IoT-POWERED OTP-BASED VAULT SECURITY SYSTEM

ABSTRACT

This project presents a secure, automated door access system utilizing a one-time password (OTP) delivered via SMS, designed to enhance security and user convenience. The system integrates motion detection, real-time OTP generation, wireless communication, and mechanical actuation to create a robust access control mechanism. A passive infrared (PIR) sensor initiates the process by detecting motion near the door, triggering the ESP32 microcontroller to generate a randomized 6-digit OTP.

Instead of using a GSM module, the ESP32 communicates with the Twilio API over Wi-Fi to send the OTP directly to the user's registered mobile number via SMS, ensuring prompt delivery to the default SMS inbox for immediate accessibility.

Users input the received OTP through a 4x4 matrix keypad, after which the ESP32 validates the code. Successful verification activates a servo motor to unlock the door (90° rotation) and updates an LCD display to "Access Granted." Invalid attempts retain the door locked and display "Access Denied." Throughout the workflow, the LCD provides real-time status updates, including "Motion Detected," "Sending OTP…," and "Enter OTP," ensuring user transparency.

By combining hardware components (PIR, ESP32, servo, keypad, LCD) with software logic for OTP generation, Twilio API integration, and code validation, the system prioritizes security against unauthorized access while maintaining user-friendly interaction. The project demonstrates practical applications in residential, commercial, or restricted environments, offering a cost-effective and scalable solution for modern access control. Testing confirms reliable operation, emphasizing its effectiveness in balancing security protocols with seamless user experience.

TABLE OF CONTENT

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In an era where security breaches and unauthorized access pose significant threats to residential, commercial, and institutional spaces, the demand for robust and intelligent access control systems has surged. Traditional security mechanisms, such as physical keys, numeric keypads, or RFID cards, are increasingly vulnerable to theft, duplication, or brute-force attacks. To address these limitations, modern systems are shifting toward dynamic authentication methods, such as one-time passwords (OTPs), which provide enhanced security through time-sensitive, non-replicable credentials.

This project introduces an innovative, IoT-enabled door access system that integrates motion detection, real-time OTP generation, and SMS-based communication to deliver a secure, user-friendly, and automated solution.

The core objective of this project is to design a system that eliminates static passwords or physical keys by leveraging ephemeral OTPs sent directly to the user's mobile device. When motion is detected near the door via a passive infrared (PIR) sensor, the system triggers an ESP32 microcontroller to generate a randomized 6-digit OTP. Instead of using a GSM module, the ESP32 utilizes Wi-Fi connectivity to communicate with the Twilio API, which securely delivers the OTP to the user's registered phone number via SMS, ensuring reliable and instant delivery.

The user then inputs the OTP using a 4x4 matrix keypad, and the ESP32 validates the code to grant or deny access. Successful authentication activates a servo motor to unlock the door, while an LCD display provides real-time feedback throughout the process, such as "Motion Detected," "Sending OTP…," "Enter OTP," "Access Granted," or "Access Denied."

This system addresses two critical challenges in modern access control:

- **Security:** By employing dynamically generated OTPs valid for a single use, the system mitigates risks associated with stolen or guessed credentials.
- **Convenience:** Users receive OTPs directly on their phones via Twilio's reliable SMS service, eliminating the need to carry additional hardware (e.g., keys or cards) and enabling remote access management.

The project combines hardware components, including the ESP32 (for processing), PIR sensor (motion detection), servo motor (door actuation), keypad (user input), and LCD (status updates)—with software logic for OTP generation, validation, and seamless integration with the Twilio API for SMS delivery.

This results in a cost-effective, scalable solution suitable for a variety of environments, offering enhanced protection without compromising on user convenience. Testing has confirmed the system's effectiveness, demonstrating its reliability in balancing stringent security protocols with smooth user experience.

RATIONALE OF THE STUDY

Traditional door access systems relying on physical keys, static codes, or RFID cards are increasingly vulnerable to theft, duplication, and brute-force attacks, compromising security in residential and commercial spaces. While some solutions utilize offline methods, they often lack dynamic authentication. In contrast, this project proposes a motion-activated, IoT-based OTP system that integrates cost-effective components to enhance security, accessibility, and user convenience.

By employing a PIR sensor to detect motion, the system proactively triggers the ESP32 microcontroller to generate a time-sensitive, 6-digit OTP. Leveraging Wi-Fi connectivity and the Twilio API, the ESP32 transmits this OTP directly to the user's mobile number via SMS, ensuring prompt delivery to their inbox for immediate access. This approach provides a secure, single-use credential resistant to replication, enhancing security without requiring dedicated GSM hardware.

The use of a 4x4 keypad and real-time LCD feedback simplifies user interaction, catering to individuals across technical proficiencies, while the servo-based locking mechanism ensures robust physical security. Unlike expensive biometric systems, this solution leverages affordable, widely available hardware, making it scalable for homes, small businesses, or environments where simple, effective access control is needed.

By merging motion detection, cloud-based SMS communication, and microcontroller automation, the project bridges the gap between dynamic security protocols and practical usability. It offers a resilient, low-cost alternative to conventional systems, emphasizing proactive security and user-centric design. Its focus on real-time operation, seamless interaction, and scalable architecture underscores its relevance in advancing modern access control solutions.

OBJECTIVE(S) OF THE STUDY

This study aims to design, implement, and evaluate a motion-triggered, SMS-based OTP door access system that enhances security, accessibility, and user convenience through IoT-enabled automation. The objectives are structured to address the technical, functional, and practical aspects of the system:

- **Design a Secure Authentication System:** Replace static credentials (physical keys, fixed codes) with time-sensitive, randomly generated 6-digit OTPs to mitigate risks of theft, duplication, or brute-force attacks.
- **Integrate Motion Detection for Proactive Security:** Utilize a PIR sensor to detect human presence near the door, triggering OTP generation only when motion is sensed. This approach reduces power consumption and minimizes false activations.
- **Implement SMS Delivery via Twilio API:** Use the ESP32's Wi-Fi capabilities to send OTPs to the user's mobile phone through the Twilio API, ensuring fast and reliable delivery directly to the SMS inbox.

- **Develop a User-Friendly Interface:** Provide real-time feedback through an LCD display (e.g., “Motion Detected,” “Sending OTP…,” “Access Granted/Denied”) and simplify OTP input using a 4x4 matrix keypad to enhance ease of use.
- **Automate Door Locking/Unlocking:** Control a servo motor to physically lock or unlock the door (90° rotation) based on OTP verification results, ensuring both electronic and physical security.
- **Validate System Reliability:** Test the system under various conditions (such as network latency, incorrect OTP entries, and multiple access attempts) to ensure consistent, dependable performance.
- **Optimize Cost and Scalability:** Employ low-cost, widely available components (ESP32, PIR sensor, servo motor) and cloud-based services to develop an affordable, scalable solution suitable for homes, offices, or rural installations.
- **Enhance Security Protocols:** Ensure OTPs are single-use and expire immediately after use or within a predefined short time frame to prevent unauthorized access.
- **Demonstrate IoT Integration:** Showcase practical IoT implementation by integrating cloud-based communication (Twilio), microcontroller logic (ESP32), and electromechanical actuation (servo motor) in a cohesive system.
- **Evaluate User Experience:** Assess the system’s intuitiveness and responsiveness through user testing, focusing on ease of OTP reception, input, and overall interaction flow.

CHAPTER 2

LITERATURE REVIEW

The rise of the Internet of Things (IoT) has revolutionized smart home security systems, offering users automated control and remote access for enhanced safety and convenience. This study focuses on designing a smart door lock system utilizing an ESP32 microcontroller, PIR sensor, keypad, LCD, and Twilio API to send a One-Time Password (OTP) directly to the registered user’s mobile phone via SMS. By leveraging real-time OTP generation and cloud-based SMS delivery, the system significantly enhances security and reliability, providing a robust, user-friendly solution for modern access control.

Book / Journal Name	Author(s)	Year of Publishing	Summary
Internet of Things: A Hands-On-Approach	Arshdeep Bahga, Vijay Madisetti	2014	Explain microcontroller integration in IoT systems. Helps understand ESP32 role in smart automation.

Book / Journal Name	Author(s)	Year of Publishing	Summary
Getting Started with the Internet of Things	Fei Hu	2016	Discusses OTP mechanisms and secure communications for access control in IoT environments.
Wireless Communications: Principles and Practice	Theodore S. Rappaport	2014	Core concepts of GSM networks. Supports understanding of SMS-based OTP delivery system.
Fundamentals of Mobile and Pervasive Computing	Adelstein et al.	2005	GSM, GPRS communication are essentials. Useful for configuring GSM modules for SMS transmission.
Practical Internet of Things Security	Brian Russell, Drew Van Duren	2016	Focuses on securing IoT devices and networks. Applicable for securing OTP generation and transmission.
Digital Communication Systems	Simon Haykin	2013	Covers modulation techniques and data transmission, relevant for reliable GSM communication.
Designing Embedded Systems with PIC Microcontrollers	Tim Wilmshurst	2010	Practical guide on designing embedded systems, useful for ESP32 and sensor integration.
Advanced Home Automation	IEEE IoT Journal	2018	Discusses automation technologies for smart homes, highlights OTP-based door locking mechanisms.
PIR Sensors for Smart Security	Texas Instruments	2017	Explains PIR sensor working and sensitivity adjustments, supporting accurate motion detection.

Researchers and industry experts have explored diverse methods of integrating IoT devices with security systems to enhance both functionality and resilience. Bahga and Madisetti (2014) explain the fundamentals of IoT hardware, providing essential knowledge for understanding the role of ESP32 microcontrollers in embedded systems [1]. Similarly, Pfister (2011) offers practical insights into IoT project development, with an emphasis on microcontroller and sensor interfacing, closely paralleling the integration of the ESP32 and PIR sensors in this project [2].

In terms of security, Hu (2016) highlights critical IoT security practices, notably the use of OTPs for secure communication, aligning directly with this project's focus on dynamic, time-sensitive authentication [3]. Russell and Van Duren (2016) further examine vulnerabilities inherent to IoT devices, underlining the necessity of secure communication protocols. This supports the project's use of trusted cloud communication services like Twilio for encrypted, reliable OTP delivery [6].

The role of cloud-based SMS platforms is well-documented. Twilio, in particular, has emerged as a leading communication API platform that enables secure and scalable message delivery across diverse networks. Adelstein et al. (2005) and Rappaport (2014) discuss the evolution of wireless communication frameworks, providing context for Twilio's utilization of global telecommunication infrastructure to ensure robust OTP transmission [4][7]. Haykin (2013) elaborates on digital communication principles, which are fundamental to understanding cloud-to-device SMS workflows [5].

Motion detection remains a critical component of this system. A technical report by Texas Instruments (2017) thoroughly examines PIR sensor operation and sensitivity adjustment, contributing valuable insights for optimizing the system's motion-triggered OTP generation [10].

Lastly, the IEEE IoT Journal (2018) discusses the integration of sensors and wireless communication in automation systems, reinforcing the viability of combining motion detection with Twilio-based OTP delivery for real-time smart security applications [9].

While prior studies have largely relied on cloud services like Firebase or third-party APIs (e.g., Fast2SMS), this project distinguishes itself by leveraging Twilio's robust global network for SMS delivery. This approach enhances message reliability and security while simplifying system integration through Twilio's API-driven architecture. Furthermore, by combining low-cost hardware with cloud-based messaging, the solution remains scalable and adaptable to homes, offices, and remote locations, provided there is basic internet connectivity.

CHAPTER 3

EXISTING METHODOLOGY

Lee, S., et al. (2020) in their study IoT-Based Smart Home Security Systems using Wi-Fi Connectivity developed a system that integrates motion sensors with Wi-Fi modules to enable real-time monitoring and communication with cloud databases. This allowed homeowners to remotely access data and receive alerts about potential intrusions. The prototype demonstrated effective

remote monitoring capabilities but revealed a significant dependency on continuous internet connectivity, which limits its reliability in remote areas or environments with congested networks. [11]

Wang, X., et al. (2021) explored a Cloud-Enabled OTP Verification System for IoT Devices, wherein OTPs are generated in the cloud and transmitted to registered devices over the internet for verification. This centralized approach ensured efficient OTP management and flexible device integration. However, during prototype testing, it was observed that the system suffered from noticeable delays during peak cloud traffic, and concerns were raised regarding data privacy and potential security breaches within cloud environments. [12]

Patil, A. V., et al. (2018) designed a system titled Firebase Cloud Messaging for Real-Time Home Security Alerts that employed motion sensors to detect intrusions, which then triggered real-time alerts sent via Firebase Cloud Messaging to users' smartphones. While the methodology enabled prompt notification delivery under optimal conditions, prototype findings indicated that the system was heavily reliant on active internet connections and required the app to be running in the background. Notifications were delayed or even missed if these conditions were not met. [13]

Sharma, P., et al. (2021) presented an Email-Based Intrusion Detection Alert System that utilized PIR sensors integrated with microcontrollers to send alerts via email using SMTP protocols when unauthorized movement was detected. The prototype confirmed the practicality of email notifications for intrusion alerts; however, findings indicated that delays were common due to email server uptime dependencies. Additionally, critical alerts could go unnoticed if users failed to check their emails promptly. [14]

Das, M., et al. (2020) developed a GSM-Based Home Security System which integrated PIR sensors with GSM modules to dispatch SMS alerts immediately upon detecting motion. The prototype testing demonstrated that GSM provided a reliable communication channel, especially in rural areas with limited or no internet access. This ensured timely delivery of alerts, although the system’s simplicity did not include advanced features like access verification or data encryption. [15]

Hernandez, L., et al. (2020) in their research on Secure SMS Communication in IoT Applications designed a system to ensure secure SMS-based communication for IoT security alerts. Their prototype employed encryption protocols over GSM networks to protect data integrity. Testing validated the reliability of SMS even in poor network areas, although the system faced constraints in data bandwidth and lacked multi-factor authentication mechanisms. [16]

Thomas, S., et al. (2019) conducted a Comparative Study of GSM and Wi-Fi Based Home Security Systems, developing prototype models for both communication types. Findings from the prototypes showed that GSM-based systems offered better reliability in rural environments, while Wi-Fi systems delivered faster notifications in urban settings but were prone to network outages and congestion. [17]

Mehta, A., et al. (2020) proposed Microcontroller-Based OTP Generation and Alert Systems for Home Security, where OTPs were generated locally using microcontrollers and sent via GSM modules. Prototype evaluations revealed reduced reliance on cloud infrastructure, ensuring faster OTP delivery and better security control. However, the system's hardware-based approach limited scalability and flexibility. [18]

Khan, F., et al. (2019) worked on Integration of IoT and GSM for Secure Communication Systems, combining sensor networks with GSM modules to transmit alerts and data securely. Prototype testing highlighted the system's robustness in low-connectivity regions, though it lacked integration with smart authentication methods and advanced cloud analytics for comprehensive threat detection. [19]

Patel, K., et al. (2021) developed Advanced Security Measures for Home Automation Systems focusing on layered security strategies including sensor integration, GSM-based alerts, and backup power supplies. Prototype results confirmed enhanced system reliability during power outages and network failures, but the complexity of hardware integration raised concerns about maintenance and initial setup costs. [20]

CHAPTER 4

PROBLEM IDENTIFICATION

IoT-Based Smart Home Security Systems using Wi-Fi Connectivity by S. Lee, J. Kim, H. Park (2020) primarily relies on Wi-Fi networks for communication between devices and the user. This heavy dependence on Wi-Fi creates vulnerabilities, especially in situations of network failure or poor signal strength, rendering the system ineffective during critical moments. Additionally, Wi-Fi networks are susceptible to hacking, raising concerns about system security and data breaches.[11]

Cloud-Enabled OTP Verification System for IoT Devices by X. Wang, L. Zhang, M. Chen (2021) utilizes cloud servers to generate and verify OTPs, which introduces latency due to dependency on internet connectivity. Moreover, cloud-based systems often pose risks related to data privacy and potential server downtimes, which can hinder timely OTP delivery and verification, compromising the effectiveness of security mechanisms.[12]

Firebase Cloud Messaging for Real-Time Home Security Alerts by A. V. Patil, R. Deshmukh, S. Kulkarni (2018) depends heavily on Firebase's cloud messaging services. However, this reliance on third-party services raises concerns about service availability and data privacy. In the event of Firebase service outages or connectivity issues, critical alerts may be delayed or completely undelivered, undermining the system's reliability.[13]

Email-Based Intrusion Detection Alert System by P. Sharma, N. Gupta, V. Singh (2021) uses email as the primary alert mechanism, which, while informative, often results in delayed

notifications. Email alerts can be filtered into spam folders or overlooked by users, reducing the urgency and effectiveness of the alert system in responding to real-time threats.[14]

GSM-Based Home Security System: Design and Implementation by M. Das, A. Sarkar, P. Roy (2020) focuses on GSM-based alert systems, which provide basic SMS notifications. However, these systems lack integration with modern IoT platforms and do not offer advanced features like real-time remote monitoring or dynamic control, limiting their usability in comprehensive smart home environments.[15]

Secure SMS Communication in IoT Applications by L. Hernandez, F. Garcia, R. Lopez (2020) emphasizes the use of SMS for secure communication. Despite SMS being a reliable medium, it suffers from limited data capacity and potential delays in message delivery. Additionally, the lack of encryption in standard SMS protocols exposes the system to interception and security breaches.[16]

Comparative Study of GSM and Wi-Fi Based Home Security Systems by S. Thomas, K. Varghese (2019) highlights the pros and cons of GSM and Wi-Fi systems individually. However, the study identifies a significant drawback in relying solely on either GSM or Wi-Fi does not provide a balanced solution. Each has limitations in either coverage, data speed, or reliability, pointing to the need for a hybrid approach.[17]

Microcontroller-Based OTP Generation and Alert Systems for Home Security by A. Mehta, P. Bansal (2020) describes the use of microcontrollers for local OTP generation. While this enhances security, the system lacks a robust communication channel to effectively deliver alerts to users, reducing the real-time responsiveness essential in-home security scenarios.[18]

Integration of IoT and GSM for Secure Communication Systems by F. Khan, R. Verma, D. Chawla (2019) integrates IoT with GSM for secure communication but falls short in providing scalability and flexible integration with emerging technologies. The system's architecture limits expansion and integration with additional smart devices, constraining its adaptability in evolving smart home ecosystems.[19]

Advanced Security Measures for Home Automation Systems by K. Patel, S. Iyer, M. Choudhury (2021) discusses advanced security strategies but focuses heavily on complex implementations that increase system cost and complexity. This makes the solution less practical for average consumers seeking an affordable yet reliable home security system.[20]

CHAPTER 5

PROPOSED METHODOLOGY

Considering the significant limitations observed in existing home security solutions, the proposed methodology aims to deliver a comprehensive, resilient, and intelligent security framework tailored for smart environments. This system harnesses the power of IoT-enabled sensors, combined with a

hybrid communication strategy that intelligently merges Twilio API, Wi-Fi, and cloud-based messaging services to ensure uninterrupted, real-time alerts and system control. By integrating microcontroller-based processing at the edge, the system achieves rapid response times and autonomous decision-making, significantly reducing latency and dependency on cloud infrastructure. Moreover, advanced features such as dynamic OTP verification, secure SMS communications, and multi-channel notification protocols bolster system reliability, even under adverse network conditions. The layered security architecture is further enhanced with encryption mechanisms and fail-safe operations, effectively mitigating risks associated with data breaches, connectivity failures, and delayed alerts. Collectively, this methodology not only overcomes the drawbacks of prior research models but also establishes a future-ready solution that delivers superior operational efficiency, robust protection, and user-centric flexibility for smart home security.

5.1 SPECIFICATIONS AND COMPONENTS:

PIR Sensor:

Figure 1 – PIR Sensor

A Passive Infrared (PIR) sensor is a crucial component in the proposed security system, as it detects motion by sensing infrared radiation emitted by objects in its vicinity. When the PIR sensor identifies movement, it sends a signal to the Arduino, which then activates both the LED and the buzzer to provide immediate visual and auditory alerts. This sensor operates within a typical range of 5 to 12 meters and is compatible with the Arduino's 3.3V to 5V operating voltage, making it ideal for small-scale, low-power applications. The PIR sensor's rapid response time and wide field of view ensure effective real-time detection, making it well-suited for basic security setups.

ESP 32:

Figure 2 – ESP 32

The ESP32 is a highly versatile and powerful microcontroller, ideal for IoT-based smart home security systems due to its advanced processing capabilities and rich set of integrated features. Equipped with a dual-core Tensilica LX6 processor, built-in Wi-Fi, and Bluetooth connectivity, the ESP32 enables seamless wireless communication and real-time data processing directly at the edge, significantly reducing latency and reliance on external servers. Its multiple GPIO pins allow easy integration with various sensors such as PIR motion detectors, cameras, and alarm modules, making it a central hub for smart security operations. Additionally, the ESP32 supports secure communication protocols, OTA (Over-the-Air) updates, and energy-efficient modes, ensuring the system remains up-to-date and power-conscious for continuous monitoring. With a compact design and robust security features, the ESP32 serves as the backbone of the proposed system, providing reliable performance and flexibility for both local processing and cloud-based alert mechanisms.

Bread Board:

Figure 3 – Bread Board

A breadboard is an essential tool for prototyping electronic circuits without the need for soldering. It features a grid of interconnected sockets where components like resistors, LEDs, and microcontrollers can be inserted and easily rearranged. The breadboard's layout typically includes horizontal and vertical rows of sockets connected internally, with power rails running along the sides for easy power distribution. This design allows for quick, flexible testing and modification of circuits, making breadboards ideal for experimenting with and refining circuit designs, particularly in educational settings or in initial project stages where frequent changes are expected.

4 X 4 Keypad:

Figure 4 – 4X4 Keypad

The 4x4 keypad is a compact and user-friendly input device that plays a crucial role in the proposed smart security system by enabling manual user interactions, such as entering OTPs (One-Time Passwords) or security codes. Comprising 16 tactile switches arranged in a matrix of 4 rows and 4 columns, the keypad offers multiple input combinations while occupying minimal space. Its simple interface allows for easy integration with the ESP32 microcontroller, requiring only a few GPIO pins to detect key presses accurately. The keypad's durable design ensures reliability for frequent use in security applications, providing users with a quick and efficient method to authenticate or disarm the system. Moreover, its cost-effectiveness and ease of programming make it an ideal component for enhancing the user control aspect of the system, ensuring that only authorized individuals can interact with and manage the home security functions.

LCD Display with I2C Module:

Figure 5 – LCD Display with I2C Module

A piezo, or piezoelectric buzzer, is a device that produces sound through the piezoelectric effect, where certain materials generate an electric charge when mechanically stressed. In a piezo buzzer, a small ceramic disc made of piezoelectric material is attached to a metal plate. When an electric current is applied, the disc vibrates rapidly, causing the metal plate to produce sound. Piezo buzzers are compact, energy-efficient, and capable of generating various tones by adjusting the input frequency, making them popular in applications such as alarms, timers, and electronic indicators. They are easy to integrate into circuits and commonly used for providing auditory feedback in electronics projects, including security and alert systems.

Servo Motor:

Figure 7 – Servo Motor

The servo motor is a crucial actuator in the proposed security system, primarily responsible for mechanical movements such as locking and unlocking mechanisms in response to authentication signals. Known for its precision and controlled angular motion, the servo motor operates based on Pulse Width Modulation (PWM) signals received from the ESP32 microcontroller. This enables the system to accurately position the motor shaft at desired angles, ensuring reliable physical security actions like door locking. Compact in size yet powerful in operation, the servo motor consumes minimal power while delivering swift and accurate responses. Its closed-loop control system continuously adjusts the position based on feedback, which enhances the reliability of the locking mechanism. With fast response time and easy integration, the servo motor significantly improves the automation aspect of the prototype, offering an additional physical layer of protection to complement electronic alerts.

5.2 SOFTWARES USED:

ARDUINO IDE:

The Arduino IDE (Integrated Development Environment) is a software platform used to write, compile, and upload code to Arduino microcontrollers. It provides an easy-to-use environment, making it accessible for beginners and professionals alike. The primary language used in the IDE is C/C++, but the environment simplifies the code structure with pre-built libraries, making it less complex for users to interact with hardware components. The platform is cross-platform, and also supports a wide range of boards beyond the traditional Arduino Uno, allowing users to explore various microcontroller options.

TWILIO API:

Twilio is a leading cloud communication platform that offers developers APIs to embed various communication capabilities such as SMS, voice, video, and messaging directly into their applications. Twilio provides a scalable and reliable infrastructure that connects to telecom networks worldwide, allowing seamless communication between IoT devices and end-users. In the context of this project, Twilio is primarily utilized to deliver One-Time Passwords (OTPs) securely and instantly to the user's registered mobile number via SMS.

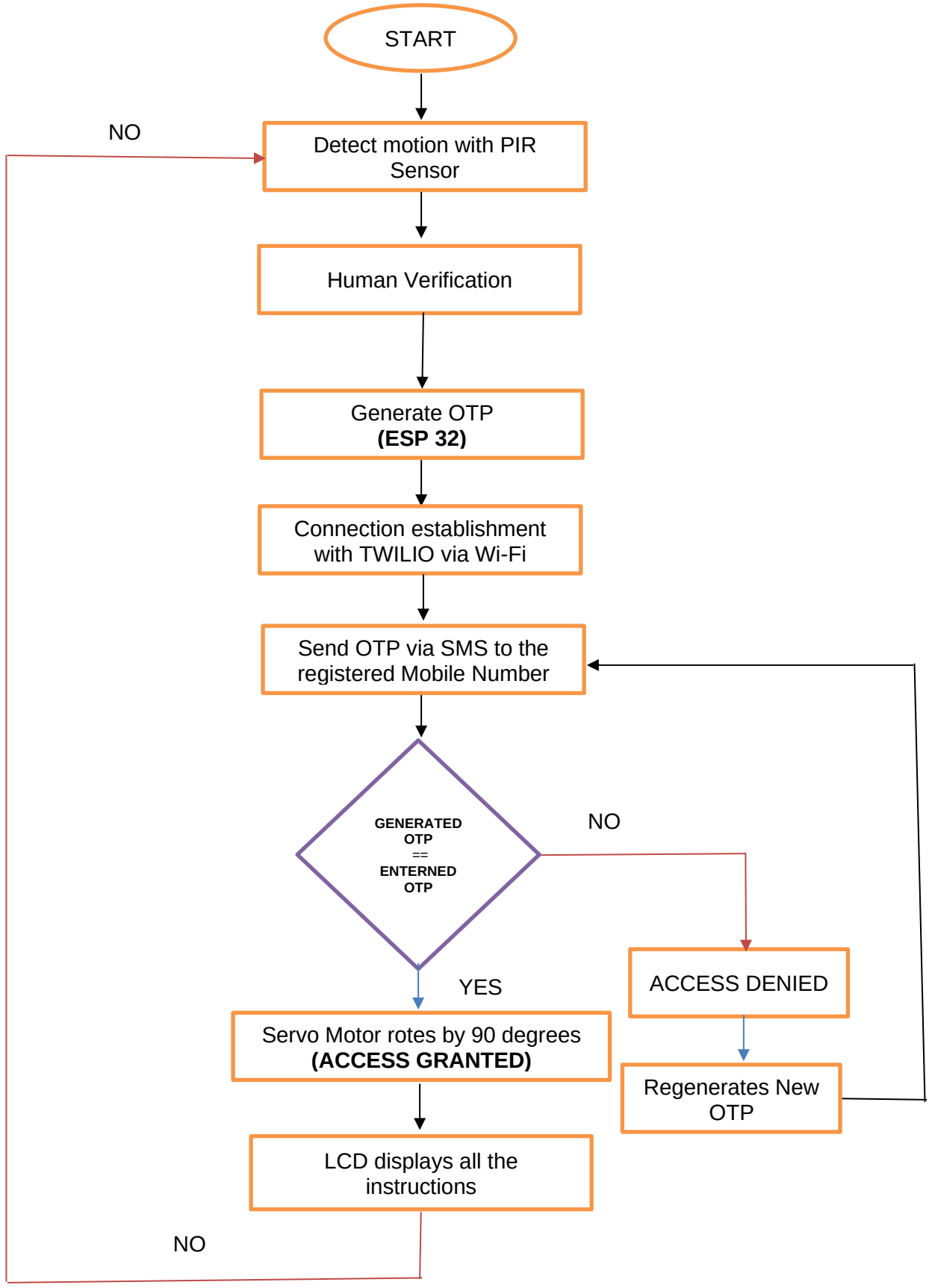
The integration of Twilio into the smart door lock system eliminates the need for traditional GSM modules and simplifies the hardware design. Unlike GSM modules that require SIM cards and dedicated hardware, Twilio operates over the internet, leveraging its cloud services to manage message queues and ensure delivery confirmation. This enhances the efficiency and reliability of the communication system, especially in urban areas with stable internet connectivity

Furthermore, Twilio offers advanced features such as message tracking, delivery status monitoring, and automated retries, which contribute to a more robust and user-friendly security solution. By using Twilio, the system benefits from secure data handling and compliance with

industry standards, ensuring that sensitive information like OTPs is transmitted safely.

Overall, Twilio serves as a critical software component in the project, enabling fast, secure, and scalable OTP delivery without the complexities of maintaining physical communication hardware. Its cloud-based nature supports future scalability and makes the system more adaptable for broader IoT applications.

5.3 FLOWCHART:



5.4 WORKING PRINCIPLE:

The proposed smart home security system is designed to enhance household safety by integrating multiple technologies such as IoT, cloud-based SMS communication via Twilio API, keypad authentication, and motion detection. The core of the system operates using the ESP32 microcontroller, which serves as the central control unit to manage all inputs and outputs efficiently.

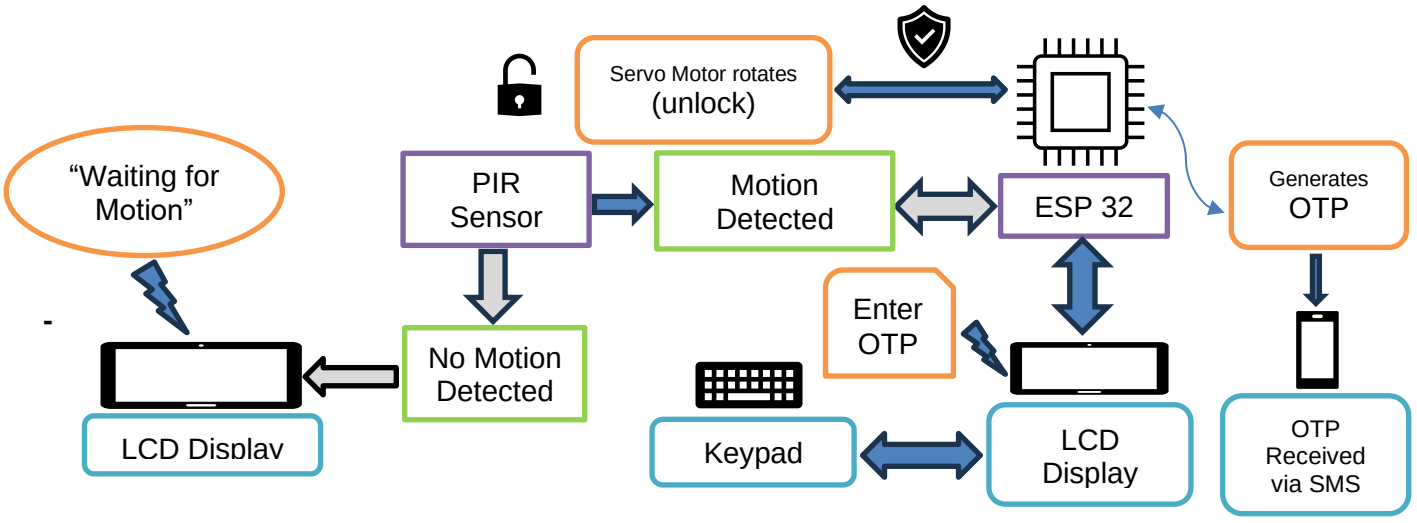


Figure 8 – Block Diagram

The proposed smart home security system is designed to enhance household safety by integrating multiple technologies such as IoT, cloud-based SMS communication via Twilio API, keypad authentication, and motion detection. The core of the system operates using the ESP32 microcontroller, which serves as the central control unit to manage all inputs and outputs efficiently.

When the PIR motion sensor detects any movement near the entrance, it triggers the system to initiate the security protocol. Upon detection, the ESP32 generates a One-Time Password (OTP), which is transmitted to the registered mobile number using the Twilio API. Twilio enables reliable and fast communication over the cloud, allowing SMS alerts to be sent instantly without relying on physical GSM modules or local SIM cards. This ensures the user is promptly alerted, as long as there is internet connectivity available for the ESP32 to access Twilio services.

The user is then required to enter the received OTP through the connected 4x4 keypad. The keypad acts as the user interface for authentication. To confirm the OTP, the user inputs the four digits followed by the '#' key, which functions as the "Enter" command. The entered OTP is verified against the system's stored OTP.

If the OTP entered is correct, the system grants access by activating the servo motor to unlock the door. However, if the OTP is incorrect, the system prompts the user on the LCD display, asking whether they would like to regenerate the OTP. If the user presses the '#' key again, a new OTP is generated and sent through Twilio via SMS. If no action is taken, the system returns to its initial state, displaying "Waiting for Motion" and monitoring the surroundings for any new activity.

5.5 Code for the Study:

```
#include <WiFi.h>
#include <WiFiClientSecure.h>
#include <LiquidCrystal_I2C.h>
#include <Keypad.h>
#include <ESP32Servo.h>
#include <base64.h>
// WiFi credentials
const char* ssid = "XXXXXXXXXXXXXXXXX";
const char* password = "YYYYYYYYYYYYYY";
// Twilio credentials
const char* account_sid = "AC****************************";
const char* auth_token = "**************************************";
const char* from_number = "+1XXXXXXXXX";
const char* to_number = "+91YYYYYYYYYY";
// LCD and PIR
LiquidCrystal_I2C lcd(0x27, 16, 2);
#define PIR_SENSOR_PIN 4
// Servo
Servo doorServo;
#define SERVO_PIN 19
// Keypad
const byte ROWS = 4;
const byte COLS = 4;
char keys[ROWS][COLS] = {
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};
byte rowPins[ROWS] = {13, 12, 14, 27};
byte colPins[COLS] = {26, 25, 33, 32};
Keypad keypad = Keypad(makeKeymap(keys), rowPins, colPins, ROWS, COLS);
// Flags & buffers
bool motionDetected = false;
bool otpSent = false;
String generatedOTP = "";
String userOTP = "";
```

```
void setup() {
  Serial.begin(115200);
  lcd.init();
  lcd.backlight();
  pinMode(PIR_SENSOR_PIN, INPUT);
  doorServo.attach(SERVO_PIN);
  doorServo.write(0);
  WiFi.begin(ssid, password);
  lcd.setCursor(0, 0);
  lcd.print("Connecting WiFi");
  while (WiFi.status() != WL_CONNECTED) {
    delay(500);
    Serial.print(".");
  }
  lcd.clear();
  lcd.print("Waiting for motion");
}
void loop() {
  if (!motionDetected && digitalRead(PIR_SENSOR_PIN) == HIGH) {
    motionDetected = true;
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Motion detected");
    delay(3000);
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Press # for OTP");
  }
  char key = keypad.getKey();
  if (motionDetected && key == '#') {
    generateAndSendOTP();
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Enter OTP:");
    userOTP = "";
  }
  if (otpSent && key && isDigit(key)) {
    userOTP += key;
```

```
      lcd.setCursor(userOTP.length() - 1, 1);
      lcd.print("*");
      if (userOTP.length() == 4) {
        if (userOTP == generatedOTP) {
          lcd.clear();
          lcd.setCursor(0, 0);
          lcd.print("OTP Correct!");
          unlockDoor();
          resetSystem();
        } else {
          lcd.clear();
          lcd.setCursor(0, 0);
          lcd.print("Wrong OTP");
          delay(2000);
          lcd.clear();
          lcd.setCursor(0, 0);
          lcd.print("Press # for OTP");
          otpSent = false;
          userOTP = "";
        }
      }
    }
  }
  void resetSystem() {
    motionDetected = false;
    otpSent = false;
    userOTP = "";
    delay(5000);
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Waiting for motion");
  }
  void unlockDoor() {
    doorServo.write(90);
    delay(5000);
    doorServo.write(0);
  }
```

```
void generateAndSendOTP() {
  randomSeed(micros());
  int otp = random(1000, 9999);
  generatedOTP = String(otp);
  String message = "Your OTP is " + generatedOTP;
  Serial.println("Generated OTP: " + message);
  otpSent = true;
  WiFiClientSecure client;
  client.setInsecure();
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Establishing");
  lcd.setCursor(0, 1);
  lcd.print("connection...");
  bool connected = false;
  for (int i = 0; i < 3; i++) {
    if (client.connect("api.twilio.com", 443)) {
      connected = true;
      break;
    }
    delay(1000);
  }
  if (!connected) {
    Serial.println("❌ Twilio connection failed");
    lcd.clear();
    lcd.setCursor(0, 0);
    lcd.print("Twilio Failed");
    delay(2000);
    lcd.clear();
    lcd.print("Press # for OTP");
    otpSent = false;
    return;
  }
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Sending OTP...");
  String credentials = String(account_sid) + ":" + String(auth_token);
  String auth = base64::encode(credentials);
```

```
  String post_data = "To=" + urlencode(to_number) +
                     "&From=" + urlencode(from_number) +
                     "&Body=" + urlencode(message);
  String request = "POST /2010-04-01/Accounts/" + String(account_sid) + "/Messages.json
HTTP/1.1\r\n";
  request += "Host: api.twilio.com\r\n";
  request += "Authorization: Basic " + auth + "\r\n";
  request += "Content-Type: application/x-www-form-urlencoded\r\n";
  request += "Content-Length: " + String(post_data.length()) + "\r\n\r\n";
  request += post_data;
  client.print(request);
  while (client.connected()) {
    String line = client.readStringUntil('\n');
    if (line == "\r") break;
  }
  String response = client.readString();
  Serial.println("📩 Twilio Response:");
  Serial.println(response);
  client.stop();
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("OTP Sent");
  delay(3000);
  lcd.clear();
  lcd.setCursor(0, 0);
  lcd.print("Enter OTP:");
}
String urlencode(String str) {
  String encoded = "";
  char c;
  char code0, code1;
  for (int i = 0; i < str.length(); i++) {
    c = str.charAt(i);
    if (isalnum(c)) {
      encoded += c;
    } else {
      code0 = (c >> 4) & 0xF;
      code1 = c & 0xF;
```

```
      encoded += '%';
      encoded += "0123456789ABCDEF"[code0];
      encoded += "0123456789ABCDEF"[code1];
    }
  }
  return encoded;
}
```

Advantages of the Proposed System

Enhanced Security: OTP (One-Time Password) based system increases security by using dynamic codes that change every time. Limits access by restricting attempts to a maximum of 3, reducing brute force risks.

- **Remote Alert System:** The Twilio API ensures fast and reliable OTP delivery via SMS to the registered mobile number, provided there is an active internet connection, enabling users to receive alerts globally.
- **User-Friendly Interface:** The LCD display and keypad provide clear, step-by-step instructions, making the system intuitive and easy to operate even for first-time users.
- **Motion Detection Integration:** The system smartly generates an OTP only when motion is detected by the PIR sensor, preventing unnecessary OTP generation and spam messages.
- **Automatic Lock Mechanism:** Upon successful OTP verification, the servo motor automatically unlocks the door, offering both security and user convenience.
- **Timeout and Lockout Protection:** If the OTP is not entered within 2 minutes, the system resets to idle mode. After 3 incorrect OTP entries, the system enforces a 1-hour lockout to prevent brute-force attacks.
- **Low Power Consumption:** The ESP32 microcontroller operates efficiently, supporting battery operation for energy savings, especially in areas with unreliable power supply.
- **Cost-Effective:** By leveraging cloud-based communication through Twilio, the system eliminates the need for dedicated GSM hardware, reducing overall hardware costs.

Limitations of the Proposed System

- **Internet Dependency**: The system requires an active and stable internet connection to access the Twilio cloud API for OTP transmission, limiting its functionality in areas with poor connectivity.
- **Cloud Service Costs:** Using Twilio involves usage-based charges for SMS delivery, which can add to operational expenses over time.
- **Delayed SMS Delivery:** Although Twilio is generally fast, SMS delivery may still experience delays due to factors like network congestion or recipient carrier issues.

• **Hardware Damage Risk**: Components like the servo motor and ESP32 can be vulnerable to voltage spikes or improper handling, necessitating proper electrical protection.

• **Physical Tampering:** While the software security is strong, the hardware components remain susceptible to physical tampering without appropriate enclosures or tamper-detection mechanisms.

• **No Remote Revocation:** Once an OTP is generated and sent via Twilio, it cannot be revoked remotely if the user changes their mind or suspects unauthorized access.

CHAPTER 6

EXPERMENTAL RESULTS

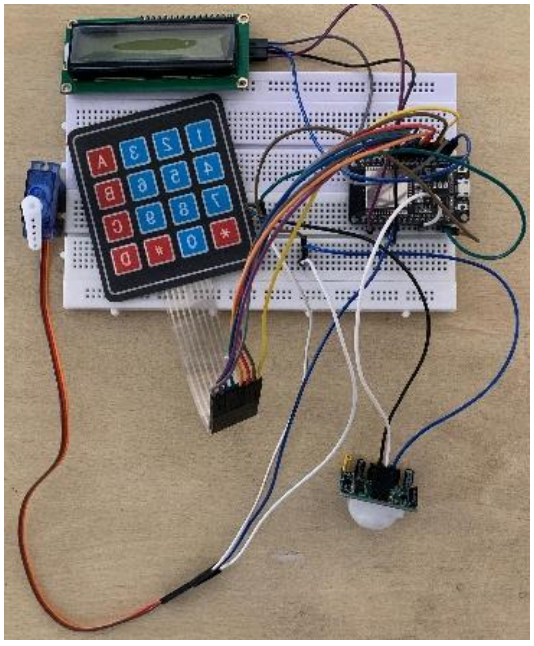


Figure 9 – IoT-Powered OTP-Based Vault Security System

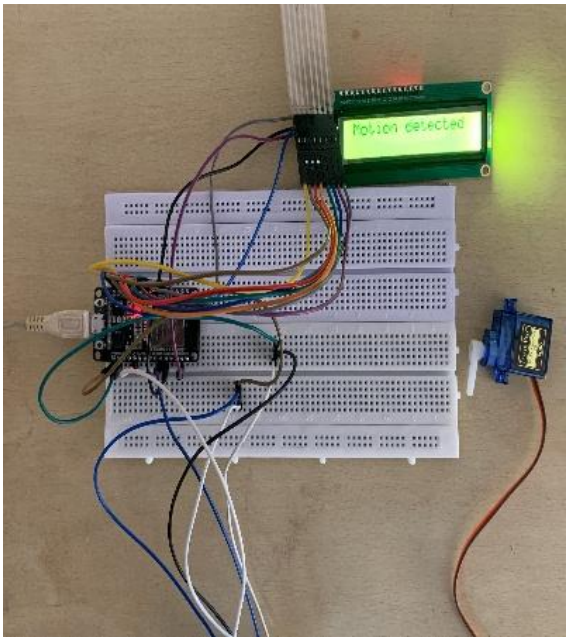


Figure 10 – Motion Detected through PIR Sensor

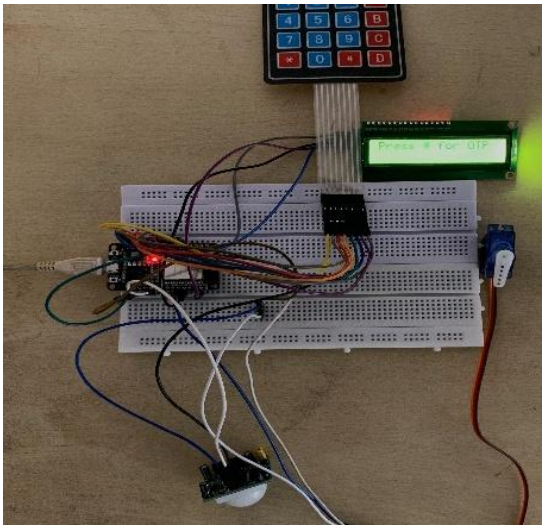


Figure 11 – Waits for Human Verification

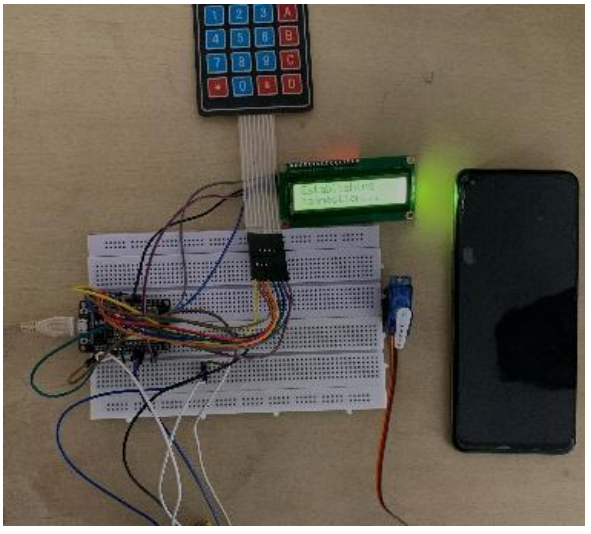


Figure12 – Establishes Connection with TWILIO API via Wi-Fi

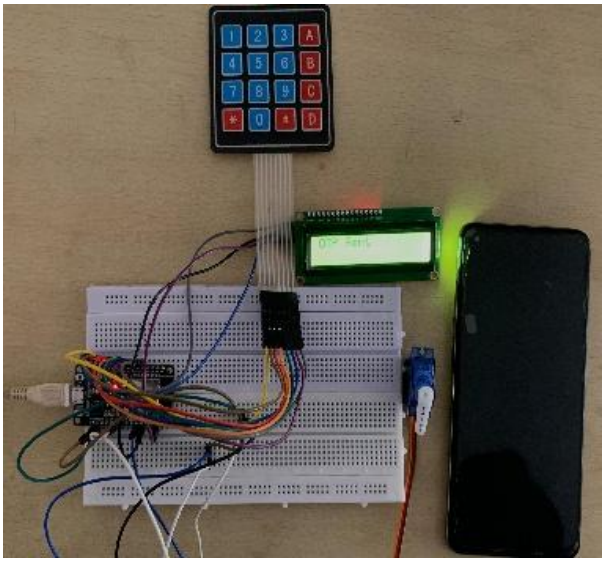


Figure 13 – OTP sent to SMS App of Registered Mobile Number

Figure 14 – OTP received via TWILIO API

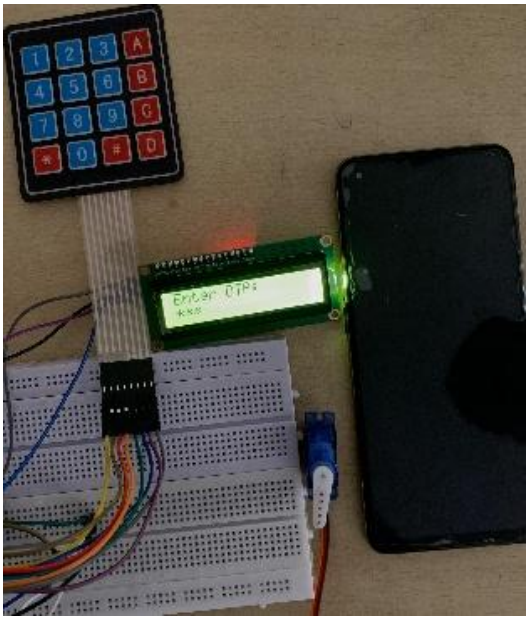


Figure 15 – Entering OTP via Keypad

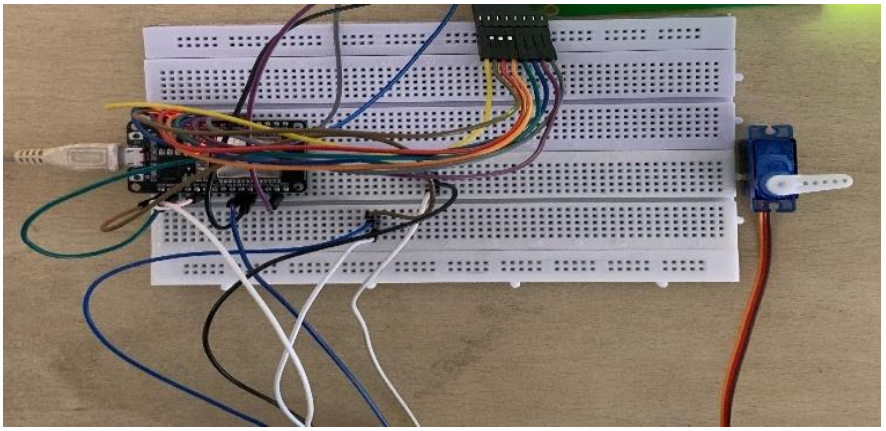


Figure 16 – Access Granted **(SERVO MOTOR ROTATES BY 90 DEGREES)**

CHAPTER 7

FUTURE SCOPE

The developed prototype presents a strong foundation for an intelligent, low-cost, and efficient security system. Moving forward, there are numerous opportunities to enhance and scale this system for broader usage and increased effectiveness:

- **Integration with Mobile Application**: Developing a dedicated mobile app for real-time notifications, OTP management, and remote system control will allow users to interact with the security system from anywhere globally.
- **Biometric Authentication:** Adding fingerprint or facial recognition alongside OTP verification will provide multi-layered security, making unauthorized access almost impossible.
- **IoT Cloud Connectivity:** By connecting the system to IoT cloud services, data like access logs and sensor activity can be stored and analyzed remotely. This also enables integration with smart homes and industrial security setups.
- **Solar-Powered Operation:** Incorporating renewable energy solutions like solar panels will ensure that the system remains operational even in power outages or remote locations without direct power supply.
- **Tamper Detection Mechanism**: Sensors for detecting tampering with the GSM module or other critical components can be added to send instant alerts if the system is compromised.
- **Camera Integration for Visual Verification:** Integrating an IP camera or WiFi camera module to capture images or stream live footage when motion is detected adds another layer of monitoring.
- **Data Encryption and Cybersecurity Improvements:** Using encrypted protocols (like HTTPS or MQTT with TLS) for data transmission enhances the privacy and security of communication between the system and the user.
- **Multiple User Access Levels:** The system can be designed to recognize multiple users with varying access levels, useful for offices or shared spaces where different permissions are needed.
- **Voice Assistance Integration:** Integrating with popular voice assistants like Alexa or Google Assistant can make the system more user-friendly and futuristic.
- **Automatic Emergency Calling Feature:** Besides sending SMS, the system can be upgraded to initiate automatic emergency calls to registered contacts or emergency services when unauthorized access is detected.
- **Maintenance Alerts:** Notifications for system health, battery status (if running on backup), or network disconnection alerts can be incorporated for proactive maintenance.
- **Expandable Keypad or Touchscreen Interface:** Replacing the 4x4 keypad with a touchscreen interface for more intuitive interaction and additional functionalities like viewing logs or adjusting settings directly.

CHAPTR 8

CONCLUSION

The development of the IoT Powered OTP-Based Vault Security System successfully demonstrates an effective and affordable solution for enhancing security through OTP-based access control. By combining motion detection, keypad verification, servo-based locking mechanism, and Twilio API for OTP delivery, the system provides a multi-layered security approach that ensures only authorized individuals gain access.

The integration of the Twilio cloud API allows for reliable and fast OTP delivery via SMS, enabling real-time alerts and secure communication. This approach leverages internet connectivity to ensure seamless OTP transmission, making the system globally accessible and easy to manage remotely. The addition of features like OTP expiration, limited login attempts, and lockout duration further strengthens the security of the system, effectively reducing the risk of unauthorized access or brute-force attacks.

Furthermore, the user-friendly interface with an LCD display and keypad makes it convenient for users to interact with the system. The modular design facilitates easy future upgrades and scalability, allowing integration with advanced cloud services, mobile applications, or additional security sensors. Overall, the project serves as a solid prototype for modern, smart security systems that can be adopted in residential, commercial, and industrial environments.

This project not only fulfills its intended goal of providing secure, OTP-based access control but also opens avenues for further enhancements, aligning with the growing demand for intelligent, IoT-enabled security solutions that are cloud-connected, scalable, and user-centric.

CHAPTER 9

BIOGRAPHY

Vidyadheesha M. Pandurangi is a 3rd-year Electronics and Communication Engineering student with a strong passion for AI, data science, automation systems, VLSI, embedded systems, and IoT. He aspires to integrate these cutting-edge fields to drive innovation and deliver impactful solutions. His academic journey is complemented by hands-on experiences through workshops, internships, and project-based learning. He has actively participated in initiatives like the 'AI for All' program by the Government of India and Intel, a VLSI beginner’s course by NIELIT, and workshops on embedded systems, Python, and IoT. Vidyadheesha’s achievements include securing top rankings in competitions like Flipkart GRiD 6.0 – Round 1 at college level and excelling in technical events.

REFERENCES

1. *Arshdeep Bahga, Vijay Madisetti — Internet of Things: A Hands-On-Approach — 2014, pp. 250–300.*

2. *Cuno Pfister — Getting Started with the Internet of Things — 2011, pp. 75–120.*

3. *Fei Hu — Security and Privacy in IoT — 2016, pp. 180–220.*

4. *Theodore S. Rappaport — Wireless Communications: Principles and Practice — 2014, pp. 450–500.*

5. *Adelstein et al. — Fundamentals of Mobile and Pervasive Computing — 2005, pp. 190–230.*

6. *Brian Russell, Drew Van Duren — Practical Internet of Things Security — 2016, pp. 220–260.*

7. *Simon Haykin — Digital Communication Systems — 2013, pp. 320–370.*

8. *Tim Wilmshurst — Designing Embedded Systems with PIC Microcontrollers — 2010, pp. 300–350.*

9. *IEEE IoT Journal — Advanced Home Automation — 2018, pp. 25–29.*

10. *Texas Instruments — PIR Sensors for Smart Security (Technical Report) — 2017, pp. 12–20.*

11. *S. Lee, J. Kim, H. Park — IoT-Based Smart Home Security Systems using Wi-Fi Connectivity — 2020, pp. 45–52*

12. *X. Wang, L. Zhang, M. Chen — Cloud-Enabled OTP Verification System for IoT Devices — 2021, pp. 1982–1990*

13. *A. V. Patil, R. Deshmukh, S. Kulkarni — Firebase Cloud Messaging for Real-Time Home Security Alerts — 2018, pp. 101–106*

14. *P. Sharma, N. Gupta, V. Singh — Email-Based Intrusion Detection Alert System — 2021, pp. 23–29*

15. *M. Das, A. Sarkar, P. Roy — GSM-Based Home Security System: Design and Implementation — 2020, pp. 88–95*

16. *L. Hernandez, F. Garcia, R. Lopez — Secure SMS Communication in IoT Applications — 2020, pp. 1567–1578*

17. *S. Thomas, K. Varghese — Comparative Study of GSM and Wi-Fi Based Home Security Systems — 2019, pp. 442–447*

18. *A. Mehta, P. Bansal — Microcontroller-Based OTP Generation and Alert Systems for Home Security — 2020, pp. 33–39*

19. *F. Khan, R. Verma, D. Chawla — Integration of IoT and GSM for Secure Communication Systems — 2019, pp. 215–222*

20. *K. Patel, S. Iyer, M. Choudhury — Advanced Security Measures for Home Automation Systems — 2021, pp. 59–66*