OTP BASED SMART WIRELESS LOCKING SYSTEM USING ARDUINO UNO

MINIPROJECT REPORT

Submitted by

GANGA KRISHNA A (SCT22EC061)

GAWTHAM CHOODAN A V (SCT22EC062)

KARTHIK PRAMODH (SCT22EC076)

MEENAKSHI H L (SCT22EC081)

to the APJ Abdul Kalam

Technological University

in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology

in

Electronics and Communication Engineering

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SREE CHITRA THIRUNAL COLLEGE OF ENGINEERING

THIRUVANANTHAPURAM

APRIL 2025

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SREE CHITRA THIRUNAL COLLEGE OF ENGINEERING, THIRUVANANTHAPURAM

2024-25

CERTIFICATE

This is to certify that the report entitled **"OTP BASED SMART WIRELESS LOCKING SYSTEM"** submitted by, **Ganga Krishna A (SCT22EC061), Gawtham Choodan A V (SCT22EC062), Karthik Pramodh (SCT22EC076) and Meenakshi H L (SCT22EC081)**, to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Electronics and communication is a bonafide record of the mini project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Prof. Kumar G S
Mini Project Coordinator
Assistant Professor,
Dept. of ECE,
SCTCE

Dr. Nisha Jose K
Mini Project Coordinator
Associate Professor
Head of the Department
Dept. of ECE,
SCTCE

DECLARATION

We undersigned hereby declare that the mini project report that is entitled as follows, “OTP BASED SMART WIRELESS LOCKING SYSTEM”, submitted for partial fulfillment of the requirements for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by us under supervision of Mr. KUMAR G S, Assistant Professor, Department of Electronics and Communication Engineering. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. We understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Thiruvananthapuram

02/04/2025

Ganga Krishna A (SCT22EC061)

Gawtham Choodan A V (SCT22EC062)

Karthik Pramodh (SCT22EC076)

Meenakshi H L (SCT22EC081)

ACKNOWLEDGEMENT

We would like to express our sincere gratitude and appreciation to all those who have contributed to the successful completion of this project. This endeavour would have been impossible without their support, guidance, and valuable input. Our deep gratitude towards **Dr C. Satish Kumar, The Principal, Sree Chitra Thirunal College of Engineering, Thiruvananthapuram** for providing this opportunity and necessary facillities for the completion of this project.

First and foremost, we extend our heartfelt thanks to our project coordinator Mini Project Co-Ordinator, **Prof. (Dr.) Nisha Jose K, Head of the Department, Department of ECE, SCT College of Engineering** for her unwavering guidance, encouragement, and expertise throughout the entire duration of this project. Her valuable insights, suggestions, and constructive feedback have been instrumental in shaping the direction and quality of this work.

We gratefully thank our Mini project coordinator **Prof. Kumar G S, Assistant Professor, Department of ECE, SCT College of Engineering** for his unwavering guidance, encouragement, and expertise throughout the entire duration of this project.

ABSTRACT

In modern security systems, OTP (One-Time Password) based authentication provides a robust method to prevent unauthorized access while maintaining user convenience. This project presents an Arduino-based door lock system using the SIM800L GSM module to deliver secure, dynamic OTPs via SMS. The system eliminates the risks associated with static passwords by generating a unique 4-digit code for each access attempt, ensuring enhanced security.

The system operates by detecting user presence via an IR sensor, triggering the Arduino to generate a random OTP. The SIM800L module transmits this OTP to the registered mobile number, while a 4×4 keypad serves as the input interface for verification. Upon successful validation, a relay activates to unlock the door; incorrect entries deny access and prompt retries.

Designed for simplicity and cost-effectiveness, this solution leverages widely available components—Arduino Uno, GSM module, and basic I/O peripherals—to create a reliable access control system without complex infrastructure. Experimental results confirm its effectiveness in real-world scenarios, balancing security and usability.

This project contributes to the field of secure access systems by offering a scalable, microcontroller-based alternative to traditional locks, suitable for homes, offices, and restricted areas where GSM connectivity is feasible. Its modular design allows for future integration with biometrics or IoT platforms.

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In modern security, OTP (One-Time Password) based authentication has become essential for enhancing access control while maintaining user convenience. While many security systems rely on complex biometric or RFID solutions, this project explores a cost-effective approach using Arduino and SIM800L GSM module to implement a secure door lock system. This design aims to demonstrate a reliable method for dynamic access control, emphasizing simplicity and effectiveness in residential and commercial applications.

1.1 BACKGROUND AND HISTORY

Traditional lock-and-key mechanisms have been the standard for centuries, but they lack security against unauthorized duplication and physical breaches. The advent of electronic locks introduced keypad-based systems, which improved security but remained vulnerable to code theft and brute-force attacks.

The concept of OTP-based systems emerged to address these vulnerabilities by providing time-sensitive, unique passwords for each access attempt. Early implementations used standalone token generators, while modern systems leverage mobile networks for OTP delivery via SMS. The evolution of microcontroller platforms like Arduino and affordable GSM modules like SIM800L has made these systems accessible for DIY and small-scale implementations.

This project builds on these advancements by combining Arduino's programmability with the SIM800L's GSM capabilities to create a standalone OTP door lock system. Unlike cloudbased solutions, this approach operates independently, making it suitable for areas with limited internet connectivity while maintaining robust security through dynamically generated passwords.

1.2 OBJECTIVE

The primary objective is to design and implement an OTP-based door lock system using Arduino and SIM800L GSM module. Key goals include:

1. **System Design**: Develop a circuit integrating Arduino, SIM800L, 4×4 keypad, and relay to control a door lock.

2. **OTP Generation & Delivery**: Implement SMS-based OTP generation and transmission to registered mobile numbers.

3. **User Authentication**: Validate OTP entries via the keypad to grant or deny access.

4. **Prototyping**: Assemble and test a functional prototype using affordable, off-the-shelf components.

5. **Documentation**: Provide a comprehensive guide for replication, including circuit diagrams, code, and troubleshooting tips.

By achieving these objectives, the project demonstrates a scalable, low-cost alternative to commercial security systems.

1.3 MOTIVATION

This project is driven by several practical considerations that address real-world security challenges while offering valuable learning opportunities:

1. **Enhanced Security**: Traditional lock-and-key systems and static passwords are vulnerable to duplication and theft. By implementing one-time passwords that expire after use, we create a more robust authentication method that significantly reduces unauthorized access risks.

2. **Accessibility**: The system leverages existing mobile phone infrastructure, eliminating the need for expensive specialized hardware. This makes advanced security technology available to a wider range of users, from homeowners to small businesses.

3. **Cost-Effective Solution**: Using affordable, readily available components like Arduino and

GSM modules demonstrates how sophisticated security systems can be implemented without large budgets. This approach makes the technology accessible for various applications.

4. **Educational Value**: The project provides hands-on experience with embedded systems, wireless communication, and sensor integration - skills that are increasingly valuable in today's technology-driven world.

5. **Practical Applications**: The system addresses genuine security needs in residential, commercial, and institutional settings, offering a flexible solution that can be adapted to different environments and requirements.

1.4 RELEVANCE

This project maintains significant relevance in today's technological landscape for several important reasons:

1. **Growing Security Needs**: As security threats become more sophisticated, there is increasing demand for reliable access control systems that go beyond traditional mechanical locks.

2. **IoT Applications**: The system serves as a practical introduction to Internet of Things concepts, particularly in how everyday objects can be connected and controlled through network communication.

3. **Technology Transition**: It demonstrates how conventional security methods can be upgraded with modern electronic solutions using widely available components.

4. **Sustainable Design**: The low-power requirements make it suitable for deployment in areas with limited power infrastructure, with potential for solar or battery operation.

5. **Skill Development**: The project encompasses multiple technical disciplines including programming, circuit design, and system integration, making it an excellent learning platform for students and hobbyists.

6. **Current Trends**: With the shift toward contactless and remote solutions, the system aligns with modern preferences for secure, convenient access control methods.

This practical approach to security system development offers both immediate utility and long-

term educational value, while demonstrating how basic electronic components can be combined to create effective solutions for real-world problem.

CHAPTER 2

LITERATURE SURVEY

[1] P. Jadhav, S. Gaul, and A. Madhwai, "A Cutting-Edge Security Solution: OTPBased Smart Wireless Locking System," in Proceedings of the 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, Dec. 2023, pp. 1-5. doi: 10.1109/ICCAKM58659.2023.10449610.

This paper focuses on the implementation of an OTP-based authentication system for secure wireless access control. It explores real-time OTP generation, transmission, and verification to prevent unauthorized access. The authors emphasize encryption techniques that enhance OTP security, reducing risks of hacking and interception. Additionally, the study discusses GSM module reliability and signal optimization, ensuring efficient OTP delivery without delays. The paper also highlights hardware stability, addressing challenges like power fluctuations and network disruptions that could affect system performance. The findings provide valuable insights into enhancing security and reliability in smart locking systems using wireless authentication.

[2] S. Sobale, S. P. Shinde, and S. S. Shinde, "OTP Based Door Lock System with Mobile Application using Arduino UNO and ESP8266 Wi-Fi Module," in Proceedings of the 2022 International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kollam, India, Mar. 2022, pp. 1-5. doi: 10.1109/SPICES52834.2022.9777286.

This research integrates OTP-based authentication with IoT technology, allowing users to control door access via a mobile application and ESP8266 Wi-Fi module. The study explores real-time OTP verification and remote access control, enhancing security and convenience. The authors focus on wireless communication reliability, addressing network delays and signal disruptions. Additionally, the paper highlights the advantages of mobile app-based authentication, allowing users

to monitor and manage access from anywhere. By incorporating cloud-based data storage, the system improves security tracking and access history logging. This paper contributes to advancing automation and remote accessibility in modern smart locking mechanisms.

[3] A. Singh, A. K. Singh, P. Gupta, and V. Verma, "Smart OTP Based Wireless Locking System," International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 5, pp. 2741-2744, May 2022. doi: 10.22214/ijraset.2022.42938.

This paper emphasizes the hardware optimization of OTP-based smart locking systems, ensuring efficiency and stability. It discusses GSM module performance, highlighting methods to enhance signal strength and reduce OTP delivery delays. The study also explores power management techniques, preventing fluctuations that could disrupt system operation. The authors focus on relay-based control mechanisms, ensuring smooth locking and unlocking processes. Furthermore, the paper introduces automatic relocking and fail-safe measures, reducing the risk of unauthorized access. These contributions make the system more reliable, secure, and efficient, supporting its practical implementation in real-world security applications.

CHAPTER 3

METHODOLOGY AND CIRCUIT DIAGRAM

3.1 WORKING PRINCIPLE

The OTP-based wireless smart locking system enhances security by generating a unique onetime password (OTP) for door access. When an IR sensor detects a user at the door, the Arduino Uno triggers the GSM module to send an OTP via SMS to the registered mobile number. The user enters the OTP on the keypad, and the Arduino verifies it. If the OTP matches, the relay activates, unlocking the solenoid lock. If incorrect, access is denied. The LCD displays system status, and after a set time, the lock re-engages automatically. This system ensures secure, OTP-based authentication for controlled access.

1. **User Detection:**

The system remains in standby mode until the IR sensor detects motion near the door. Once movement is detected, the Arduino Uno activates the system, displaying a message on the LCD screen indicating that an OTP is being generated. This ensures that the system only operates when someone is present, conserving energy and preventing unnecessary OTP requests.

2. **OTP Generation & Transmission:**

After detecting a user, the Arduino generates a random OTP and sends it to the registered mobile number via the GSM module. This OTP serves as a unique, time-sensitive access code. The LCD screen notifies the user that the OTP has been sent, instructing them to check their SMS for further access.

3. **User OTP Input:**

Once the user receives the OTP on their phone, they must enter it using the keypad. The LCD screen prompts them to input the code, and the Arduino stores the entered value for verification. This step ensures that only authorized individuals with the correct OTP can proceed to unlock the door.

4. **OTP Verification:**

The Arduino compares the entered OTP with the generated one. If the codes match, the system grants access and moves to the unlocking process.

5. **Lock Control:**

Upon successful verification, the relay module activates, disengaging the solenoid lock and allowing the user to enter. The LCD displays a confirmation message, indicating that access has been granted. If the OTP is incorrect, the system denies access, keeping the door locked for security.

6. **Auto Reset & Re-Locking:**

After a short duration, the system automatically resets, re-engaging the solenoid lock to secure the door again. The LCD screen updates to indicate that the door is locked, ensuring that unauthorized access is prevented once the user has entered. The system then returns to standby mode, ready for the next authentication process.

3.2 CIRCUIT DIAGRAM

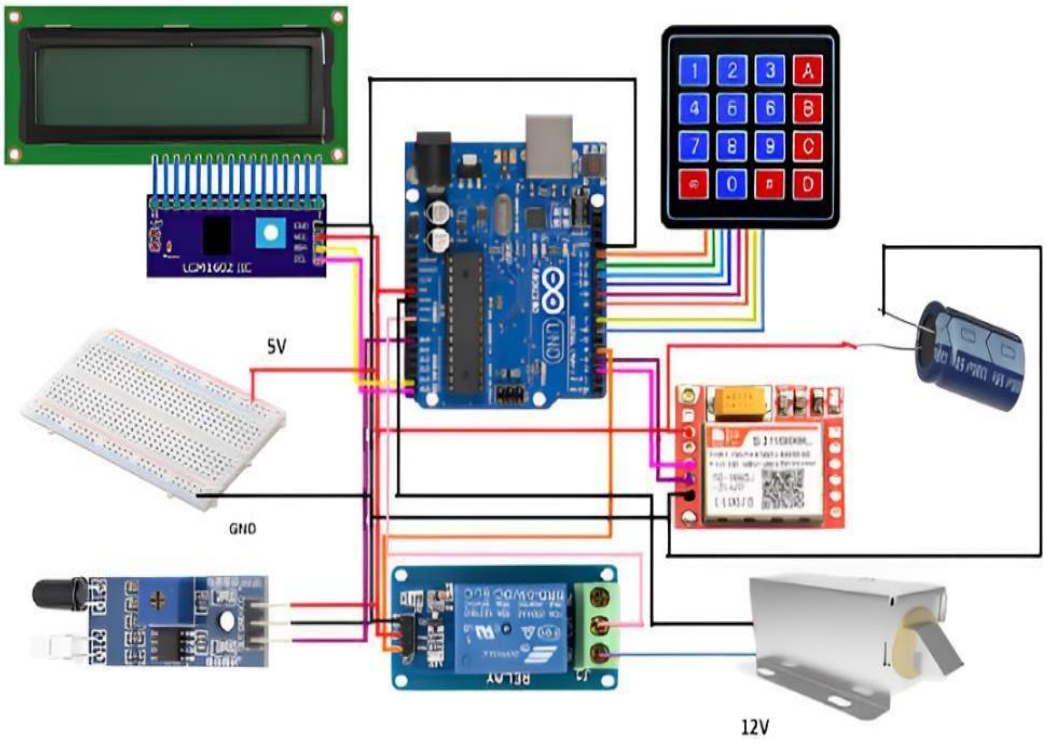

Fig 3.1 Circuit Diagram

CHAPTER 4

HARDWARE REQUIREMENTS

4.1 POWER SUPPLY

12V Adapter:

A 12V adapter is used to supply DC voltage to the Arduino Uno, ensuring stable operation for the connected components. The Arduino Uno has a built-in voltage regulator that steps down the 12V input to the required 5V for its internal circuits and connected peripherals. It provides sufficient current (at least 1A–2A) to handle all components.

Figure 4.1 12V Adapter

4.2 MICROCONTROLLER

Arduino UNO:

The Arduino Uno is a popular microcontroller board based on the ATmega328 chip. It acts as the brain of electronic projects, processing inputs from sensors and controlling connected components like displays, motors, and relays. It operates at 5V and has 14 digital I/O pins, 6 analog inputs, and supports communication via USB, UART, SPI, and I2C.

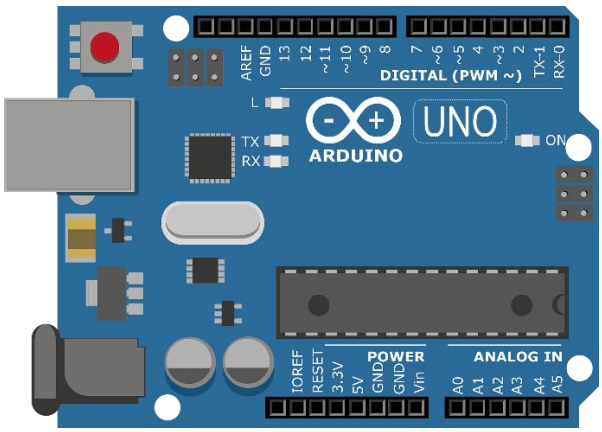

Figure 4.2 Arduino UNO

4.3 MOTION SENSING COMPONENT

IR Sensor:

It acts as a motion-sensing component to detect the presence of a person near the door. It works by emitting infrared light and measuring the reflection from nearby objects. When movement is detected, the Arduino Uno triggers the OTP generation process, activating the GSM module to send an OTP to the user's phone. This ensures that the system only operates when someone is present, enhancing security and power efficiency.

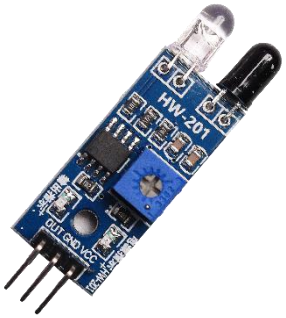

Figure 4.3 IR Sensor

4.4 PASSIVE COMPONENT

Capacitor:

A 3300µF capacitor is used to stabilize the power supply and reduce voltage fluctuations. When a high power component like the GSM module operates, sudden voltage drops occurs. The

capacitor helps by storing and releasing charge as needed, ensuring a steady voltage for the Arduino Uno and other components, preventing resets or malfunctions.

Figure 4.4 Capacitor

4.5 DISPLAY COMPONENT

16×2 LCD Display with I2C:

It is used to show system messages such as "Generating OTP," "Enter OTP," "Access Granted," and "Access Denied." It helps the user interact with the system by providing real-time feedback on OTP entry and door lock status. The I2C module allows easy connection to the Arduino Uno using only SDA and SCL pins, reducing wiring complexity while ensuring efficient communication.

Figure 4.5 16×2 LCD Display with I2C

4.6 WIRELESS COMMUNICATION MODULE

GSM SIM800L Module:

It is used for wireless communication, allowing the system to send the OTP via SMS to the registered mobile number. It connects to the Arduino Uno via serial communication (TX and RX pins) and operates on a SIM card with a mobile network. This ensures secure, remote authentication by verifying the user before unlocking the door.

Figure 4.6 GSM Sim800L Module

4.7 CIRCUIT ASSEMBLY COMPONENTS

Breadboard:

It is used as a prototyping tool to connect components like the IR sensor, keypad, LCD with I2C, GSM module, relay, and solenoid lock without soldering. It allows easy wiring and modification of connections, making testing and troubleshooting more efficient before finalizing the circuit.

Figure 4.7.1 Breadboard

Connecting Wires:

Used to establish electrical connections between different components in the circuit. They ensure proper signal transmission and power distribution, enabling smooth communication and operation of the system.

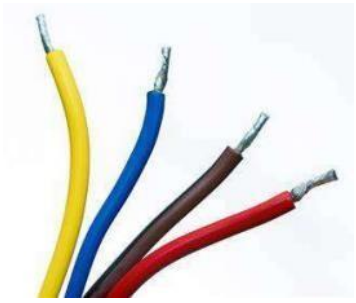

Figure 4.7.2 Connecting Wires

4.8 TOOLS AND TESTING EQUIPMENTS

Soldering Iron and Solder:

Tools used for soldering components onto a PCB or making permanent connections.

Figure 4.8.1 Soldering Iron and Solder

Wire Cutters and Strippers:

Tools used to cut and strip insulation from wires to appropriate lengths for connections. Facilitates neat and precise wiring, ensuring reliable electrical connections.

Figure 4.8.2 Wire Cutters and Strippers

Multimeter:

An electronic tool used to measure voltage, current, and resistance in electrical circuits. Essential for testing circuit parameters, diagnosing faults, and ensuring proper operation during assembly and troubleshooting phases.

Figure 4.8.3 Multimeter

CHAPTER 5
RESULTS

This project demonstrates successful and secure access control. When a person is detected by the IR sensor, the Arduino generates a unique OTP and sends it via SMS through the GSM module. Upon entering the correct OTP using the 4×4 keypad, the system verifies it and activates the relay module to unlock the solenoid lock, granting access. The LCD display provides clear status updates, such as "OTP Sent," "Enter OTP," and "Access Granted" or "Access Denied." If an incorrect OTP is entered multiple times, the system restricts access for security. The power stabilization using a 3300µF capacitor ensures smooth operation, preventing voltage drops. Overall, the system functions reliably, providing secure, automated, and wireless door access through OTP verification.

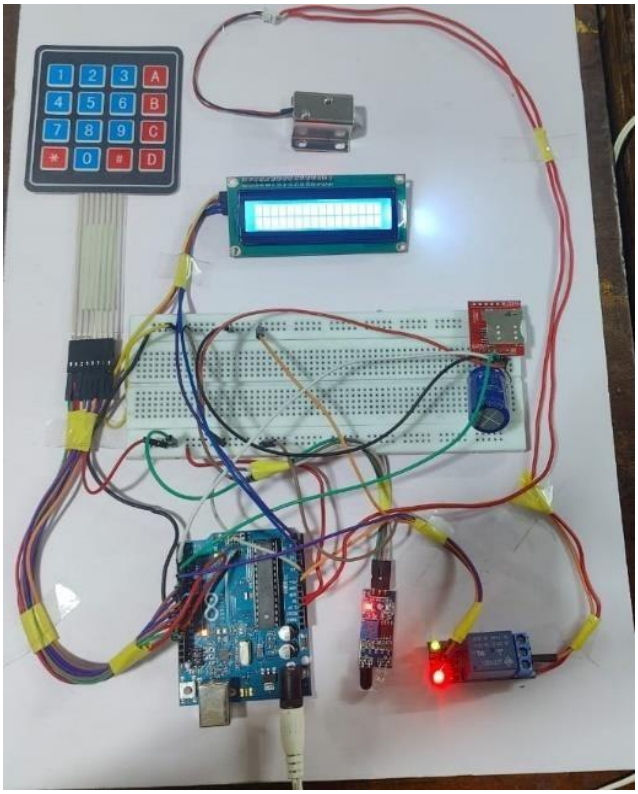

Figure 5.1 Prototype

5.1 OBSERVATIONS

1. The system effectively generates and sends a unique OTP via the GSM module (SIM800L) whenever motion is detected.

2. The 16×2 LCD with I2C provides clear status updates, ensuring ease of use.

3. When a correct OTP is entered, the relay module successfully activates the solenoid lock, allowing access.

4. After a delay, the system automatically re-locks the door, ensuring security.

5. The system effectively integrated multiple components to provide automated, userfriendly, and remote authentication, enhancing security.

FUTURE SCOPES

1. A mobile app can be developed to generate and verify OTPs, reducing network dependency and improving response time.

2. Adding a fingerprint sensor or facial recognition alongside OTP verification can enhance security by implementing multi-factor authentication.

3. Adding a camera module with AI-based human detection can enhance the by preventing unwanted generation of OTPs.

CHAPTER 6
CONCLUSION

The OTP-based wireless smart locking system successfully enhances security by allowing access only to authorized users through a one-time password (OTP) sent via GSM module. The integration of Arduino Uno, IR sensor, keypad, LCD display, relay, and solenoid lock ensures a fully automated and secure door-locking mechanism. The system effectively prevents unauthorized access, provides real-time user feedback, and ensures stable operation with proper power management. While minor challenges like network delays in OTP delivery were observed, the system overall met the intended objective of secure and efficient remote authentication.

Throughout the development and implementation of this project, several key outcomes have been achieved:

1. Secure Authentication: The system ensured that only authorized users could access the door through OTP-based verification.

2. Automated Motion Detection: The IR sensor successfully detected user presence, preventing unnecessary OTP generation.

3. Automated Motion Detection: The IR sensor successfully detected user presence, preventing unnecessary OTP generation.

4. Scalability for Future Enhancements: The system can be upgraded with biometric authentication, camera-based human detection, or mobile app integration for improved security.

REFERENCES

[1] P. Jadhav, S. Gaul, and A. Madhwai, "A Cutting-Edge Security Solution: OTP-Based Smart Wireless Locking System," in Proceedings of the 2023 4th International Conference on Computation, Automation and Knowledge Management (ICCAKM), Dubai, United Arab Emirates, Dec. 2023, pp. 1-5. doi: 10.1109/ICCAKM58659.2023.10449610.

[2] S. Sobale, S. P. Shinde, and S. S. Shinde, "OTP Based Door Lock System with Mobile Application using Arduino UNO and ESP8266 Wi-Fi Module," in Proceedings of the 2022 International Conference on Signal Processing, Informatics, Communication and Energy Systems (SPICES), Kollam, India, Mar. 2022, pp. 1-5. doi: 10.1109/SPICES52834.2022.9777286.

[3] A. Singh, A. K. Singh, P. Gupta, and V. Verma, "Smart OTP Based Wireless Locking System," International Journal for Research in Applied Science and Engineering Technology, vol. 10, no. 5, pp. 2741-2744, May 2022. doi: 10.22214/ijraset.2022.42938.

APPENDIX I

ARDUINO CODE

```
#include <SoftwareSerial.h>
#include <Wire.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
// Pin Definitions
#define relay 4
#define red 16
#define green 15
#define rxGSM 2
#define txGSM 3
int irsensor = A0;
// Keypad Setup
const byte ROWS = 4;
const byte COLS = 4;
char hexaKeys[ROWS][COLS] = {
{ '1', '2', '3', 'A' }, { '4', '5', '6', 'B' }, { '7', '8', '9', 'C' }, { '*', '0', '#', 'D' }
};
byte rowPins[ROWS] = { 13, 12, 11, 10 };
byte colPins[COLS] = { 9, 8, 7, 6 };
Keypad customKeypad = Keypad(makeKeymap(hexaKeys), rowPins, colPins, ROWS,
COLS);
LiquidCrystal_I2C lcd(0x27, 16, 2);
// SIM800L on SoftwareSerial (RX = 2, TX = 3)
SoftwareSerial sim800l(rxGSM, txGSM); // RX, TX
// OTP Storage
int otp;
String otpstring = "";
void setup() {
// Initialize IO
pinMode(relay, OUTPUT);
pinMode(red, OUTPUT);
pinMode(green, OUTPUT);
pinMode(irsensor, INPUT_PULLUP);
digitalWrite(relay, LOW); // Lock the door initially
digitalWrite(red, LOW); // Red LED OFF initially
digitalWrite(green, HIGH); // Green LED ON initially (Ready)
// Start serials
Serial.begin(9600);
sim800l.begin(4800);
// Initialize LCD
lcd.init();
lcd.backlight();
Serial.println("Welcome to SIM800L Project");
lcd.setCursor(0, 0);
lcd.print("System Ready");
// SIM800L Check
sim800l.println("AT");
```

```
updateSerial();
delay(500);
sim800l.println("AT+CSQ"); // Signal quality
updateSerial();
delay(500);
sim800l.println("AT+CMGF=1"); // Set SMS text mode
updateSerial();
}
void loop() {
lcd.setCursor(0, 0);
lcd.print(" OTP Based ");
lcd.setCursor(0, 1);
lcd.print(" Door Lock ");
// IR sensor triggered?
if (digitalRead(irsensor) == LOW) {
// Generate OTP
otp = random(2000, 9999);
otpstring = String(otp);
Serial.print("Generated OTP: ");
Serial.println(otpstring);
// Wait for sensor to go back to HIGH (object moved)
while (digitalRead(irsensor) == LOW);
// Notify user
lcd.clear();
lcd.setCursor(0, 0);
lcd.print(" OTP Sent to ");
lcd.setCursor(0, 1);
lcd.print(" Your Mobile ");
delay(500);
SendSMS(); // Send OTP via SMS
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Enter OTP :");
// Get user input from keypad
getotp();
}
}
// Function to read from keypad and verify OTP
void getotp() {
String enteredOTP = "";
lcd.setCursor(0, 1);
lcd.print("____"); // Display placeholders
while (enteredOTP.length() < 4) {
char customKey = customKeypad.getKey();
if (customKey) {
enteredOTP += customKey;
lcd.setCursor(enteredOTP.length() - 1, 1);
lcd.print(customKey);
}
}
Serial.print("Entered OTP: ");
Serial.println(enteredOTP);
// OTP validation
if (enteredOTP == otpstring) {
lcd.clear();
```

```
lcd.setCursor(0, 0);
lcd.print("Access Granted");
lcd.setCursor(0, 1);
lcd.print("Door Opening");
digitalWrite(relay, HIGH); // Unlock door
digitalWrite(red, HIGH); // Red LED ON
digitalWrite(green, LOW); // Green LED OFF
delay(5000); // Keep door open for 5 seconds
digitalWrite(relay, LOW); // Lock door again
digitalWrite(red, LOW); // Red LED OFF
digitalWrite(green, HIGH); // Green LED ON
} else {
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("Access Failed");
lcd.setCursor(0, 1);
lcd.print("Try Again!!!");
delay(3000);
}
}
// Function to send SMS with OTP
void SendSMS() {
Serial.println("Sending SMS...");
sim800l.println("AT+CMGF=1"); // SMS text mode
updateSerial();
delay(500);
sim800l.println("AT+CMGS=\"+917907134126\""); // Replace with your phone number
updateSerial();
delay(500);
sim800l.print("Your OTP is " + otpstring + ". Type OTP to unlock the door.");
delay(500);
sim800l.write(26); // CTRL+Z to send SMS
updateSerial();
Serial.println("Text Sent.");
lcd.clear();
lcd.setCursor(0, 0);
lcd.print("OTP Sent!");
}
// Function to sync serial comms between PC and SIM800L
void updateSerial() {
delay(500);
while (Serial.available()) {
sim800l.write(Serial.read());
}
while (sim800l.available()) {
Serial.write(sim800l.read());
}
}
```

APPENDIX II

LIST OF COMPONENTS

Sl.No	COMPONENTS	COST	QUANTITY
1	Arduino Uno	RS 300	1
2	16x2 LCD Display with I2C	RS 100	1
3	4x4 Keypad	RS 50	1
4	Sim8001 GSM Module	RS 190	1
5	5V Relay Module	RS 50	1
6	IR Sensor	RS 30	1
7	12V Adapter	RS 80	1
8	Solenoid Lock	RS 100	1
9	Connecting Wires	RS 100	10
10	Breadboard	RS 40	1
TOTAL		**RS 1040**	