Automatic Door Opener

MINOR PROJECT REPORT

By

ABHI GOVIL(RA2211003011493)
ARAV FERNANDEZ (RA2211003011505)
KHUSHI PATIL (RA2211003011497)

Under the guidance of

Dr. M. Karthikeyan

In partial fulfilment for the Course

of

21CSC201T – COMPUTER ORGANIZATION AND ARCHITECTURE

in Department of Computing Technology

FACULTY OF ENGINEERING AND TECHNOLOGY

SCHOOL OF COMPUTING

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

KATTANKULATHUR

NOVEMBER 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that this minor project report for the course **21CSC201T COMPUTER ORGANIZATION AND ARCHITECTURE** entitled in "**Automatic Door Lock Opener** " is the bonafide work of **ABHI GOVIL (RA2211003011493), ARAV FERNANDEZ (RA2211003011505)** and **KHUSHI PATIL (RA2211003011497)** who carried out the work under my supervision.

SIGNATURE

Dr. M. Karthikeyan
Assistant Professor
Department Of Computing Technology
SRM Institute of Science and Technology
Kattankulathur

ABSTRACT

In the realm of modern security systems, the Secure Automatic Door Lock Opener presented in this project leverages cutting-edge technology to provide both convenience and enhanced security. This project integrates the powerful Arduino Nano microcontroller and the HC-05 Bluetooth module, eliminating the need for traditional physical keys. A mobile device is used to capture and transmit fingerprint data for secure verification, revolutionizing the way we access controlled environments.

The heart of the system lies in the Arduino Nano, which efficiently processes fingerprint data and controls the door mechanism. The HC-05 module establishes seamless communication between the Arduino Nano and an Android mobile device, allowing users to interact with the lock system with ease.

Key features of this project include robust security measures to protect against unauthorized access. Fingerprint verification ensures that only authorized individuals can control the door lock, offering an additional layer of protection beyond traditional key-based systems. Furthermore, the system is designed to handle error cases gracefully and provides user feedback through LEDs or a dedicated Android app.

With a focus on both hardware and software, this project embodies the principles of Computer Organization and Architecture, showcasing how microcontrollers, Bluetooth technology, and biometric authentication can be harmoniously integrated to create a secure, user-friendly, and technologically advanced automatic door lock opener. This project paves the way for innovative advancements in door access control systems, setting a new standard for security and convenience in this domain.

ACKNOWLEDGEMENT

We express our heartfelt thanks to our honorable **Vice Chancellor Dr. C. Muthamizhchelvan**, for being the beacon in all our endeavors.

We would like to express my warmth of gratitude to our **Registrar Dr. S. Ponnusamy,** for his encouragement.

We express our profound gratitude to our **Dean (College of Engineering and Technology) Dr. T. Gopal,** for bringing out novelty in all executions.

We would like to express my heartfelt thanks to Chairperson, School of Computing **Dr. Revathi Venkataraman,** for imparting confidence to complete my course project.

We extend my gratitude to our **HoD Dr. M. Pushpalata Head of the Department, Department of Computing Technology.**

We are highly thankful to my Course project Faculty **Dr. M. Karthikeyan, Assistant Professor, Department of Computing Technology,** for his assistance, timely suggestion and guidance throughout the duration of this course project.

Finally, we thank our parents and friends near and dear ones who directly and indirectly contributed to the successful completion of our project. Above all, I thank the almighty for showering his blessings on me to complete my Course project.

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Motivation

The motivation behind this project stems from the pressing need for modernizing and fortifying door access control systems. Traditional key-based systems are susceptible to various security vulnerabilities, including unauthorized key duplication and the risk of key loss or theft. In an increasingly digital world, biometric authentication, such as fingerprint recognition, offers a more secure and convenient solution for controlling access to secure environments.

Furthermore, the project's aim is to exemplify the practical application of Computer Organization and Architecture principles in real-life scenarios. By using an Arduino Nano and the HC-05 Bluetooth module, we bridge the gap between theoretical knowledge and practical implementation. The project not only provides a tangible solution for secure door access but also serves as a valuable educational exercise, showcasing the potential for innovative, technology-driven enhancements to everyday security systems. It highlights the integration of hardware and software to address contemporary security challenges and sets the stage for the future development of advanced, user-centric security solutions.

1.2 Objective

The primary objective of this project is to design and develop a Secure Automatic Door Lock Opener with Fingerprint Verification using the Arduino Nano and HC-05 Bluetooth module. The project aims to enhance security by implementing a robust access control system that relies on biometric fingerprint verification, offering a higher level of security compared to traditional key-based systems.

Additionally, it seeks to provide users with a seamless and user-friendly method for controlling access to secure areas, eliminating the need to carry physical keys or remember passcodes.

The project serves as a practical application of knowledge by applying the principles of Computer Organization and Architecture to build a tangible system that combines hardware and software components, thus bridging the gap between theoretical knowledge and real-world solutions. It also prioritizes error handling and user feedback to ensure that the system can gracefully handle unexpected inputs and errors, enhancing the overall user experience and reliability.

Furthermore, the project focuses on establishing a secure and efficient communication link between the Arduino Nano and an Android mobile device, enabling users to manage the door lock through a dedicated app. Beyond its practical applications, this project holds educational value as it demonstrates the potential for technology-driven security enhancements and sets the stage for further development and integration with home automation and remote access control solutions.

1.3 Problem Statement

The problem at hand revolves around the need to modernize and fortify traditional door access control systems. Conventional key-based mechanisms pose security vulnerabilities such as unauthorized duplication and the risk of key loss or theft. To address these issues, this project endeavors to create a Secure Automatic Door Lock Opener using the Arduino Nano and HC-05 Bluetooth module, implementing biometric fingerprint verification to enhance security.

The project also aims to provide a user-friendly and efficient solution, eliminate the dependency on physical keys, and serve as an educational platform to bridge theoretical knowledge of Computer Organization and Architecture with practical, technology-driven security solutions.

1.4 Challenges

During the development of the Secure Automatic Door Lock Opener project, several challenges were encountered. Firstly, ensuring the reliability and security of the fingerprint verification system was a major challenge. Fingerprint data capture and matching required careful programming and extensive testing to minimize false positives and false negatives, as these could compromise the system's security.

Another challenge was the seamless integration of the Arduino Nano with the HC-05 Bluetooth module and the Android mobile device. Ensuring consistent and secure communication between these components was a complex task, requiring a deep understanding of hardware and software interfaces.

Error handling and feedback mechanisms posed an additional challenge. Designing the system to respond gracefully to unexpected inputs and provide meaningful feedback to the user required meticulous coding and thorough testing.

Physical security and tamper resistance were also critical concerns, as any vulnerability in the physical lock mechanism could compromise the entire system. Overall, developing this project required a combination of hardware and software expertise, rigorous testing, and a keen focus on security and user experience to overcome these challenges and deliver a robust, secure, and user-friendly automatic door lock opener.

2. LITERATURE SURVEY

The literature survey on secure automatic door lock systems with fingerprint verification reveals a growing interest in modernizing access control solutions, incorporating biometric authentication and wireless technologies. This survey highlights key findings from relevant research and publications.

Biometric Authentication: Various studies have emphasized the advantages of biometric authentication methods, particularly fingerprint recognition, in enhancing security for door access. Fingerprint recognition has been lauded for its uniqueness, reliability, and user convenience. Research has focused on optimizing fingerprint capture and matching algorithms to improve the accuracy and speed of verification.

Wireless Communication: Research frequently highlights the significance of wireless communication in access control systems. Bluetooth modules, like the HC-05 used in this project, have gained popularity for enabling secure and convenient communication between mobile devices and locking mechanisms. Researchers have explored Bluetooth's potential for secure data transmission and integration with various platforms, such as Android devices.

Security Considerations: A common thread in the literature is the paramount importance of security in door access control systems. Several studies emphasize the need for robust encryption and secure data storage to protect sensitive fingerprint information. Mitigating potential vulnerabilities, such as replay attacks and device theft, has been a focal point.

User Experience: User experience and ease of use have been highlighted in the literature as critical factors for the success of these systems. Researchers have explored the development of user-friendly mobile applications, feedback mechanisms, and error handling to enhance the overall user experience.

Integration and Future Directions: Literature suggests the potential for integrating automatic door lock systems with broader home automation solutions and remote access control. This integration could enhance the flexibility and functionality of access control, aligning with the growing trend of smart homes.

In summary, the literature survey underscores the convergence of biometrics and wireless technologies in secure door access control systems. Researchers and developers are increasingly focused on improving security, user experience, and integration with emerging technologies to meet the evolving needs of access control systems. This project aligns with these research trends and contributes to the growing body of knowledge in this field.

3. REQUIREMENT ANALYSIS

The requirement analysis phase of the Secure Automatic Door Lock Opener with Fingerprint Verification project aimed to define the essential elements and functions of the system. This phase encompassed gathering and prioritizing user and system requirements to guide the project's design and development. Key requirements included:

Security: Ensuring robust security was paramount. The system needed to provide secure fingerprint verification to prevent unauthorized access.

User-Friendly Interface: The system should be intuitive for users. The mobile app needed to offer a straightforward interface for fingerprint enrollment and door control.

Reliability: The system must reliably grant access to authorized users while minimizing false positives and false negatives in fingerprint recognition.

Communication: Efficient and secure communication between the mobile app and the Arduino Nano was a critical requirement. Data encryption was necessary to protect sensitive fingerprint information.

Error Handling: The system should gracefully manage unexpected inputs and provide clear feedback to users in case of errors.

Integration: The project aimed to seamlessly integrate the Arduino Nano, HC-05 module, Android app, and physical lock mechanism into a unified system.

Educational Value: The project was designed to serve as an educational tool, demonstrating the application of Computer Organization and Architecture principles. The requirement analysis phase set the foundation for the project's subsequent design and implementation, ensuring that it met user needs while prioritizing security and user experience.

4. ARCHITECTURE & DESIGN

System Architecture

The system architecture of the Secure Automatic Door Lock Opener with Fingerprint Verification comprises several interconnected components, ensuring both security and user-friendliness. At its core is the Arduino Nano, serving as the central processing unit, responsible for managing fingerprint data and controlling the door mechanism. The HC-05 Bluetooth module facilitates communication between the Arduino Nano and an Android mobile device, which is used for fingerprint data capture and user interaction.

The Android mobile app serves as the user interface, allowing individuals to enroll their fingerprints and control the door lock. The app securely communicates with the Arduino Nano via Bluetooth, sending authentication requests and lock/unlock commands. The Arduino, upon receiving a fingerprint match from the mobile app, triggers the relay to control the door lock's physical mechanism, ensuring secure access.

The hardware components also include the relay, which acts as the interface between the Arduino and the physical door lock. Additionally, the fingerprint sensor, while primarily part of the mobile device, plays a crucial role in the system's security. The system architecture emphasizes security, efficient communication, and user interaction, creating a robust and user-friendly automatic door lock system.

System Design

The system design is centered around security, user experience, and efficient communication. Users interact with the system through an Android mobile app, where they can enroll their fingerprints and control the door lock. Fingerprint data is captured securely by the mobile device and transmitted to the Arduino Nano via the HC-05 Bluetooth module. The Arduino Nano processes incoming data, verifies the fingerprint, and, upon successful authentication, triggers a relay to control the physical door lock.

The Android app provides a user-friendly interface for enrolling fingerprints and sending lock/unlock commands. The app communicates securely with the Arduino Nano using Bluetooth, implementing encryption to protect sensitive data. The Arduino's code includes error handling to gracefully manage unexpected inputs and provides feedback through LEDs to enhance user understanding and system reliability. The physical lock mechanism ensures that access control is tamper-resistant. Overall, the system design blends hardware and software components to create a secure, user-centric, and efficient automatic door lock opener.

5. IMPLEMENTATION

The implementation of the Secure Automatic Door Lock Opener with Fingerprint Verification project involved a step-by-step process that combined both hardware and software components to create a functional and secure system.

1. Hardware Setup: The hardware components included the Arduino Nano, HC-05 Bluetooth module, relay, and a mobile device equipped with a fingerprint sensor. The Arduino Nano served as the central processing unit, controlling the door lock mechanism via a relay. The HC-05 module established communication between the Arduino Nano and the Android mobile device. The fingerprint sensor on the mobile device captured and processed fingerprint data.

2. Software Development: The software component consisted of Arduino code and an Android mobile app. The Arduino code was responsible for receiving fingerprint data and control commands from the mobile app. It included functions for processing fingerprint data, error handling, and relay control. The Android app was designed to enroll and manage fingerprints and send lock/unlock commands to the Arduino. It was equipped with secure communication protocols to protect the integrity of fingerprint data.

3. Fingerprint Verification: Fingerprint data captured by the mobile device was sent to the Arduino Nano for verification. The system employed fingerprint matching algorithms to confirm the user's identity before granting access. The fingerprint sensor was rigorously tested to ensure accurate and consistent verification.

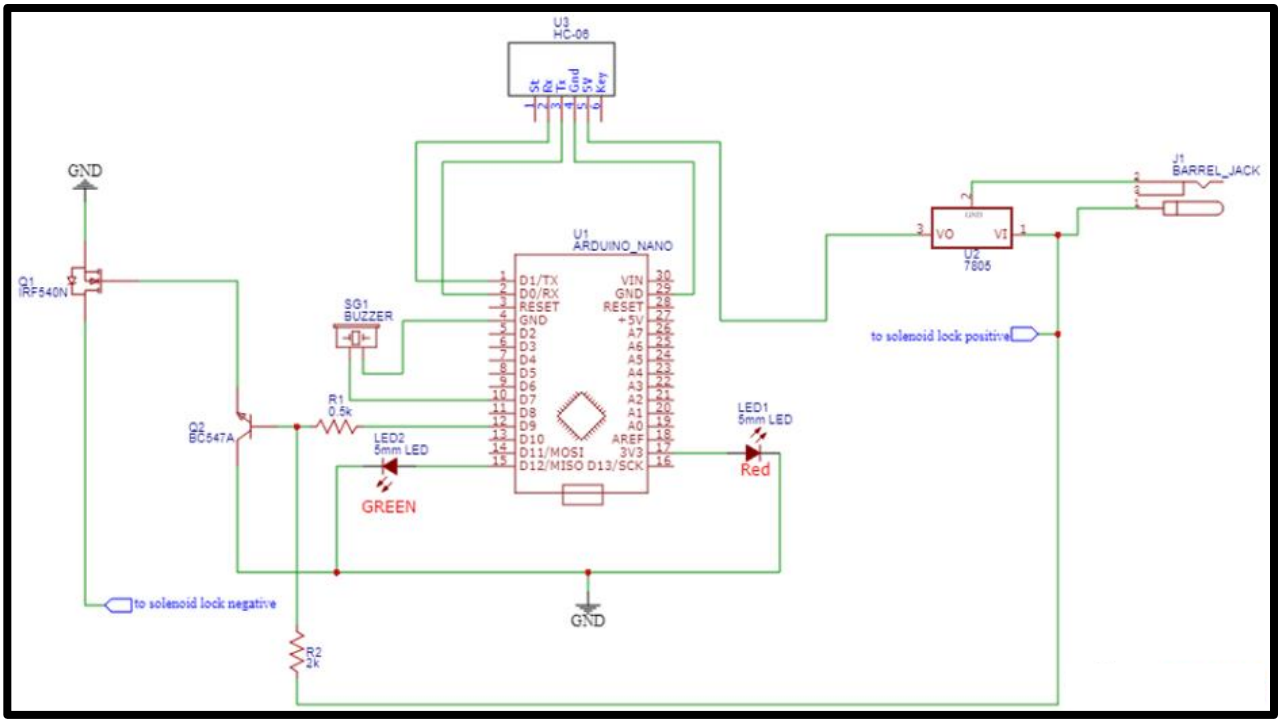
4. Error Handling: Robust error-handling mechanisms were implemented in the Arduino code to manage unexpected inputs and ensure the system's stability. Feedback was provided to the user through LEDs to indicate the system's status and any errors.

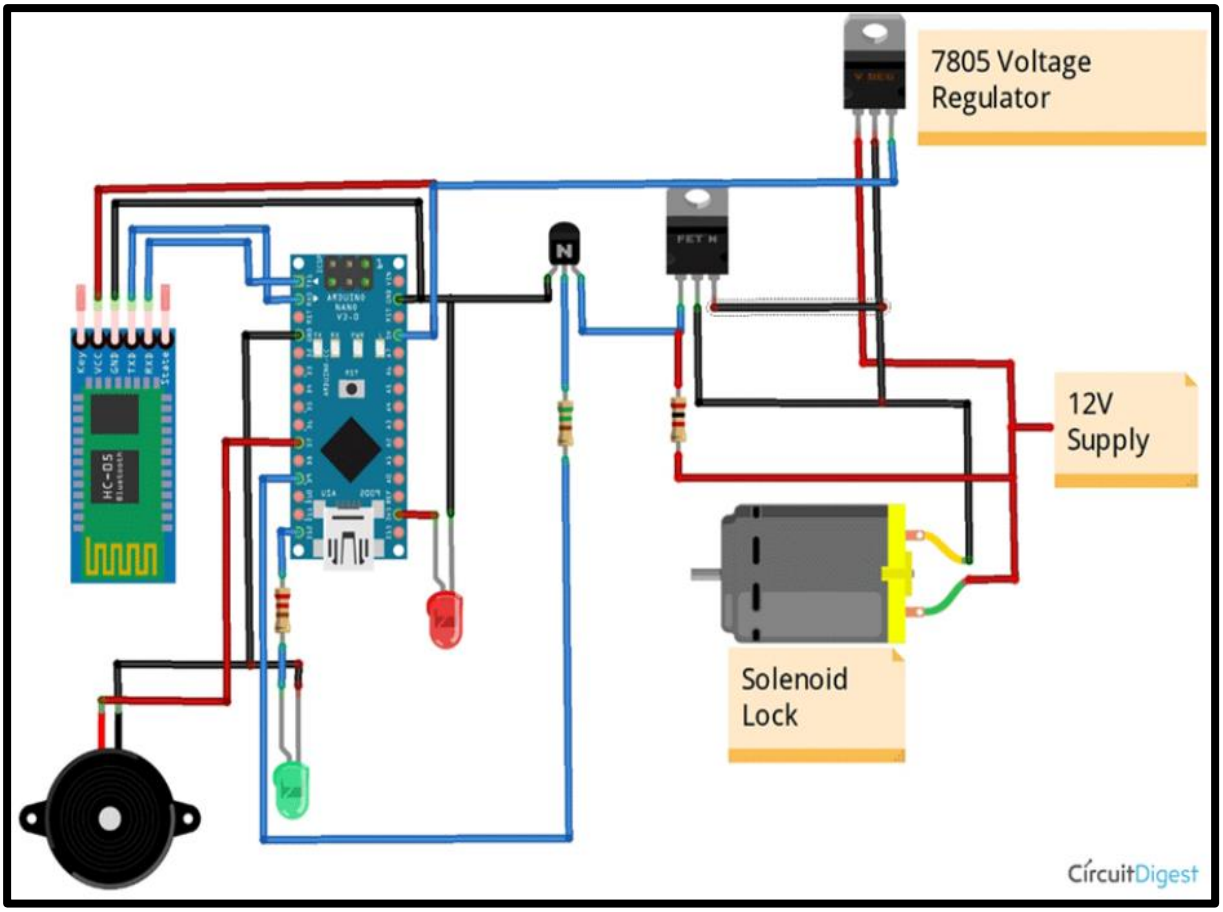
5. Integration and Testing: The components were integrated to ensure seamless communication between the mobile app and the Arduino Nano. Extensive testing was conducted to validate the system's functionality, security, and reliability. User feedback and user experience were key considerations during this phase.

6. Physical Lock Mechanism: The physical lock mechanism, controlled by the relay, was tested and integrated with the system to ensure that access control was executed securely and reliably.

The successful implementation of this project has resulted in a secure, user-friendly, and educationally valuable automatic door lock opener that showcases the practical application of Computer Organization and Architecture principles in creating a modern access control solution.

6. CIRCUIT AND CONNECTION DIAGRAM



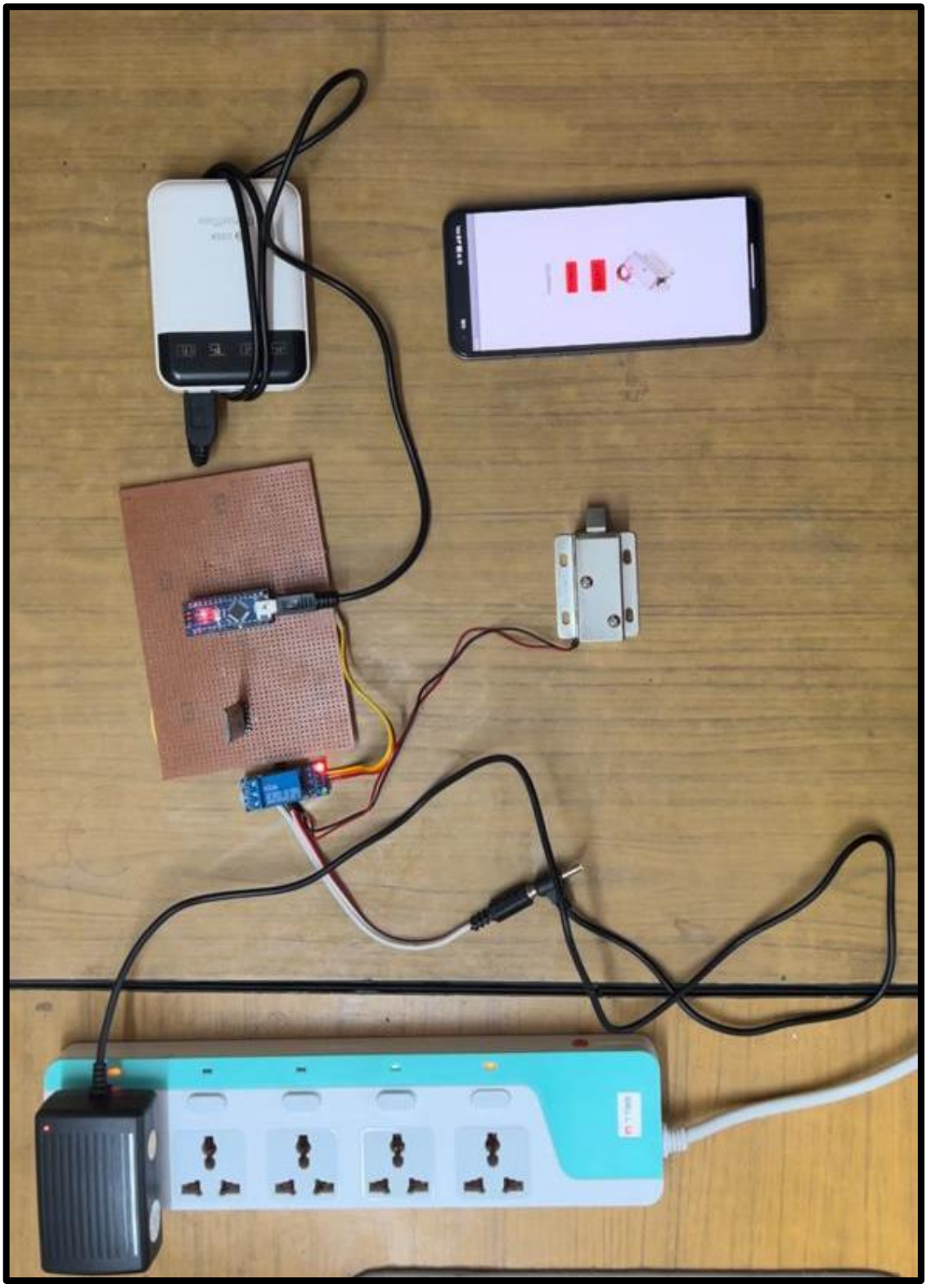

7805 Voltage Regulator
12V Supply
Solenoid Lock
CircuitDigest

7. ARDUINO CODE

```
char data = 0;                //Variable for storing received data
void setup()
{
Serial.begin(9600);
pinMode(12,OUTPUT);
digitalWrite(12,HIGH);
}


void loop()
{
  if(Serial.available() > 0)  // Send data only when you receive data:
  {
   data = Serial.read();      //Read the incoming data and store it into variable data
   if(data=='L')
    {
    digitalWrite(12,HIGH);
    }
    if(data=='U')
    {
    digitalWrite(12,LOW);
    }
   }
}
```

7. PROTOTYPE



8. CONCLUSION

In conclusion, the Secure Automatic Door Lock Opener with Fingerprint Verification project represents a successful fusion of cutting-edge technology and security, addressing the need for modern access control solutions. By leveraging the Arduino Nano and the HC-05 Bluetooth module, this project has demonstrated the practical application of Computer Organization and Architecture principles in creating a secure and user-friendly automatic door lock system.

The utilization of biometric fingerprint authentication enhances security by eliminating the risks associated with traditional key-based systems. This approach not only offers a higher level of protection but also provides a convenient and efficient means of accessing secure areas.

Throughout the development process, several challenges were encountered, including ensuring the reliability and security of the fingerprint verification system, seamless integration of hardware components, and robust error handling. These challenges were successfully addressed, resulting in a system that gracefully handles errors and provides users with essential feedback.

The system design emphasizes both security and user experience, and the integration of the Android app with the Arduino Nano ensures efficient and secure communication. The project holds significant educational value, demonstrating the practical application of theoretical knowledge while offering a foundation for future expansion and integration with emerging technologies.

Overall, this project stands as a testament to the potential for technology-driven security enhancements, setting a new standard for secure access control systems that prioritize both security and user convenience.

9. REFERENCES

1) CarlHamacher,ZvonkoVranesic,SafwatZaky,ComputerOrganization,5thed.,McGraw-Hill,2015

2) KaiHwang,FayeA.Briggs,Computer Architecture andParallelProcessing",3rded.,McGrawHill,2016

3) GhoshT.K.,ComputerOrganizationandArchitecture,3rded.,TataMcGraw-Hill,2011