SMART LOCK

1st Tuong Minh Ha, 2nd Nguyen Hien Trung Nam, 3rd Nguyen Thanh Hai,
and Dang Ngoc Minh Duc
FPT University, Ho Chi Minh Campus, Vietnam
{hamtse180009, namnhtse18376, haintse182766}@fpt.edu.vn, and ducdnm2@fe.edu.vn

Abstract

This project presents the design and implementation of a smart lock system that integrates enhanced security features and convenient access management. The system leverages a combination of hardware components and software programming to achieve reliable performance in various environments. Experimental results demonstrate the effectiveness of the proposed system in real-world applications.

I. Introduction

In recent years, the demand for smart home security systems has surged globally, driven by increasing concerns about personal safety and the convenience offered by modern technology [1], [2]. This project addresses critical research areas by focusing on localized security standards and market-specific features for domestic applications, as well as cross-border compatibility and export regulations for international markets.

A. Necessity and Topicality

The significance of this research lies in its ability to address several critical aspects:

- Enhanced Security: Smart locks integrate state-of-the-art security features such as robust encryption algorithms, tamper detection mechanisms, and automatic locking capabilities. These advancements significantly elevate protection against unauthorized access compared to traditional locks, meeting the stringent security needs of modern homeowners.
- Convenience: One of the key benefits of smart locks is their ability to offer unparalleled convenience. Users can remotely control door access through smartphone apps, voice commands, or biometric authentication methods. This eliminates the inconvenience of carrying physical keys, reduces the risk of lockouts, and enhances overall user experience.
- Access Management: Smart locks revolutionize access control by facilitating seamless management of digital keys. Homeowners can effortlessly issue temporary or permanent access permissions to family members, friends, or service providers, all of which can be monitored and modified in real-time. This flexibility not only enhances security but also simplifies home management tasks.
- Increasing Smart Home Adoption: As part of the expanding smart home ecosystem, smart locks play a pivotal role in enhancing connectivity and automation. They seamlessly integrate with other IoT devices such as security cameras, lighting systems, and voice assistants. This interconnectedness fosters a more cohesive and responsive home environment, where various systems work together to enhance security and convenience.
- Growing Security Concerns: The increasing prevalence of security threats and burglaries has underscored the need for robust home security solutions. Smart locks address these concerns by providing real-time alerts and remote monitoring capabilities, empowering homeowners with greater control and peace of mind over their property's security.
- Technological Advancements: Continuous advancements in technology, including improved encryption protocols, AI-driven features for predictive security, and enhanced compatibility with IoT platforms, continually enhance the functionality and reliability of smart locks. These technological innovations make smart locks increasingly attractive to consumers seeking sophisticated yet user-friendly home security solutions.

B. Scientific and Practical Significance

The project contributes to both scientific research and practical applications:

- Research and Development: By exploring cutting-edge advancements in smart lock technology, this project drives innovation and sets new benchmarks for future security solutions. It aims to expand the capabilities of smart locks, making them more adaptable to diverse user needs and environmental conditions.
- Real-World Applications: Practical implementations of smart locks in residential settings demonstrate their efficacy in enhancing security and convenience. Case studies and field trials showcase how smart locks improve daily living experiences by streamlining access control and bolstering home security measures.
- Economic Impact: The widespread adoption of smart home technologies, including smart locks, stimulates economic growth by creating new markets for innovative products and services. It fosters job creation, promotes technological investment, and enhances consumer spending in the home security sector.

- Social Impact: Beyond economic benefits, smart locks contribute to a safer and more connected community environment. By enhancing home security and simplifying access management, smart locks empower homeowners to better protect their families and properties, fostering a sense of security and peace of mind.
- Biometric and Authentication Research: They advance research in biometric authentication, encryption techniques, and secure communication protocols.
- Convenience: They provide keyless entry, remote locking/unlocking, and integration with other smart home devices, enhancing user convenience.

II. System Models and Block Diagram

The developed system comprises both hardware and software components. On the hardware side, the system includes input devices (keypad and fingerprint sensor), output devices (LCD 16x2, servo motor, LED, buzzer), and a wireless communication module (ESP8266). On the software side, the system utilizes various computer codes to perform the desired functions, including unlocking the door, registering fingerprints, changing passwords, and logging access attempts to a Google Sheet via the ESP8266 module.A block diagram of the Smart Lock system is presented in Figure 1 to provide an easy visualization of the entire system. From the diagram, a discrete idea of all the incorporated modules/devices and their responsibilities can be achieved on a macro level.

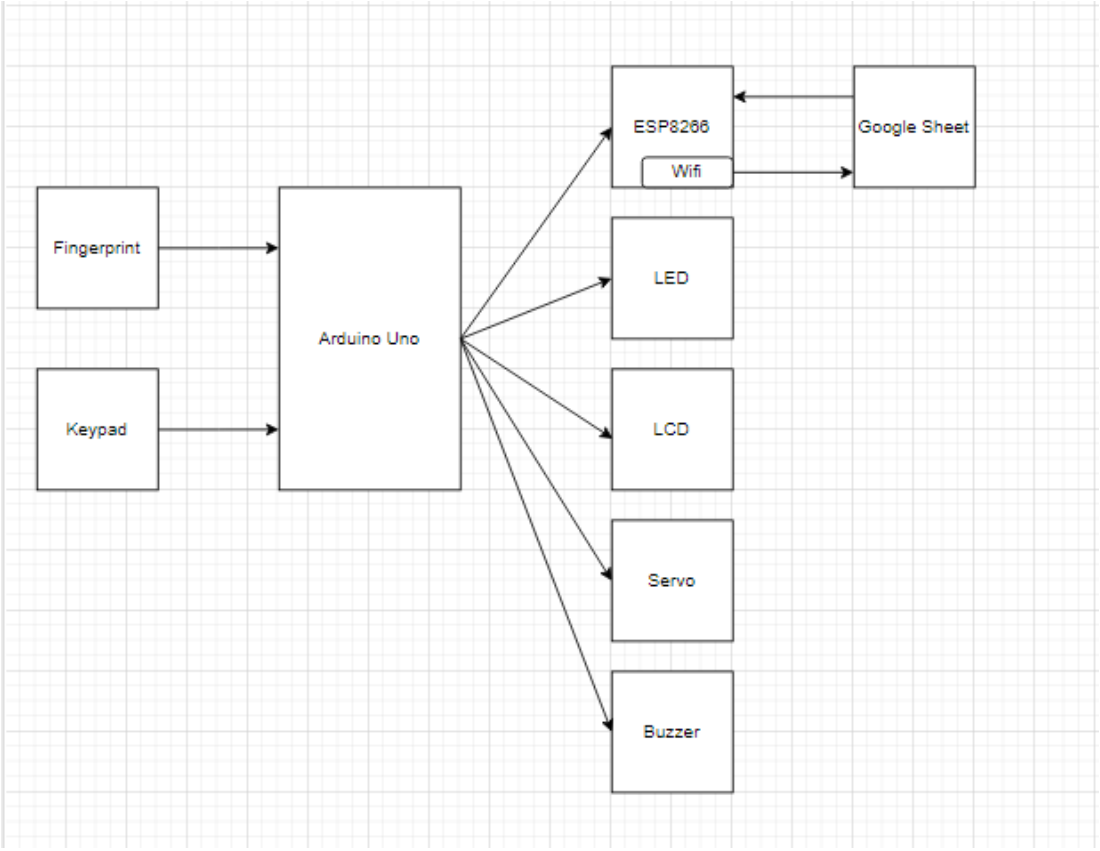


Fig. 1: Block Diagram of Smart Lock System

The block diagram shows the interconnection between input devices (keypad and fingerprint sensor), output devices (LCD 16x2, servo motor, LED, buzzer), and the wireless communication module (ESP8266).

III. Components and Peripheral Devices

The Smart Lock system integrates a variety of electronic devices and components to ensure secure and efficient access control. Key components include an Arduino [3] and ESP8266 (NodeMCU) [4] as the central processing units, sensors for biometric authentication (fingerprint sensor) and user input (keypad), and output devices such as an LCD 16x2 display, servo motor, LED indicators, and a buzzer. These components work together to facilitate secure door unlocking, user authentication, and logging of access attempts. The total list of required components and tools is provided in Table I.

Components/devices	ID/remarks
Arduino Uno R3	ATmega328P based
NodeMCU	ESP8266
Keypad	4x4 matrix keypad
Fingerprint sensor	AS608
Liquid-crystal display(LCD)	16 x 2 LCD
Servo motor	SG90
LED	
Buzzer	Piezo Speaker

TABLE I: System's components and peripheral devices

- **INPUT**: Keypad, Fingerprint sensor
- **OUTPUT**: LCD 16x2, Servo motor, LED, buzzer
- **WIRELESS**: ESP8266

A. Input Devices

1) Keypad

Keypads are a popular input device used in Arduino projects, including Internet of Things (IoT) applications [5]. Keypads provide a simple way for users to interact with the system by entering numeric or alphabetic data. In this project, the keypad is used to input numerical codes or passwords, playing a crucial role in the system's security and user interaction.

2) Fingerprint Sensor

Fingerprint sensors are critical in IoT systems, particularly in security applications. These sensors authenticate users based on their fingerprints, offering a high level of security compared to traditional methods. In this project, the fingerprint sensor provides biometric authentication, ensuring secure access control based on unique fingerprint patterns.

B. Output Devices

1) LCD 16x2

The 16x2 LCD display is widely used in Arduino projects for its ability to display 16 characters across 2 lines, making it ideal for presenting clear information to users. In this project, the LCD 16x2 display shows messages and feedback, serving as a user-friendly interface for system interactions.

2) Servo Motor

Servo motors provide precise control over angular position, making them valuable for applications requiring accurate movement control. In this project, the servo motor is employed to control physical locks or mechanisms, responding to input from the keypad and fingerprint sensor to secure or release access.

3) LED

LEDs (Light Emitting Diodes) are versatile components used in various IoT projects to indicate system status through illumination. In the Smart Lock system, LEDs serve as visual indicators, signaling events such as successful authentication or system errors.

4) Buzzer

Buzzers generate audible alerts, useful for notifying users about system events or errors. In this project, the buzzer provides auditory feedback, alerting users to events like successful access, incorrect password attempts, or other critical alerts.

C. Wireless Communication

1) ESP8266

The ESP8266 is a cost-effective Wi-Fi module enabling IoT devices like Arduino to connect to Wi-Fi networks and the internet [6], [7]. It simplifies data exchange and remote control capabilities in IoT applications. In the Smart Lock project, the ESP8266 module facilitates wireless communication, enabling remote access management and data logging capabilities over Wi-Fi networks..

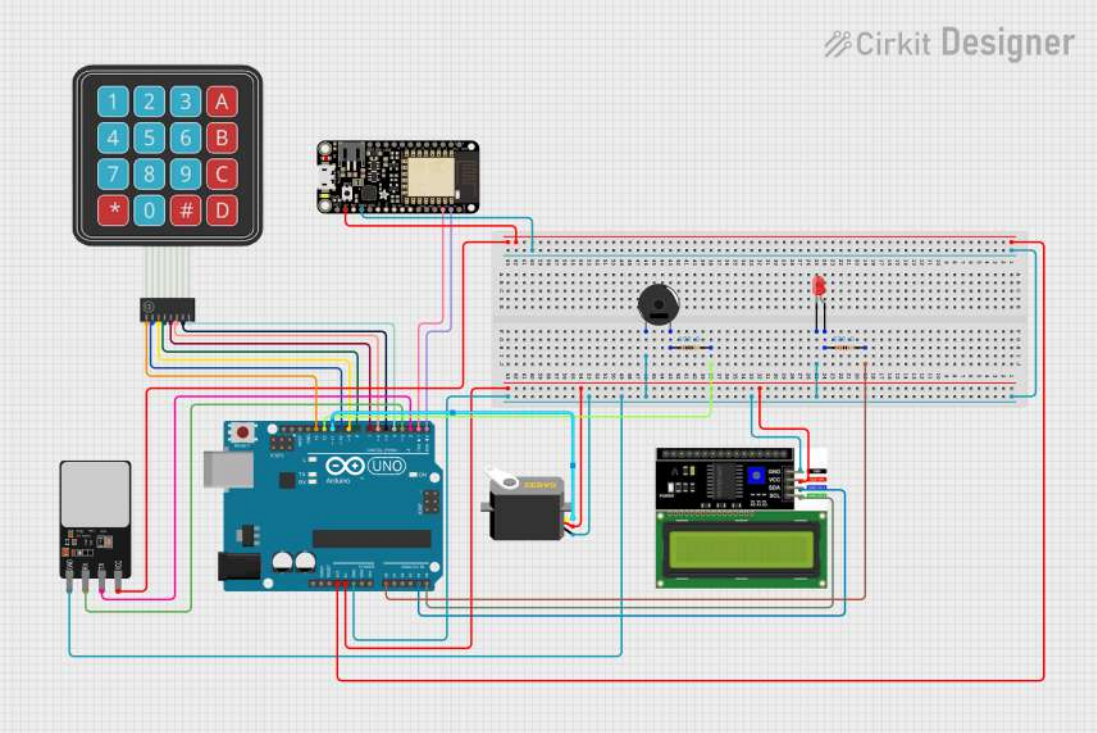


Fig. 2: Circuit schematic/hardware interfacing

IV. Electronic Circuit/Hardware Interfacing

Arduino Uno R3 and NodeMCU ESP8266-12E are integral to the Smart Lock system, managing tasks such as user authentication and door control based on input from the keypad and fingerprint sensor. Figure 2 illustrates the circuit schematic, detailing how components like the keypad, fingerprint sensor, LCD display, servo motor, LED indicators, and buzzer are connected to Arduino Uno. NodeMCU ESP8266 facilitates wireless communication for remote access management and data logging. Detailed interfacing specifications can be found in Tables II.

Arduino Uno	Keypad	Fingerprint	ESP8266	LED	LCD display	Servo motor	Buzzer
GND		GND	GND	GND	GND	GND	Negative
VCC (5v)					VCC	VCC	
VCC (3.3v)		VCC	VCC				
Pin - 0			TX				
Pin - 1			RX				
Pin - 2		TX					
Pin - 3		RX					
Pin - 4	C4						
Pin - 5	C3						
Pin - 6	C2						
Pin - 7	C1						
Pin - 8	R4						
Pin - 9	R3						
Pin - 10	R2						
Pin - 11						Control	
Pin - 12							Pin - 12 (positive)
Pin - 13	R1						
A0				A0(anode)			
A4					SDA		
A5					SCL		

TABLE II: Interfacing between Arduino Uno and its components (pin-to-pin)

V. Software Programming

The system's functionality is programmed using the Arduino IDE [8], [9], ensuring ease of implementation and future scalability. It includes modules for reading inputs from the keypad and fingerprint sensor, processing authentication requests, controlling the servo motor and buzzer, and interfacing with the LCD display for user feedback.

A. Programming Flowchart

This flowchart outlines the sequential steps involved in the Smart Lock system's operation. It begins with initializing components and verifying the fingerprint sensor's presence. Subsequently, the system waits for user input from either the keypad or fingerprint sensor. Depending on the input received, it executes the corresponding authentication process. If the authentication is successful, it triggers the servo motor to unlock the door and provides appropriate feedback. If unsuccessful, it manages retry attempts and activates security measures if necessary. Flowchart arduino and esp8266 can be found in Figure 3 and Figure 4

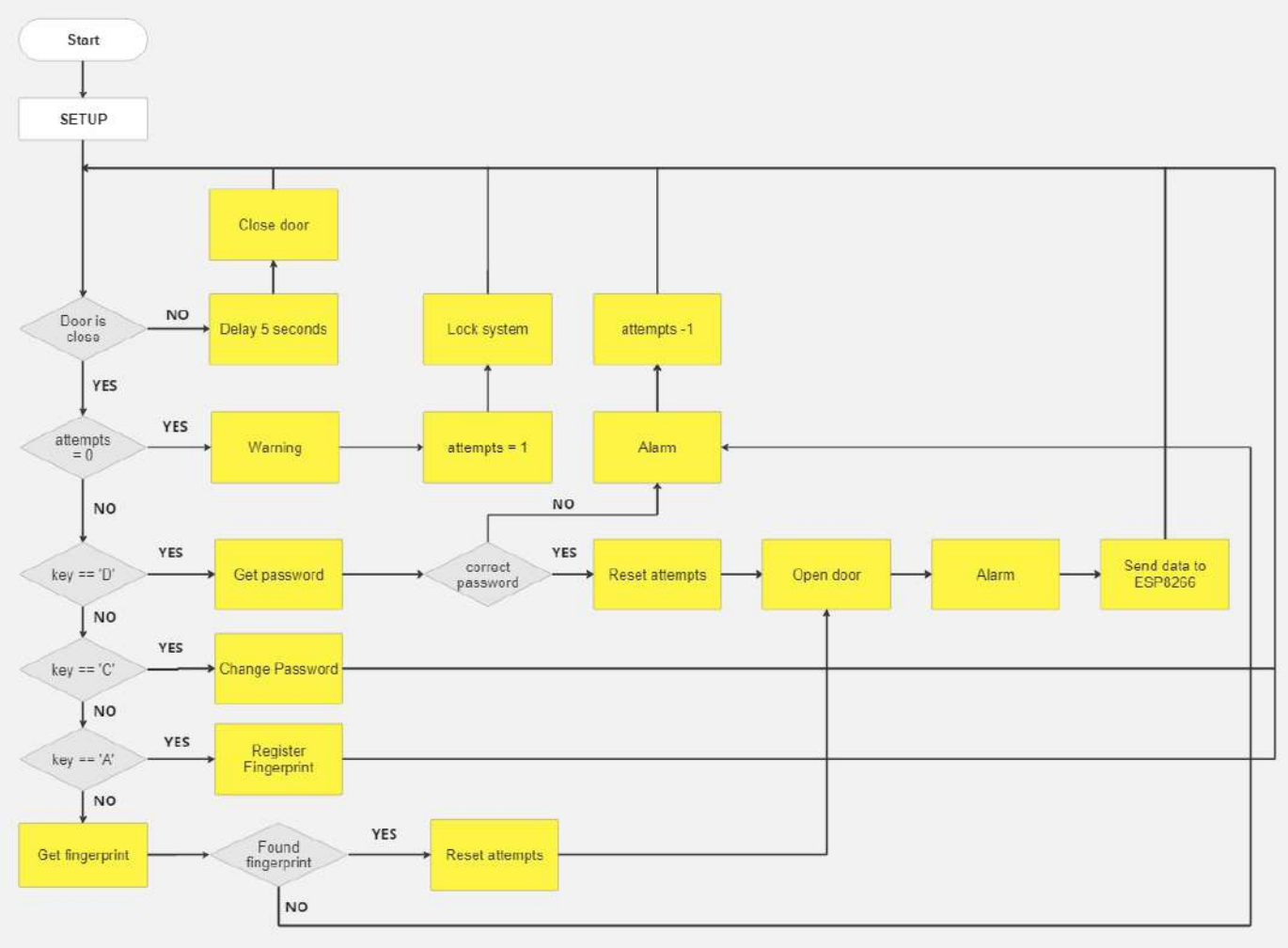


Fig. 3: Programming flowchart of Smart Lock System

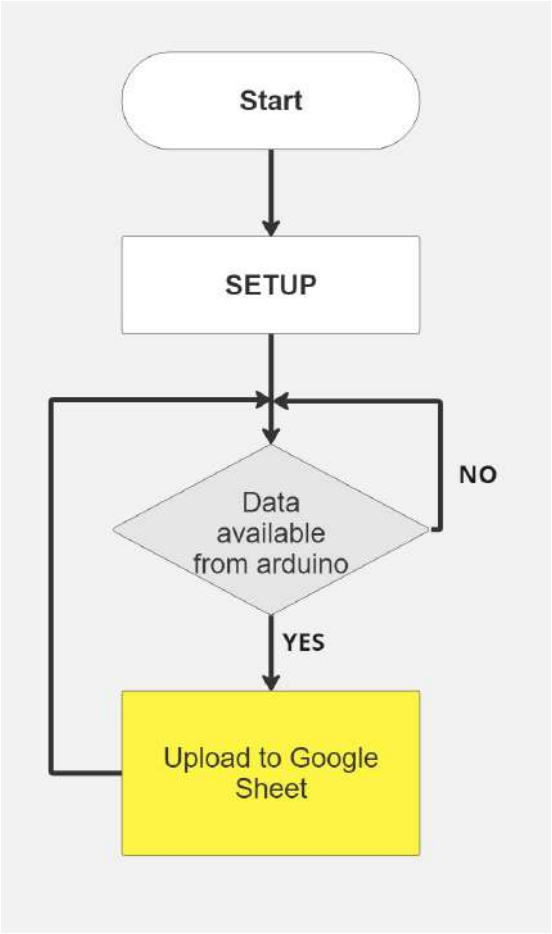


Fig. 4: Programming flowchart of ESP8266 of Smart Lock System

The flowchart delineates the operational workflow of a smart lock system, beginning with an initialization phase, followed by a series of conditional checks and user interactions. Initially, the system checks if the door is closed. If the door is opened, the door will close after 5 seconds, else if the door is closed and user enter not thing then system will repeat until have new operation. The system then checks for the number of failed attempts. If there have been three failed attempts, a warning is issued, and the system is locked. Otherwise, it proceeds to check for specific key inputs.

If the key ”D” is pressed, the system prompts the user to enter a password. Upon entering the correct password, the attempt counter is reset, the door is opened, and data is sent to the ESP8266 module. If the password is incorrect, the attempt counter is incremented.

For key ”C”, the system enters password change mode, allowing the user to change the password.

For key ”A”, the system enters fingerprint registration mode to register a new fingerprint.

When the system prompts for a fingerprint, it checks for a valid fingerprint match. If a valid fingerprint is found, the attempt counter is reset, the door is opened, and data is sent to the ESP8266. If a valid fingerprint is not found, the attempt counter is incremented.

This structured approach ensures that the smart lock system responds effectively to user inputs while maintaining security by locking the system after multiple failed attempts and providing functionalities for password and fingerprint management.

B. Setting Up IoT Server (Google Sheet)

In order to integrate your IoT device with a Google Sheet server for data logging, follow these steps:

1) **Network Setup:** Connect ESP8266 device to local WiFi network.
2) **Google Script Deployment ID:** Obtain Google Script Deployment ID (GScriptId).
3) **HTTPS Connection Setup:**
   - Initialize the WiFi connection with network credentials.
   - Use the `HTTPSRedirect` library to establish a secure connection to Google’s server.
4) **Sending Data:**

- Construct a JSON payload with the required data.
- Send the data to Google Sheets using a POST request to the specified URL.

VI. Results and Discussion

A. Prototype Implementation

The smart lock prototype was implemented and tested for functionality. The components were integrated seamlessly to ensure reliable performance. Relevant studies and previous research were cited to support our methodology Figure 5 and shows the prototype of the practical device with the labeling of its components.

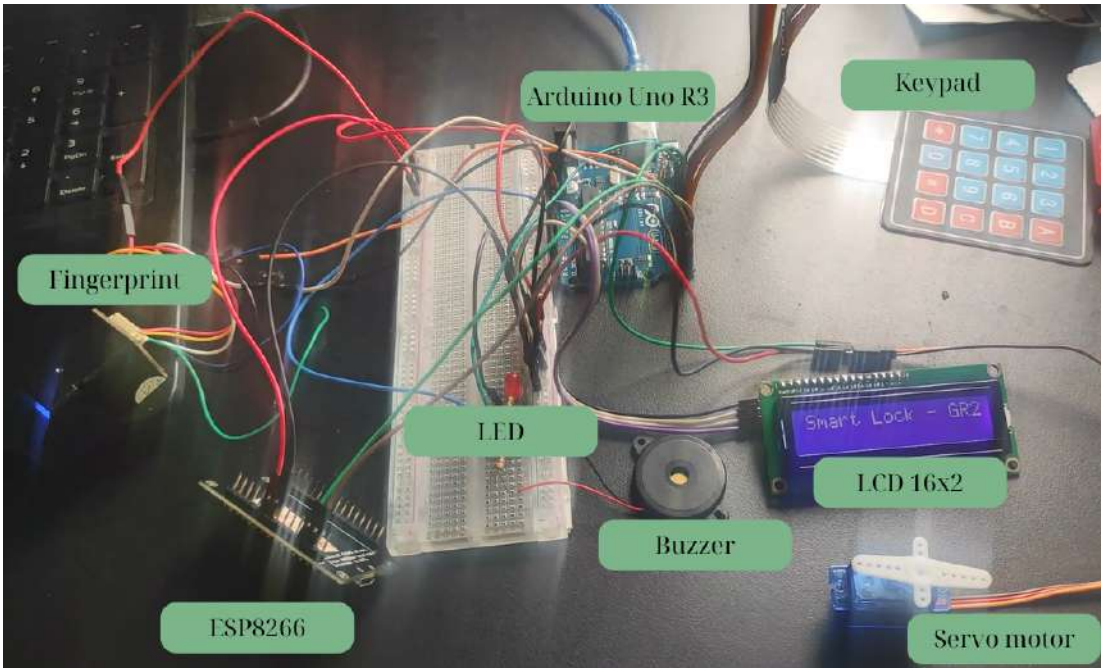


Fig. 5: Prototype of the Smart Lock System

B. Results from Prototype Testing

Door Opening Test

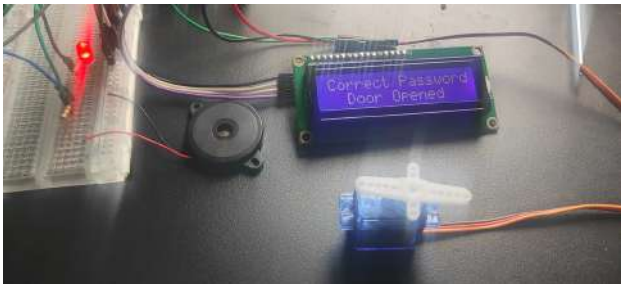
In the door opening test, authorized users approached the smart lock system and authenticated themselves using registered fingerprints or passwords. Upon successful authentication, indicated by a LED and a confirmation message on the LCD screen (Fig. 6a), the servo motor activated, unlocking the door. The system logged the access event, including the date, method (fingerprint or password), and success status, which was then transmitted to a Google Sheet for record-keeping and analysis (Fig. 7).

Incorrect Password Test

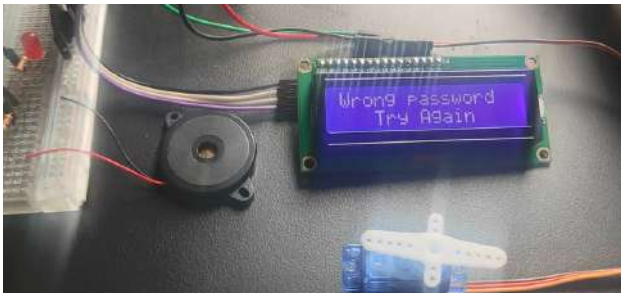
During the incorrect password entry test, unauthorized attempts to access the smart lock were made using incorrect passwords. The system promptly detected these attempts, displaying a red LED indicator and an error message on the LCD screen (Fig. 6b). Additionally, the system recorded the third failed access attempt, including the date, method (password), and failure status, updating the Google Sheet accordingly.

C. Experimental Results

The experimental results demonstrated the effectiveness of the smart lock system in enhancing security and providing convenient access management. The system was tested under various conditions to validate its robustness.



(a) Door open



(b) LCD screen displaying wrong password

Fig. 6: Prototype Test

2024/07/14	13:54:42	Fingerprint	Fail to open
2024/07/14	13:54:05	Keypad	Fail to open
2024/07/14	13:53:09	Keypad	Success to open
2024/07/14	13:52:43	Keypad	Success to open
2024/07/14	13:52:05	Keypad	Fail to open

Fig. 7: Check log time on Google Sheet

D. Discussion

The results of the project were discussed in the context of current market trends and technological advances. In today's market, there is a significant increase in smart home technology aimed at improving security, convenience, and connectivity. Our information locking system aligns with this trend by optimally integrating with IoT ecosystems, allowing users to manage remotely via mobile applications or voice commands. This flexibility not only enhances user convenience but also provides a smarter and more connected living environment.

Technological advances, especially in the fields of AI and machine learning, open up opportunities to improve the features of our smart lock systems. Future versions can leverage this progress to provide advanced security features, version adaptive access control, and interaction based on behavioral data and environmental conditions. These developers not only enhance security but also effectively expect and respond to user needs in real time.

Furthermore, the potential for future growth is unlimited in the field of technology whose expansion has demonstrated wide scalability and applicability in various practical problems. The system's reliable performance in tests validates its stability under a variety of environmental conditions, ensuring security and continuous performance in residential environments.

The practical application of our smart lock system is not limited to households but also includes common areas, short-term rentals and commercial real estate. The system's flexibility and appropriate computing make it suitable for streamlined integration into large smart city projects, contributing to urban urban improvement and infrastructure management.

VII. Conclusion

The project successfully developed a robust smart lock system that addresses fundamental security and convenience concerns. By leveraging advanced hardware components and sophisticated software programming, the system demonstrated reliable performance and practical applicability in real-world scenarios. The outcomes underscore the project's significant contributions to enhancing security through innovative IoT solutions [10]. The research and development efforts focused on integrating state-of-the-art security features, including robust encryption, biometric authentication, and remote access management capabilities. These advancements not only meet the stringent security needs of homeowners but also enhance the overall user experience by eliminating traditional lock-related inconveniences. Future iterations will aim to further optimize system compatibility with diverse environmental conditions and expand functionality to meet evolving consumer demands.

VIII. Author's Contribution

TABLE III: Author's Contribution

#	Student ID	Student Name	Tasks	Contribution
1	SE183876	Nguyen Hien Trung Nam	Draw program flowchart, Integrate ESP8266 for WiFi connectivity and Google Sheets logging, Design and implement user interface for LCD and keypad interactions, video clip	40%
2	SE180009	Tuong Minh Ha	Draw block diagram, Implement Arduino code for keypad and fingerprint sensor integration, Circuit installation	30%
3	SE182766	Nguyen Thanh Hai	Draw block diagram, Implement Arduino code for keypad and fingerprint sensor integration, Circuit installation	30%
Total			100%	

References

[1] R. Banerjee, "Smart lock system using arduino and iot," in *2019 International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 5, no. 2. IJSR, 2019, pp. 2456–3307.

[2] H. Patel and S. Patel, "Design and implementation of a smart lock system using iot," in *2017 International Journal of Computer Applications*. IJCA, 2017, pp. 23–26.

[3] S. Monk, *Programming Arduino: Getting Started with Sketches*. McGraw-Hill, 2016.

[4] M. Schwartz, *Internet of Things with ESP8266*. Packt Publishing, 2016.

[5] K. Ramachandran, A. Dey, and S. Mukherjee, "An iot based smart lock system using rfid and password protection," in *2019 IEEE International Conference on Distributed Computing, VLSI, Electrical Circuits and Robotics (DISCOVER)*. IEEE, 2019, pp. 1–6.

[6] E. Khorov, A. Lyakhov, and R. Yusupov, "Two-slot based model of the ieee 802.11ah restricted access window with enabled transmissions crossing slot boundaries," in *IEEE 19th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM)*, 2018, pp. 1–9.

[7] M. Tellez, S. El-Tawab, and H. M. Heydari, "Improving the security of wireless sensor networks in an iot environmental monitoring system," in *2016 IEEE systems and information engineering design symposium (SIEDS)*. IEEE, 2016, pp. 72–77.

[8] J. Nussey, *Arduino Projects for Dummies*. Wiley, 2013.

[9] J. Boxall, *Arduino Workshop: A Hands-On Introduction with 65 Projects*. No Starch Press, 2013.

[10] T. Anagnostopoulos, A. Zaslavsky, K. Kolomvatsos, A. Medvedev, P. Amirian, J. Morley, and S. Hadjieftymiades, "Challenges and opportunities of waste management in iot-enabled smart cities: a survey," *IEEE Transactions on Sustainable Computing*, vol. 2, no. 3, pp. 275–289, 2017.