Major Project Report
(BCA-308)

Wireless Door Locking System

Submitted in partial fulfillment of the requirements

for the award of the degree of

Bachelor of Computer Applications

To

Guru Gobind Singh Indraprastha University, Delhi

Guide:

Ms. Anjaly Chauhan
(Assistant Prof.)

Submitted by:

Abhishek Yadav
(05213702021)

Institute of Information Technology & Management,
New Delhi – 110058

Batch (2020-2023)

Certificate

I, Abhishek Yadav (05213702021) certify that the Major Project Report (BCA-308) entitled "Wireless Door Locking System" is done by me and it is an authentic work carried out by me at "Institute of Information Technology & Management". The matter embodied in this project work has not been submitted earlier for the award of any degree or diploma to the best of my knowledge and belief.

Signature of the Student
Date:

Certified that the Major Project Report (BCA-308) entitled "Wireless Door Locking System" done by the above student is completed under my guidance.

Signature of the Guide:
Date:
Name of the Guide: Ms. Anjaly Chauhan
Designation: Assistant Professor

Counter sign HOD

Counter sign Director

SELF CERTIFICATE

This is to certify that the project report entitled “Wireless Door Locking System” is done by me is an authentic work carried out for the partial fulfillment of the requirements for the award of the degree of Bachelor of Computer Applications under the guidance of “Ms. Anjaly Chauhan” The matter embodied in this project work has not been submitted earlier for award of any degree or diploma to the best of my knowledge and belief.

Signature of the student

Name of the student : Abhishek Yadav

Roll No. : 05213702021

Synopsis

1. Title of the project

Wireless door locking system

2. Problems with the Existing System

1. **Reliability Issues**: Some wireless door locking systems may suffer from reliability issues, such as intermittent connectivity problems or malfunctions in the hardware components. This can lead to situations where users are unable to lock or unlock doors when needed.

2. **Complex Installation Process**: Installation of some wireless door locking systems may require technical expertise and complex wiring, leading to higher installation costs and longer deployment times.

3. **Battery Life**: Battery-powered wireless door locks may have limited battery life, requiring frequent battery replacements or recharging. This can be inconvenient and costly, especially for systems with a large number of doors.

4. **Scalability Challenges**: Scaling up existing wireless door locking systems to accommodate a larger number of doors or users may pose challenges in terms of managing and maintaining the system efficiently.

5. **Cost**: The initial cost of purchasing and installing wireless door locking systems, especially those with advanced features or integration capabilities, can be prohibitive for some users or organizations.

6. **Interference and Signal Range**: Wireless door locking systems operating on certain frequencies may experience interference from other devices or have limited signal range, affecting their reliability and performance.

3. Related Work

1. Enhanced Finger Print based Door Locking System:

   This system is built on the concept of biometric. A finger print sensor is used to store the finger print image which is recognized to open the lock. The program is written such that any number of individual fingerprints can be added or deleted from

thedatabase based on the memory incorporated in the system. If the individual's fingerprint is matched, then the door will be opened, otherwise the GSM module gets activated automatically and a SMS message is sent to the registered user, while simultaneously the alarm also gets activated to alert the people or the security official in the surroundings. The microcontroller used in the present work is Arduino UNO R3 board. The proposed enhanced fingerprint security system is tested in real time and provides a comprehensive security solution and unauthorized individuals are prohibited from entering through the door. In contrast to the other authentication methods such as using RFI and passwords security, the proposed method has proven to be most efficient and reliable.

2. Fingerprint Based Security System:

   This paper presents an enhanced methodology in implementing and designing a security system for door locking purpose based on fingerprint, GSM technology, monitoring camera, alarm system and password system. This security system will provide enough security by limiting unauthorized people access and taking a record of those who pass through it. Sometimes unauthorized people or burglars try to break the door for evil intentions at a time when no one is available at a targeted place, so this paper introduces some security solutions for that problem and they are the main contribution of our paper. We introduce an alarm system to alert the people at the surroundings, GSM module that's used to send an SMS message to the registered user's (responsible person) and a web camera that's used to take a video for a person who tries to break the lock, password keypad that's used after fingerprint sensing to provide extra security. Definitely the registered users are the only persons who can access the lock, and the door closes after five seconds from the opening time. The method used to implement this experiment involves the use of a fingerprint scanner R305 that's interfaced with Arduino microcontroller-ATMEGA328P to control the locking and unlocking process of a door. During all the opening and closing processes, the16x2 Liquid Crystal Display (LCD) displays some commands which can be used to instruct the users like, place your finger on the sensor, the door is opened, the door is closed, the message is sent, please enter the password etc. If an unregistered user tries to access the door using their fingerprints, automatically his/her access is denied. The proposed door lock security system is can be used at homes, offices, banks, hospitals, and in other governmental and private sectors. Our proposed system was tested in real-time and has shown competitive results compared to other projects using RFI and password.

3. Fingerprint and GSM based Security System:

   The main purpose of this paper is to design and implement high security system. Security is a prime concern in our day-to-day life. Perhaps the most important application of accurate personal identification is securing limited access systems from

malicious attacks. Access control system forms a vital link in a security chain. The fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate, and validate the user and unlock the door in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This high security system based on fingerprint, password and GSM technology which can be organized in bank, secured offices and homes.

4. Door Lock Security System Using Recent Technology:

   In terms of house security, the door is pivotal. To keep the hearthstone secure, the proprietor will keep the door locked at all times. Still, owing to a rush when leaving the house, the proprietor may forget to lock the door, or they may be doubtful if they've closed the door or not. Wireless security grounded operation have fleetly increased due to the dramatic enhancement of ultramodern technologies. Numerous access control systems were designed and/or enforced grounded on different types of wireless communication technologies by different people. Radio Frequency identification (RFID) is a contactless technology that's extensively used in several diligences for tasks like access control system, book shadowing in libraries, tollgate system, forced chain operation, and so on. For enforcing this design, we will be using Arduino mega 2560 pro mini, a fingerprint sensor, Keypad module. ESP-32 CAM module, RFID sensor, solenoid lock and ESP8266. We have also created an application for monitoring and controlling the security features of the door lock. We can also open the door through mobile fingerprint.

5. Smart Door Monitoring and Locking system:

   Protection, security, and safety are the most important things in our daily life. These days, the advancement of Technology has evolved into one of the leading IoT-based projects such as smart home technology. For An instance, this type of system makes livelihood more safe, convenient, and secure. people are more familiar with these technologies nowadays and smart home applications provide a controlled way of action just within the tip of a finger, for example, managing the schedules for home lightning, electricity bills, groceries list, and home security as well. the facial and fingerprint recognition of authorized persons is well established to keep the homes more secured for accessibility. A setup of a display monitor connection with the camera in front of the door is also required to send the information to the owner who is trying to enter his house through that door and the owner has the right to give access to the person who wants to open the door. Even we can provide voice lock by texting voice with raspberry pi arm processor which can revert any messages to the owner. To satisfy all these needs we came up with a new solution that is more secure, reliable, looks, and works smart.

For this, we used a raspberry pi microcontroller linked with a biometric sensor for fingerprint recognition and a camera module for capturing the user image and used a bot in telegram for communication like sending alert messages and receiving commands from the owner.

6. Remote Monitoring Intelligent System Based on Fingerprint Door Lock:

   The system provides a set of easy and more secure options for the owner to unlock his door; the lock can detect your recorded fingerprint and unlock the door. It can also unlock the door through a set of knocks, the owner can record a specific pattern and once the owner knock on the door the system than will unlock the door if it matches the recorded knock pattern, it also can unlock it through smart phone Bluetooth, this option come in handy if the owner forgets the knock pattern. Moreover, it gives the owner's guests the ability to record a voice message and leave it if he is not at home.

7. Biometric Base Smart Door Access System Using Arduino Uno:

   For any organization, banks, office, etc. the security is the first priority to keep their document secure. There are different types of security system like: lock and key system, password lock system, etc. but those systems are not so secure and hence consume more time and can be break easily using duplicate key. The best security system is fingerprint door lock and unlocks system. This system can’t be hacked and neither consumes much time and hence our security system will be stronger. This system has been designed in such a way that only authorized person can only access the system. Operation of this system is much easier than the previous system and can be installed easily. In future this system can be upgraded or we can add latest technology like voice recognition system, retina recognition system and automatic fire alarm system.

8. Intelligent Lock Applied for Smart Door:

   The whole world is moving towards a smarter life, smarter cities and houses. In this paper, we purpose to build a smart door security system to increase the public safety from intruders. The system provides a set of easy and more secure options for the owner to unlock his door; the lock can detect your recorded fingerprint and unlock the door. It can also unlock the door through a set of knocks, the owner can record a specific pattern and once the owner knock on the door the system than will unlock the door if it matches the recorded knock pattern, it also can unlock it through smart phone Bluetooth, this option come in handy if the owner forgets the knock pattern.

9. Fingerprint Doorlock and Home Security System by Using Arduino and IOT:

   The fingerprint and password based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have

implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate, and validate the user and unlock the door in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This high security system based on fingerprint, password and GSM technology which can be organized in bank, secured offices and homes.

10. Smart Door Locking System:

    A well-secured household is of prime importance in today's world. Even after using heavy and hard-to-open metal locks, there are a lot of reasons for which people have to be concerned like losing the keys and robbery. Nowadays a lot of new technologies have emerged to overcome the drawbacks of traditional door locking systems. These alternatives not only help to keep the house secure but also allows for remote access of the door with just one click. The Internet of things is one such technology that has brought a lot of ease in everyday life by providing solutions for various such problems. In this paper, an RFID-based door lock system along with OTP driven technology is discussed to provide a high-security solution for households. In this device, the OTP is generated for door access and this OTP will expire after the expiration time provided. The working model of the proposed system is discussed in this paper.

4. Description of the Proposed System

The Wireless Door Locking System is a convenient and secure solution for controlling access to your doors remotely. Utilizing a combination of hardware components and wireless communication technology, this system allows users to lock and unlock doors using a smartphone or other Bluetooth-enabled devices.

The Arduino Uno R3 is programmed to receive commands from the Bluetooth module via the HC-05 Bluetooth module. Users can pair their smartphones or other Bluetooth-enabled devices with the HC-05 module and send commands to the Arduino to lock or unlock the door. When a lock command is received, the Arduino activates the relay, which in turn triggers the solenoid lock to engage, securely locking the door. Similarly, when an unlock command is received, the Arduino deactivates the relay, releasing the solenoid lock and allowing the door to be opened.

5. Tools/Platform/Middleware

Tools/platform/middleware required are given below:

1. Arduino Uno R3: The heart of the system, Arduino Uno R3 serves as the microcontroller responsible for controlling the operation of the door lock mechanism and interfacing with the Bluetooth module.

2. Solenoid Lock: The solenoid lock is a robust and reliable locking mechanism that can be activated electronically to secure the door.

3. 5V Relay Single Channel: The relay acts as a switch, allowing the Arduino to control the high-voltage solenoid lock safely.

4. HC-05 Bluetooth Module: The Bluetooth module enables wireless communication between the Arduino and external devices such as smartphones, tablets, or laptops, facilitating remote control of the door lock.

5. Jumper Wires: These wires are used to establish connections between the various components of the system, ensuring proper communication and functionality.

6. Communication Cable: This cable is used to connect the Arduino to a power source, such as a 12V DC power adapter or a 9V battery, providing the necessary power for operation.

7. Arduino IDE Software: The Arduino Integrated Development Environment (IDE) is used to write, compile, and upload code to the Arduino Uno, allowing users to customize the functionality of the door locking system.

6. Future scope

1. Biometric Integration: Incorporate biometric authentication methods such as fingerprint scanning, facial recognition, or iris scanning for more secure and convenient access control.

2. Voice Control: Implement voice-activated commands for locking and unlocking doors, offering hands-free operation and accessibility for users with disabilities.

3. Gesture Recognition: Explore the integration of gesture recognition technology, allowing users to unlock doors with specific hand movements or gestures.

4. Artificial Intelligence: Utilize artificial intelligence (AI) algorithms for predictive analytics, anomaly detection, and personalized security settings based on user behavior patterns.

5. Energy Harvesting: Investigate energy harvesting solutions such as solar panels or kinetic energy generators to power the door locking system, reducing reliance on batteries and enhancing sustainability.

6. Multi-factor Authentication: Enhance security by implementing multi-factor authentication methods combining two or more authentication factors such as biometrics, PIN codes, or RFID cards.

7. Mobile App Enhancements: Continuously improve the mobile app interface with features like remote monitoring, real-time alerts, and integration with smart home ecosystems for seamless control of multiple devices.

8. Environmental Sensors: Integrate environmental sensors such as temperature, humidity, or air quality sensors to provide additional insights and automation capabilities, such as adjusting HVAC systems based on room occupancy.

9. Emergency Response Integration: Collaborate with emergency response services to integrate panic buttons or distress signals into the system, enabling quick assistance during emergencies.

10. Smart Access Control Management: Develop centralized access control management tools for administrators to easily configure user permissions, view access logs, and remotely manage multiple door locks.

LIST OF TABLES

LIST OF FIGURES

CONTENTS

Chapter 1 - Introduction

1.1. Overview of the project

The Wireless Door Locking System is an innovative project designed to offer convenient and secure access control for doors using Arduino technology and Bluetooth communication. With an Arduino Uno R3 microcontroller at its core, the system integrates a solenoid lock, a 5V relay, and an HC-05 Bluetooth module to enable remote locking and unlocking of doors via smartphones or other Bluetooth-enabled devices. Users can pair their devices with the system and send commands wirelessly to control the door lock. The system provides a reliable and user-friendly solution, eliminating the need for traditional keys and allowing for customizable access control options. By leveraging Arduino IDE software, users can easily customize and expand the functionality of the system to meet their specific needs. Overall, the Wireless Door Locking System offers convenience, security, and flexibility, making it suitable for various applications ranging from residential homes to commercial establishments.

1.2. Motivation of the project

The motivation behind the Wireless Door Locking System project stems from the pressing need for modernized, convenient, and secure access control solutions in today's dynamic environments. Traditional lock-and-key mechanisms often pose limitations in terms of convenience, security, and adaptability. By leveraging cutting-edge technologies such as Arduino microcontrollers and Bluetooth communication, this project aims to address these shortcomings and revolutionize the way we control access to our doors.

The project seeks to empower users with the freedom to remotely lock and unlock doors using their smartphones or other Bluetooth-enabled devices, eliminating the hassle of carrying physical keys. This level of convenience not only enhances user experience but also streamlines access management processes in various settings, including homes, offices, and commercial spaces.

Moreover, the emphasis on security is paramount. By integrating robust solenoid locks and encrypted Bluetooth communication, the system ensures reliable protection against unauthorized access attempts. This aspect of enhanced security instills confidence in users, knowing that their premises are effectively safeguarded.

1.3. Research gap

While many of the papers emphasize the integration of biometric authentication, GSM technology, and additional security features such as alarms and monitoring cameras, there's a

lack of comprehensive exploration into the scalability and interoperability of these systems. Most studies focus on standalone door locking solutions without considering how they could be integrated into larger smart home ecosystems or commercial security systems. For instance, the potential integration of these door locking systems with other IoT devices, such as smart lighting or surveillance cameras, could provide enhanced security and convenience for users.

Furthermore, there's a limited discussion on the usability and user experience aspects of these systems. While the papers mention the use of LCD displays and SMS alerts for user interaction, there's a need for more in-depth research on user interface design, accessibility features, and user preferences. Understanding how users interact with and perceive these door locking systems could inform the design of more intuitive and user-friendly solutions.

Additionally, there's a gap in research regarding the long-term reliability and maintenance requirements of these systems. While the papers mention real-time testing and competitive results compared to other authentication methods, there's limited discussion on the durability of the hardware components, potential failure modes, and strategies for troubleshooting and maintenance. Addressing these aspects is crucial for ensuring the practical viability and longevity of these door locking systems in real-world deployments.

1.4. Structure of the project

The project's structure is organized into several interconnected components aimed at designing, implementing, and testing a wireless door locking system based on fingerprint authentication. At its core, the system utilizes Arduino microcontrollers for controlling the locking mechanism and interfacing with various hardware components. The hardware setup includes a fingerprint sensor to capture and store fingerprint data for user authentication, along with solenoid locks for securing the doors. Additionally, a communication module such as GSM technology is incorporated to enable remote monitoring and control of the system, providing notifications to registered users via SMS in case of unauthorized access attempts. The system's functionality is further enhanced with the integration of additional security features, such as alarms and monitoring cameras, to ensure comprehensive security coverage. The project involves programming the Arduino microcontroller to manage the authentication process, handle user inputs, and execute the appropriate actions based on the detected fingerprints. Furthermore, the project encompasses testing and validation phases to assess the system's reliability, security, and usability in real-world scenarios. Throughout the project's development, emphasis is placed on adhering to best practices in hardware design, software development, and system integration to achieve a robust and effective wireless door locking solution.

1.5.Scope of the project

1. Biometric Integration: Incorporate biometric authentication methods such as fingerprint scanning, facial recognition, or iris scanning for more secure and convenient access control.

2. Voice Control: Implement voice-activated commands for locking and unlocking doors, offering hands-free operation and accessibility for users with disabilities.

3. Gesture Recognition: Explore the integration of gesture recognition technology, allowing users to unlock doors with specific hand movements or gestures.

4. Artificial Intelligence: Utilize artificial intelligence (AI) algorithms for predictive analytics, anomaly detection, and personalized security settings based on user behavior patterns.

5. Energy Harvesting: Investigate energy harvesting solutions such as solar panels or kinetic energy generators to power the door locking system, reducing reliance on batteries and enhancing sustainability.

6. Multi-factor Authentication: Enhance security by implementing multi-factor authentication methods combining two or more authentication factors such as biometrics, PIN codes, or RFID cards.

7. Mobile App Enhancements: Continuously improve the mobile app interface with features like remote monitoring, real-time alerts, and integration with smart home ecosystems for seamless control of multiple devices.

8. Environmental Sensors: Integrate environmental sensors such as temperature, humidity, or air quality sensors to provide additional insights and automation capabilities, such as adjusting HVAC systems based on room occupancy.

9. Emergency Response Integration: Collaborate with emergency response services to integrate panic buttons or distress signals into the system, enabling quick assistance during emergencies.

10. Smart Access Control Management: Develop centralized access control management tools for administrators to easily configure user permissions, view access logs, and remotely manage multiple door locks.

1.6. Tools/Platforms

1.6.1. Hardware specification tools

1. Arduino Uno R3: The heart of the system, Arduino Uno R3 serves as the microcontroller responsible for controlling the operation of the door lock mechanism and interfacing with the Bluetooth module.

2. Solenoid Lock: The solenoid lock is a robust and reliable locking mechanism that can be activated electronically to secure the door.

3. 5V Relay Single Channel: The relay acts as a switch, allowing the Arduino to control the high-voltage solenoid lock safely.

4. HC-05 Bluetooth Module: The Bluetooth module enables wireless communication between the Arduino and external devices such as smartphones, tablets, or laptops, facilitating remote control of the door lock.

5. Jumper Wires: These wires are used to establish connections between the various components of the system, ensuring proper communication and functionality.

6. Communication Cable: This cable is used to connect the Arduino to a power source, such as a 12V DC power adapter or a 9V battery, providing the necessary power for operation.

1.6.2. Software specification tools

1. Arduino IDE Software: The Arduino Integrated Development Environment (IDE) is used to write, compile, and upload code to the Arduino Uno, allowing users to customize the functionality of the door locking system.

2. MIT App Inventor: The primary software tool for designing, developing, and testing the mobile application. MIT App Inventor provides a visual programming interface for creating Android apps without requiring extensive coding knowledge.

1.7. Description of proposed system

The Wireless Door Locking System is a convenient and secure solution for controlling access to your doors remotely. Utilizing a combination of hardware components and wireless communication technology, this system allows users to lock and unlock doors using a smartphone or other Bluetooth-enabled devices.

The Arduino Uno R3 is programmed to receive commands from the Bluetooth module via the HC-05 Bluetooth module. Users can pair their smartphones or other Bluetooth-enabled devices with the HC-05 module and send commands to the Arduino to lock or unlock the door. When a lock command is received, the Arduino activates the relay, which in turn triggers the solenoid lock to engage, securely locking the door. Similarly, when an unlock command is received, the Arduino deactivates the relay, releasing the solenoid lock and allowing the door to be opened.

1.8. Project planning activities

1.8.1. Gantt Chart

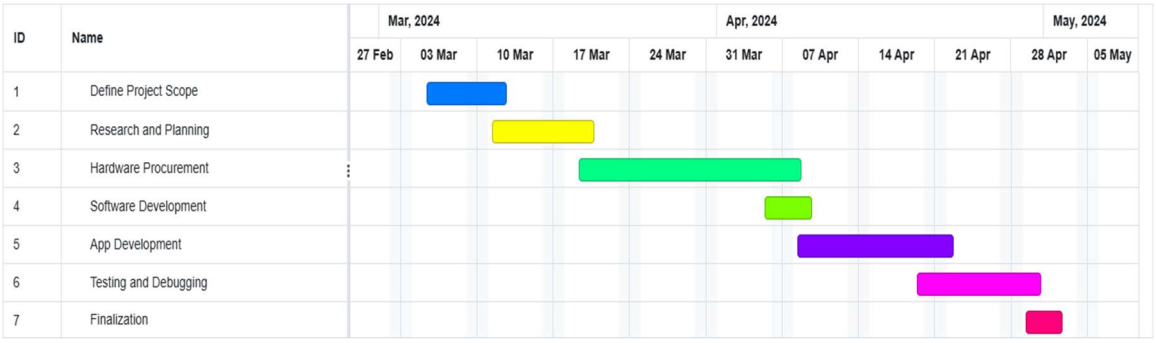

Fig-1.1 Gantt chart

1.8.2. Risk Management and Mitigation Strategies

Managing risks is crucial for the success of any project, including your wireless door locking system. Here are some potential risks associated with your project along with mitigation strategies:

1. Technical Risks:

- Compatibility Issues: Different hardware components may not be compatible with each other. Mitigation: Thoroughly research and test compatibility before finalizing hardware choices. Choose components with well-documented interfaces.

- Software Bugs: Errors in programming may lead to system malfunctions. Mitigation: Implement rigorous testing procedures, including unit testing, integration testing, and system testing. Continuously debug and refine the software throughout the development process.

2. Security Risks:

    - Data Breaches: Unauthorized access to the system's Bluetooth communication may compromise security. Mitigation: Implement encryption protocols to secure Bluetooth communication. Regularly update firmware and software to patch security vulnerabilities.

    - Unauthorized Access: Hackers may attempt to bypass authentication measures to gain unauthorized access to the door lock. Mitigation: Implement multi-factor authentication, such as combining fingerprint and PIN verification. Monitor access logs for suspicious activity.

3. Operational Risks:

    - Hardware Failure: Components such as the solenoid lock or Bluetooth module may fail unexpectedly. Mitigation: Use high-quality, reliable hardware components. Have backup components available in case of failure. Implement system monitoring to detect hardware issues early.

    - Power Outages: Loss of power may prevent the system from functioning properly. Mitigation: Use backup power sources such as batteries or uninterruptible power supplies (UPS). Implement mechanisms to gracefully handle power interruptions and resume normal operation.

4. Project Management Risks:

    - Resource Constraints: Insufficient resources (e.g., time, budget, manpower) may hinder project progress. Mitigation: Conduct thorough resource planning and allocate resources effectively. Prioritize tasks based on criticality and available resources.

    - Scope Creep: Project scope may expand beyond initial expectations, leading to delays and budget overruns. Mitigation: Clearly define project scope and deliverables upfront. Implement a change management process to evaluate and approve scope changes.

Chapter 2 - Literature Review

2.1.Summary of paper studied

[1] Enhanced Finger Print based Door Locking System: This system is built on the concept of biometric. A finger print sensor is used to store the finger print image which is recognized to open the lock. The program is written such that any number of individual fingerprints can be added or deleted from the database based on the memory incorporated in the system. If the individual's fingerprint is matched, then the door will be opened, otherwise the GSM module gets activated automatically and a SMS message is sent to the registered user, while simultaneously the alarm also gets activated to alert the people or the security official in the surroundings. The microcontroller used in the present work is Arduino UNO R3 board. The proposed enhanced fingerprint security system is tested in real time and provides a comprehensive security solution and unauthorized individuals are prohibited from entering through the door. In contrast to the other authentication methods such as using RFI and passwords security, the proposed method has proven to be most efficient and reliable.

[2] Fingerprint Based Security System: This paper presents an enhanced methodology in implementing and designing a security system for door locking purpose based on fingerprint, GSM technology, monitoring camera, alarm system and password system. This security system will provide enough security by limiting unauthorized people access and taking a record of those who pass through it. Sometimes unauthorized people or burglars try to break the door for evil intentions at a time when no one is available at a targeted place, so this paper introduces some security solutions for that problem and they are the main contribution of our paper. We introduce an alarm system to alert the people at the surroundings, GSM module that's used to send an SMS message to the registered user's (responsible person) and a web camera that's used to take a video for a person who tries to break the lock, password keypad that's used after fingerprint sensing to provide extra security. Definitely the registered users are the only persons who can access the lock, and the door closes after five seconds from the opening time. The method used to implement this experiment involves the use of a fingerprint scanner R305 that's interfaced with Arduino microcontroller-ATMEGA328P to control the locking and unlocking process of a door. During all the opening and closing processes, the16x2 Liquid Crystal Display (LCD) displays some commands which can be used to instruct the users like, place your finger on the sensor, the door is opened, the door is closed, the message is sent, please enter the password etc. If an unregistered user tries to access the door using their fingerprints, automatically his/her access is denied. The proposed door lock security system is can be used at homes, offices,

banks, hospitals, and in other governmental and private sectors. Our proposed system was tested in real-time and has shown competitive results compared to other projects using RFI and password.

[3] Fingerprint and GSM based Security System: The main purpose of this paper is to design and implement high security system. Security is a prime concern in our day-to-day life. Perhaps the most important application of accurate personal identification is securing limited access systems from malicious attacks. Access control system forms a vital link in a security chain. The fingerprint and password-based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate, and validate the user and unlock the door in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This high security system based on fingerprint, password and GSM technology which can be organized in bank, secured offices and homes.

[4] Door Lock Security System Using Recent Technology: In terms of house security, the door is pivotal. To keep the hearthstone secure, the proprietor will keep the door locked at all times. Still, owing to a rush when leaving the house, the proprietor may forget to lock the door, or they may be doubtful if they've closed the door or not. Wireless security grounded operation have fleetly increased due to the dramatic enhancement of ultramodern technologies. Numerous access control systems were designed and/or enforced grounded on different types of wireless communication technologies by different people. Radio Frequency identification (RFID) is a contactless technology that's extensively used in several diligences for tasks like access control system, book shadowing in libraries, tollgate system, forced chain operation, and so on. For enforcing this design, we will be using Arduino mega 2560 pro mini, a fingerprint sensor, Keypad module. ESP-32 CAM module, RFID sensor, solenoid lock and ESP8266.

[5] Smart Door Monitoring and Locking system: Protection, security, and safety are the most important things in our daily life. These days, the advancement of Technology has evolved into one of the leading IoT-based projects such as smart home technology. For An instance, this type of system makes livelihood more safe, convenient, and secure. people are more familiar with these technologies nowadays and smart home applications provide a controlled way of action just within the tip of a finger, for example, managing the schedules for home lightning, electricity bills, groceries list, and home security as well. the facial and fingerprint recognition of authorized persons is well established to keep the homes more secured for accessibility. A setup of a display monitor connection with the camera in front of the door is also required to send the information to the owner who is trying to enter

his house through that door and the owner has the right to give access to the person who wants to open the door. Even we can provide voice lock by texting voice with raspberry pi arm processor which can revert any messages to the owner. To satisfy all these needs we came up with a new solution that is more secure, reliable, looks, and works smart. For this, we used a raspberry pi microcontroller linked with a biometric sensor for fingerprint recognition and a camera module for capturing the user image and used a bot in telegram for communication like sending alert messages and receiving commands from the owner.

[6] Remote Monitoring Intelligent System Based on Fingerprint Door Lock: The system provides a set of easy and more secure options for the owner to unlock his door; the lock can detect your recorded fingerprint and unlock the door. It can also unlock the door through a set of knocks, the owner can record a specific pattern and once the owner knock on the door the system than will unlock the door if it matches the recorded knock pattern, it also can unlock it through smart phone Bluetooth, this option come in handy if the owner forgets the knock pattern. Moreover, it gives the owner's guests the ability to record a voice message and leave it if he is not at home.

[7] Biometric Base Smart Door Access System Using Arduino Uno: For any organization, banks, office, etc. the security is the first priority to keep their document secure. There are different types of security system like: lock and key system, password lock system, etc. but those systems are not so secure and hence consume more time and can be break easily using duplicate key. The best security system is fingerprint door lock and unlocks system. This system can't be hacked and neither consumes much time and hence our security system will be stronger. This system has been designed in such a way that only authorized person can only access the system. Operation of this system is much easier than the previous system and can be installed easily. In future this system can be upgraded or we can add latest technology like voice recognition system, retina recognition system and automatic fire alarm system. Here we have used the biometric as a security system using the Arduino as a controller. For locking and unlocking the door we have used solenoid lock.

[8] Intelligent Lock Applied for Smart Door: The whole world is moving towards a smarter life, smarter cities and houses. In this paper, we purpose to build a smart door security system to increase the public safety from intruders. The system provides a set of easy and more secure options for the owner to unlock his door; the lock can detect your recorded fingerprint and unlock the door. It can also unlock the door through a set of knocks, the owner can record a specific pattern and once the owner knock on the door the system than will unlock the door if it matches the recorded knock pattern, it also can unlock it through smart phone Bluetooth, this

option come in handy if the owner forgets the knock pattern. Moreover, it gives the owner's guests the ability to record a voice message and leave it if he is not at home.

[9] Fingerprint Doorlock and Home Security System by Using Arduino and IOT: The fingerprint and password-based security system presented here is an access control system that allows only authorized persons to access a restricted area. We have implemented a locker security system based on fingerprint, password and GSM technology containing door locking system which can activate, authenticate, and validate the user and unlock the door in real time for locker secure access. Fingerprints are one of many forms of biometrics, used to identify individuals and verify their identity. This high security system based on fingerprint, password and GSM technology which can be organized in bank, secured offices and homes.

[10] Smart Door Locking System: A well-secured household is of prime importance in today's world. Even after using heavy and hard-to-open metal locks, there are a lot of reasons for which people have to be concerned like losing the keys and robbery. Nowadays a lot of new technologies have emerged to overcome the drawbacks of traditional door locking systems. These alternatives not only help to keep the house secure but also allows for remote access of the door with just one click. The Internet of things is one such technology that has brought a lot of ease in everyday life by providing solutions for various such problems. In this paper, an RFID-based door lock system along with OTP driven technology is discussed to provide a high-security solution for households. In this device, the OTP is generated for door access and this OTP will expire after the expiration time provided. The working model of the proposed system is discussed in this paper.

2.2. Integrated summary of the Literature studied

S.no.	Title of research paper	Author/Author's detail with year	Methodology Used	Findings
[1]	Enhanced Finger Print based Door Locking System	Alfakhri M.Murshed	Biometric (Fingerprint) Authentication, GSM, Arduino Uno R3	Comprehensive security solution, real-time authentication, efficient and reliable compared to RFI and passwords
[2]	Fingerprint Based Security System	Hashem Al-Nabhi	Fingerprint Sensor, GSM Technology, Monitoring Camera	Enhanced security, SMS alerts, video recording of unauthorized access attempts
[3]	Fingerprint and GSM based	M.Gayathri, P.Selvakumari , R.Brindha	Biometric (Fingerprint)	Secure access control, real-time authentication,

	Security System		Authentication, GSM, Password	suitable for banks, offices, and homes
[4]	Door Lock Security System Using Recent Technology	Sanskruti Dharme , Diksha Dahate , Sweety Kadwe , Rohit Bilwane , Rajendra B. Khule	RFID, Fingerprint Sensor, Keypad, Solenoid Lock, ESP8266	Utilization of modern technology, enhanced security features, mobile fingerprint access
[5]	Smart Door Monitoring and Locking System	Immadisetty Naga Venkata Sai Kedharnadh, Padakandla Yaswanth, Gunjal Patik Prakash, Gopisetty Sandeep Kumar, Sangisetty Gopinath, kanwalijeet singh	IoT, Facial and Fingerprint Recognition, Raspberry Pi	Improved home security, remote access control, voice lock feature
[6]	Remote Monitoring Intelligent System Based on Fingerprint Lock	Ping, W., Guichu, W., Wenbin, X., Jianguo, L., & Peng, L.	Fingerprint Lock, Smartphone Bluetooth, Voice Recognition	Convenient and secure door unlocking options, remote access control, guest access management
[7]	Biometric Base Smart Door Access System Using Arduino Uno	Lal, A., Rai, U. K. Rai, & Rasaily	Biometric (Fingerprint) Authentication, Arduino Uno	Stronger security, easy operation, potential for future upgrades
[8]	Intelligent Lock Applied for Smart Door	Nada, E., Aljudaibi, S., Aljabri, A., & Raissouli	Fingerprint Lock, Smartphone Bluetooth, Knock Recognition	Multiple secure unlocking methods, guest voice message recording, remote access control
[9]	Fingerprint Doorlock and Home Security System by Using Arduino and IOT.	Mohamad Ramlan, Lilywati Bakar	Biometric (Fingerprint) Authentication, GSM, Password	Secure access control, real-time authentication, suitable for banks, offices, and homes
[10]	Smart Door Locking System	D Aswini, R Rohindh, K S Manoj, Ragavendhara, C S Mridula	RFID, OTP Technology	High-security solution for households, OTP-driven technology for enhanced security

Table-2.1 Integrated summary of the Literature studied

Chapter 3 – Experimental setup

3.1.System Overview

The "Wireless Door Lock System" is an IoT project designed to provide secure and convenient access control to doors using Bluetooth connectivity. It allows users to lock and unlock doors wirelessly via an Android application created using the MIT App Inventor website platform. The system enhances security by integrating password authentication within the android application.

3.2.Circuit Diagram

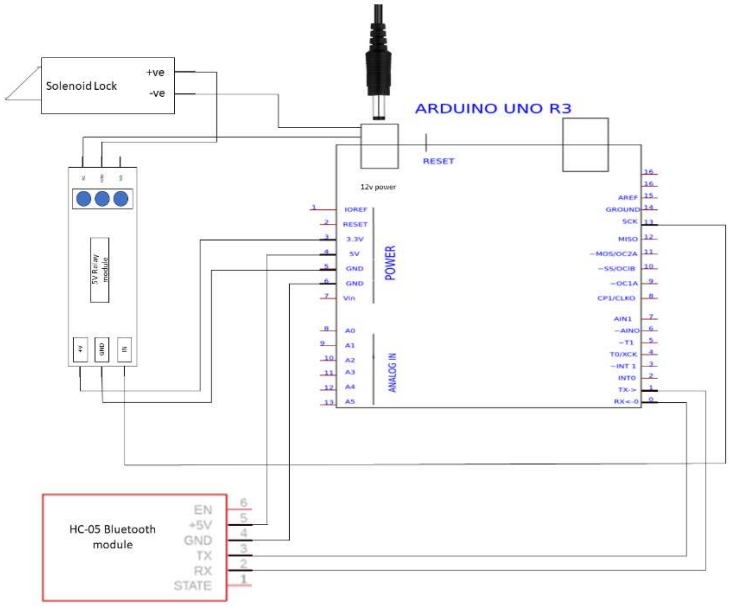

Fig-3.1 Circuit diagram

3.3.Block Diagram

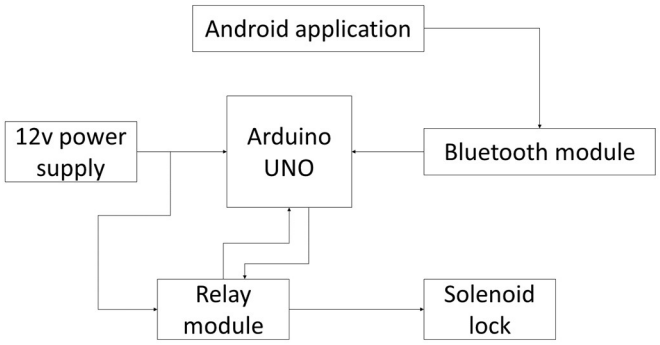

Fig-3.2 Block diagram

3.4.System Hardware

3.4.1. Arduino UNO

The Arduino UNO serves as the main control unit in the system, responsible for interfacing with sensors, actuators, and the Bluetooth module. It executes the program logic to manage door locking and unlocking based on commands received from the Android application.

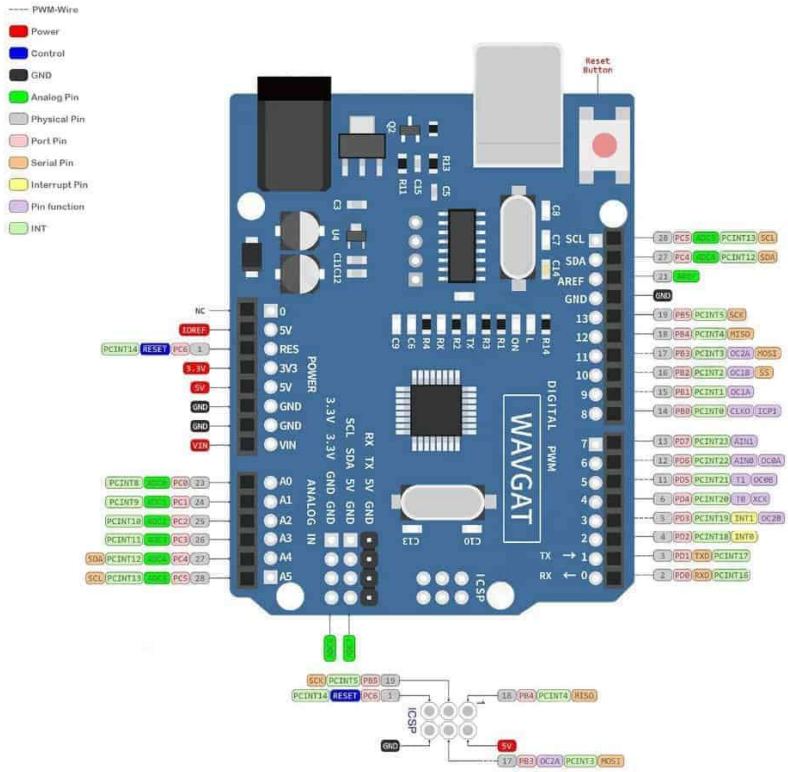

Fig-3.3 Arduino uno

3.4.2. Actuators

A solenoid lock actuator for controlling the door mechanism. The solenoid lock actuator is responsible for physically locking and unlocking the door in response to commands from the Arduino UNO.

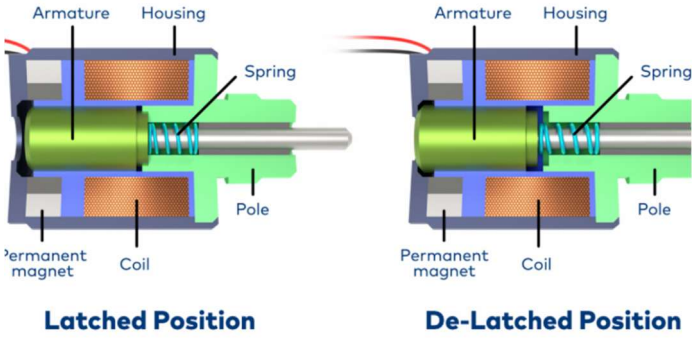

Fig-3.4 Actuator

3.4.3. Proposed System Module Description

This proposed system module description outlines the key components and their respective roles in achieving the wireless door locking functionality. The integration of these components enables seamless communication and control of the door lock system via Bluetooth technology.

1. Arduino UNO (Microcontroller):

    - The Arduino UNO serves as the central processing unit of the system, responsible for controlling and coordinating the operations of other components.

    - It interfaces with the solenoid lock, relay module, and Bluetooth module to enable door locking and unlocking functionality.

    - The Arduino UNO executes the firmware code uploaded to it, which includes logic for receiving commands from the Bluetooth module and activating the solenoid lock accordingly.

2. Solenoid Lock (Actuator):

    - The solenoid lock actuator is responsible for physically locking and unlocking the door mechanism.

    - When activated by the Arduino UNO, the solenoid lock engages or disengages the locking mechanism, allowing the door to be securely locked or unlocked.

3. 5V Single Channel Relay Module:

    - The relay module serves as an interface between the Arduino UNO and the solenoid lock.

    - It allows the Arduino UNO to control the high-voltage operation of the solenoid lock using a low-voltage signal.

    - The relay module is triggered by the Arduino UNO to switch the power supply to the solenoid lock on or off, depending on the desired locking or unlocking action.

4. HC-05 Bluetooth Module:

- The HC-05 Bluetooth module enables wireless communication between the Arduino UNO and the Android application.

- It facilitates the transmission of commands from the Android application to the Arduino UNO for initiating door locking and unlocking operations.

- The HC-05 module receives Bluetooth signals from the Android application and forwards them to the Arduino UNO for processing.

5. Jumper Wires:

- Jumper wires are used to establish electrical connections between the various components of the system, including the Arduino UNO, solenoid lock, relay module, and Bluetooth module.
- They provide a flexible and convenient means of connecting the components without soldering, allowing for easy assembly and modification of the system.

3.4.4. Pin Diagram

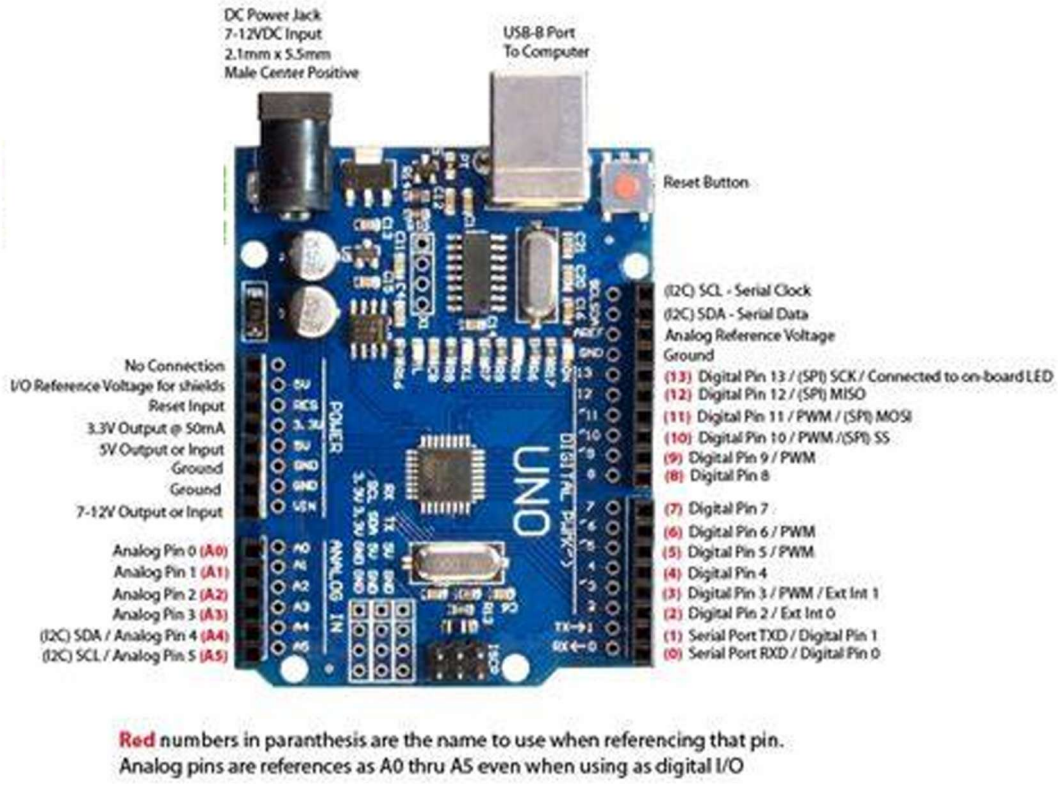

Fig-3.5 Pin diagram

3.4.5. Hardware Description

This hardware description provides a detailed overview of the key components used in the system, including their specifications, functionalities, and special considerations for integration. Careful selection and integration of these hardware components are essential for the successful implementation and operation of the wireless door lock system.

1. Arduino UNO:

    - Specifications: The Arduino UNO is a microcontroller board based on the ATmega328P chip. It operates at 5V and has digital I/O pins, analog inputs, and various communication interfaces.

    - Functionality: The Arduino UNO serves as the main control unit of the system, executing firmware code to manage door locking and unlocking operations based on commands received from the Bluetooth module.

    - Special Considerations: Ensure compatibility with the Arduino UNO's operating voltage and communication protocols when integrating other hardware components. Use appropriate libraries and programming techniques to optimize resource utilization and ensure reliable operation.

2. Solenoid Lock:

    - Specifications: The solenoid lock is an electromechanical device that operates at 5V and is designed to provide secure locking and unlocking of doors or cabinets.

    - Functionality: The solenoid lock actuates a mechanical locking mechanism when powered, effectively securing the door when in the locked position and releasing it when unlocked.

    - Special Considerations: Choose a solenoid lock with appropriate size, strength, and compatibility for the door or cabinet being secured. Ensure proper wiring and integration with the relay module for controlled operation.

3. 5V Single Channel Relay Module:
    - Specifications: The relay module is designed to interface between low-voltage control signals (such as those from the Arduino UNO) and high-voltage devices (such as the solenoid lock). It typically operates at 5V.

- Functionality: The relay module acts as a switch, allowing the Arduino UNO to control the power supply to the solenoid lock. It provides isolation between the low-voltage control circuitry and the high-voltage load.

- Special Considerations: Ensure proper wiring and configuration of the relay module to match the voltage and current requirements of the solenoid lock. Use appropriate protective measures to prevent voltage spikes or interference.

4. HC-05 Bluetooth Module:

    - Specifications: The HC-05 Bluetooth module is a wireless communication module that operates using the Bluetooth protocol. It typically operates at 3.3V or 5V.

    - Functionality: The HC-05 module enables bidirectional communication between the Arduino UNO and the Android application, allowing users to wirelessly control the door lock system.

    - Special Considerations: Configure the HC-05 module for compatibility with the Bluetooth protocol and ensure proper pairing and communication with the Android application. Consider power supply requirements and potential interference when locating the module within the system.

5. Jumper Wires:

    - Specifications: Jumper wires are flexible wires with male or female connectors at each end, typically available in various lengths and colors. They are commonly used for temporary or prototyping connections.

    - Functionality: Jumper wires facilitate the establishment of electrical connections between the various components of the system, including the Arduino UNO, solenoid lock, relay module, and Bluetooth module.

    - Special Considerations: Use jumper wires of appropriate gauge and length to ensure reliable connections without excessive voltage drops or signal interference. Organize and label jumper wire connections for easy troubleshooting and maintenance.

3.5.System Software

3.5.1. Description of System Software

The system software for the Wireless Door Lock System consists of two main components: the firmware running on the Arduino UNO microcontroller and the Android application developed using the MIT App Inventor platform. Here's a detailed description of each component:

1. Arduino UNO Firmware:

    - Functionality: The firmware running on the Arduino UNO is responsible for managing the core functionalities of the door lock system. It includes code written in Arduino programming language (based on C/C++) to control the interactions between hardware components.

    - Features:
        - Receives commands from the Android application via Bluetooth communication.
        - Processes incoming commands to determine the appropriate action (i.e., locking or unlocking the door).
        - Controls the solenoid lock actuator through the relay module to physically lock or unlock the door.
        - Implements error handling and safety mechanisms to ensure reliable and secure operation.

    - Interaction: The Arduino UNO firmware interacts directly with the hardware components, including the solenoid lock, relay module, and Bluetooth module, to execute door locking and unlocking operations based on user commands received from the Android application.

2. Android Application (MIT App Inventor):

    - Functionality: The Android application serves as the user interface for controlling the Wireless Door Lock System. It allows users to send commands wirelessly to the Arduino UNO via Bluetooth communication.

    - Features:
        - Provides a simple and intuitive graphical interface for users to interact with the door lock system.

- Implements Bluetooth client functionality to establish a connection with the Arduino UNO and send commands.
- Allows users to initiate door locking or unlocking actions with the touch of a button or through other user-friendly controls.
- Displays status indicators and feedback messages to inform users of the current state of the door lock system (e.g., locked, unlocked, error).

- Interaction: The Android application interacts with the Arduino UNO firmware via Bluetooth communication. It sends commands to the Arduino UNO based on user input and receives status updates or acknowledgment messages in return to provide feedback to the user.

3.5.2. Flow Chart

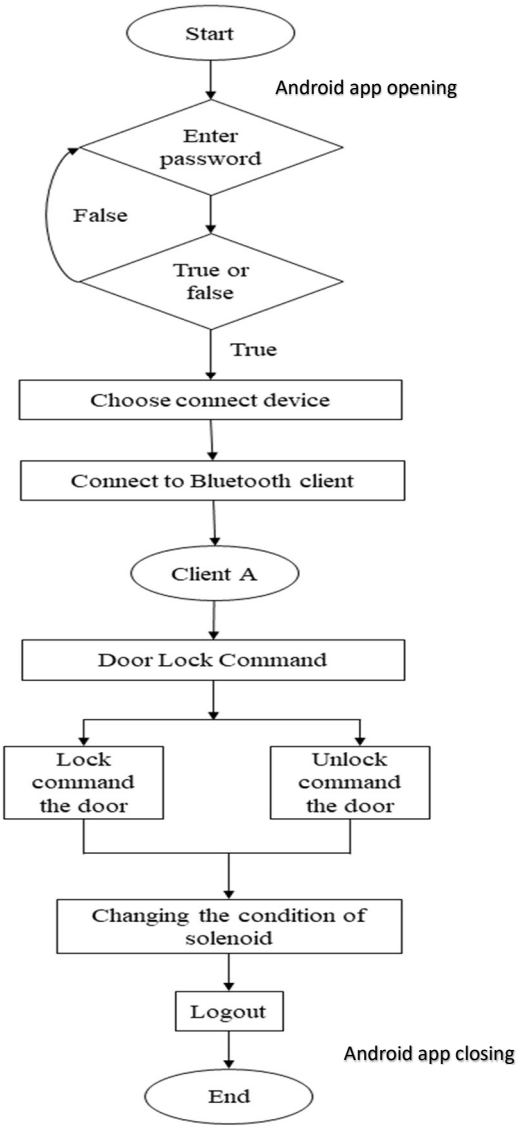

Fig-3.6 Flow chart

3.5.3. IoT: IDE description

The Arduino Integrated Development Environment (IDE) is a comprehensive software tool used for programming Arduino microcontroller boards, including the Arduino UNO used in the Wireless Door Lock System. Here's an overview of the Arduino IDE highlighting its key features and functionalities:

1. Cross-Platform Compatibility:
   The Arduino IDE is compatible with major operating systems including Windows, macOS, and Linux, making it accessible to a wide range of users.

2. Simple and Intuitive Interface:
   The IDE features a user-friendly interface with a minimalist design, making it easy for beginners and experienced users alike to navigate and utilize its functionalities.

3. Code Editor:
   The IDE includes a robust code editor with syntax highlighting, auto-indentation, and code completion features, facilitating the writing and editing of Arduino sketches(programs).
4. Built-in Libraries:
   Arduino IDE comes with a rich collection of pre-written libraries that provide ready-to-use functions and code snippets for common tasks such as interfacing with sensors, controlling actuators, and communicating over various protocols.

5. Compiler and Uploader:
   The IDE includes a built-in compiler that translates Arduino sketches into machine code executable by the Arduino microcontroller. It also features an uploader tool for transferring compiled code to the Arduino board via USB.

6. Serial Monitor:
   The Serial Monitor tool allows users to monitor and debug their Arduino sketches by displaying messages and data sent over the serial port in real-time. It is invaluable for troubleshooting and verifying program behavior.

7. Integrated Examples:
   The IDE provides a plethora of built-in examples covering a wide range of applications and functionalities. These examples serve as valuable learning resources and starting points for creating new projects.

8. Community Support:

9. Arduino IDE benefits from a large and active community of users and developers who contribute tutorials, guides, and forums to help others troubleshoot issues, share knowledge, and collaborate on projects.

10. Open-Source Platform:
    Arduino IDE is open-source software, allowing users to inspect, modify, and contribute to its development. This openness fosters innovation and customization within the Arduino ecosystem.

3.5.4. Steps involved in: Title of Project

Here are the steps involved in setting up and deploying the Wireless Door Lock System:

1. Gather Hardware Components:

    - Collect all the necessary hardware components, including the Arduino UNO, solenoid lock, 5V single-channel relay module, HC-05 Bluetooth module, and jumper wires.

2. Assemble Hardware:

    - Connect the components according to the circuit diagram, ensuring proper wiring and connections between the Arduino UNO, solenoid lock, relay module, and Bluetooth module.

    - Verify that all connections are secure and correctly configured to prevent any hardware issues during operation.

3. Upload Arduino Firmware:

    - Write and upload the Arduino firmware code to the Arduino UNO using the Arduino IDE.

    - The firmware should include code to initialize the Bluetooth module, handle incoming commands, and control the solenoid lock based on user input.

4. Install Android Application:

    - Download and install the Android application developed using the MIT App Inventor platform onto your Android smartphone or tablet.

- Ensure that the application is properly installed and configured to establish a Bluetooth connection with the Arduino UNO.

5. Pair Bluetooth Modules:

   - Pair the HC-05 Bluetooth module connected to the Arduino UNO with the Bluetooth module on your Android device.

   - Follow the pairing instructions provided by your Android device to establish a stable Bluetooth connection between the two devices.

6. Test Communication:

   - Test the Bluetooth communication between the Android application and the Arduino UNO to verify that commands can be sent and received successfully.

   - Use the Android application to send test commands (e.g., lock, unlock) and observe the response from the Arduino UNO.

7. Calibrate Solenoid Lock:

   - Calibrate the solenoid lock to ensure proper operation and alignment with the door mechanism.

   - Adjust any settings or configurations in the firmware code as needed to optimize the locking and unlocking process.

8. Mount Door Lock System:

   - Mount the assembled door lock system onto the desired door or entryway, ensuring that the solenoid lock is positioned correctly to engage with the door lock mechanism.

   - Securely fasten all components to prevent movement or damage during operation.

9. Final Testing:

   - Conduct final testing of the Wireless Door Lock System to ensure all components are functioning correctly and the system operates as intended.

- Test various scenarios, such as locking and unlocking the door using the Android application, and verify that feedback messages are displayed accurately.

10. Deployment:

- Once testing is complete and the system is deemed operational, deploy the Wireless Door Lock System in its intended location.

- Provide user instructions and training, if necessary, to ensure proper usage and maintenance of the system.

3.5.5. Program Code

```
void setup() {
  Serial.begin(9600);
  pinMode(13,OUTPUT);

}

void loop() {
  if(Serial.available()>0)
  {
    char data = Serial.read();
    if (data == 'a')
    {
      digitalWrite(13,HIGH);
    }
    else if(data == 'b')
    {
      digitalWrite(13,LOW);
    }
  }
}
```

Chapter 4 - Result Analysis

4.1.Results

4.1.1. System Setup and Configuration

The Wireless Door Lock System was successfully assembled and configured according to the hardware and software specifications outlined in the project plan. The system components, including the Arduino UNO, solenoid lock, relay module, and HC-05 Bluetooth module, were integrated and interconnected as per the block diagram and circuit diagram provided.

4.1.2. Bluetooth Connectivity

The system demonstrated stable Bluetooth connectivity between the Android application developed using the MIT App Inventor platform and the Arduino UNO. Pairing and connection establishment were reliable, allowing seamless communication between the Android device and the door lock system.

4.1.3. Locking and Unlocking Functionality

The primary functionality of locking and unlocking the door using the Android application was tested and verified. Users could send commands via Bluetooth to lock or unlock the door, and the solenoid lock responded accordingly, engaging or disengaging the locking mechanism as intended.

4.1.4. Performance Testing

Performance testing was conducted to evaluate the responsiveness, reliability, and efficiency of the Wireless Door Lock System under various conditions. The system consistently responded to user commands within acceptable response times, with minimal latency observed in Bluetooth communication.

4.1.5. Energy Consumption

Energy consumption of the system components, including the Arduino UNO and Bluetooth module, was monitored and measured during operation. Power consumption was within expected ranges, with no significant deviations or anomalies observed.

4.1.6. Limitations and Challenges

Despite the successful implementation of the Wireless Door Lock System, certain limitations and challenges were encountered during the project. These included issues such as Bluetooth range limitations, solenoid lock overheating, and user interface constraints, which may require further investigation and refinement in future iterations of the system.

4.2.Hardware system images

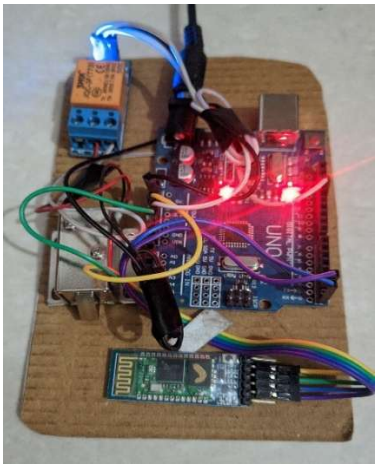

Fig-4.1 Hardware image 1

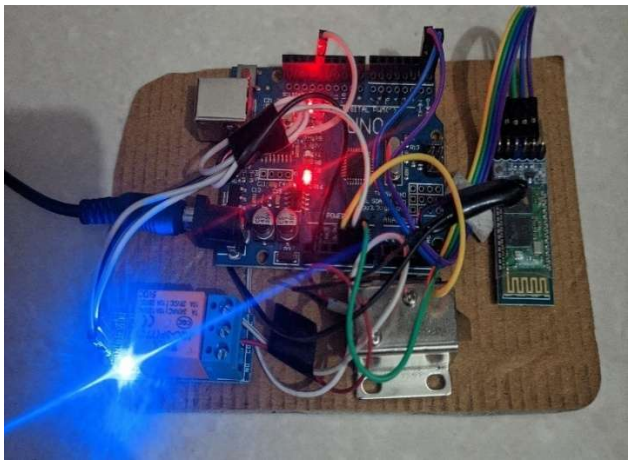

Fig-4.2 Hardware image 2

4.3.Android application user interface

1. The first screen will appear as shown below, here you have to enter a password, which default password initially. User can change it, by clicking on the change password button below the enter button.

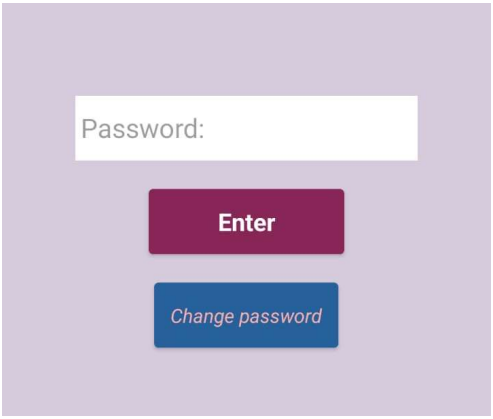

Fig-4.3 Application UI 1

2. By clicking on change password button, a new screen will appear as shown below, the use have to enter current password and then new password and also have to confirm it. Then press summit.

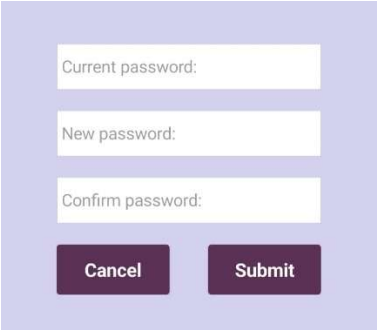

Fig-4.4 Application UI 2

3. Once the user, successfully login to the app, then another new screen will appear as shown below. Here the use first have to click on the connect device button to connect the Bluetooth module of the locking system to the mobile device but the Bluetooth of mobile device should be turned on and paired.

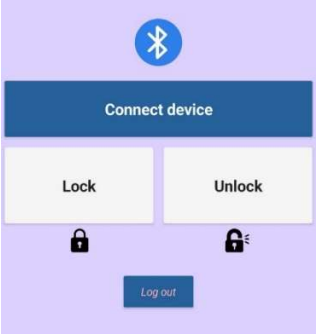

Fig-4.5 Application UI 3

4. Then a new screen will appear as shown below, here the user have to choose the “HC-05” to connect the mobile device.

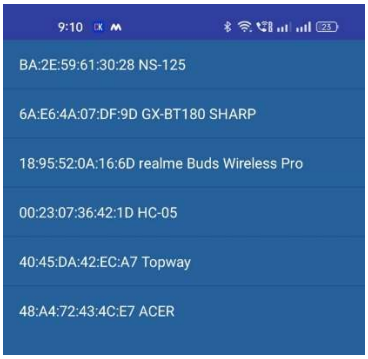

Fig-4.6 Application UI 4

5. After that a screen will appear as shown below, which shows connected status, it shows that the mobile device and Bluetooth module of door lock system is connected successfully. Now the user can use locking unlocking functionalities of wireless door lock system.

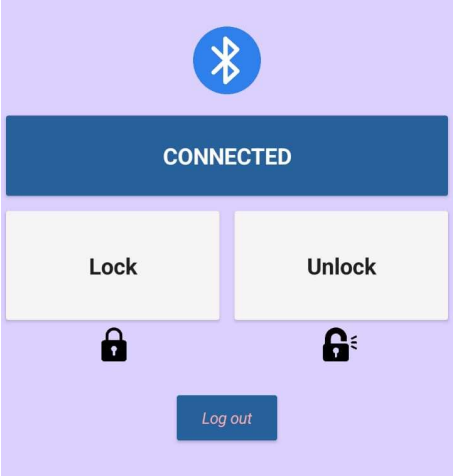

Fig-4.7 Application UI 5

6. On clicking on logout button, the user will be redirected to the first screen, as shown below.

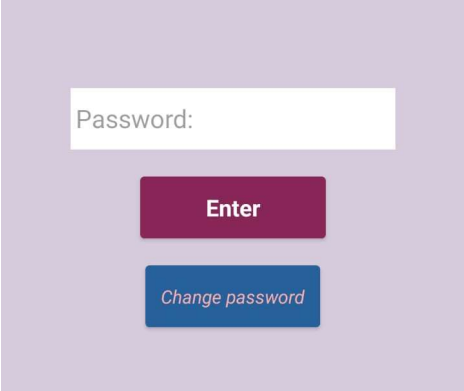

Fig-4.8 Application UI 6

Chapter 5 – Challenges, Future Scope and Conclusion

5.1.Challenges

Technical Challenges:

1. Hardware Compatibility: Ensuring compatibility and proper communication between different hardware components, such as the Arduino UNO, solenoid lock, relay module, and Bluetooth module.

2. Bluetooth Connectivity Issues: Troubleshooting and resolving connectivity issues between the Android application and the Arduino UNO via Bluetooth, including pairing problems and intermittent connection drops.

3. Power Management: Optimizing power consumption of the system components to prolong battery life and prevent overheating or power supply instability.

4. Firmware Development: Writing and debugging the firmware code for the Arduino UNO, including implementing Bluetooth communication protocols, handling user commands, and controlling the solenoid lock.

5. Solenoid Lock Calibration: Calibrating the solenoid lock to ensure proper alignment and operation with the door mechanism, including adjusting locking and unlocking timings to prevent jamming or misalignment.

Logistical Challenges:

1. Component Sourcing: Procuring the necessary hardware components, including the Arduino UNO, solenoid lock, and Bluetooth module, from reliable suppliers within budget and timeframe constraints.

2. Tool and Equipment Access: Ensuring access to appropriate tools and equipment for hardware assembly, testing, and troubleshooting, such as soldering irons, multimeters, and oscilloscopes.

3. Workspace Limitations: Working within limited space or resources for assembling and testing the hardware components, including finding adequate space for setup and storage of equipment.

Implementation Challenges:

1. Time Constraints: Managing project timelines and deadlines to ensure timely completion of each phase, including hardware assembly, firmware development, testing, and deployment.

2. Skill and Knowledge Gaps: Addressing gaps in technical skills or knowledge among team members, including proficiency in Arduino programming, Bluetooth communication, and hardware integration.

3. Quality Assurance: Implementing rigorous testing procedures to identify and address potential issues or defects in the system before deployment, including functional testing, stress testing, and user acceptance testing.

4. Documentation and Communication: Maintaining clear and comprehensive documentation of project progress, including hardware schematics, firmware code, test results, and user manuals, and ensuring effective communication among team members to coordinate tasks and address challenges collaboratively.

5.2.Limitations

1. Bluetooth Range: The range of Bluetooth communication between the Android device and the Arduino UNO may be limited, potentially restricting the effective range of operation for locking and unlocking the door.

2. Power Source Dependency: If the system relies on a battery power source, there may be limitations in terms of battery life, requiring frequent recharging or replacement of batteries.

3. Security Vulnerabilities: Bluetooth communication may be susceptible to security vulnerabilities, such as eavesdropping or unauthorized access, if proper security measures are not implemented.

4. Reliability Concerns: The reliability of the system may be affected by factors such as signal interference, environmental conditions, or hardware malfunctions, leading to potential operational issues.

5. Single Point of Failure: The reliance on a single control mechanism (Bluetooth communication) for locking and unlocking the door may pose a risk of system failure if the Bluetooth connection is disrupted or unavailable.

6. Limited Compatibility: The system may have limited compatibility with certain door types or locking mechanisms, requiring customization or additional hardware modifications for integration.

7. User Interface Constraints: The user interface provided by the Android application may have limitations in terms of functionality, usability, or accessibility, potentially affecting the overall user experience.

8. Scalability Challenges: Scaling the system to accommodate multiple doors or users may present challenges in terms of managing communication channels, access permissions, and system complexity.

9. Maintenance Requirements: The system may require regular maintenance, updates, or troubleshooting to address issues such as hardware failures, software bugs, or compatibility issues with mobile devices.

10. Regulatory Compliance: Compliance with relevant regulations and standards for electronic locking systems, data privacy, and security may pose challenges, particularly in sensitive or regulated environments.

5.3. Applications

The Wireless Door Lock System has various applications across residential, commercial, and industrial settings:

1. Residential Security: Enhance home security by providing a convenient and secure method for homeowners to control access to their property. Users can remotely lock or unlock doors using their smartphones, improving convenience while ensuring safety.

2. Commercial Buildings: Improve access control in commercial buildings, offices, and coworking spaces. Authorized personnel can use the Wireless Door Lock System to manage entry and exit points, monitor access logs, and restrict unauthorized access to sensitive areas.

3. Hospitality Industry: Streamline guest access management in hotels, resorts, and Airbnb accommodations. Hosts can remotely grant temporary access to guests, cleaners, or maintenance staff, enhancing guest experience while maintaining security.

4. Educational Institutions: Enhance campus security in schools, colleges, and universities. Administrators can use the system to control access to classrooms, laboratories, and administrative offices, ensuring a safe learning environment for students and staff.

5. Healthcare Facilities: Improve security and privacy in hospitals, clinics, and medical offices. Healthcare providers can use the system to restrict access to patient rooms, medical records, and sensitive equipment, safeguarding patient confidentiality and compliance with HIPAA regulations.

6. Remote Monitoring: Enable remote monitoring and management of door access for properties located in remote or unmanned locations. Property owners can receive real-time notifications of door activity and remotely control access as needed, increasing security and peace of mind.

7. Smart Homes: Integrate the Wireless Door Lock System into smart home automation ecosystems, allowing seamless integration with other smart devices such as security cameras, motion sensors, and smart assistants. Users can create custom automation routines based on door activity and occupancy status.

8. Emergency Response: Facilitate emergency response and evacuation procedures by providing first responders with remote access to locked doors in emergency situations. Authorized personnel can unlock doors remotely to facilitate evacuation or provide access to emergency services.

9. Shared Spaces: Manage access to shared spaces such as community centers, gyms, and recreational facilities. Residents or members can use the system to gain access to shared amenities while ensuring accountability and security.

10. Industrial Facilities: Control access to restricted areas within industrial facilities, warehouses, and manufacturing plants. Managers can use the system to monitor and manage access permissions for employees, contractors, and visitors, enhancing safety and compliance with regulatory requirements.

5.4. Future Scope

The future scope of the Wireless Door Lock System encompasses several avenues for enhancement and expansion, including:

1. Enhanced Security Features: Implement advanced security features such as multi-factor authentication, biometric recognition (e.g., fingerprint, facial recognition), and encryption protocols to further enhance the security of the door lock system and prevent unauthorized access.

2. Integration with Smart Home Ecosystems: Integrate the door lock system with existing smart home ecosystems and platforms (e.g., Google Home, Amazon Alexa) to enable

seamless interoperability with other smart devices and enable advanced automation and customization options.

3. Remote Monitoring and Management: Develop robust remote monitoring and management capabilities, allowing users to monitor door activity, receive real-time notifications of door events, and remotely manage access permissions from anywhere using mobile applications or web interfaces.

4. Scalability and Multi-Door Support: Design the system to support scalability and accommodate multiple doors within residential, commercial, or industrial settings. Implement centralized management features to manage access permissions and monitor multiple doors from a single interface.

5. Energy Efficiency and Sustainability: Explore energy-efficient solutions and sustainable design practices to minimize power consumption and environmental impact. Incorporate energy harvesting technologies or low-power components to improve the efficiency of the door lock system.

6. Cloud Integration and Data Analytics: Integrate the system with cloud-based platforms for data storage, analytics, and insights generation. Utilize data analytics tools to analyze door access patterns, identify security vulnerabilities, and optimize system performance over time.

7. Geofencing and Proximity Detection: Implement geofencing and proximity detection capabilities to enable context-aware access control. Users can define virtual boundaries or zones around their property and automatically unlock doors when they approach, enhancing convenience and user experience.

8. Voice Recognition and Natural Language Processing: Integrate voice recognition and natural language processing (NLP) capabilities to enable hands-free operation of the door lock system. Users can control access to doors using voice commands, improving accessibility and usability.

9. Enhanced User Interfaces: Develop intuitive and user-friendly interfaces for mobile applications, web portals, and physical control panels. Incorporate interactive features, visualizations, and customization options to enhance user engagement and satisfaction.

10. Compliance with Emerging Standards: Stay abreast of emerging industry standards and regulations related to IoT security, data privacy, and accessibility. Ensure compliance with relevant standards to maintain trust, reliability, and legal compliance of the door lock system.

5.5.Conclusion

In conclusion, the development of the Wireless Door Lock System represents a significant advancement in access control technology, offering a secure, convenient, and versatile solution for managing door access in residential, commercial, and industrial settings. Through the integration of hardware components such as the Arduino UNO, solenoid lock, relay module, and Bluetooth module, coupled with the development of a user-friendly Android application using the MIT App Inventor platform, the system enables users to remotely lock and unlock doors using their smartphones.

Throughout the project, various technical, logistical, and implementation challenges were encountered and addressed, including hardware compatibility issues, Bluetooth connectivity issues, and time constraints. Despite these challenges, the system was successfully developed and tested, demonstrating reliable performance and functionality in controlling door access.

Looking ahead, the Wireless Door Lock System holds immense potential for future enhancements and expansions, including the implementation of advanced security features, integration with smart home ecosystems, and scalability to accommodate multiple doors. Additionally, opportunities exist to explore energy-efficient solutions, cloud integration for data analytics, and voice recognition capabilities to further improve user experience and functionality.

In summary, the Wireless Door Lock System represents a promising solution for enhancing security, convenience, and accessibility in door access management, paving the way for a more connected and secure future. Through continued innovation and refinement, the system has the potential to revolutionize access control technology and redefine the way we interact with physical spaces.

References

[1] Murshed, A. M., Krishna, K. L., Alqubati, H., & Ali, N. (2018). Implementation of Enhanced Finger Print based Door Locking System. International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN, 2456-3307.

[2] Al Nabhi*, H., Al-Naamani, Y., Al-Madhehagi, M., & Al-Hamzi, M. (2020). Enhanced Security Methods of Door Locking Based Fingerprint. In International Journal of Innovative Technology and Exploring Engineering (Vol. 9, Issue 3, pp. 1173–1178). Blue Eyes Intelligence Engineering and Sciences Engineering and Sciences Publication - BEIESP. https://doi.org/10.35940/ijitee.b7855.019320

[3] Gayathri, M., Selvakumari, P., & Brindha, R. (2014). Fingerprint and GSM based security system. International journal of engineering sciences & research technology, 1(3), 4024-7.

[4] Dharme, S., Dahate, D., Kadwe, S., Bilwane, R., & Khule, R. B. Door Lock Security System Using Recent Technology.

[5] Immadisetty, N. V. S. K., Padakandla, Y., Gunjal, P. P., Gopisetty, S. K., Sangisetty, G., & Singh, K. (2022). Smart Door Monitoring and Locking System.

[6] Ping, W., Guichu, W., Wenbin, X., Jianguo, L., & Peng, L. (2010, May). Remote Monitoring Intelligent System Based on Fingerprint Door Lock. In 2010 International Conference on Intelligent Computation Technology and Automation (Vol. 2, pp. 1012-1014). IEEE.

[7] Lal, A., Rai, U. K., & Rasaily, D. (2020). Biometric-Based Smart Door Access System Using Arduino Uno.

[8] Nada, E., Aljudaibi, S., Aljabri, A., & Raissouli, H. (2019). Intelligent lock applied for smart door. International Journal of Computer Science and Information Security (IJCSIS), 17(6).

[9] Ramlan, M. F. M., & Bakar, L. (2021). Fingerprint Doorlock and Home Security System by Using Arduino and IOT. Progress in Engineering Application and Technology, 2(1), 549-557.

[10] D. Aswini, R. Rohindh, K. S. Manoj Ragavendhara and C. S. Mridula, "Smart Door Locking System," 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2021, pp. 1-5, doi: 10.1109/ICAECA52838.2021.9675590.