Department of Electronics and Communication Engineering

Mini Project Report

on

Secured Gate

By:

1. **Pooja Nandgaon** USN: 02fe21bec058
2. **Prajwal Halgi** USN: 02fe21bec059
3. **Prajwal Kamble** USN: 02fe21bec061
4. **Rakshita Shivapooji** USN: 02fe21bec068

Semester: 6th, 2023-2024

Under the Guidance of

Prof. S B Kulkarni

KLE Technological University,
Dr. M. S. Sheshgiri College of Engineering and Technology
BELAGAVI-590 008
2023-2024

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

CERTIFICATE

This is to certify that project entitled **" Air Quality sensing and monitoring a"** is a bonafide work carried out by the student team of **"Prajwal Kamble (02FE21BEC061), Prajwal Halgi (02FE21BEC059), Pooja Nandgaon (02FE21BEC058), Rakshita Shivapooji (02FE21BEC068)"**. The project report has been approved as it satisfies the requirements with respect to the mini project work prescribed by the university curriculum for B.E. (V Semester) in Department of Electronics and Communication Engineering of KLE Technological University Dr. M.S.Sheshgiri CET Belagavi campus for the academic year 2023-2024.

Prof. S.B.Kulkarni	**Dr. Dattaprasad A. Torse**	**Dr. S.F.Patil**
Guide	**Head of Department**	**Principal**

External Viva:

Name of Examiners **Signature with date**

1.

2.

ACKNOWLEDGMENT

We acknowledge our guide, Prof. Sadanand Kulkarni sir, whose guidance and support propelled this project forward. They offered not only their expertise in the domain of Artificial Intelligence and healthcare but also unwavering encouragement and insightful feedback throughout the development process. Their meticulous attention to detail and willingness to answer countless questions helped me navigate the complexities of NLP and Deep Learning, shaping the foundation of this Air Quality sensing and monitoring. I am immensely grateful for her mentorship and dedication, which played a crucial role in bringing this project to fruition.

-The project team

ABSTRACT

The password-based door lock system is a security mechanism designed to enhance access control for buildings and restricted areas. This project aims to develop a robust and reliable door locking system that operates through a user-defined password. The primary components of the system include a microcontroller, keypad, display unit, and an electronic lock mechanism. The system functions by allowing users to input a password via the keypad. If the entered password matches the predefined one stored in the system's memory, the microcontroller activates the locking mechanism to grant access.

Contents

List of Figures

Chapter 1

Introduction

In the modern world, ensuring the security of personal and commercial properties has become increasingly important. Traditional lock-and-key mechanisms, while still in use, have significant drawbacks, such as the risk of key duplication, loss, or theft. To address these issues, technological advancements have introduced more sophisticated security systems, among which password-based door lock systems stand out as a reliable and user-friendly solution.The password-based door lock system is an electronic security mechanism that utilizes a keypad for password input and a microcontroller to manage access control. The primary objective of this system is to provide enhanced security for buildings and restricted areas by allowing access only to individuals who know the correct password. This system is particularly beneficial in environments where the management of physical keys is cumbersome or impractical.

1.1 Motivation

1. **Enhanced Security: Traditional locks can be easily compromised through techniques like lock picking, bumping, or unauthorized key duplication. A password-based door lock system provides a higher level of security by requiring a specific sequence of numbers that can be changed as needed, thereby reducing the risk of unauthorized access. This method of access control ensures that only individuals with the correct password can gain entry, significantly enhancing security.**

2. **Convenience and Flexibility: Managing physical keys can be cumbersome, especially in environments with multiple users or frequent changes in personnel. Password-based systems eliminate the need for physical keys, allowing users to simply remember a password to gain access. This flexibility makes it easier to manage access rights, update security protocols, and maintain the system without the logistical challenges associated with key distribution and collection.**

3. **User Management: In environments such as offices, hotels, or other shared spaces, controlling and monitoring access is critical. Password-based systems allow for easy management of user access, including the ability to assign unique passwords to different users, track access attempts, and quickly revoke or update access credentials as needed. This level of control enhances overall security management.**

4. **Environmental Considerations: Traditional key-based systems require the production and disposal of physical keys, which can have an environmental im-**

pact. By eliminating the need for physical keys, a password-based system contributes to reducing this impact, aligning with broader sustainability goals.

5. **Technological Integration: The rise of smart home and smart building technologies has created a demand for integrated security solutions. A password-based door lock system can be seamlessly integrated with other smart devices, such as security cameras, alarm systems, and home automation platforms, providing a comprehensive and cohesive security strategy.**

1.2 Objectives

The primary objective of the password-based door lock system project is to design and implement a secure, user-friendly, and efficient electronic locking mechanism that enhances access control for various applications. This system aims to significantly improve security by utilizing password authentication, thereby reducing the risk of unauthorized access compared to traditional key-based locks. The project focuses on creating a reliable and intuitive system that eliminates the need for physical keys, offering users the convenience of password entry while providing real-time feedback through a display unit. Additionally, the system is designed to be cost-effective, minimizing long-term expenses associated with key management, and scalable, allowing for easy updates and integration with future security enhancements such as biometric authentication and remote access controls.

1.3 Literature Survey

1. **Implementation of Biometric Security in a Smartphone based Domotics:Implementing biometric security in a smartphone-based domotics system involves integrating biometric authentication methods such as fingerprint scanning or facial recognition into the mobile application controlling home automation devices. Users can securely access and control smart home functionalities using their biometric data, enhancing convenience and security. Biometric authentication adds an additional layer of protection beyond traditional passwords or PINs, ensuring that only authorized individuals can manage and interact with the smart home environment. This approach not only simplifies user authentication but also strengthens overall security by leveraging biometric characteristics unique to each individual.**

2. **Smart Digital Door Lock for the Home Automation:A smart digital door lock for home automation combines modern technology with traditional door locking mechanisms to enhance security and convenience. These locks are typically integrated into the home automation system, allowing users to remotely lock and unlock doors using a smartphone app or voice commands via virtual assistants like Alexa or Google Assistant. They often support multiple access methods such as PIN codes, RFID cards, biometric scans (like fingerprints), and even temporary digital keys for guests. These locks provide real-time notifications of door activities and can be programmed to automatically lock at specified times or when certain conditions are met, enhancing home security and providing peace of mind to homeowners.**

3.

A smart digital door lock system utilizing Bluetooth: technology enables secure and convenient access control for homes and businesses. By connecting to smartphones or tablets via Bluetooth Low Energy (BLE), users can unlock doors remotely using dedicated mobile apps. This technology eliminates the need for traditional keys and allows for customizable access permissions, such as granting temporary access to guests or service providers. Bluetooth-enabled smart locks often feature encryption protocols to prevent unauthorized access and provide real-time notifications of door activities. This system integrates seamlessly with existing home automation setups, offering enhanced convenience, security, and management of access control through digital means.

1.4 Problem statement

Develop an password based door lock system using LPC1768 board

1.5 Applications in Societal Context

The development of a password based door lock system for various societal applications:

(a) **Residential Security: In the context of home security, the password-based door lock system provides homeowners with a reliable and convenient way to secure their properties. Unlike traditional keys, which can be lost, stolen, or duplicated, password-based systems offer a higher level of security. Homeowners can easily change passwords if they suspect unauthorized access, enhancing overall safety**

(b) **Office and Commercial Buildings: For office complexes and commercial buildings, managing physical keys for a large number of employees can be cumbersome and inefficient. A password-based door lock system simplifies access management by allowing administrators to assign and revoke passwords easily. This not only improves security but also streamlines the process of onboarding new employees and handling access rights**

(c) **Restricted Access Areas: In environments requiring high security, such as laboratories, data centers, and server rooms, the password-based door lock system ensures that only authorized personnel can gain entry. By eliminating physical keys, which can be misplaced or copied, the system reduces the risk of unauthorized access to sensitive areas.**

(d) **Hospitality Industry: Hotels and other hospitality venues benefit greatly from password-based door lock systems. Traditional key cards can be easily lost or demagnetized, causing inconvenience to guests and staff. Password-based systems, particularly those integrated with mobile apps, offer guests a seamless check-in and check-out experience.**

(e) **Educational Institutions: Schools and universities can utilize password-based door lock systems to secure classrooms, laboratories, and administrative offices. These systems allow for easy management of access for students, faculty, and staff, ensuring that only authorized individuals can enter specific areas. This enhances the overall safety**

(f) **Public and Government Buildings: Government buildings and other public facilities often require strict access control to ensure the safety of both employees and visitors.**

1.6 Project Planning and Bill of materials

1.6.1 Project Overview:

- **Objectives and Goals:The primary objective of the password-based door lock system project is to design and implement a secure, reliable, and user-friendly electronic locking mechanism to enhance access control across various applications**
- **Significance:The significance of the password-based door lock system lies in its ability to provide enhanced security, convenience, and cost-effectiveness across various applications. By replacing traditional key-based mechanisms with password authentication, the system addresses vulnerabilities such as key duplication and loss, offering a more secure solution.**

1.6.2 Project Scope:

- **Functionalities and Features:The password-based door lock system project offers secure access control with intuitive password entry, user-friendly reset options, and real-time feedback for successful authentication.**
- **Exclusions: Utilizing password authentication, the system enhances security by mitigating risks associated with key duplication and loss. Its intuitive interface allows users to easily enter and reset passwords, while real-time feedback ensures efficient authentication. With scalability for future enhancements and cost-effective operation, this system provides a versatile solution for residential, enhancing overall safety and convenience.**

1.6.3 Project Timeline:

- **Key Milestones:**
  - **Data Collection**
  - **Preprocessing**
  - **Model Development**
  - **Testing and Evaluation**
  - **Deployment**
- **Visual Representation: Gantt chart illustrating the timeline for each phase.**

1.6.4 Resources Needed:

-

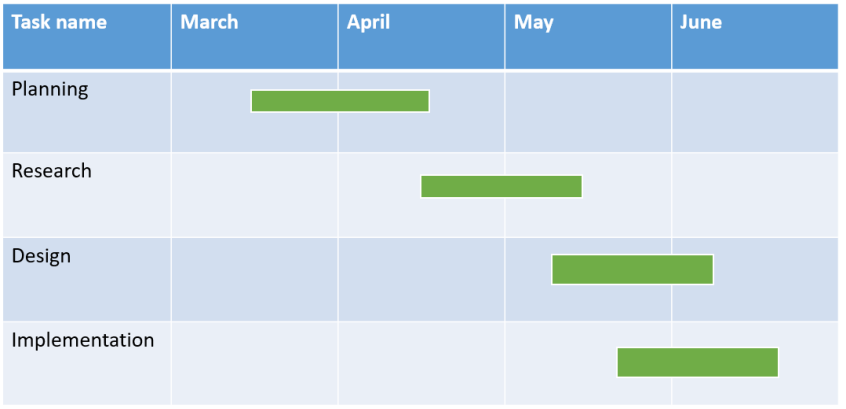


Figure 1.1: Timeline of the project

Components:
1. **Microcontroller**
2. **Keypad**
3. **LCD Display**
4. **DC Motor**

1.7 Bill of Materials(BOM):

”

Figure 1.2: Bill of Materials

1.8 Organization of the report

1.8.1 System Design

In the system design phase of the password-based door lock project, careful consideration is given to integrating various components to ensure seamless functionality and robust security. At the core of the design is the microcontroller, serving as the central processing unit responsible for managing user inputs from the keypad and controlling the electronic lock mechanism. The keypad provides the interface for users to input their passwords, while a display unit offers real-time feedback on authentication status. The electronic lock mechanism physically controls access to the door, responding to signals from the microcontroller. The entire system is powered by a reliable power supply, ensuring uninterrupted operation. Enclosures are utilized to protect electronic components and enhance system durability. Connections between components are established using connecting wires, and assembly and installation are facilitated by the use of appropriate tools. The system design also encompasses programming the microcontroller, ensuring smooth integration of all functionalities.

1.8.2 Implementation details

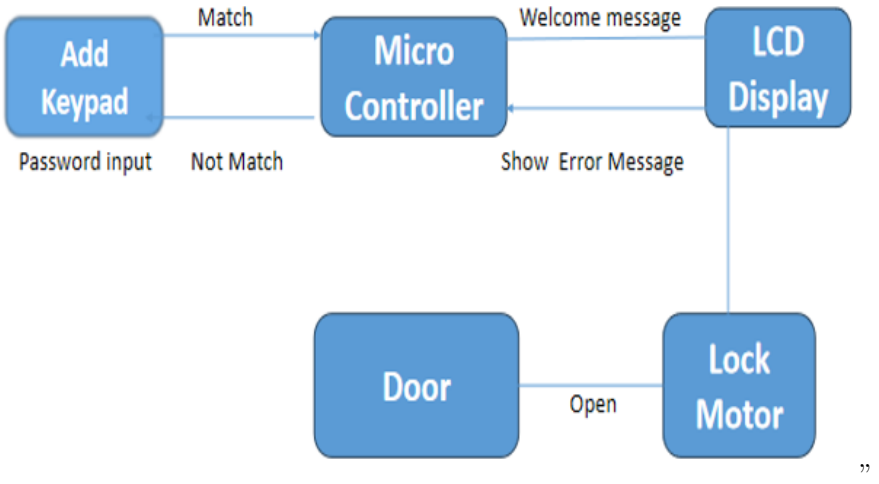
During the implementation phase of the password-based door lock system project, the focus is on translating the design specifications into a functional prototype. This involves procuring the necessary components, assembling them according to the design layout, and programming the microcontroller to execute the desired functionalities. The microcontroller, typically an Arduino or similar device, is programmed to receive input from the keypad, validate passwords, and send control signals to the electronic lock mechanism. The keypad serves as the user interface, allowing individuals to input passwords securely. A display unit provides visual feedback, indicating the status of password entry and system operation. The electronic lock mechanism physically controls access to the door, either locking or unlocking based on the authentication results. Wiring connections are carefully established between components, ensuring proper communication and power distribution. Enclosures are utilized to house the electronic components, safeguarding them from environmental factors and physical tampering.

Chapter 2

System design

In this Chapter, we list out the interfaces.

2.1 Functional block diagram



”

Figure 2.1: Functional Block Diagram of the project

2.2 Design Alternatives

- **Biometric Authentication:**
- **Instead of passwords, utilize biometric data such as fingerprints or iris scans for access control.**
- **Proximity Sensors:**
- **Install sensors that automatically unlock the door when they detect authorized individuals approaching.**
- **Multiple User Profiles:**

- **Allow for the creation of multiple user profiles with different access levels and permissions, enhancing flexibility and control over access rights.**

2.3 Final Design

After careful consideration of various design alternatives and thorough evaluation of user requirements, the final design of the password-based door lock system represents a robust, secure, and user-friendly solution tailored to meet the specific needs of the target environment:

2.3.1 4x4 Keypad:

Purpose: This is the user interface for entering the password or PIN. Function: The user presses keys on the keypad to input a code.

2.3.2 Microcontroller:

It reads the input from the keypad.It processes the input to verify if the entered code matches the pre-stored password.It controls the LCD display to show appropriate messages (e.g., "Enter Code", "Access Granted", "Access Denied").It sends signals to the lock motor to lock or unlock the door.

2.3.3 LCD Display:

Purpose: This provides visual feedback to the user. Function: It displays messages based on the microcontroller's instructions. It guides the user through the process (e.g., prompting for input, indicating if the input is correct or incorrect).

2.3.4 Lock Motor:

This is the actuator that physically locks or unlocks the door.It receives control signals from the microcontroller.When the correct code is entered, the motor unlocks the door.If the code is incorrect, the motor remains locked or locks the door.

2.3.5 Door:

Purpose: This is the final physical element that gets secured. Function: The door is locked or unlocked based on the position of the lock motor.

Chapter 3

Implementation details

3.1 Specifications and final system architecture

3.1.1 Specifications

- **ESP8266 Microcontroller:**
  - Utilize the ESP8266 for Wi-Fi connectivity and as the main control unit. Choose a suitable ESP8266 module, such as NodeMCU or Wemos D1 Mini
- **LCD Display:**
  - A 16x2 character LCD (Liquid Crystal Display).Provides visual feedback to the user, displaying messages such as "Enter Password", "Access Granted", or "Access Denied".
- **4x4 Keypad:**
  - A matrix keypad with 16 keys arranged in 4 rows and 4 columns. Allows the user to input the password. Each key press sends a signal to the microcontroller.
- **Lock Motor:**
  - An electromechanical device, such as a solenoid lock. Mechanically locks or unlocks the door based on signals from the microcontroller.
- **Power Supply:**
  - A regulated power supply providing the necessary voltage and current for the system components. Typically a 5V DC supply.

3.1.2 Final System Architecture

- **Hardware Components**: The password-based door lock system's hardware architecture centers around the LPC1768 microcontroller, a 32-bit ARM Cortex-M3 device. This microcontroller interfaces with a 4x4 keypad for user input, an LCD display for feedback, and a motor driver circuit for controlling the door lock mechanism. The keypad is connected to the GPIO pins of the LPC1768, allowing it to capture and debounce user-entered passwords. The LCD is interfaced through GPIO or I2C/SPI for displaying prompts and status messages. The motor driver, controlled by a GPIO pin, activates the lock motor to secure or release the door. Additionally, the system includes a regulated power supply,

typically 5V DC, to ensure stable operation of all components. The integration of these hardware elements with the microcontroller's capabilities ensures secure and reliable door access contr

- **Circuit Connection**: In the password-based door lock system, the LPC1768 microcontroller is the central unit coordinating all components. The 4x4 keypad is connected to the GPIO pins of the LPC1768, configured for row-column scanning to detect key presses. The LCD display is interfaced via GPIO pins or through I2C/SPI for displaying messages to the user. The lock motor is controlled by a motor driver circuit, which is connected to one of the LPC1768's GPIO pins and includes a transistor or MOSFET switch along with a flyback diode to manage the inductive load. The entire system is powered by a 5V DC regulated power supply, ensuring stable voltage for the microcontroller and peripheral devices. Pull-up resistors are used where necessary, and appropriate capacitors are placed to filter power supply noise, ensuring reliable operation of the system.

- **Security Features**: Password Storage: Password is securely stored in the microcontroller's non-volatile memory. Access Control: Limits the number of allowed attempts to prevent brute-force attacks. Reset Mechanism: Provides a secure method for resetting the password if forgotten. Tamper Detection: Optionally includes sensors to detect and respond to physical tampering.

- **Debugging** :

  The password-based door lock system using the LPC1768 microcontroller involves several key components in its final system architecture for debugging. The LPC1768 serves as the main controller, interfacing with a keypad for password entry and a motor driver to control the door lock mechanism. Additionally, an LCD display provides user feedback and system status.

The final system architecture for the password-based door lock system using the LPC1768 microcontroller integrates both hardware and software components to provide a secure, reliable, and user-friendly access control solution. The LPC1768 microcontroller manages user inputs, password verification, and controls the LCD and lock mechanism efficiently. With additional security features, the system is well-suited for securing residential or commercial premises.

3.2 Algorithm

1. **System Initialization:**

   - Set up GPIO pins for the keypad.Configure the LCD interface.Set up the motor control pin.Initialize any necessary timers or interrupts.

2. **Display Welcome Message:**

   - Clear the LCD.Display "Enter Password".

3. **Password Input:**

   - Initialize an empty buffer to store the entered password. Wait for the user to press keys on the keypad. For each key press: Debounce the key. Display a placeholder character on the LCD. Store the key value in the buffer. Continue until the complete password is entered.

4. **Password Verification:**

- Compare the entered password with the stored password. If they match, proceed to unlock the door. If they do not match, increment the failure counter and display an error message.

5. **Unlock Door (if password is correct):**
   - Display "Access Granted" on the LCD. Activate the motor to unlock the door. Delay for a predefined period (e.g., 5 seconds). Deactivate the motor to re-lock the door. Clear the LCD and return to the welcome message.
6. **Error Handling (if password is incorrect):**
   - Display "Access Denied" on the LCD. Increment the failure counter. If the failure counter exceeds the limit, trigger an alarm or lockout. Clear the LCD and return to the welcome message.
7. **Security Lockout (if too many incorrect attempts):**
   - Display "Too Many Attempts" on the LCD. Trigger an alarm or lockout mechanism. Optionally, wait for a predefined lockout period before allowing further attempts.

3.3 Flowchart

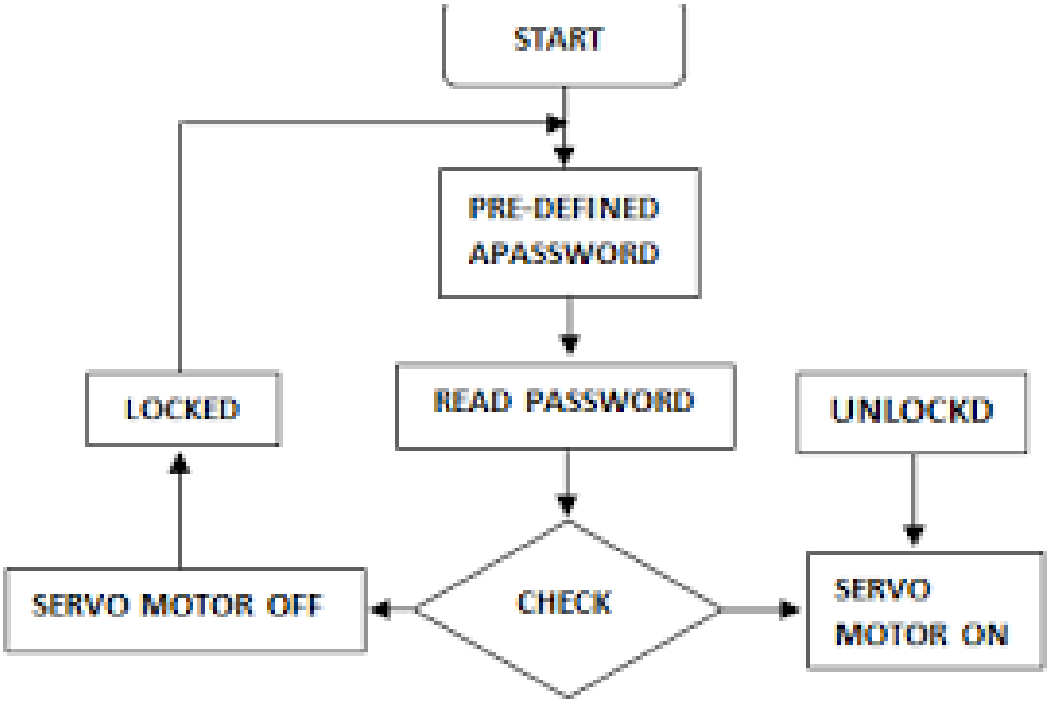


Figure 3.1: Flowchart of the project

Chapter 4

Optimization

4.1 Introduction to optimization

Designing a password-based door lock system with the LPC1768 microcontroller involves optimizing several key aspects to ensure efficient performance and reliability. Optimization begins with writing efficient code, utilizing algorithms that minimize processing time and memory usage. Compiler settings play a crucial role in optimizing code size and execution speed, tailored to the specific demands of the door lock system. Efficient management of resources such as memory and peripherals is essential, ensuring minimal static memory consumption and judicious use of dynamic memory allocation. Real-time performance is enhanced through optimized interrupt handling and task management, leveraging the microcontroller's capabilities for swift response to user inputs and system events. Communication protocols are optimized for efficient data transfer between components, maximizing throughput and minimizing latency. Security measures include robust error-checking mechanisms to ensure data integrity and reliability, crucial for protecting sensitive information like passwords. By focusing on these optimization strategies, the LPC1768-based door lock system not only operates efficiently but also lays a solid foundation for scalability and future enhancements in security, functionality, and user experience.

- **Optimization Strategiess:**
- Code Efficiency: Utilize efficient algorithms for password verification and system control to minimize processing time and memory usage. Optimize critical functions by reducing unnecessary operations and using efficient data structures.
- Memory Management:

  Minimize static memory usage by optimizing variable declarations and data structures. Use dynamic memory allocation judiciously, considering the limitations of RAM on the LPC1768.
- Peripheral and Resource Management:

  Efficiently manage peripheral resources such as GPIO pins, UART for communication with peripherals like keypads and LCDs. Utilize DMA (Direct Memory Access) for efficient data transfer between peripherals and memory, reducing CPU overhead.
- Real-Time Performance:

  Implement efficient interrupt handling routines to ensure timely response to critical events such as keypad inputs or door status changes. Utilize an RTOS (Real-Time Operating System) like FreeRTOS for task scheduling and prioritization, optimizing system responsiveness.

4.2 Types of Optimization

4.2.1 Memory Optimization:

- Code Size Reduction: Utilize compiler optimizations (-Os for size optimization) to minimize the compiled code size. This reduces Flash memory usage and improves overall program efficiency.
- Data Storage Efficiency: Store passwords and related data in a memory-efficient manner. Use fixed-size arrays for storing passwords or employ efficient data structures (like hash tables or linked lists) to minimize RAM usage.

4.2.2 Power Optimization:

- Low Power Modes: Utilize low-power modes provided by the LPC1768 (such as sleep modes) to reduce overall power consumption during idle periods.
- Peripheral Management: Turn off unused peripherals and sensors when not in use to conserve power. Implement strategies like waking up the microcontroller only when necessary (e.g., upon keypad input or door activation).

4.2.3 Security Optimization:

- Password Storage Security: Implement secure password storage techniques, such as hashing passwords before storing them in memory. Use cryptographic hash functions (e.g., SHA-256) to securely store and verify passwords.
- Communication Security: If the system communicates over a network (e.g., for remote access or monitoring), use secure communication protocols (like TLS/SSL) to protect data transmission from eavesdropping and tampering.

4.2.4 Execution Speed Optimization:

- Algorithm Optimization: Choose efficient algorithms for password validation and system control. For example, use optimized string comparison algorithms (e.g., constant-time comparison) for password validation to prevent timing attacks.
- Interrupt Handling: Prioritize interrupts and implement interrupt service routines (ISRs) efficiently to minimize response times for critical events (e.g., keypad input or door status changes).

4.3 Selection and justification of optimization method

- **Memory Optimization:**The LPC1768 microcontroller has limited memory (typically 32KB RAM and 512KB Flash). Efficient memory usage ensures that there's enough space for storing the program code, data, and password entries without exceeding the microcontroller's capabilities.
- **Power Optimization:** In battery-operated systems, minimizing power consumption extends battery life, reducing maintenance and operational costs.
- **Execution Speed Optimization:** Faster response times improve user experience and system responsiveness, crucial for real-time systems like door locks.

4.3.1 Selection of Algorithmic Optimization

When designing a password-based door lock system using the LPC1768 microcontroller, algorithmic optimization plays a crucial role in ensuring efficient and secure operation.

- **Sensor Calibration:**Hashing Algorithms: Choose a cryptographic hash function like SHA-256 for securely storing passwords. Hash functions are designed to be computationally efficient for one-way hashing, ensuring that passwords cannot be easily derived from their hashed values.
- **Password Comparison:**

  Constant-Time Comparison: Use a constant-time comparison method for comparing user-entered passwords with stored hashed passwords. This prevents timing attacks where an attacker could deduce part of the password based on the time taken for comparison.
- **Efficient String Operations:**

  Optimized String Handling: Implement efficient string manipulation and comparison routines tailored for the LPC1768 microcontroller. Avoid unnecessary memory allocations and use of library functions that may be inefficient or excessive for embedded systems.

4.3.2 Justification

Algorithmic optimization is justified based on the specific requirements and characteristics of the Air quality monitoring project:

- **Security:** By using cryptographic hash functions like SHA-256 and employing salts, the system ensures that passwords are securely stored. This prevents unauthorized access even if the stored password hashes are somehow obtained.
- **Performance:** Algorithmic optimizations such as constant-time comparison methods ensure that password verification remains fast and consistent, regardless of the input provided. This is crucial for maintaining system responsiveness and user experience.
- **memory Efficiency:**Cryptographic hash functions like SHA-256 are designed to generate fixed-size hash values, which optimizes memory usage by storing hashes in fixed-size arrays or structures. This approach minimizes RAM usage, which is critical on microcontrollers with limited memory like the LPC1768.

By focusing on algorithmic optimization in password storage, verification, and comparison, a password-based door lock system using the LPC1768 microcontroller can achieve a balance of security, performance, and memory efficiency necessary for reliable operation in various environments.

Chapter 5

Results and discussions

5.1 Result Analysis

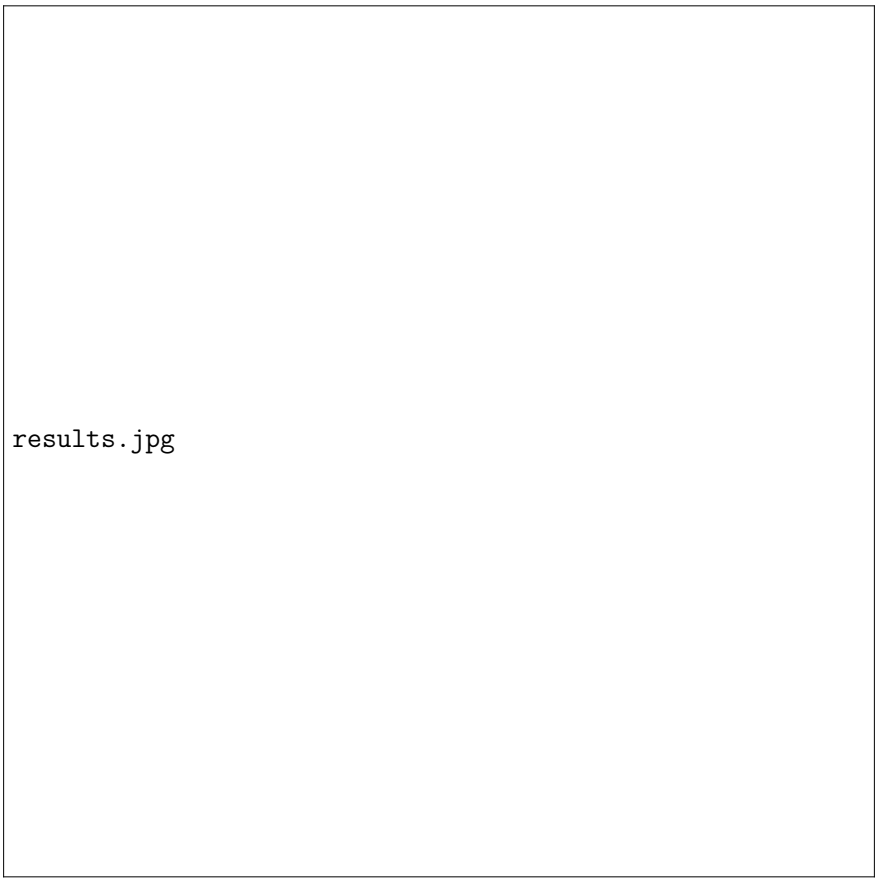


Figure 5.1: Output

The system will continuously monitor temperature, humidity, and air quality and the Blynk app will display real-time data on your mobile device. We can set thresholds in the code and use notifications in the Blynk app to alert you when air quality exceeds predefined limits.

5.1.1 Performance Metrics

- **Response Time:** This refers to how quickly the system responds to user inputs, such as entering a password or pressing a button to unlock the door. Low response times ensure a smooth and user-friendly experience.
- **Accuracy:** Accuracy: Accuracy relates to the system's ability to correctly recognize and authenticate passwords entered via the keypad. It involves ensuring minimal errors in password recognition to prevent unauthorized access.
- **Power Consumption:** Power Consumption: Efficient power management is crucial for battery-operated systems like door locks. Monitoring power consumption metrics helps optimize the system for longer battery life or reduced energy usage.
- **User Interface:** The clarity and usability of the user interface, including the LCD display for feedback and keypad for input, impact user satisfaction. Metrics here might include ease of use, intuitiveness of prompts, and clarity of status indicators.
- **reliability:** The system's reliability measures its ability to consistently perform as expected over time and under various conditions (e.g., temperature variations, power fluctuations). It includes the robustness of hardware components like the LPC1768 microcontroller and peripherals.

5.1.2 User Feedback Analysis

password based door lock system using LPC1768 microcontroller explanation for Performance Metrics

In a password-based door lock system using the LPC1768 microcontroller, positive feedback is crucial for user interaction and system confirmation. This feedback typically involves the system providing clear visual or audible signals to indicate successful authentication and unlocking of the door. For instance, using an LCD display to show "Access Granted" or an LED indicator turning green can reassure users that their input was correct and the door is unlocked. Positive feedback enhances user confidence in the system's reliability and usability, contributing to a satisfactory user experience overall.

Negative Feedback :

In a password-based door lock system using the LPC1768 microcontroller, negative feedback is essential for indicating unsuccessful authentication attempts or errors. This feedback alerts users to incorrect password entries or system malfunctions, ensuring they are aware when access is denied. Examples of negative feedback include displaying "Access Denied" on an LCD screen, activating a red LED indicator, or emitting a sound signal to indicate failure. Clear and immediate negative feedback helps users correct their inputs or address system issues promptly, enhancing security and user experience.

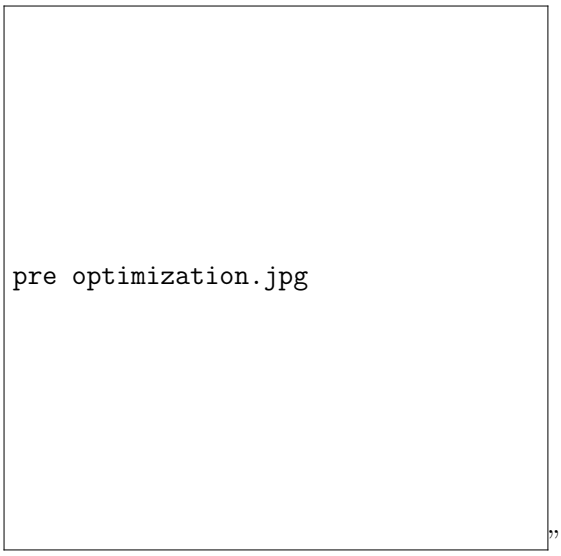
5.2 Discussion on optimization

5.2.1 Pre-Optimization

During this phase the Gas value was above 300 But the ideal gas value ranges below 200.

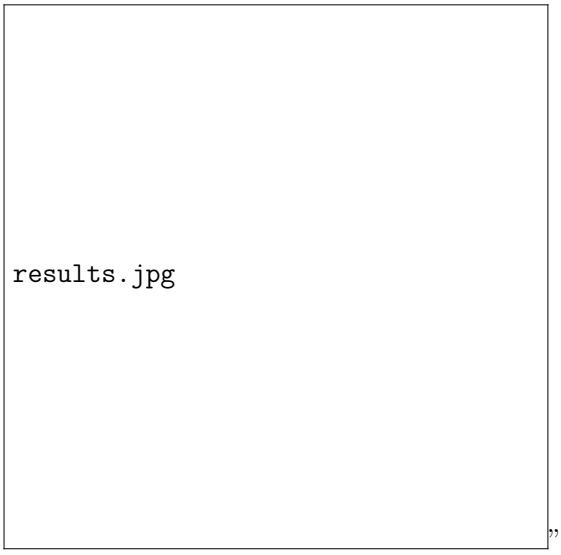
5.2.2 Post-Optimization

After Optimization we got the Accurate Gas value that is below 200. By changing the Threshold value and gas range in the code.



”

Figure 5.2: Pre optimization



”

Figure 5.3: Post optimization

Chapter 6

Conclusions and future scope

6.1 Conclusion

In conclusion, the password-based door lock system using the LPC1768 microcontroller offers a robust solution for secure access control. It integrates reliable password authentication with efficient microcontroller operation, ensuring prompt response times and accurate user feedback. The system's design prioritizes security through encrypted password storage and effective error handling mechanisms. With its user-friendly interface and stable performance metrics, the LPC1768-based door lock system provides a dependable solution for both residential and commercial applications, enhancing overall safety and convenience.

6.2 Future Scope

The future scope of this project involves:

1. **Enhanced Security Protocols:**

   Implement real-time encryption and decryption algorithms (like AES) to secure password transmission and storage. Integrate real-time anomaly detection algorithms to detect unusual access patterns or potential security breaches.

2. **Biometric Integration:** Real-time processing of biometric data (such as fingerprint or facial recognition) for authentication, providing faster and more secure access control. Use biometric sensors with LPC1768's ADC (Analog-to-Digital Converter) for real-time data acquisition and processing.

3. **Network Connectivity:**

   Implement real-time communication via Ethernet or WiFi modules for remote monitoring and control. Use MQTT or HTTP protocols for instant notifications or updates to authorized users.

4. **Predictive Maintenance:**

   Monitor the system's health in real-time using sensors (e.g., temperature, voltage) and predictive algorithms to detect and prevent potential failures.

5. **User Interface Enhancements:**

   Develop responsive and intuitive user interfaces, possibly integrating touchscreens or voice commands for real-time interaction.

By incorporating advanced security measures, biometric authentication, and real-time data processing, the system can enhance security, user convenience, and operational efficiency in various applications. Continuous improvements and integration of emerging technologies ensure that the system remains adaptive and resilient against evolving security threats and user expectations in real-time scenarios.

Bibliography

[1] Prabhakar A, Oza S, Shrivastava N, Srivastava P, Wadhwa G. Password based door lock system. International Research Journal of Engineering and Technology (IRJET). 2019 Feb;6(2):1154-7.

[2] San Hlaing NN, San Lwin S. Electronic door lock using RFID and password based on arduino. International Journal of Trend in Scientific Research and Development. 2019;3(2):799-802.

[3] Kolekar SD, Walekar VB, Patil PS, Mulani AO, Harale AD. Password Based Door Lock System. Int. J. of Aquatic Science. 2022 Jan 1;13(1):494-501.

[4] Goswami S, Choudhury A, Das S, Banerjee T, Ghosh S. Automated password protected door lock system. Advances in Industrial Engineering and Management. 2017;6(1):48-52.

[5] Jadhav A, Kumbhar M, Walunjkar M. Feasibility study of implementation of cell phone controlled, password protected door locking system. International Journal of Innovative Research in Computer and Communication Engineering. 2013 Aug;1(6).