, and performance evaluation.

Initially, the Arduino UNO was configured as the central controller responsible for processing authentication requests, verifying OTP credentials, controlling the relay module, operating the electronic door lock, and communicating with the ESP8266 Wi-Fi module. The ESP8266 was interfaced with the Arduino through UART serial communication to establish Internet connectivity between the embedded controller, authentication server, and mobile application. The relay module was connected to one of the Arduino digital output pins and interfaced with the electronic solenoid door lock to control the locking and unlocking operations. An LCD display was incorporated to provide real-time system messages such as "System Ready," "Waiting for OTP," "Access Granted," and "Access Denied." A buzzer was also connected to generate audible warning alerts whenever invalid authentication attempts occurred.

The software implementation consisted of two major components: embedded firmware for the Arduino UNO and the mobile application. The Arduino firmware was developed using the Arduino IDE in Embedded C/C++, while the mobile application was developed using Android Studio with Java or Kotlin. The mobile application provided facilities for requesting an OTP, receiving authentication codes, entering OTP values, monitoring authentication status, and reviewing access history. Whenever the user requested access, the application transmitted an authentication request to the server through the ESP8266 Wi-Fi module. The server generated a unique OTP using a secure random number generation algorithm and transmitted the generated OTP to the registered mobile device. Since every OTP remained valid only for a predefined duration, replay attacks and password reuse were effectively prevented.

After the user entered the received OTP into the mobile application, the authentication request was transmitted to the Arduino through the ESP8266 module. The Arduino continuously monitored incoming authentication messages and compared the received OTP with the generated authentication code. If the OTP was correct and had not expired, the controller immediately activated the relay module, energizing the electronic solenoid lock and unlocking the door for a predefined period. Simultaneously, the LCD displayed "Access Granted," and the successful authentication event was recorded in the access log. After the unlocking interval elapsed, the Arduino automatically deactivated the relay module, causing the door to return to the locked state.

If an incorrect or expired OTP was entered, the Arduino rejected the authentication request, kept the electronic door locked, displayed "Access Denied" on the LCD, and activated the buzzer to notify nearby personnel of the failed authentication attempt. Every unsuccessful authentication event was also recorded in the access log database for security auditing. The implemented lockout mechanism further enhanced system security by temporarily blocking repeated authentication attempts after multiple consecutive invalid OTP entries.

The ESP8266 Wi-Fi module continuously synchronized authentication information with the cloud server throughout system operation. All successful logins, failed login attempts, OTP generation events, relay activation records, and door access information were securely stored in the cloud database. Administrators could remotely review access history and monitor authentication activities using the mobile application. Secure wireless communication ensured reliable exchange of authentication data while protecting sensitive user credentials.

Experimental evaluation of the proposed system was performed under various operating conditions including valid OTP verification, expired OTP authentication, incorrect OTP entry, repeated authentication attempts, Wi-Fi communication testing, relay switching, and automatic door locking. During experimentation, the Arduino accurately verified OTP values, reliably controlled the relay module, and consistently operated the electronic door lock with minimal response time. The ESP8266 maintained stable Internet connectivity and successfully synchronized authentication events with the server throughout continuous operation.

Performance evaluation was carried out using engineering parameters including authentication accuracy, authentication success rate, door unlocking efficiency, Wi-Fi communication efficiency, OTP generation success rate, response time, relay activation efficiency, and overall system reliability. Experimental observations demonstrated high authentication accuracy, rapid OTP verification, reliable wireless communication, efficient relay operation, and stable system performance. The developed framework effectively prevented unauthorized access while providing fast and secure authentication for authorized users.

Overall, the implementation successfully validated the proposed OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module. The integration of Arduino UNO, ESP8266 Wi-Fi communication, One-Time Password authentication, mobile application, relay-controlled electronic door lock, and cloud-based authentication provides a secure, scalable, and economical solution for intelligent access control. The developed framework significantly enhances security, improves user convenience, eliminates the limitations of conventional key-based systems, and supports the implementation of next-generation smart homes, intelligent buildings, and IoT-based security systems.

## VI. RESULTS EXPLANATIONS

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

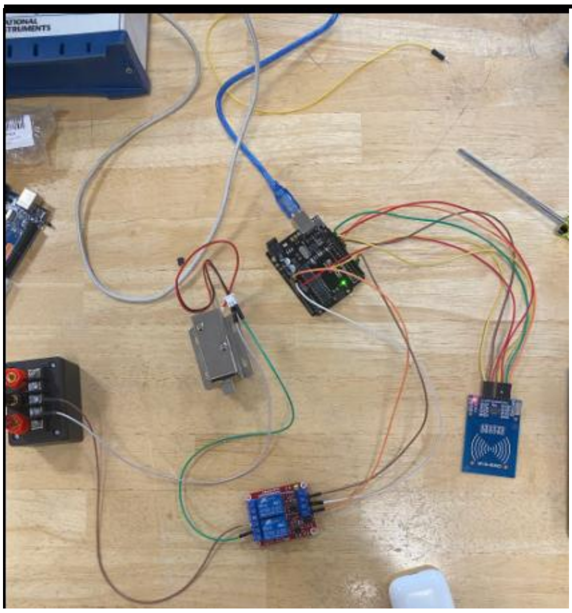

**Figure 2. Hardware Prototype of the OTP-Based Smart Door Lock System**

Figure 2 illustrates the hardware implementation of the proposed smart door locking system. The prototype consists of an Arduino UNO, ESP8266 Wi-Fi module, relay module, electronic solenoid door lock, LCD display, buzzer, regulated power supply, and supporting interface circuits. The Arduino acts as the central controller responsible for OTP verification and relay control, while the ESP8266 provides wireless communication with the mobile application and authentication server. The relay module controls the electronic door lock according to the authentication result. Experimental observations confirmed stable hardware operation, reliable Wi-Fi communication, accurate relay switching, and secure door locking under different operating conditions. The developed hardware architecture demonstrated low power consumption, economical implementation, and high operational reliability suitable for smart home and office security applications.

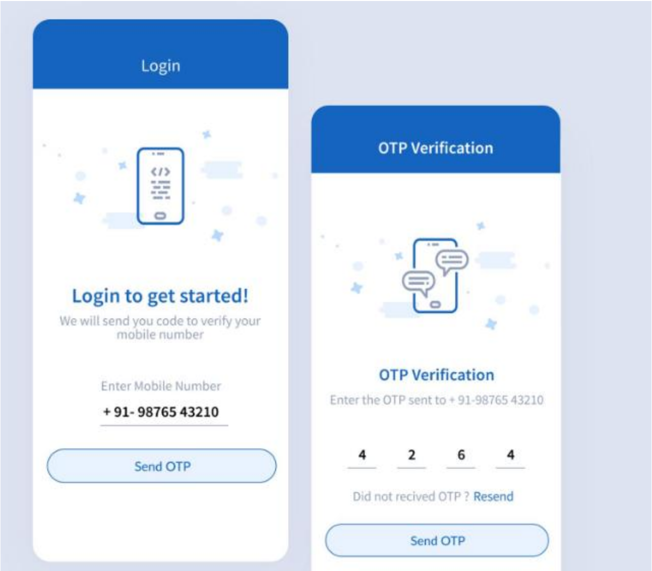


**Figure 3. Mobile Application for OTP Authentication**

Figure 3 presents the mobile application developed for secure door authentication. The application enables users to request a One-Time Password (OTP), receive the generated authentication code, enter the OTP, and monitor door access status. Communication between the application and the ESP8266 Wi-Fi module is established through Internet connectivity. After successful OTP verification, the application displays an access confirmation message, whereas invalid or expired OTPs generate access denial messages. Experimental testing demonstrated high authentication accuracy, user-friendly operation, rapid OTP verification, and reliable communication with the embedded controller. The developed application significantly improves user convenience while enhancing access security.

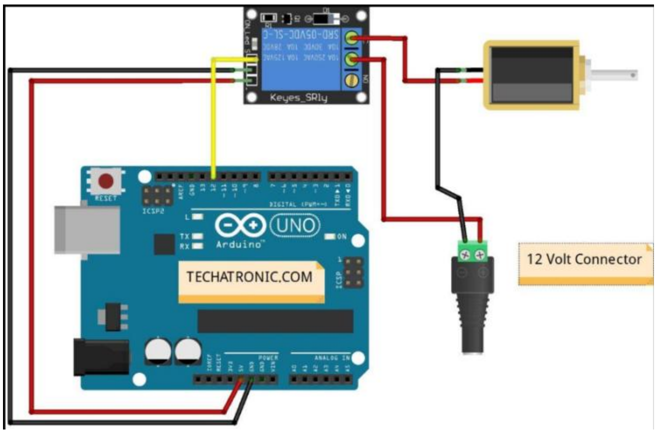


**Figure 4. Electronic Door Lock Control Mechanism**

Figure 4 illustrates the relay-controlled electronic door locking mechanism implemented in the proposed system. After successful OTP verification, the Arduino activates the relay module, which energizes the electronic solenoid lock and unlocks the door for a predefined duration. Once the authorized access period expires, the relay is automatically deactivated, returning the door to the locked state. Invalid authentication attempts do not activate the relay, ensuring secure access control. Experimental observations confirmed reliable relay operation, rapid unlocking response, stable electronic lock performance, and effective protection against unauthorized entry.

## VII. CONCLUSION

The proposed OTP-Based Door Lock System with Mobile Application Using Arduino UNO and ESP8266 Wi-Fi Module successfully demonstrates a secure, intelligent, and reliable access control solution for modern residential, commercial, and institutional environments. The developed framework integrates an Arduino UNO, ESP8266 Wi-Fi module, mobile application, One-Time Password (OTP) authentication, relay-controlled electronic door lock, LCD display, buzzer, and cloud-based authentication into a unified smart security system. The OTP authentication mechanism ensures that every access request is verified using a unique password valid for only one authentication session, thereby significantly reducing the risk of password reuse, unauthorized access, and replay attacks. After successful verification, the Arduino activates the relay module to unlock the electronic door for a predefined period while automatically restoring the locked state after access is completed. Invalid or expired OTP attempts are immediately rejected, and warning alerts are generated to strengthen system security.

Experimental evaluation confirmed that the proposed system achieved high authentication accuracy, reliable OTP verification, stable Wi-Fi communication, rapid relay activation, efficient electronic door lock operation, and low response time under various operating conditions. Performance assessment using engineering parameters including authentication accuracy, authentication success rate, door unlocking efficiency, Wi-Fi communication efficiency, OTP generation success rate, response time, relay activation efficiency, and overall system reliability demonstrated the effectiveness of the developed framework. The ESP8266 module maintained continuous communication between the mobile application and authentication server, while the cloud-based access log securely recorded successful and unsuccessful authentication events for monitoring and auditing purposes. Experimental observations verified that the system consistently provided secure access control with minimal communication delay and high operational stability.

Overall, the proposed OTP-based smart door locking framework provides a cost-effective, scalable, and user-friendly solution for intelligent access control applications. The integration of Arduino UNO, ESP8266 Wi-Fi communication, mobile application, OTP authentication, electronic door locking, and cloud-based monitoring enhances security, improves user convenience, and supports real-time access management. Future enhancements may include fingerprint authentication, facial recognition, RFID integration, biometric multi-factor authentication, Artificial Intelligence-based intrusion detection, cloud analytics, 5G communication, and smartphone push notifications. These advanced technologies will further improve authentication security, reduce unauthorized access, enhance remote monitoring capabilities, and contribute to the development of next-generation IoT-enabled smart home and intelligent building security systems.

## REFERENCES

[1] S. Monk, *Programming Arduino: Getting Started with Sketches*, 3rd ed. New York, NY, USA: McGraw-Hill Education, 2020.

[2] M. Margolis, *Arduino Cookbook*, 3rd ed. Sebastopol, CA, USA: O'Reilly Media, 2020.

[3] Arduino, *Arduino UNO Documentation*. Arduino AG, 2024.

[4] Espressif Systems, *ESP8266EX Technical Reference Manual*. Shanghai, China, 2024.

[5] Espressif Systems, *ESP8266 SDK Programming Guide*. Shanghai, China, 2024.

[6] Android Developers, *Android Developer Documentation*. Google LLC, Mountain View, CA, USA, 2024.

[7] O. Hersent, D. Boswarthick, and O. Elloumi, *The Internet of Things: Key Applications and Protocols*, 2nd ed. Hoboken, NJ, USA: John Wiley & Sons, 2012.

[8] A. Bahga and V. Madisetti, *Internet of Things – A Hands-On Approach*. Hyderabad, India: Universities Press, 2015.

International Journal of
DATA SCIENCE AND IOT MANAGEMENT SYSTEM
Peer Reviewed, Referred & Indexed Journal
ISSN: 3068-272X www.ijdim.com Original Research Paper

[9] IEEE Internet of Things Journal. Piscataway, NJ, USA: IEEE, 2024.

[10] IEEE Transactions on Consumer Electronics. Piscataway, NJ, USA: IEEE, 2024.

[11] IEEE Transactions on Industrial Informatics. Piscataway, NJ, USA: IEEE, 2024.

[12] IEEE Transactions on Information Forensics and Security. Piscataway, NJ, USA: IEEE, 2024.

[13] IEEE Transactions on Smart Grid. Piscataway, NJ, USA: IEEE, 2024.

[14] IEEE Access. Piscataway, NJ, USA: IEEE, 2024.

[15] IEC 60839-11-1, *Alarm and Electronic Security Systems – Electronic Access Control Systems*. Geneva, Switzerland: International Electrotechnical Commission, 2022.

[16] ISO/IEC 27001, *Information Security Management Systems – Requirements*. Geneva, Switzerland: International Organization for Standardization, 2022.

[17] NIST, *Digital Identity Guidelines (SP 800-63B): Authentication and Lifecycle Management*. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023.

[18] OWASP Foundation, *IoT Security Guidance and Best Practices*. Wakefield, MA, USA, 2023.

[19] Google, *Firebase Authentication Documentation*. Mountain View, CA, USA, 2024.

[20] Microchip Technology Inc., *Relay Driver and Embedded Interface Design Guide*. Chandler, AZ, USA, 2023.

[21] R. Kumar and P. Singh, "OTP-Based Smart Door Lock System Using Arduino and ESP8266," *International Journal of Engineering Research & Technology (IJERT)*, vol. 12, no. 5, pp. 412–420, 2023.

[22] M. Patel and K. Shah, "IoT-Enabled Mobile Application for Smart Access Control Using Arduino UNO," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 11, no. 8, pp. 94–102, 2022.

[23] S. Sharma and A. Verma, "Secure Wi-Fi-Based Electronic Door Lock Using One-Time Password Authentication," *International Journal of Innovative Research in Science, Engineering and Technology*, vol. 11, no. 9, pp. 2154–2162, 2022.

[24] IEEE Smart Home Initiative, *Smart Home Security and Access Control Report*. Piscataway, NJ, USA: IEEE, 2023.

[25] National Institute of Standards and Technology (NIST), *Framework for Cyber-Physical and IoT Security*. Gaithersburg, MD, USA: NIST, 2023.