

Mobile-Controlled Door Locking System

**Bachelor of Technology
In
Computer Science and Engineering (Internet of Things)**

Design & developed by

R. Sai Deepak Goud	2111CS050110
S. Srinath	2111CS050096
V. Ganga Manikanta Reddy	2111CS050076
N. Harshitha	2111CS050078

Under the esteemed guidance

Mr. P. Shanmukha Kumar

Assistant Professor



Department of Computer Science and Engineering (Internet of Things)

School of Engineering

MALLA REDDY UNIVERSITY

Maisammaguda , Dulapally , Hyderabad, Telanagana 500100

2024



MALLA REDDY UNIVERSITY

(Telangana State Private Universities Act No.13 of 2020 and G.O.Ms.No.14, Higher Education (UE) Department)

Department of Computer Science and Engineering (Internet of Things)

CERTIFICATE

This is to certify that the application development project entitled “**Mobile-Controlled Door Locking System**”, submitted by **R.Sai Deepak Goud (2111CS050110), S. Srinath (2111CS050096), V. Ganga Manikanta Reddy (2111CS050076), N. Harshitha (2111CS050078)**, towards the partial fulfillment for the award of **Bachelor’s Degree in Internet of Things** from the **Department of Computer Science and Engineering, Malla Reddy University, Hyderabad**, is a record of bonafide work done by him/ her. The results embodied in the work are not submitted to any other University or Institute for the award of any degree or diploma.

Internal Guide

Mr. P. Shanmukha Kumar

Assistant Professor

Head of the department

Dr. G. Anand Kumar

CSE(IOT)

External Examiner

DECLARATION

We hereby declare that the project report entitled “**Mobile Controlled Door locking System**” has been carried out by us and this work has been submitted to the **Department of Computer Science and Engineering (Internet of Things), Malla Reddy University, Hyderabad** in partial fulfillment of the requirements for the award of degree of Bachelor of Technology. We further declare that this project work has not been submitted in full or part for the award of any other degree in any other educational institutions.

Place:

Date:

R. Sai Deepak Goud	2111CS050110
S. Srinath	2111CS050096
V. Ganga Manikanta Reddy	2111CS050076
N. Harshitha	2111CS050078

ACKNOWLEDGEMENT

We extend our sincere gratitude to all those who have contributed to the completion of this project report. Firstly, we would like to extend our gratitude to **Dr. V. S. K Reddy**, Vice Chancellor, for his visionary leadership and unwavering commitment to academic excellence.

We would also like to express my deepest appreciation to our project guide and our class PRC project Coordinator **Mr. P. Shanmukha Kumar (Assistant Professor)**, whose invaluable guidance, insightful feedback, and unwavering support have been instrumental throughout the course of this project for successful outcomes.

We extend our gratitude to our **PRC-convenor, Dr. G. Latha**, for giving valuable inputs and timely quality of our project through a critical review process.

We are also grateful to **Dr. G. Anand Kumar, Head of the Department of Internet of Things**, for providing with the necessary resources and facilities to carry out this project.

We would like to thank **Dr. Kasa Ravindra, Dean, School of Engineering**, for his encouragement and support throughout my academic pursuit.

My heartfelt thanks also go to **Dr. Harikrishna Kamatham, Associate Dean School of Engineering** for his guidance and encouragement. We are deeply indebted to all of them for their support, encouragement, and guidance, without which this project would not have been possible.

R. Sai Deepak Goud	2111CS050110
S. Srinath	2111CS050096
V. Ganga Manikanta Reddy	2111CS050076
N. Harshitha	2111CS050078

ABSTRACT

Technology has improved, and smart locking systems have become more sophisticated. In this case, the android-based Smart System is primarily intended for multimode operations. Such a system is necessary in banks and businesses since it provides functions that let users control locks. The implementation's efficiency the system is incredibly helpful because of its functionality and user friendly interface. Some homeowners aim to connect their home's numerous home automation devices. Those connected to a Windows-based PC are the most popular home controllers. In our study, we introduced a form of smart technology that utilized Bluetooth while using a mobile smartphone. Consequently, using it will be simpler and more effective. Additionally, it supported the free and open source Android and Arduino platforms. This paper proposes a door lock automation system that uses an Android smartphone with Bluetooth as the first piece of hardware. Following a description of the design and software development process, a Bluetooth-based Smartphone application for locking and unlocking doors is demonstrated. The task module acts as the agent in the hardware design for the door-lock system, the Arduino microcontroller serves as the controller and data processing hub, and the solenoid acts as the door lock output. The results of each test show that it is compatible with the original plan for this study.

INDEX

Contents	Page No.
Cover Page	i
Certificate	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
1. Introduction	1-2
1.1 Problem Definition & Description	1-2
1.2 Objectives of the Project	2
1.3 Scope of the Project	2
2. System Analysis	3-6
2.1 Existing System	3-4
2.1.1 Background & Literature Survey	3-4
2.1.2 Limitations of Existing System	4
2.2 Proposed System	4-5
2.2.1 Advantages of Proposed System	5
2.3 Software & Hardware Requirements	5
2.3.1 Software Requirements	5
2.3.2 Hardware Requirements	5
2.4 Feasibility Study	5-6
2.4.1 Technical Feasibility	5
2.4.2 Robustness & Reliability	6
2.4.3 Economic Feasibility	6
3. Architectural Design	7-12
3.1 Modules Design	7
3.1.1 Module 1 (Servo Motor) (Description)	7
3.1.2 Module 2 (Arduino Uno) (Description)	7
3.1.3 Module 3 (HC-05 Bluetooth Module) (Description)	7

3.2	Method & Algorithm design	7-8
3.2.1	Method 1 (Description)	7-8
3.2.2	Algorithm 1 (Description)	8
3.3	Project Architecture	9-12
3.3.1	Architectural Diagram	9
3.3.2	Data Flow Diagram	9-10
3.3.3	Class Diagram	10-11
3.3.4	Use case Diagram	11
3.3.5	Sequence Diagram	11-12
3.3.6	Activity Diagram	12
4.	Implementation & Testing	13-15
4.1	Coding Blocks	13
4.2	Execution Flow	13-14
4.3	Testing	15
4.3.1	Test case 1	15
4.3.2	Test case 2	15
4.3.3	Test case 3	15
5.	Results	16
5.1	Resulting Screens	16
5.1.1	Screen shot 1	16
5.1.2	Screen shot 2	16
5.1.3	Screen shot 3	16
5.1.4	Result Summary	16
6.	Conclusions & Future Scope	17
6.1	Conclusions	17
6.2	Future Scope	17
6.3	Reference	17

Bibliography

Paper Publication	18-24
-------------------	-------

Web Link of project

CHAPTER-1

INTRODUCTION

1.1 Problem Definition & Description

Lock systems have been around for centuries, and traditional lock systems are still being used today. However, these systems are no longer considered secure and convenient as they are prone to various vulnerabilities. The rise of technology has led to the development of advanced door lock systems that are more secure and convenient than traditional lock systems. Biometric door lock systems are one such technology that uses a person's unique physical traits for authentication purposes. Fingerprint door lock systems are becoming increasingly popular due to their security and convenience. This presents the design and implementation of a fingerprint door lock system using Arduino Uno microcontroller.

The technology of keys and locks remained the same for the last century while everything else is evolving exponentially. So why not use current technologies and apply it with old ones to build something new and innovative. Around 4000 years ago, the concept of Locks and Keys were invented and until today, regardless of some minimal variation in security and sustainability locks are installed in doors stimulated mechanically by the right key. Recently, the Internet was enhanced, and everything was connected to it (phones, television, laptops, tablets, cars and so on). This was done because we wanted to make systems smarter in other term a more productive. Why not do the same thing with Locks? Enhancing the locks mechanism by connecting them to the internet, making them more robust and productive. Today, the number of mobile device users including smart phone users has rapidly been increasing worldwide, and various convenient and useful smartphone applications have been Smart-Lock- System is a complete reinvention of the standard Key-Door lock, where all the digital keys are stored in a Digital Key chain kept on the owner as phone. Encrypted and secured Smart-Lock-System can be connected to the Internet via internet cable (UTP) or wirelessly (Wi-Fi).

This record is meant to address the security issue of unauthorized persons getting into our houses, shops or offices. Security problems can be solved the usage of a traditional padlock, but there may be usually the opportunity that someone will free up it even without breaking using a replica key. the usage of those varieties of locks additionally reasons trouble if we lose the key and we have to bring the important thing with us at all times. Once more, using patterns in the padlock can decorate security, however once more, it may be opened if the password or patterns are in some way recognized.

So leaving each system in this assignment, we are able to put in force one which makes use of biometrics. In the case of biometrics, the pattern with a purpose to act as the important thing might be specific. Right here, to make the challenge, we are able to use the fingerprint as the important thing. This Arduino undertaking will use specific gadgets to do the security key wherein there might be exceptional features to boom the safety degree. In short, we are saying that we are setting up a door-to-door system that uses Arduino using fingerprints. to determine who permits and who does not permit within the house, office, door items, and so forth. We attempt to try this by way of the usage of a simple, commonplace door lock hooked up in each domestic to reduce the price of the device as a product.

Problem Statement

There may exist smart door locking and unlocking system using Digital Code Lock System operates on keypad. Any person can open the door who knows the pass keys. Hence, Digital code lock system cannot authenticate the person hence any one can easily enter which results in theft occurrence or mishappening. To overcome the problem of Authentication in previous system, we introduced the fingerprint-based Door Lock System.

1.2 Objective of the Project

The project employs key components such as the Arduino Uno microcontroller, a servo motor, a door latch, and a mobile phone fingerprint sensor. The synergy between these elements results in a secure and user-friendly system that replaces traditional keys with personalized biometric data.

Enhanced Security: The system can offer higher security compared to traditional locks by incorporating features such as password protection, biometric verification (fingerprint, facial recognition), or RFID card access. This reduces the risk of unauthorized access.

Remote Control: The system can be controlled remotely via a smartphone or computer, allowing users to lock or unlock doors from a distance. This is particularly useful for managing access to homes, offices, or other secure areas when the user is not physically present.

Automated Locking and Unlocking: The microcontroller can be programmed to automatically lock or unlock the door at certain times of the day, enhancing security and convenience. For example, it can ensure the door is locked at night and unlocked in the morning.

Access Logging: The system can keep a log of access attempts, recording who accessed the door and when. This is useful for monitoring and auditing purposes, especially in sensitive or high-security environments.

Energy Efficiency: Some systems can be designed to be energy-efficient, using low-power components and operating modes to reduce energy consumption while maintaining security.

1.3 Scope of the project

The main Aim of this project is to design and develop a mobile application for fingerprint enrollment, authentication, and door unlocking functionality. Implementation of a backend server for user management, access control, and logging. Integration with the physical door lock mechanism to enable remote unlocking.

The main objective is to design secure lock and designing secured door lock to prevent unwanted access in the server room. And it to Replace RFID based lock system with the smart phone. And also to give the user hassle free access without compromising security.

The scope of a micro-controlled door locking system project involves a comprehensive approach to design, development, deployment, and maintenance.

CHAPTER - 2

SYSTEM ANALYSIS

2.1 Existing System

2.1.1 Background & Literature Survey

There are just a few digital approaches for door security locks in the current system. This contemporary smart locking system takes the place of the classic lock and key locking method. Modern living is largely reliant on technological advancements, such as opening doors, managing the air conditioning, and regulating the curtains. People want to feel safe in their own homes, offices, and stores. The primary motivation for the development of smart locks is to meet the needs of people. Some of these systems will be discussed in this section.

• Fingerprint Locking System

A fingerprint locking system is a locking system that uses a fingerprint sensor module to secure the user's fingerprint. The fingerprint sensor module uses an Arduino or a Raspberry Pi to operate. In the proposed system, there is three-level security. Any two levels of security users have to face to unlock the system. This is the ideal option for avoiding the hassles of a stolen or lost key or illegal access. The authorized user must register his or her fingerprint in the system. The registered person's mobile number is then added to GSM, and a permanent image password is assigned to this user. As a first step, the unauthorized individual must choose unauthorized as the user type. The admin receives a random picture. The person must properly choose the random image. Otherwise, the system will go back to the first page.

• Internet of Things

The internet of things, or IoT, is a wireless link that works in a door lock. With the help of IoT-enabled applications, the user may unlock the door with his smartphone. The servo library is introduced after the application is developed by creating a string variable that contains the unique device ID for the lock. The essential concept underlying the door lock's operation is the ID supplied by the Android phone via the created app.

• Knock-Pattern Using Arduino and GSM Communication

This system, which consists of Arduino, GSM Module, Servo Motor, and other components, employs a 'Secret Knocking Pattern' that is only known by the owner of the safe, luggage, or other property or item on which the device is mounted. For the lock to open, the knocking pattern must be used only at a certain location, which is only known by the owner. The secret pattern can only be changed after the secret knock has been unlocked. Because there is no key to be copied, this approach fully eliminates the worry of duplication.

• Keyless Entry System Based on Arduino Board with Wi-Fi Technology

A keyless entry system that focuses on the use of an Arduino circuit board, a Wi-Fi module, and the PHP programming language to provide access to a closed door. The suggested solution, which uses an Arduino Uno board and a Wi-Fi shield to unlock the door without a key, is described. The internet connection allows the system to unlock the door from any place, unlike traditional systems, which have a limited range.

• **RFID Based Access Control System**

A magnetic door lock is administered through an RFID reader in the suggested system, which begins the authentication and validation of the user or regulates access in short. In addition, the systems keep track of each user's access and exit records in the form of a log report for each access. To avoid unforeseen circumstances, the administrator of the central subsystem can terminate the validity of any user at any moment. Many automated advanced door locking system has been developed and its popularly used in many places like commercial buildings and organization. Some of these automated doors locking system are based on RFID (Radio- frequency identification).The RFID card reader detects and checks the user accessibility. When the card is brought near the reader, it identifies the radio frequency of the card and thus verifies the key but these systems are very expensive. Various control systems are being designed over the years to prevent unauthorized access. The main aim for providing locks for our home, school, office, and building is for security of our lives and property.

2.1.2 Limitations of Existing System

The most commonly used system for locking and unlocking the door is a lock and a physical key . The entire process is a mechanical one. If the key is lost, misplaced or stolen, then the entire locking mechanism has to be replaced. This problem with the physical keys intensifies when it comes to big companies where employees are needed to carry several keys for different doors . Apart from the vehicle keys or office tables key as per the person needs.

The Smart door Unlocking system are also getting into market where the finger print sensor is embedded near the door it self. For this purpose the person who want to unlock or lock the door they need to move to door each time. This problem will overcome using our system.

2.2 Proposed System

Normally in human life safety is very most. In this, we used a fingerprint sensor to open the door lock and close the door lock. These processes are controlled by Arduino Uno microcontroller. In this method who is an authorized person they only can open the door. The user journey begins with a dedicated mobile application, designed to manage fingerprints securely. Users are prompted to register their fingerprints through the phone's sensor, creating a unique biometric signature. This signature serves as the digital key to unlock the door, offering a seamless and secure access experience.

The Arduino Uno plays a pivotal role in processing the biometric data received from the mobile app. The processed information then triggers the servo motor, which in turn controls the physical door latch. This mechanism ensures that only authorized individuals with registered fingerprints can gain access.

2.2.1 Advantages of proposed System

- **Remote Access:** Lock or unlock doors from anywhere using a smartphone.
- **Enhanced Security:** Receive real-time notifications of lock status changes and unauthorized access attempts.
- **Multiple Access Methods:** Support for passwords, biometric authentication, and RFID cards for added security and flexibility.
- **Integration with Smart Home Devices:** Seamlessly integrate with other smart home devices for a cohesive and automated home security ecosystem.
- **Temporary Access:** Easily grant temporary access to guests or service personnel without physical keys.
- **Customizable Settings:** Configure automated locking and unlocking schedules based on user preferences and needs.
- Maximum control over who enters your home
- High security
- The door automatically locks when it gets shut
- Speed and time saving
- More economical

2.3 Software & Hardware Requirements

2.3.1 Software Requirements

Arduino IDE, Installed Libraries(Servo Motor)

2.3.2 Hardware Requirements

- Arduino Uno
- Servo Motor
- Door Latch
- Bluetooth Module(HC-05)
- Phone Fingerprint Sensor(Mobile Phone Which is having the inbuilt sensor)
-

2.4 Feasibility Study

2.4.1 Technical Feasibility

A feasibility study for the Smart Door Unlock System using fingerprint authentication from a mobile device would involve a detailed examination of various aspects to determine the viability and potential success of the project. Firstly, the technical feasibility of the project needs to be assessed. This involves evaluating the availability of necessary hardware and software components, such as smartphones with fingerprint sensors, and ensuring compatibility with existing door lock mechanisms or the feasibility of integrating new smart locks. Evaluating the availability of relevant technologies and expertise in biometric authentication, mobile development, and server-side programming is crucial in determining technical feasibility.

2.4.2 Robustness & Reliability

Robustness and reliability are paramount in the development of the Smart Door Unlock System using fingerprint authentication from a mobile device. Robustness entails the system's ability to maintain functionality and integrity under various conditions, including hardware failures, network disruptions, and malicious attacks. To achieve this, thorough testing procedures must be implemented to identify and address potential vulnerabilities and points of failure. Furthermore, redundancy and failover mechanisms should be integrated to minimize downtime and ensure continuous operation in the event of hardware or software failures. Reliability, on the other hand, involves the system's ability to consistently deliver accurate and secure authentication, without errors or performance degradation over time. This requires employing advanced fingerprint recognition algorithms and technologies, coupled with rigorous quality assurance measures to verify the system's functionality and accuracy. By prioritizing robustness and reliability throughout the development process, stakeholders can instill confidence in the Smart Door Unlock System's ability to provide secure and seamless access control for users, thereby enhancing user satisfaction and trust in the system.

2.4.3 Economic Feasibility

This includes estimating the costs associated with hardware procurement, software development, infrastructure setup, and ongoing maintenance and support. A cost-benefit analysis should be conducted to determine whether the potential benefits of the Smart Door Unlock System, such as improved security, convenience, and operational efficiency, outweigh the associated costs. Additionally, consideration should be given to potential revenue streams, such as selling the system to residential or commercial customers, to assess the project's long-term financial viability.

CHAPTER - 3

ARCHITECTURAL DESIGN

3.1 Module Design

3.1.1 Servo Motor

- A servo motor is an electromechanical device that is used for precise control of angular or linear position. It consists of a motor and a sensor for position feedback . The motor is typically either a DC or an AC motor, and the sensor is often a potentiometer that provides feedback on the motor's position.
- A sensor, often a potentiometer, is used to monitor the position of the motor's output shaft and provide feedback to the control system.
- Servo motors can rotate over a limited range, typically 180 degrees or 360 degrees, depending on the specific model.
- Servo motors are typically controlled using pulse-width modulation (PWM) signals. The width of the pulse determines the position of the servo motor.

3.1.2 Arduino Uno

- Arduino UNO is a low-cost, flexible, and easy-to-use programmable open-source microcontroller board that can be integrated into a variety of electronic projects. This board can be interfaced with other Arduino boards.
- Arduino is used for the control of traffic lights, it can also be used for the real time control system with programmable timings, pedestrian lighting etc.

3.1.3 HC-05 Bluetooth Module

- HC-05 is a Bluetooth module which is designed for wireless communication. This module can be used in a master or slave configuration.
- The data transfer rate of HC-05 module can vary up to 1Mbps is in the range of 10 meters.

3.2 Method & Algorithm design

3.2.1 Method-1: Working

User Registration:

The process begins with users registering their fingerprints through a dedicated mobile app. This app utilizes the fingerprint sensor integrated into the user's smartphone. Users follow the prompts to add their unique biometric data securely.

Mobile App Communication:

Once the fingerprints are registered, the mobile app communicates with the Arduino Uno. The app sends the encrypted biometric data to the Arduino for real-time processing and authentication.

Arduino Processing:

The Arduino Uno serves as the central processing unit. It receives the fingerprint data from the mobile app and compares it with the stored templates of authorized users. The Arduino is programmed to handle the matching process efficiently.

Fingerprint Matching:

The Arduino performs the fingerprint matching algorithm to verify the identity of the user. If the received fingerprint data matches an authorized entry in its database, the Arduino triggers the next step in the process.

Servo Motor Activation:

Upon a successful fingerprint match, the Arduino sends a command to the servo motor. The servo motor, connected to the door latch, is activated. The motor's rotational motion is utilized to manipulate the door latch, either unlocking or locking the door, depending on its current state.

Door Unlocking:

With the servo motor's movement, the physical door latch is disengaged, allowing the door to be opened. The user, having successfully authenticated their fingerprint, gains access to the secured space.

3.2.2 Algorithm

A mobile-controlled door locking system uses an algorithm to manage the communication and operations between a smartphone app and a smart door lock.

Step 1: Initialization:

- Set up the door lock with electronic components and a wireless communication module (Bluetooth).
- Install the mobile app on the user's smartphone.
- Connect the app to the lock using the appropriate communication protocol (Bluetooth for short-range control).
- Authenticate the user through the mobile app.

Step 2: User Input:

- In the app, wait for the user to input biometric scan.
- Process the user's input to determine the action to perform.

Step 3: Command Execution:

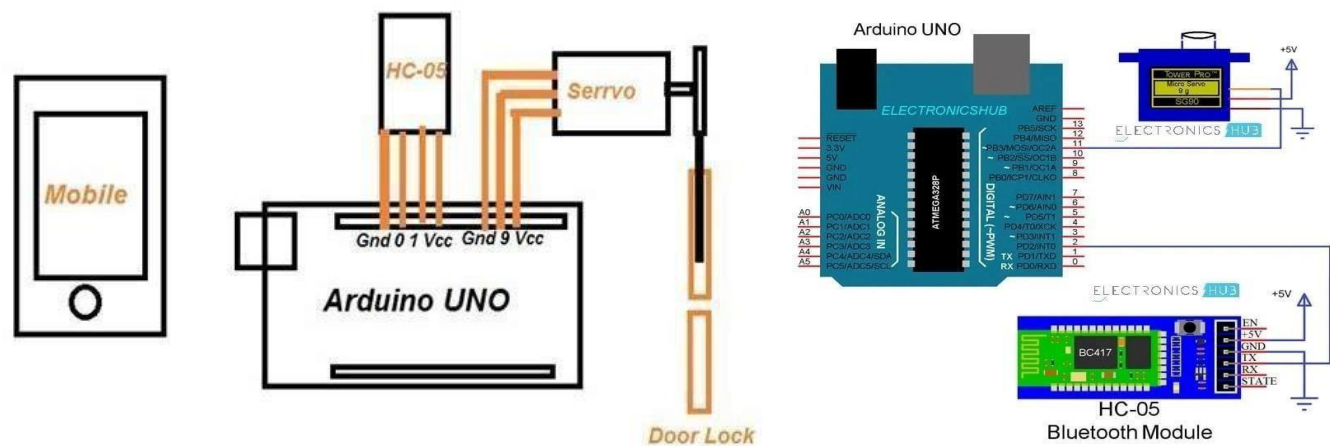
- If the user wants to lock or unlock the door
- The door lock receives the command and activates the motor to lock or unlock the door.

Step 4: Status Feedback:

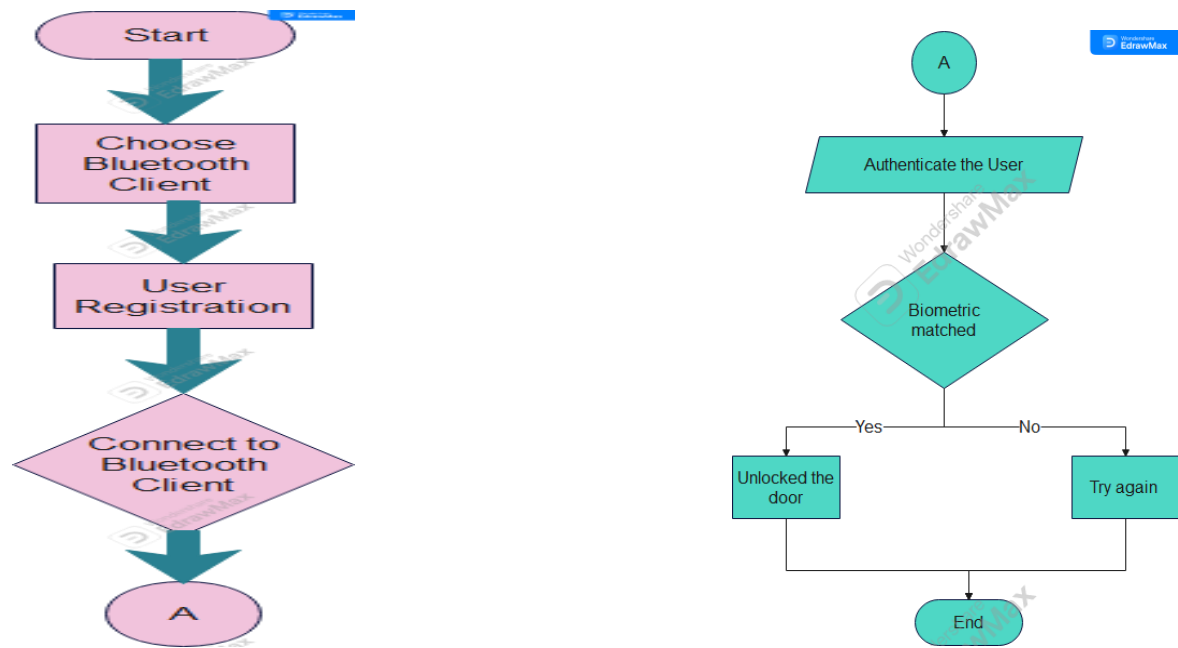
- After executing the command, the door lock sends a response back to the app, confirming the action taken and providing the current status of the door (e.g., locked, unlocked).

3.3 Project Architecture

3.3.1. Architecture Diagram



3.3.2 Data Flow Diagram

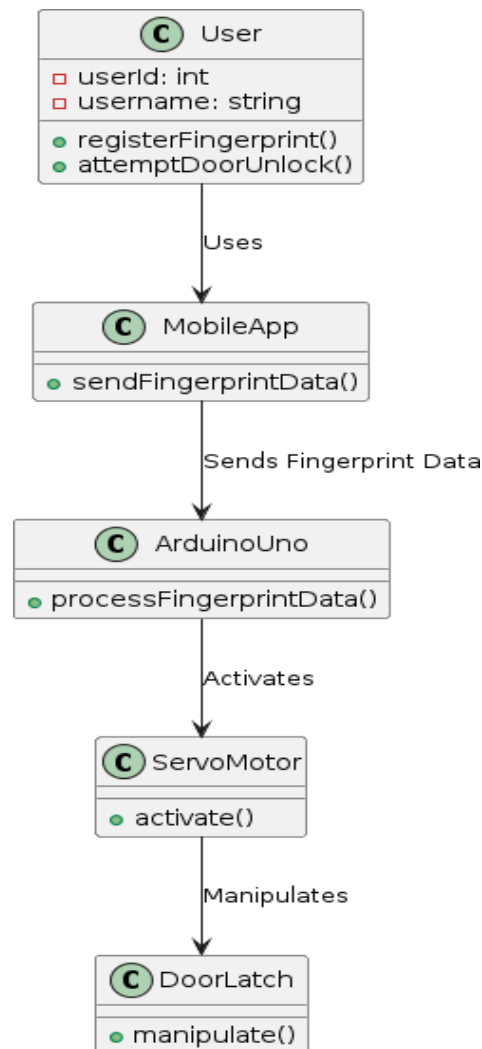


User Registration: The user sends login credentials to the User Authentication process, which verifies these against the User Database. An authentication response (success/failure) is then sent back to the user.

Authenticating the user: The user sends a lock/unlock command via their mobile device to the Command Processing process. This process logs the command in the Command Log and sends the lock/unlock command to the Lock/Unlock Door process.

Lock/Unlock Door Process: The Lock/Unlock Door process executes the command by interacting with the Door Lock. A status update (confirmation of lock/unlock) is sent back to the Command Processing process, which then sends a command confirmation to the user.

3.3.3 Class Diagram



The User class may have an association with the Mobile Application class because a user interacts with the mobile application to control the door lock.

- The Mobile Application class communicates with the Door Lock class to send requests and receive status updates.
- The Mobile Application may also communicate with the Server class if the architecture involves a server for processing and forwarding requests.
- The Door Lock class may have an association with the Lock Controller class, which handles the logic for processing lock and unlock requests and communicates with the door lock hardware.
- An association line connects two classes that have a relationship (e.g., Mobile Application and Door Lock).

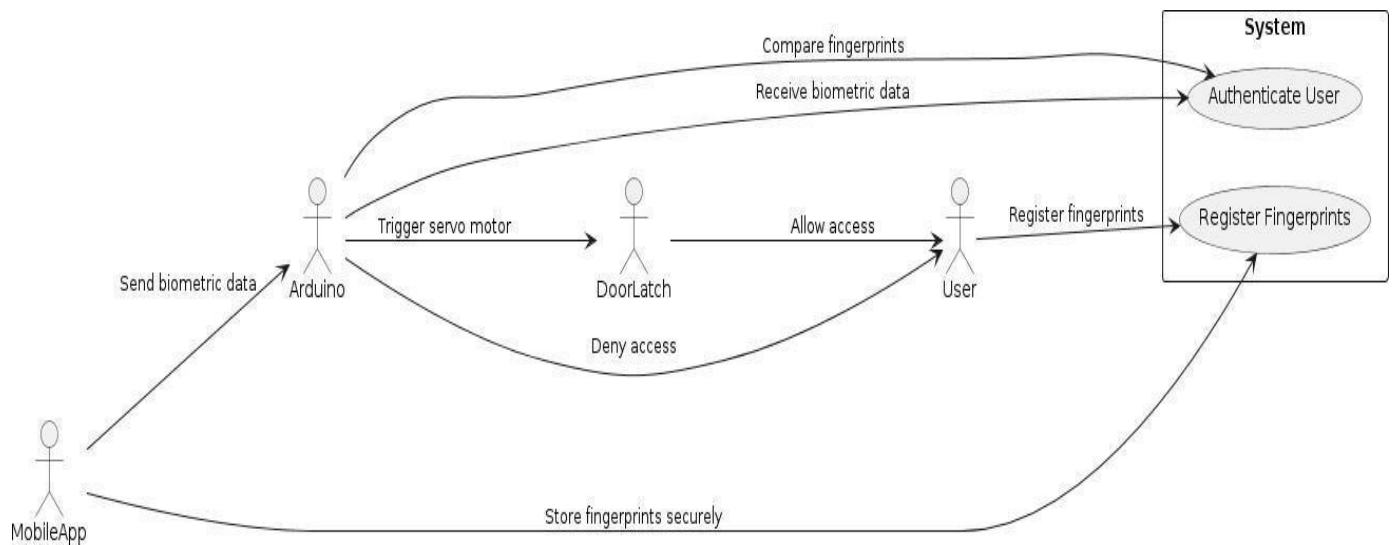
- A directed association line (with an arrowhead) indicates the direction of interaction or dependency (e.g., Mobile Application sending requests to Door Lock).

3.3.4 Use Case Diagram

User: The individual who uses the mobile app to register their fingerprint and control the door lock.

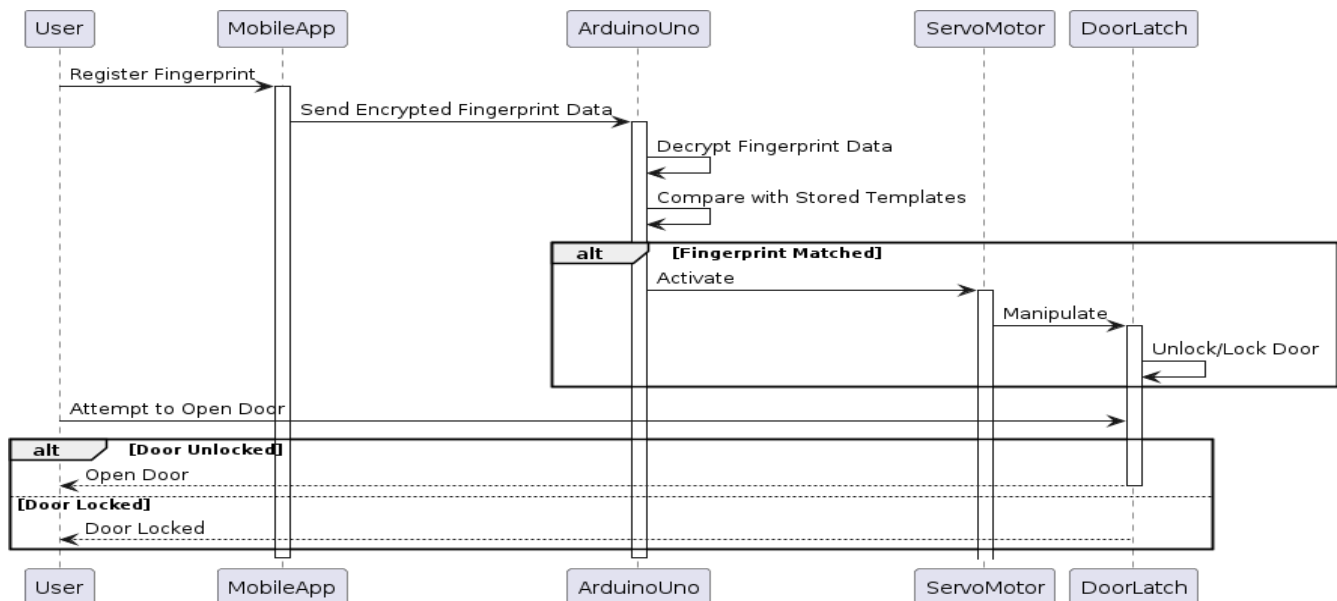
Mobile Application: The mobile app acts as an intermediary between the user and the door lock system.

Arduino Uno: The Arduino Uno is the central processing unit that handles the fingerprint matching and door control.



Use case Diagram

3.3.5 Sequence Diagram



User → Mobile Application: Sends a request to lock/unlock the door.

Mobile Application → Server : Forwards the request to the server for processing and authentication.

Server → Door Lock: Sends the request to the door lock.

Door Lock: Processes the request and performs the lock/unlock action.

Door Lock → Server : Sends the status of the action (success/failure) back to the server.

Server → Mobile Application: Sends the response from the door lock back to the mobile application.

Mobile Application → User: Sends the status of the action to the user (e.g., door locked/unlocked).

3.3.6 Activity Diagram

User Registration:

Start: The process begins when the user decides to register their fingerprint.

Register Fingerprint: The user uses the mobile app to register their fingerprint through the smartphone's Integrated fingerprint sensor.

Secure Fingerprint Data: The app securely stores the fingerprint data.

Mobile App Communication:

Send Encrypted Data: The app sends the encrypted biometric data to the Arduino Uno.

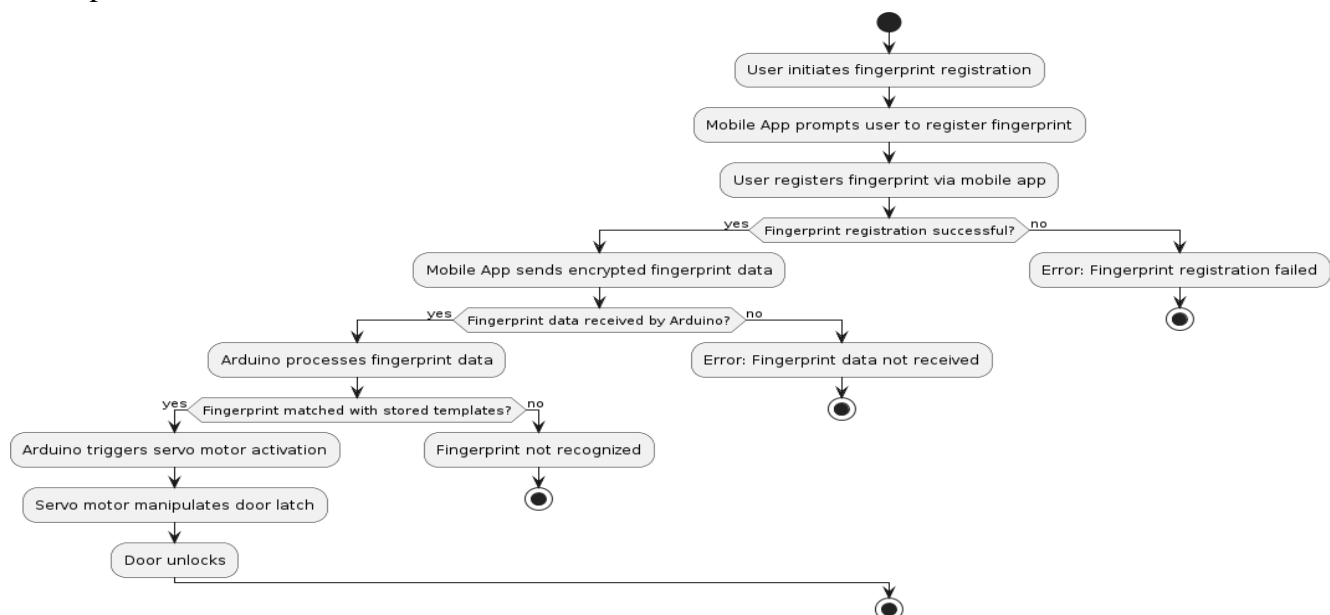
Receive Acknowledgment: The app may receive acknowledgment from Arduino that data has been received.

Arduino Processing:

Receive Data: Arduino Uno receives the encrypted fingerprint data from the mobile app.

Match Fingerprint: Arduino processes the data and performs the fingerprint matching algorithm.

Decision Point: If the fingerprint matches a stored template of an authorized user, the process proceeds to the next step.



CHAPTER - 4

Implementation & Testing

4.1 Code Block

```
String readString;
#include <Servo.h>
Servo myservo; //Connect relay1 to pin D3
void setup(){
  Serial.begin(9600); //Set rate for communicating with phone
  myservo.attach(9); //Switch relay1 off
}
void loop(){
  while(Serial.available()) {
    delay(10); //Delay to make it stable
    char c = Serial.read(); //Conduct a serial read
    if (c == '#'){
      break;}
    readString += c; //Means readString = readString + c
  } if (readString.length() >0){
    Serial.println(readString);
    if(readString == "f success"){
      myservo.write(180);
      delay(4000);
      myservo.write(90);
    }readString="";
  }
}
```

4.2 Execution Flow

1. User Initiation

- **User Action:** The user opens the mobile app and decides to lock or unlock the door.
- **UI/UX:** The app displays an interface with options to lock or unlock.

2. Authentication

- **User Action:** The user might need to log in or verify identity (e.g., fingerprint, face recognition, PIN).
- **Backend:** The app sends authentication credentials to the server for validation.
- **Server:** The server verifies the credentials. If valid, it sends a confirmation to the app.

3. Command Initiation

- **User Action:** The user selects the lock or unlock option.
- **App Action:** The app creates a command (e.g., LOCK or UNLOCK).

4. Command Transmission

- **App Action:** The app sends the command to the backend server via a secure protocol (e.g., HTTPS).
- **Backend:** The server receives the command and logs the request.

5. Device Authentication

- **Backend Action:** The server authenticates the request and checks if the user's device has permission to control the specific door lock.
- **Device Check:** It verifies the device ID or user permissions.

6. Command Forwarding

- **Server Action:** The server forwards the command to the microcontroller managing the door lock. This might be done via:
 - **Direct Communication:** Using Wi-Fi, Bluetooth, or a cellular network.
 - **Indirect Communication:** Through a message queue or intermediary service if the lock is not directly accessible.

7. Command Reception

- **Microcontroller:** The microcontroller in the door lock receives the command.
- **Security Check:** It authenticates the command to ensure it is from a trusted source.

8. Command Execution

- **Microcontroller Action:** The microcontroller interprets the command and activates the lock/unlock mechanism.
 - **Locking:** It might trigger a motor or solenoid to move the lock into the locked position.
 - **Unlocking:** It might reverse the motor or solenoid action to release the lock.

9. Status Feedback

- **Microcontroller Action:** After execution, the microcontroller sends a status update back to the server.
 - **Status Check:** It checks if the action was successful (e.g., lock is engaged, or the door is open)

4.3 Testing

4.3.1 Test Cases-1:

- Writing the code in the Arduino Ide and Compiling the Arduino Code if there were no error in the code we can directly upload the code to the Arduino Board.
- If we encounter any error in the code we have to debug it and then we have to compile and upload.

4.3.2 Test Case-2:

- We have to register the biometric data in our mobile device for the access of the door.
- Only authorized users are allowed to unlock/lock the door.
- We have to pair our HC-05 Bluetooth module with our mobile device for the easy communication in between the board and the mobile device.

4.3.3. Test Case-3:

- When there is a successful match of our Biometric data the door will unlock and it will automatically lock after some time.
- If the mobile Bluetooth is not paired with the module we have to try with another device.
- It is mandatory to pair with the mobile and the connections are given as per the circuit diagram.

CHAPTER - 5

RESULTS

5.1 Resulting Screens:

5.1.1 Screen Shot 1

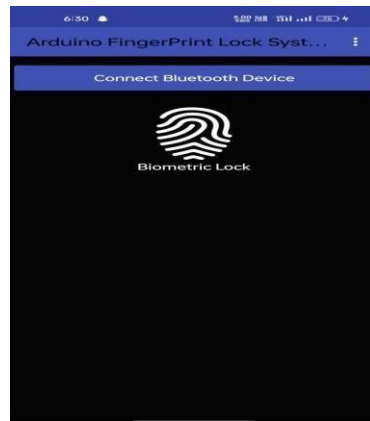
```
BT_AndroidFingerprint_Lock_1.ino
6
7 void setup()
8 {
9   Serial.begin(9600); //Set rate for communicating with phone
10  myservo.attach(9); //Switch relay1 off
11 }
12 void loop()
13 {
14   while(Serial.available()) //Check if there are available bytes to read
15   {
16     delay(10); //Delay to make it stable
17     char c = Serial.read(); //Conduct a serial read
18     if (c == 'H'){
19       //When this condition is satisfied, the relay will be switched on
20     }
21   }
22 }
```

Output

```
"C:\Users\sai55\AppData\Local\Arduino15\packages\arduino\tools\avr-gcc\7.3.0-atmel3.6.1-arduino7/bin/avr-objcopy" -O ihex
Using library Servo at version 1.2.1 in folder: C:\Users\sai55\AppData\Local\Arduino15\libraries\Servo
"C:\Users\sai55\AppData\Local\Arduino15\packages\arduino\tools\avr-gcc\7.3.0-atmel3.6.1-arduino7/bin/avr-size" -A "C:\Users\sai55\AppData\Local\Arduino15\packages\arduino\tools\avr-gcc\7.3.0-atmel3.6.1-arduino7/bin/avr-size" -A "C:\Users\sai55\AppData\Local\Arduino15\packages\arduino\tools\avr-gcc\7.3.0-atmel3.6.1-arduino7/bin/avr-size" -A "C:\Users\sai55\AppData\Local\Arduino15\packages\arduino\tools\avr-gcc\7.3.0-atmel3.6.1-arduino7/bin/avr-size"
Sketch uses 4642 bytes (14%) of program storage space. Maximum is 32256 bytes.
Global variables use 255 bytes (12%) of dynamic memory, leaving 1793 bytes for local variables. Maximum is 2048 bytes.
```

Code Execution

5.1.2 Screen Shot 2



Mobile Interface

5.1.3 Screen Shot 3



User Verified

5.1.4 Result Summary

The figures will describe about interface which directly interact with the user for the communication and the accessing the door lock.

CHAPTER - 6

CONCLUSION & FUTURE SCOPE

6.1. Conclusion

The mobile-controlled door locking system project provides a modern, secure, and convenient solution for remote access management. Integrating mobile technology with traditional locking mechanisms, this system allows users to control door locks via their smartphones, enhancing both security and convenience. By implementing robust security features like multi-layered authentication and encrypted communication, the system ensures that only authorized users can manage the locks, thus safeguarding against unauthorized access. The user-friendly interface and real-time status feedback offer peace of mind and ease of use, making the system accessible to a broad audience. The project's architecture is designed to be reliable and scalable, capable of expanding to multiple locks and users, which makes it suitable for diverse applications from homes to commercial spaces. Future enhancements could include integration with smart home systems, the addition of advanced features such as biometric authentication, and improved offline functionality, ensuring continuous control even without internet access. Overall, the project not only meets current needs for secure and convenient access control but also lays a foundation for future innovations in smart security technology, underscoring its potential to transform how we manage security in our daily lives.

6.2 Future Scope

The proposed system will be enhanced in the future with more extensions. This device can be made economical in future so that anyone can afford it at low price. Some features like camera can be attached to help identify any intruders who attempt to unlock the door using the wrong key. We can run this work by building own app rather than using an existing app, like Blynk.

6.3 Reference

- [1] Meenakshi N, Dikshit KJ, Monish M, Bharath S. Arduino based totally smart Fingerprint Authentication device. In 2019 1st global convention on innovations in facts and communicate technology (ICIICT) 2019 Apr 25 (pp. 17). IEEE.
- [2] Moyashir R, Baidya J, Saha T, Palit R. layout and implementation of a fingerprint-primarily based key device for shared access. 2017 IEEE seventh Annual laptop and conversation conference and conference (CCWC) 2017 January 9 (pp. 1-6).IEEE.
- [3] Gupta RP. Implementation of Biometric Security in Smartphone Based Domotics. 2018 International Conference on Computer Development, Communication and Network Management (CCWC) 2018 Oct 12 (pp. 80-85). IEEE.
- [4] Karma Toshomo has presented Dual Door Lock System Using Radio Frequency Identification and Fingerprint Recognition.
- [5] G. Sowmya, G. Divya Jyothi, N. Shirisha, K. Navya, and B. Padmaja, "Iot Based Smart Door Lock System," Int. J. Eng. Technol. Vol 7, No 3.6 Spec. Issue 6, 10.14419/ijet.v7i3.6.14975. 2018.
- [6] S. Kavde, R. Kavde, S. Bodare, and G. Bhagat, "Smart digital door lock system using Bluetooth technology," in 2017 International Conference on Information Communication and Embedded Systems (ICICES),

Mobile–Controlled Door Locking System

Reddymalla Sai Deepak Goud¹, Suram Srinath², Velma Gangamanikanta Reddy³,
Nalla Harshitha⁴, P. Shanmuka Kumar⁵

¹⁻⁴Department Of Internet of Things, Malla Reddy University, Hyderabad, Telangana, India.

⁵Assistant Professor, Department of Internet of Things, Malla Reddy University, Hyderabad, Telangana, India.

2111cs050110@mallareddyuniversity.ac.in, 2111cs050096@mallareddyuniversity.ac.in²,
2111cs050076@mallareddyuniversity.ac.in³, 2111cs050078@mallareddyuniversity.ac.in⁴,

p-shanmukhakumar@mallareddyuniversity.ac.in⁵

ABSTRACT

Technology has improved, and smart locking systems have become more sophisticated. In this case, the android-based Smart System is primarily intended for multimode operations. Such a system is necessary in banks and businesses since it provides functions that let users control locks. The implementation's efficiency the system is incredibly helpful because of its functionality and user-friendly interface. Some homeowners aim to connect their home's numerous home automation devices. Those connected to a Windows-based PC are the most popular home controllers. In our study, we introduced a form of smart technology that utilized Bluetooth while using a mobile smartphone. Consequently, using it will be simpler and more effective. Additionally, it supported the free and open-source Android and Arduino platforms. This paper proposes a door lock automation system that uses an Android smartphone with Bluetooth as the first piece of hardware. Following a description of the design and software development process, a Bluetooth-based Smartphone application for locking and unlocking doors is demonstrated. The task module acts as the agent in the hardware design for the door-lock system, the Arduino microcontroller serves as the controller and data processing hub, and the solenoid acts as the door lock output. The results of each test show that it is compatible with the original plan for this study.

The Internet of Things (IoT) has gained widespread attention among many research areas. The modern automation has made the life more sophisticated and easier. An IoT based smart digital automated system plays a crucial part that assist people by reducing work load and implementing interactive technology in everyday life. Through our project, Smart Doors, we are making a small contribution to the enormous efforts being made to improve and simplify our lives. This is a simple project that helps users in accessing the doors within a specific range. Android software will access the door lock and the transfer of

data will be performed by using the Bluetooth technique. So, the end users need not to bother about the door lock as they can manage it through their cell phone within a certain proximity, and additionally, users need not to be concerned about handling a physical key. This work comprises software and hardware development. This approach intends to do away with the need for keys to open doors and the everyday struggle involved in carrying a lot of keys and prepared for installation anywhere and everywhere with the greatest haste. This helps to create a secure environment inside and outside by preventing security breaches.

Keywords: Crypto-ransomware, forensic analysis, cyber extortion, digital currencies, encryption, cybersecurity, malware detection, threat mitigation.

I. INTRODUCTION

The Internet of Things (IoT) is a network of connected smart devices, digital and mechanical systems, items, animals, or people that may exchange data across a network without having social or machines interaction. An IoT environment is comprised of smart devices having sensors, integrated processors, and networking equipment to gather, share, and respond on environmental data. IoT systems exchange the sensor information they gathered, by linking to an IoT connection or any other system, where information is either transferred to a cloud or evaluated locally. The things get associated with internal or external conditions due to embedded development, which affects the decisions that are made [1]. Everyone wants to be safe, whether that protection is in regards to his possessions or his own priceless life. We have now been taking numerous efforts to achieve a stress-free lifestyle. Smart door control system is highly demanded & applicable project [2]. A door acts as a first line of defence to keep the house physically

secure. A physical key was initially required to open or close a door, but as technology advanced, a highly sophisticated smart door lock has been invented, which can unlock or lock doors without needing a physical key [3]. The majority of people act carelessly while in an urgent circumstances. This may be the reason they missed to lock the door of their residence or business. Additionally, storing multiple sets of keys at once could be a challenge. If we lose or misplace the keys and cannot access our place in any other way than by making another set of spare keys, it is also a problem. In addition, if a disabled person finds it difficult to move near the entrance, it may be difficult for them to lock and unlock the door [4]. The main aim of this Smart door project is to simplify and improve our lifestyle and help users to access the doors within a specific range. Through this approach, we can control the lock using biometric using our own smartphone [5]. This Arduino based smart lock system uses Bluetooth to wirelessly communicate and control device using app on their own smartphone [6]. LCD is connected which is used for displaying lock or unlock doors state and relay is attached to show door position. With the smart lock, no need to worry about handling physical key, remotely we can lock or unlock the door [7].

These days office/corporate environment security is a major threat faced by every individual when away from home or at the home. When it comes to security systems, it is one of the primary concerns in this busy competitive world, where human cannot find ways to provide security to his/her confidential belongings manually. Instead, he/she finds an alternative solution which provides better, reliable and atomized security. This is an era where everything is connected through network, where anyone can get hold of information from anywhere around the world. Thus chances of one's info being hacked are a serious issue. Due to these risks it's very important to have some kind of personal identification system to access one's own information. Now a day, personal identification is becoming an important issue all around. Among mainstream personal identification methods, we mostly see password and identification cards techniques. But it is easy to hack password now and identification cards may get lost, thus making these methods quite unreliable. There are certain situations which are very annoying like when a person locks himself out of his house or office or he leaves his key inside or sometimes when a thief just breaks the lock and steals everything. These kinds of situations always trouble people who use manual door lock with keys. Although in some places people use smart cards, there might arise a situation when

someone loses the card or keeps the card inside. Then in other scenarios there are caretakers for locking houses or offices and keeping the keys safe. But then again there are times when a person in charge of the keys might not be available or has gone to some emergency routine, which can cause unwanted delay for people who need the key straightaway. These are some of the hassles that people might face when using keys or smart cards. That is when our system, fingerprint door lock system comes into play. Our design is implemented to provide better securities as users don't need to remember passwords and don't need any sort of keys or cards that often get lost. If someone's fingerprint is authorized in the systems he/she would not face any sort of delays to enter a room. Fingerprint recognition is one of the most secure systems because a fingerprint of one person never matches with others. Therefore, unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users and unlock the system when a match is found. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone. The popularity and reliability of fingerprint scanner can be easily guessed from its use in recent hand-held devices like mobile phones and laptops. This paper is about solving the problem regarding security of unauthorized people trespassing in our home, shops or offices. Security issues can be fixed using traditional locks but there is always possibility of someone opening the lock even without breaking it with the use of duplicate key. Using these kinds of locks also create problem if we lose keys and also, we have to carry keys along with us always. Again, using patterns in the locks can increase security but again it can be opened if somehow the passwords or patterns are known. So, leaving every system in this project we will implement a system using biometrics. In case of biometrics, the pattern which will be used as key will be unique. Here, to implement the project we will use fingerprint as the key. This Arduino project will make use of different devices for the implementation of the security lock where there will be different features to increase the security level. In simple words, we can say that we are implementing a door access system using Arduino which make use of fingerprints to identify whom to allow and who not to allow inside our homes, offices, shops, etc. We are trying to implement it using a normal and simple door lock which is fitted in every home so as to minimize the cost of the device as a product.

II. LITERATURE SURVEY

Various smart locks are previously available. The majority of them are expensive. In this paper “Arduino based electronic lock using RFID and password” which was proposed by “Ni Ni San Hlaing, San SanLwin”. This digital door lock runs on the technology of audio-frequency identification and passcode-based with the help of an Arduino Uno MCU[8].

In another paper named “Secured password-based lock system” was put forward by “Arpita Mishra, Siddharth Sharma, Sachin Dubey, S.K.Dubey”. This methodology is targeted to prevent unlocking of the door by unknown individuals. The formation of the home safety Service consists of the numeric keypad, the hook which is used for lifting, and a GSM module to establish dependable connection for communication conferred with the MCU. The control panel conferred with the device is employed because the passcode access combination opens/closes the door[9].

In another paper named “Smart Lock System Using RFID” was proposed by “Shrinidhi Gindi, Naiyer Shaikh, Kashif Beig, Abdeali Sabuwala”. Here may be a Room security solution supported IoT using RFID, the system is often monitored from anywhere within the world thanks to the continual updating of the status of the door[10].

Moving forward to another paper named “An OTP-based wireless smart door locking system” was proposed by “Mr. L. David William Raj, M. Deepika, V. Bhubaneshwar, R. Harshitha, K. Haripriya”. In this innovation, the key phrase for security is initially put away within the Electrically Erasable Programmable ROM. At the purpose when the client enters the proper secret phrase then the two-way confirmation of a haphazardly produced OTP is shipped off the client gadget. On the off chance that the OTP is coordinated, the framework is going to be opened, and therefore the required capacity is often started[11].

Coming to the next paper named “SMART DOOR UNLOCK SYSTEM USING FINGERPRINT” was proposed by K. Rajesh, Asst. Prof. B. Venkata Rao, P. A. V. S. K. Chaitanya, A. Ruchitha Reddy. In our paper, we apply the finger mark detector to scan one's character to instinctually function the gate of the car, under such situation we prefer to use a MCU for enabling for both opening and closing of the door

if both the match for scanned and existing facts are true[12]

In the upcoming document termed “DOORWAY ROBOTIZATION network supported by CORDLESS for android Smartphone” was proposed by “Lia Kamelia, Alfin Noorhassan S.R, Mada Sanjaya, and W.S., Edi Mulyana”. In this a tool called a automated door lock with the support of Bluetooth and Android smartphone door locks automation system using Bluetooth-based Android Smartphone's is recommended and prototyped. The equipment structure for the door lock setup is that a combination with an android[13]

Numerous studies have been suggested to improve the ease and security of digital door locks. Ilkyu et al. [14] designed a system that works with Internet of things and offers increased security features. It can convey captured pictures to the user's smartphone when an ineligible user tries to do an illegal action; and can also provide alert notifications when the door lock is destroyed physically. To improve convenience, the suggested solution gives users the ability to remotely verify the access information and control the door lock. Jeong et al. [15] put forward a solution in their studies which employs IoT technology and the integration of smartphone connection technologies that uses authentication to remotely open or close a door. This study specifically suggests the Smart Door Lock System based on improved security strategy for the safety concern brought on by the physical key used in unmanned automation equipment like KIOSKS, vending machines, and ATMs. Karthik et al. [16] project's objective is to develop a smart locking system using the IoT. Although using traditional keyed locks has been a necessity since the dawn of mankind, there is a significant likelihood that keys may be misplaced or fall into the wrong hands. To increase the security of their homes or businesses, many people now prefer biometric locks over conventional keyed locks. Modern biometric locks employ a biometric sensor rather than a key to lock or unlock the door, in contrast to traditional locks. With this idea, an adaptive working tool based on an Arduino nano is created that offers physical security using the biometric sensor found in a smartphone. Park et al. [17] proposed a system based on ZigBee framework which is integrated in a digital door lock and for entire home automation system it acts as the primary controller. The system consists of actuators and a network of sensor nodes, as well as a base station that functions as a digital door lock. An RFID reader for user identification, a touch-screen LCD, a motor component to close and open the door, a communication unit, sensor component to inspect

the home environment, and a control unit to operate other components. Sensor nodes are deployed in strategic locations throughout the house to sense the environment. Each ZigBee module's status can be monitored and controlled by the central control unit, which is a digitized locking system. It also allows customers to access the property status remotely via the Internet or another open network. The prime advantage of the proposed module is that it can be built quickly where and when it is needed, with no infrastructure or careful planning requirement. Sowmya et al. [18] presented a simple "smart doors" project that helps users to take control of their access to doors. A simple Arduino board, a hexadecimal keyboard, and some jumper wires are used in this project. The Arduino board, which makes this project easier to use, is its most important feature. With this, it is prepared to be set up anywhere, at any time, with the greatest haste. This helps create a secure environment inside and outside by preventing security breaches. Kavde et al. [19] presented a smart door lock system in their paper as a component of the smart house. The owner in this case can operate their door by seeing the live broadcast on their smartphone. Information about visitors is stored in one database. The system functions as a whole using Bluetooth technology.

III. SYSTEM ANALYSIS AND DESIGN

Existing System:

All over the world, homes, workplaces, shops, banks are looking for extreme security features with safety motives. To ensure the security of these regions, a smart lock system is installed. many types of smart door locks are made to lock and unlock the device. Those form of locks has fingerprint, RFID card, pin, password or IOT by way of unlocking the machine using mobile cellphone. consumer the use of those boiler systems both use a pin code or fingerprint or RFID card to release the gadget. These gadget does not have safety pecking order to develop the safety. To develop the safety the consumer have to unbolt the gadget through minimal security order. In residence lock machine there ought to be unlocking option for visitor. One day thieves may miss out on the option and enter the house.

Limitations of Existing System:

The most commonly used system for locking and unlocking the door is a lock and a physical key . The entire process is a mechanical one. If the key is lost, misplaced or stolen, then the entire locking mechanism has to be replaced. This problem with the physical keys intensifies when it comes to big companies where employees are needed to carry

several keys for different doors . Apart from the vehicle keys or office tables key as per the person needs.

The Smart door Unlocking system are also getting into market where the finger print sensor is embedded near the door itself . For this purpose the person who want to unlock or lock the door they need to move to door each time. This problem will overcome using our system.

Proposed System:

Normally in human life safety is very most. In this, we used a fingerprint sensor to open the door lock and close the door lock. These processes are controlled by Arduino Uno microcontroller. In this method who is an authorized person they only can open the door. The user journey begins with a dedicated mobile application, designed to manage fingerprints securely. Users are prompted to register their fingerprints through the phone's sensor, creating a unique biometric signature. This signature serves as the digital key to unlock the door, offering a seamless and secure access experience.

The Arduino Uno plays a pivotal role in processing the biometric data received from the mobile app. The processed information then triggers the servo motor, which in turn controls the physical door latch. This mechanism ensures that only authorized individuals with registered fingerprints can gain access.

Advantages of proposed System:

- Maximum control over who enters your home.
- High security
- The door automatically locks when it gets shut
- Speed and time saving
- More economical

IV SYSTEM DESCRIPTION

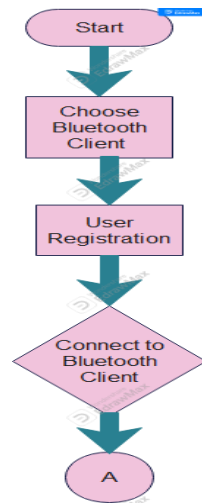


Figure 1: Flow chart

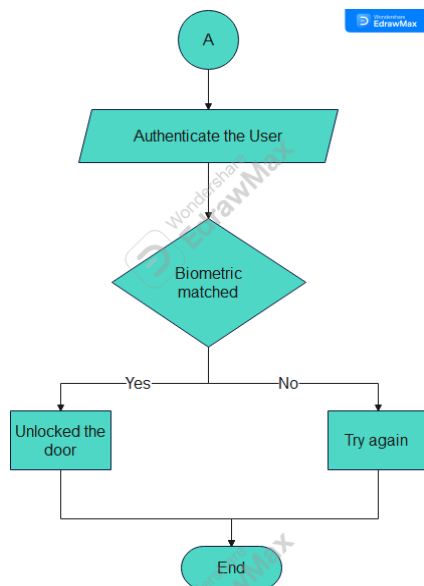


Figure 2: sequence flow chart

IV. HARDWARE AND SOFTWARE REQUIREMENTS:

Hardware Components:

Arduino Uno:

The central brain of our project, the Arduino Uno microcontroller, acts as the control unit. It processes data received from the mobile app, manages the fingerprint matching process, and ultimately controls the servo motor to unlock the door latch.

Servo Motor:

The servo motor is the physical executor of the system. Connected to the door latch, it receives commands from the Arduino Uno based on successful fingerprint authentication. The servo motor's rotational motion is used to manipulate the door latch, either unlocking or locking the door.

Door Latch:

The door latch is the mechanical component responsible for securing or releasing the door. It interacts with the servo motor, which, upon receiving the appropriate signal from the Arduino Uno, either engages or disengages the latch, allowing the door to be opened or secured.

Software Components:

Phone Fingerprint Sensor:

Leveraging the existing fingerprint sensor on a mobile phone adds a layer of convenience to our system. Users can register and manage their fingerprints through a dedicated mobile app. The phone's fingerprint sensor captures and stores unique biometric data, allowing for secure and easy access control.

Mobile App:

The mobile application serves as the user interface for managing fingerprints and controlling access. Developed for ease of use, the app guides users through the process of registering fingerprints. It communicates with the Arduino Uno, sending fingerprint data for authentication and receiving commands to unlock the door.

The mobile application designed for our Fingerprint Door Lock project serves as a user-friendly interface, empowering individuals to manage their fingerprints and control access securely. Here's a brief explanation of the key features and functionalities:

User Registration:

The app provides a straightforward process for users to register their fingerprints. Through the mobile phone's integrated fingerprint sensor, individuals can enroll their unique biometric data, creating a secure digital key for accessing the door.

Fingerprint Management:

Users have the flexibility to manage their registered fingerprints within the app. This includes adding new fingerprints, removing outdated ones, or updating existing ones. The app acts as a centralized

hub for biometric data, ensuring an organized and user-friendly experience.

IV. IMPLEMENTATION

Working of Fingerprint Door Lock with Arduino Uno:

User Registration:

The process begins with users registering their fingerprints through a dedicated mobile app. This app utilizes the fingerprint sensor integrated into the user's smartphone. Users follow the prompts to add their unique biometric data securely.

Mobile App Communication:

Once the fingerprints are registered, the mobile app communicates with the Arduino Uno. The app sends the encrypted biometric data to the Arduino for real-time processing and authentication.

Arduino Processing:

The Arduino Uno serves as the central processing unit. It receives the fingerprint data from the mobile app and compares it with the stored templates of authorized users. The Arduino is programmed to handle the matching process efficiently.

Fingerprint Matching:

The Arduino performs the fingerprint matching algorithm to verify the identity of the user. If the received fingerprint data matches an authorized entry in its database, the Arduino triggers the next step in the process.

Servo Motor Activation:

Upon a successful fingerprint match, the Arduino sends a command to the servo motor. The servo motor, connected to the door latch, is activated. The motor's rotational motion is utilized to manipulate the door latch, either unlocking or locking the door, depending on its current state.

Door Unlocking:

With the servo motor's movement, the physical door latch is disengaged, allowing the door to be opened. The user, having successfully authenticated their fingerprint, gains access to the secured space.

Real-time Status Updates:

Throughout this process, the mobile app receives real-time status updates. Users are notified of the authentication result, providing transparency and

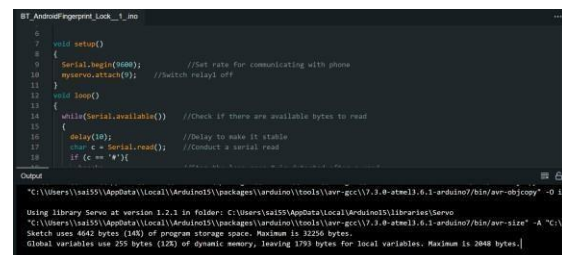
feedback regarding the success or failure of the fingerprint matching process.

Future Trends:

The future of mobile-controlled door locking systems is poised for significant advancements as the technology continues to evolve. Integration with smart home ecosystems will become increasingly seamless, allowing users to control and monitor their door locks remotely through a single app alongside other smart devices. Enhanced security features such as biometric authentication (fingerprint and facial recognition) and AI-driven anomaly detection will provide greater peace of mind and protection against unauthorized access. Additionally, the use of blockchain technology may offer tamper-proof access logs and secure communication protocols. As smart locks become more common, compatibility and interoperability with different smart home platforms and virtual assistants will improve, making installation and use more user-friendly. Finally, the convergence of IoT and machine learning will allow door locks to adapt and anticipate user preferences, offering personalized access control and automation based on user patterns.

V. RESULTS & DISCUSSION

Results:



```
07_ArduinoFingerprint_Lock_v1.ino
1 //
2 //
3 //
4 //
5 //
6 //
7 //
8 //
9 //
10 //
11 //
12 //
13 //
14 //
15 //
16 //
17 //
18 //
19 //
20 //
21 //
22 //
23 //
24 //
25 //
26 //
27 //
28 //
29 //
30 //
31 //
32 //
33 //
34 //
35 //
36 //
37 //
38 //
39 //
40 //
41 //
42 //
43 //
44 //
45 //
46 //
47 //
48 //
49 //
50 //
51 //
52 //
53 //
54 //
55 //
56 //
57 //
58 //
59 //
60 //
61 //
62 //
63 //
64 //
65 //
66 //
67 //
68 //
69 //
70 //
71 //
72 //
73 //
74 //
75 //
76 //
77 //
78 //
79 //
80 //
81 //
82 //
83 //
84 //
85 //
86 //
87 //
88 //
89 //
90 //
91 //
92 //
93 //
94 //
95 //
96 //
97 //
98 //
99 //
100 //
101 //
102 //
103 //
104 //
105 //
106 //
107 //
108 //
109 //
110 //
111 //
112 //
113 //
114 //
115 //
116 //
117 //
118 //
119 //
120 //
121 //
122 //
123 //
124 //
125 //
126 //
127 //
128 //
129 //
130 //
131 //
132 //
133 //
134 //
135 //
136 //
137 //
138 //
139 //
140 //
141 //
142 //
143 //
144 //
145 //
146 //
147 //
148 //
149 //
150 //
151 //
152 //
153 //
154 //
155 //
156 //
157 //
158 //
159 //
160 //
161 //
162 //
163 //
164 //
165 //
166 //
167 //
168 //
169 //
170 //
171 //
172 //
173 //
174 //
175 //
176 //
177 //
178 //
179 //
180 //
181 //
182 //
183 //
184 //
185 //
186 //
187 //
188 //
189 //
190 //
191 //
192 //
193 //
194 //
195 //
196 //
197 //
198 //
199 //
200 //
201 //
202 //
203 //
204 //
205 //
206 //
207 //
208 //
209 //
210 //
211 //
212 //
213 //
214 //
215 //
216 //
217 //
218 //
219 //
220 //
221 //
222 //
223 //
224 //
225 //
226 //
227 //
228 //
229 //
230 //
231 //
232 //
233 //
234 //
235 //
236 //
237 //
238 //
239 //
240 //
241 //
242 //
243 //
244 //
245 //
246 //
247 //
248 //
249 //
250 //
251 //
252 //
253 //
254 //
255 //
256 //
257 //
258 //
259 //
260 //
261 //
262 //
263 //
264 //
265 //
266 //
267 //
268 //
269 //
270 //
271 //
272 //
273 //
274 //
275 //
276 //
277 //
278 //
279 //
280 //
281 //
282 //
283 //
284 //
285 //
286 //
287 //
288 //
289 //
290 //
291 //
292 //
293 //
294 //
295 //
296 //
297 //
298 //
299 //
300 //
301 //
302 //
303 //
304 //
305 //
306 //
307 //
308 //
309 //
310 //
311 //
312 //
313 //
314 //
315 //
316 //
317 //
318 //
319 //
320 //
321 //
322 //
323 //
324 //
325 //
326 //
327 //
328 //
329 //
330 //
331 //
332 //
333 //
334 //
335 //
336 //
337 //
338 //
339 //
340 //
341 //
342 //
343 //
344 //
345 //
346 //
347 //
348 //
349 //
350 //
351 //
352 //
353 //
354 //
355 //
356 //
357 //
358 //
359 //
360 //
361 //
362 //
363 //
364 //
365 //
366 //
367 //
368 //
369 //
370 //
371 //
372 //
373 //
374 //
375 //
376 //
377 //
378 //
379 //
380 //
381 //
382 //
383 //
384 //
385 //
386 //
387 //
388 //
389 //
390 //
391 //
392 //
393 //
394 //
395 //
396 //
397 //
398 //
399 //
400 //
401 //
402 //
403 //
404 //
405 //
406 //
407 //
408 //
409 //
410 //
411 //
412 //
413 //
414 //
415 //
416 //
417 //
418 //
419 //
420 //
421 //
422 //
423 //
424 //
425 //
426 //
427 //
428 //
429 //
430 //
431 //
432 //
433 //
434 //
435 //
436 //
437 //
438 //
439 //
440 //
441 //
442 //
443 //
444 //
445 //
446 //
447 //
448 //
449 //
450 //
451 //
452 //
453 //
454 //
455 //
456 //
457 //
458 //
459 //
460 //
461 //
462 //
463 //
464 //
465 //
466 //
467 //
468 //
469 //
470 //
471 //
472 //
473 //
474 //
475 //
476 //
477 //
478 //
479 //
480 //
481 //
482 //
483 //
484 //
485 //
486 //
487 //
488 //
489 //
490 //
491 //
492 //
493 //
494 //
495 //
496 //
497 //
498 //
499 //
500 //
501 //
502 //
503 //
504 //
505 //
506 //
507 //
508 //
509 //
510 //
511 //
512 //
513 //
514 //
515 //
516 //
517 //
518 //
519 //
520 //
521 //
522 //
523 //
524 //
525 //
526 //
527 //
528 //
529 //
530 //
531 //
532 //
533 //
534 //
535 //
536 //
537 //
538 //
539 //
540 //
541 //
542 //
543 //
544 //
545 //
546 //
547 //
548 //
549 //
550 //
551 //
552 //
553 //
554 //
555 //
556 //
557 //
558 //
559 //
560 //
561 //
562 //
563 //
564 //
565 //
566 //
567 //
568 //
569 //
570 //
571 //
572 //
573 //
574 //
575 //
576 //
577 //
578 //
579 //
580 //
581 //
582 //
583 //
584 //
585 //
586 //
587 //
588 //
589 //
590 //
591 //
592 //
593 //
594 //
595 //
596 //
597 //
598 //
599 //
600 //
601 //
602 //
603 //
604 //
605 //
606 //
607 //
608 //
609 //
610 //
611 //
612 //
613 //
614 //
615 //
616 //
617 //
618 //
619 //
620 //
621 //
622 //
623 //
624 //
625 //
626 //
627 //
628 //
629 //
630 //
631 //
632 //
633 //
634 //
635 //
636 //
637 //
638 //
639 //
640 //
641 //
642 //
643 //
644 //
645 //
646 //
647 //
648 //
649 //
650 //
651 //
652 //
653 //
654 //
655 //
656 //
657 //
658 //
659 //
660 //
661 //
662 //
663 //
664 //
665 //
666 //
667 //
668 //
669 //
670 //
671 //
672 //
673 //
674 //
675 //
676 //
677 //
678 //
679 //
680 //
681 //
682 //
683 //
684 //
685 //
686 //
687 //
688 //
689 //
690 //
691 //
692 //
693 //
694 //
695 //
696 //
697 //
698 //
699 //
700 //
701 //
702 //
703 //
704 //
705 //
706 //
707 //
708 //
709 //
710 //
711 //
712 //
713 //
714 //
715 //
716 //
717 //
718 //
719 //
720 //
721 //
722 //
723 //
724 //
725 //
726 //
727 //
728 //
729 //
730 //
731 //
732 //
733 //
734 //
735 //
736 //
737 //
738 //
739 //
740 //
741 //
742 //
743 //
744 //
745 //
746 //
747 //
748 //
749 //
750 //
751 //
752 //
753 //
754 //
755 //
756 //
757 //
758 //
759 //
760 //
761 //
762 //
763 //
764 //
765 //
766 //
767 //
768 //
769 //
770 //
771 //
772 //
773 //
774 //
775 //
776 //
777 //
778 //
779 //
780 //
781 //
782 //
783 //
784 //
785 //
786 //
787 //
788 //
789 //
790 //
791 //
792 //
793 //
794 //
795 //
796 //
797 //
798 //
799 //
800 //
801 //
802 //
803 //
804 //
805 //
806 //
807 //
808 //
809 //
810 //
811 //
812 //
813 //
814 //
815 //
816 //
817 //
818 //
819 //
820 //
821 //
822 //
823 //
824 //
825 //
826 //
827 //
828 //
829 //
830 //
831 //
832 //
833 //
834 //
835 //
836 //
837 //
838 //
839 //
840 //
841 //
842 //
843 //
844 //
845 //
846 //
847 //
848 //
849 //
850 //
851 //
852 //
853 //
854 //
855 //
856 //
857 //
858 //
859 //
860 //
861 //
862 //
863 //
864 //
865 //
866 //
867 //
868 //
869 //
870 //
871 //
872 //
873 //
874 //
875 //
876 //
877 //
878 //
879 //
880 //
881 //
882 //
883 //
884 //
885 //
886 //
887 //
888 //
889 //
890 //
891 //
892 //
893 //
894 //
895 //
896 //
897 //
898 //
899 //
900 //
901 //
902 //
903 //
904 //
905 //
906 //
907 //
908 //
909 //
910 //
911 //
912 //
913 //
914 //
915 //
916 //
917 //
918 //
919 //
920 //
921 //
922 //
923 //
924 //
925 //
926 //
927 //
928 //
929 //
930 //
931 //
932 //
933 //
934 //
935 //
936 //
937 //
938 //
939 //
940 //
941 //
942 //
943 //
944 //
945 //
946 //
947 //
948 //
949 //
950 //
951 //
952 //
953 //
954 //
955 //
956 //
957 //
958 //
959 //
960 //
961 //
962 //
963 //
964 //
965 //
966 //
967 //
968 //
969 //
970 //
971 //
972 //
973 //
974 //
975 //
976 //
977 //
978 //
979 //
980 //
981 //
982 //
983 //
984 //
985 //
986 //
987 //
988 //
989 //
990 //
991 //
992 //
993 //
994 //
995 //
996 //
997 //
998 //
999 //
1000 //
1001 //
1002 //
1003 //
1004 //
1005 //
1006 //
1007 //
1008 //
1009 //
1010 //
1011 //
1012 //
1013 //
1014 //
1015 //
1016 //
1017 //
1018 //
1019 //
1020 //
1021 //
1022 //
1023 //
1024 //
1025 //
1026 //
1027 //
1028 //
1029 //
1030 //
1031 //
1032 //
1033 //
1034 //
1035 //
1036 //
1037 //
1038 //
1039 //
1040 //
1041 //
1042 //
1043 //
1044 //
1045 //
1046 //
1047 //
1048 //
1049 //
1050 //
1051 //
1052 //
1053 //
1054 //
1055 //
1056 //
1057 //
1058 //
1059 //
1060 //
1061 //
1062 //
1063 //
1064 //
1065 //
1066 //
1067 //
1068 //
1069 //
1070 //
1071 //
1072 //
1073 //
1074 //
1075 //
1076 //
1077 //
1078 //
1079 //
1080 //
1081 //
1082 //
1083 //
1084 //
1085 //
1086 //
1087 //
1088 //
1089 //
1090 //
1091 //
1092 //
1093 //
1094 //
1095 //
1096 //
1097 //
1098 //
1099 //
1100 //
1101 //
1102 //
1103 //
1104 //
1105 //
1106 //
1107 //
1108 //
1109 //
1110 //
1111 //
1112 //
1113 //
1114 //
1115 //
1116 //
1117 //
1118 //
1119 //
1120 //
1121 //
1122 //
1123 //
1124 //
1125 //
1126 //
1127 //
1128 //
1129 //
1130 //
1131 //
1132 //
1133 //
1134 //
1135 //
1136 //
1137 //
1138 //
1139 //
1140 //
1141 //
1142 //
1143 //
1144 //
1145 //
1146 //
1147 //
1148 //
1149 //
1150 //
1151 //
1152 //
1153 //
1154 //
1155 //
1156 //
1157 //
1158 //
1159 //
1160 //
1161 //
1162 //
1163 //
1164 //
1165 //
1166 //
1167 //
1168 //
1169 //
1170 //
1171 //
1172 //
1173 //
1174 //
1175 //
1176 //
1177 //
1178 //
1179 //
1180 //
1181 //
1182 //
1183 //
1184 //
1185 //
1186 //
1187 //
1188 //
1189 //
1190 //
1191 //
1192 //
1193 //
1194 //
1195 //
1196 //
1197 //
1198 //
1199 //
1200 //
1201 //
1202 //
1203 //
1204 //
1205 //
1206 //
1207 //
1208 //
1209 //
1210 //
1211 //
1212 //
1213 //
1214 //
1215 //
1216 //
1217 //
1218 //
1219 //
1220 //
1221 //
1222 //
1223 //
1224 //
1225 //
1226 //
1227 //
1228 //
1229 //
1230 //
1231 //
1232 //
1233 //
1234 //
1235 //
1236 //
1237 //
1238 //
1239 //
1240 //
1241 //
1242 //
1243 //
1244 //
1245 //
1246 //
1247 //
1248 //
1249 //
1250 //
1251 //
1252 //
1253 //
1254 //
1255 //
1256 //
1257 //
1258 //
1259 //
1260 //
1261 //
1262 //
1263 //
1264 //
1265 //
1266 //
1267 //
1268 //
1269 //
1270 //
1271 //
1272 //
1273 //
1274 //
1275 //
1276 //
1277 //
1278 //
1279 //
1280 //
1281 //
1282 //
1283 //
1284 //
1285 //
1286 //
1287 //
1288 //
1289 //
1290 //
1291 //
1292 //
1293 //
1294 //
1295 //
1296 //
1297 //
1298 //
1299 //
1300 //
1301 //
1302 //
1303 //
1304 //
1305 //
1306 //
1307 //
1308 //
1309 //
1310 //
1311 //
1312 //
1313 //
1314 //
1315 //
1316 //
1317 //
1318 //
1319 //
1320 //
1321 //
1322 //
1323 //
1324 //
1325 //
1326 //
1327 //
1328 //
1329 //
1330 //
1331 //
1332 //
1333 //
1334 //
1335 //
1336 //
1337 //
1338 //
1339 //
1340 //
1341 //
1342 //
1343 //
1344 //
1345 //
1346 //
1347 //
1348 //
1349 //
1350 //
1351 //
1352 //
1353 //
1354 //
1355 //
1356 //
1357 //
1358 //
1359 //
1360 //
1361 //
1362 //
1363 //
1364 //
1365 //
1366 //
1367 //
1368 //
1369 //
1370 //
1371 //
1372 //
1373 //
1374 //
1375 //
1376 //
1377 //
1378 //
1379 //
1380 //
1381 //
1382 //
1383 //
1384 //
1385 //
1386 //
1387 //
1388 //
1389 //
1390 //
1391 //
1392 //
1393 //
1394 //
1395 //
1396 //
1397 //
1398 //
1399 //
1400 //
1401 //
1402 //
1403 //
1404 //
1405 //
1406 //
1407 //
1408 //
1409 //
1410 //
1411 //
1412 //
1413 //
1414 //
1415 //
1416 //
1417 //
1418 //
1419 //
1420 //
1421 //
1422 //
1423 //
1424 //
1425 //
1426 //
1427 //
1428 //
1429 //
1430 //
1431 //
1432 //
1433 //
1434 //
1435 //
1436 //
1437 //
1438 //
1439 //
1440 //
1441 //
1442 //
1443 //
1444 //
1445 //
1446 //
1447 //
1448 //
1449 //
1450 //
1451 //
1452 //
1453 //
1454 //
1455 //
1456 //
1457 //
1458 //
1459 //
1460 //
1461 //
1462 //
1463 //
1464 //
1465 //
1466 //
1467 //
1468 //
1469 //
1470 //
1471 //
1472 //
1473 //
1474 //
1475 //
1476 //
1477 //
1478 //
1479 //
1480 //
1481 //
1482 //
1483 //
1484 //
1485 //
1486 //
1487 //
1488 //
1489 //
1490 //
1491 //
1492 //
1493 //
1494 //
1495 //
1496 //
1497 //
1498 //
1499 //
1500 //
1501 //
1502 //
1503 //
1504 //
1505 //
1506 //
1507 //
1508 //
1509 //
1510 //
1511 //
1512 //
1513 //
1514 //
1515 //
1516 //
1517 //
1518 //
1519 //
1520 //
1521 //
1522 //
1523 //
1524 //
1525 //
1526 //
1527 //
1528 //
1529 //
1530 //
1531 //
1532 //
1533 //
1534 //
1535 //
1536 //
1537 //
1538 //
1539 //
1540 //
1541 //
1542 //
1543 //
1544 //
1545 //
1546 //
1547 //
1548 //
1549 //
1550 //
1551 //
1552 //
1553 //
1554 //
1555 //
1556 //
1557 //
1558 //
1559 //
1560 //
1561 //
1562 //
1563 //
1564 //
1565 //
1566 //
1567 //
1568 //
1569 //
1570 //
1571 //
1572 //
1573 //
1574 //
1575 //
1576 //
1577 //
1578 //
1579 //
1580 //
1581 //
1582 //
1583 //
1584 //
1585 //
1586 //
1587 //
1588 //
1589 //
1590 //
1591 //
1592 //
1593 //
1594 //
1595 //
1596 //
1597 //
1598 //
1599 //
1600 //
1601 //
1602 //
1603 //
1604 //
1605 //
1606 //
1607 //
1608 //
1609 //
1610 //
1611 //
1612 //
1613 //
1614 //
1615 //
1616 //
1617 //
1618 //
1619 //
1620 //
1621 //
1622 //
1623 //
1624 //
1625 //
1626 //
1627 //
1628 //
1629 //
1630 //
1631 //
1632 //
1633 //
1634 //
1635 //
1636 //
1637 //
1638 //
1639 //
1640 //
1641 //
1642 //
1643 //
1644 //
1645 //
1646 //
1647 //
1648 //
1649 //
1650 //
1651 //
1652 //
1653 //
1654 //
1655 //
1656 //
1657 //
1658 //
1659 //
1660 //
1661 //
1662 //
1663 //
1664 //
1665 //
1666 //
1667 //
1668 //
1669 //
1670 //
1671 //
1672 //
1673 //
1674 //
1675 //
1676 //
1677 //
1678 //
1679 //
1680 //
1681 //
1682 //
1683 //
1684 //
1685 //
1686 //
1687 //
1688 //
1689 //
1690 //
1691 //
1692 //
1693 //
1694 //
1695 //
1696 //
1697 //
1698 //
1699 //
1700 //
1701 //
1702 //
1703 //
1704 //
1705 //
1706 //
1707 //
1708 //
1709 //
1710 //
1711 //
1712 //
1713 //
1714 //
1715 //
1716 //
1717 //
1718 //
1719 //
1720 //
1721 //
1722 //
1723 //
1724 //
1725 //
1726 //
1727 //
1728 //
1729 //
1730 //
1731 //
1732 //
1733 //
1734 //
1735 //
1736 //
1737 //
1738 //
1739 //
1740 //
1741 //
1742 //
1743 //
1744 //
1745 //
1746 //
1747 //
1748 //
1749 //
1750 //
1751 //
1752 //
1753 //
1754 //
1755 //
1756 //
1757 //
1758 //
1759 //
1760 //
1761 //
1762 //
1763 //
1764 //
1765 //
1766 //
1767 //
1768 //
1769 //
1770 //
1771 //
1772 //
1773 //
1774 //
1775 //
1776 //
1777 //
1778 //
1779 //
1780 //
1781 //
1782 //
1783 //
1784 //
1785 //
1786 //
1787 //
1788 //
1789 //
1790 //
1791 //
1792 //
1793 //
1794 //
1795 //
1796 //
1797 //
1798 //
1799 //
1800 //
1801 //
1802 //
1803 //
1804 //
1805 //
1806 //
1807 //
1808 //
1809 //
1810 //
1811 //
1812 //
1813 //
1814 //
1815 //
1816 //
1817 //
1818 //
1819 //
1820 //
1821 //
1822 //
1823 //
1824 //
1825 //
1826 //
1827 //
1828 //
1829 //
1830 //
1831 //
1832 //
1833 //
1834 //
1835 //
1836 //
1837 //
1838 //
1839 //
1840 //
1841 //
1842 //
1843 //
1844 //
1845 //
1846 //
1847 //
1848 //
1849 //
1850 //
1851 //
1852 //
1853 //
1854 //
1855 //
1856 //
1857 //
1858 //
1859 //
1860 //
1861 //
1862 //
1863 //
1864 //
1865 //
1866 //
1867 //
1868 //
1869 //
1870 //
1871 //
1872 //
1873 //
1874 //
1875 //
1876 //
1877 //
1878 //
1879 //
1880 //
1881 //
1882 //
1883 //
1884 //
1885 //
1886 //
1887 //
1888 //
1889 //
1890 //
1891 //
1892 //
1893 //
1894 //
1895 //
1896 //
1897 //
1898 //
1899 //
1900 //
1901 //
1902 //
1903 //
1904 //
1905 //
1906 //
1907 //
1908 //
1909 //
1910 //
1911 //
1912 //
1913 //
1914 //
1915 //
1916 //
1917 //
1918 //
1919 //
1920 //
1921 //
1922 //
1923 //
1924 //
1925 //
1926 //
1927 //
1928 //
1929 //
1930 //
1931 //
1932 //
1933 //
1934 //
1935 //
1936 //
1937 //
1938 //
1939 //
1940 //
1941 //
1942 //
1943 //
1944 //
1945 //
1946 //
1947 //
1948 //
1949 //
1950 //
1951 //
1952 //
1953 //
1954 //
1955 //
1956 //
1957 //
1958 //
1959 //
1960 //
1961 //
1962 //
1963 //
1964 //
1965 //
1966 //
1967 //
1968 //
1969 //
1970 //
1971 //
1972 //
1973 //
1974 //
1975 //
1976 //
1977 //
1978 //
1979 //
1980 //
1981 //
1982 //
1983 //
1984 //
1985 //
1986 //
1987 //
1988 //
1989 //
1990 //
1991 //
1992 //
1993 //
1994 //
1995 //
1996 //
1997 //
1998 //
1999 //
2000 //
2001 //
2002 //
2003 //
2004 //
2005 //
2006 //
2007 //
2008 //
2009 //
2010 //
2011 //
2012 //
2013 //
2014 //
2015 //
2016 //
2017 //
2018 //
2019 //
2020 //
2021 //

```

VI. CONCLUSION

mobile-controlled door locking systems are on the brink of transforming the way we manage access to our homes and properties. As technology advances, these systems will become more integrated, secure, and user-friendly, making them an essential part of the modern smart home. The introduction of biometric authentication, AI-powered security measures, and blockchain technology will enhance safety and reliability. Seamless compatibility with smart home platforms will simplify user experiences, while the convergence of IoT and machine learning will enable personalized and intelligent access control. These developments signal a promising future for mobile-controlled door locking systems, offering convenience, safety, and efficiency for users.

VII. FUTURE SCOPE

The proposed system will be enhanced in the future with more extensions. This device can be made economical in future so that anyone can afford it at low price. Some features like camera can be attached to help identify any intruders who attempt to unlock the door using the wrong key. We can run this work by building our own app rather than using an existing app, like Blynk..

VIII. REFERENCE

- [1] Ericsson AB. Iot security, white paper. <https://www.ericsson.com/assets/local/publications/white-papers/wp-iot-security-february-2017.pdf>. Accessed: 2017.
- [2] Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *Internet of Things Journal*, IEEE, 4(5):1125–1142, October 2017.
- [3] Kewei Sha, Ranadheer Errabelly, Wei Wei, T Andrew Yang, and Zhiwei Wang. Edgesec: Design of an edge layer security service to enhance iot security. In *Fog and Edge Computing (ICFEC)*, 2017 IEEE 1st International Conference on, pages 81–88. IEEE, 2017.
- [4] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. Smart locks: Lessons for securing commodity internet of things devices. Master's thesis, University of California, Berkeley, 2016.
- [5] Nan Zhang, Soteris Demetriou, Xianghang Mi, Wenrui Diao, Kan Yuan, Peiyuan Zong, Feng Qian, XiaoFeng Wang, Kai Chen, Yuan Tian, Carl A. Gunter, Kehuan Zhang, Patrick Tague, and Yue-H
- [6] Abdillahi Hassan Adnan, Mohamed Abdirazak, A.B.M Shamsuzzaman Sadi, Towfique Anam, Sazid Zaman Khan, and Mohammed Mahmudur Rahman. A comparative study of wlan security protocols: Wpa, wpa2. <http://ieeexplore.ieee.org/document/7506822/>, 2015.
- [7] Indiana University. What is the principle of least privilege? <https://kb.iu.edu/d/amsv>, 2017.
- [8] A. Perrig et al. In *The Tesla Broadcast Authentication Protocol*, *CryptoByte*, vol 5, pages 2–13.
- [9] George Hatzivasilis, Ioannis Papaefstathiou, Konstantinos Fysarakis, and Ioannis Askoxylakis. Secroute: 2end-to-end secure communications for wireless ad-hoc networks. In *Computers and Communications (ISCC)*, 2017 IEEE Symposium on, pages 558–563. IEEE, 2017.
- [10] Earlene Fernandes, Justin Paupore, Amir Rahmati, Daniel Simionato, Mauro Conti, and Atul Prakash. Flowfence: Practical data protection for emerging iot application frameworks. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 531–548, Austin, TX, 2016. USENIX Association.
- [11] Yan Michalevsky, Suman Nath, and Jie Liu. Mashable: Mobile applications of secret handshakes over bluetooth le. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, pages 387–400. ACM, 2016.
- [12] Aurelien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. <https://eprint.iacr.org/2010/332.pdf>.
- [13] Torry Harris. Cloud computing services—a comparison. *International Journal of Computer and Information Systems*, 3:1–18, 2010. 54
- [14] Google inc. Eddystone format. <https://developers.google.com/beacons/eddytone>.
- [15] Google inc. Eddystone ephemeral identifier. <https://developers.google.com/beacons/eddytone-eid>.
- [16] Sitepoint tutorials. What is a rest api. <https://www.sitepoint.com/developers-rest-api/>.
- [17] Tutorialspoint. Android architectural layers. https://www.tutorialspoint.com/android/android_architecture.htm.
- [18] Android developers. Android manifest. <https://developer.android.com/guide/topics/manifest/manifest-intro.html>.
- [19] Particle IO. Security check list of internet of things. Security check for iot devices, 3:7–9, 2017

MOBILE-CONTROLLED DOOR LOCKING SYSTEM



Guided By: Mr. P. Shanmukha Kumar
Assistant Professor

Abstract:

Technology has improved, and smart locking systems have become more sophisticated. Such a system is necessary in banks and businesses since it provides functions that let users control locks. The implementation's efficiency the system is incredibly helpful because of its functionality and user-friendly interface. Some homeowners aim to connect their home's numerous home automation devices. Those connected to a Windows-based PC are the most popular home controllers

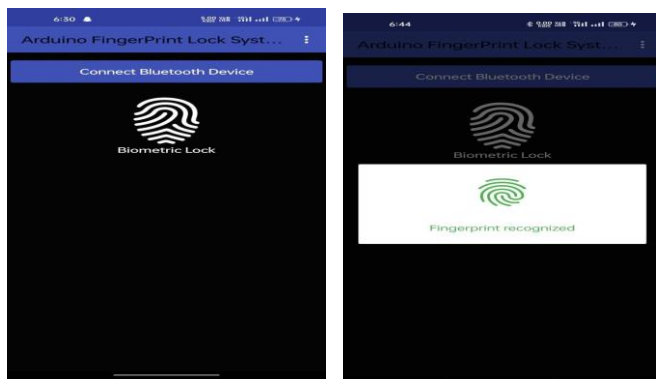
Introduction:

Everyone wants to be safe, whether that protection is in regards to his possessions or his own priceless life. Smart door control system is highly demanded & applicable project. A door acts as a first line of defense to keep the house physically secure. A physical key was initially required to open or close a door, but as technology advanced, a highly sophisticated smart door lock has been invented, which can unlock or lock doors without needing a physical key.

Objective:

The project employs key components such as the Arduino Uno microcontroller, a servo motor, a door latch, and a mobile phone fingerprint sensor. The synergy between these elements results in a secure and user-friendly system that replaces traditional keys with personalized biometric data.

Results:



The figures will describe about interface which directly interact with the user for the communication and the accessing the door lock.

[1] N. Jiwani, K. Gupta, and P. Whig, "Novel HealthCare Framework for Cardiac Arrest With the Application of AI Using ANN," in 2021.

[2] N. Jiwani, K. Gupta, and N. Afreen, "Automated Seizure Detection using Theta Band," in 2022.

Methods :

•**User Registration:** The process begins with users registering their fingerprints through a dedicated mobile app.

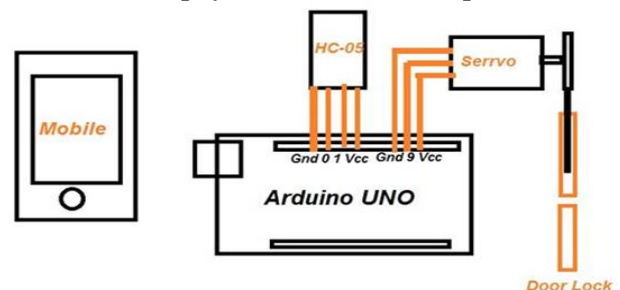
•**Mobile App Communication:** Once the fingerprints are registered, the mobile app communicates with the Arduino Uno.

•**Arduino Processing:** The Arduino Uno serves as the central processing unit. It receives the fingerprint data from the mobile app and compares.

•**Fingerprint Matching:** The Arduino performs the fingerprint matching algorithm to verify the identity of the user.

•**Servo Motor Activation:** Upon a successful fingerprint match, the Arduino sends a command to the servo motor. The servo motor is activated.

•**Door Unlocking:** With the servo motor's movement, the physical door latch is opened.



Conclusion:

Mobile-controlled door locking systems are on the brink of transforming the way we manage access to our homes and properties. As technology advances, these systems will become more integrated, secure, and user friendly, making them an essential part of the modern smart home.

Future Scope

The proposed system will be enhanced in the future with more extensions. This device can be made economical in future so that anyone can afford it at low price. Some features like camera can be attached to help identify any intruders who attempt to unlock the door using the wrong key. We can run this work by building own app rather than using an existing app, like Blynk..

Acknowledgement

Project Team : Batch 19

2111CS050110 – R. Sai Deepak Goud

2111CS050096 – S. Srinath

2111CS050076 – V. Ganga Manikanta Reddy

2111CS050078 – N. Harshitha

MALLA REDDY UNIVERSITY

DEPARTMENT OF INTERNET OF THINGS