INNOVATIVE SMART LOCK SYSTEM FOR EFFICIENT DOOR MANAGEMENT

By

ADEL ALJAED	**2036396**	**COMPUTER**
AWS ALSAEDI	**2035072**	**COMPUTER**
AHMED BADAHDH	**2035096**	**COMPUTER**

TEAM NO.: 08 **FALL 2024 INTAKE**

Project Advisor

DR.SAUD WASLY

Project Customer

DR.SAUD WASLY

EE 499 SENIOR DESIGN PROJECT

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
FACULTY OF ENGINEERING
KING ABDULAZIZ UNIVERSITY
JEDDAH – SAUDI ARABIA

DECEMBER 2024 G – JUMADA II 1446 H

INNOVATIVE SMART LOCK SYSTEM FOR EFFICIENT DOOR MANAGEMENT

By

ADEL ALJAED	**2036396**	**COMPUTER**
AWS ALSAEDI	**2035072**	**COMPUTER**
AHMED BADAHDH	**2035096**	**COMPUTER**

TEAM NO.: 08 **FALL 2024 INTAKE**

A senior design project report submitted in partial fulfillment of the requirements for the degree of

Bachelor of Science

in

Electrical and Computer Engineering

King Abdulaziz University, Jeddah, Saudi Arabia

Checked and Approved (Advisor): 

SDP Evaluator: _____

ABSTRACT

INNOVATIVE SMART LOCK SYSTEM FOR EFFICIENT DOOR MANAGEMENT

Access control is a crucial element of modern building security. Traditional physical locks have several limitations, including key misplacement, unauthorized duplication, and lack of centralized management. Our project aims to design and implement a Smart Lock System that leverages Bluetooth Low Energy (BLE) communication, local authentication, and a structured backend database to provide a secure, scalable, and user-friendly access solution.

The system consists of a custom ESP32-based smart lock controller and a mobile application built using Flutter. Key features include seamless BLE broadcasting communication without formal pairing, fast login using biometric authentication on mobile devices, and dynamic attendance and door operation history merging. Validation experiments confirmed operational range up to 10 meters, mobile app response within 2 seconds and stable BLE communication.

This project demonstrates a reliable, energy-efficient smart lock system ready for deployment in residential, academic, and commercial environments.

Index Terms — e.g. Smart Lock, Remote Access, Mobile Application, Security, Encryption, Home Automation, Bluetooth Connectivity.

ACKNOWLEDGEMENT

We, the members of Team 8, would like to sincerely express our deepest gratitude to our advisor, Dr. Saud Wasly, for his invaluable support, expert guidance, and continuous encouragement throughout the development of our Smart Lock System project.

We also extend our sincere appreciation to Dr. Ehab Ashary, Eng. Abdulhadi Bashathi, and Eng. Abdulaziz Ghurab for their insightful feedback, technical advice, and valuable contributions, which significantly enhanced the quality of our work.

Furthermore, we recognize and appreciate the dedication, teamwork, and collaboration among our team members: Eng. Aws Hazzaa Alsaedi, Eng. Adel Saer F. Aljaed, and Eng. Ahmed Khalid Badahdh. The success of this project would not have been possible without the collective efforts and shared commitment of every team member.

Finally, we would like to thank the Electrical and Computer Engineering Department at King Abdulaziz University for providing the resources and environment necessary for the successful completion of this project.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER – 1 INTRODUCTION

1.1 BACKGROUND

With the rapid evolution of smart entity technology, security has become a top priority for companies. Smart locks, integrated with mobile applications, offer a convenient and secure solution for managing access to residential properties. As cyber-attacks and unauthorized access attempts increase, designing systems with enhanced encryption and security protocols becomes imperative.

Smart locks function using electrical systems, they can verify the user in a variety of ways, including (but not limited to) passwords, fingerprints, facial recognition, and, in some advanced ways, retinal scans. The problem lies within the management of each lock, and some loosely designed locks pose a health hazard to each user. To better provide a grip on managing each lock, some companies opted to add visual data through cameras and a log system that is similarly difficult to manage.

While a log system provides stable control, a camera functioning above every door remains a pipe dream to manage and implement. However, a smart lock system still retains qualities that can be taken advantage of to provide an advanced user experience. One can schedule events, record employee attendance, add/delete doors smoothly, control temporary and emergency access, and much more.

1.2 PROBLEM STATEMENT

Traditional locks are prone to break-ins and unauthorized access; they are also unable to provide comprehensive reports for access. While many smart lock systems either lack advanced security features or are expensive and difficult to use, they can also be tough to customize and improve. Thus, leading to poor experience, potential break-ins, authentication issues, and unclear structure. Many locks also use biometric authentication, which introduces health hazards. As a result, many doors still use physical-based locks that are growing increasingly difficult to manage and sustain.

1.3 Project Objectives

1.3.1 Higher-level objectives

i. Enhance Security: facilitate corporate door security by providing remote access management, as well as hashing algorithms with public and private keys for encryption.
ii. Eliminate Unauthorized Access: lockdown doors that are vulnerable to access incidents by implementing authentication mechanisms.
iii. Advanced Access: create a seamless method of access that eliminates the need for a centralized locking mechanism.
iv. Comprehensive Management: Introduce an efficient management system across the employee base to track attendance and performance.
v. Secure Data Storage: Handle and store all sensitive data in a specialized relational database, and provide secure access to it.

1.3.2 Lower-level objectives

i. Wireless Lock: Design a smart lock chip that integrates seamlessly with a mobile app for remote control, through BLE technology.
ii. Advanced Alerts: Provide real-time alerts and notifications for door activities (lock/unlock status, attempted break-ins).
iii. Server Side: Construct a centralized server, handling all access requests and data transfer.
iv. Secure APIs: Introduce several API points to facilitate and secure data access.
v. Encrypted Channels: Achieve secure communication using encryption protocols.
vi. Informative Attendance: Implement a robust employee attendance system to better manage employee performance.

1.4 Product Design Specifications (PDS)

1.4.1 Musts

i. Mobile App Integration: The system must include a comprehensive mobile application capable of both user and admin actions.
ii. Encryption: Communication between the lock and the mobile app must be safely end-to-end encrypted.
iii. Bluetooth Range: The lock must be operable on a range of 5 meters (16 feet).
iv. Response Time: The system must process unlock commands within 2 seconds from receiving the user’s input in the mobile app.

1.4.2 Wants

i. Storage Capacity: The electronic chip should be able to store up to 100 access logs locally for retrieval in the mobile app.

ii. Admin Features: The mobile app should allow administrators to add or remove up to 10 users, schedule temporary access for specific times, and view access logs for the past 30 days.

iii. Proximity Unlock: The system should allow automatic unlocking when the authorized user is within a 1-meter radius, with a detection accuracy of 95% or higher.

iv. Alerts and Notifications: The mobile app should notify users within 3 seconds of any failed access attempts or low battery warnings.

1.4.3 Constraints

i. Budget: The total cost for the prototype, including hardware components and software development, must not exceed 2000 SAR.

ii. Physical Dimensions: The smart lock mechanism must fit within a standard lock cavity measuring 100mm x 50mm x 40mm to ensure compatibility with existing door frames.

1.4.4 Assumptions

i. Building Infrastructure: It is assumed that the building where the smart lock system will be implemented has clear, well-defined entrance and exit points to ensure proper access control. Additionally, the building should be equipped with existing electrically-based locking mechanisms compatible with the smart lock system.

ii. User Equipment: We assume that the users (homeowners, property managers, tenants) will have access to a smart device, such as a smartphone or tablet, with Bluetooth and WiFi capabilities to interact with the smart lock system efficiently.

iii. Network and Connectivity: The building is assumed to have a reliable and stable WiFi network to ensure the system functions seamlessly for remote access and control of the locks.

iv. Power Supply: A consistent and reliable power supply is assumed to be available within the building to support the continuous operation of the locking system and its components.

v. User Proficiency: Users are assumed to have basic knowledge of operating smart devices and mobile applications, as the system will rely on a user-friendly app for efficient door management.

vi. Security Protocols: The building's WiFi network is expected to have adequate security measures in place to prevent unauthorized access to the smart lock system.

vii. Electrical Connection: The door should be installed with secure, measured electrical connections.

1.4.5 Engineering Standards

i. IEEE 802.11 (Wi-Fi Standards): This standard defines specifications for implementing wireless local area network (WLAN) communication, enabling smart locks to connect to Wi-Fi networks and support remote access.

ii. IEEE 802.15.1 (Bluetooth Standards): Establishes guidelines for Bluetooth Low Energy (BLE) technology, which supports proximity-based smart lock control and efficient energy consumption.

iii. IEEE 2410-2021 (IoT Security and Privacy): Provides a framework for securing IoT devices, emphasizing encryption, secure APIs, and data privacy for smart lock systems.

iv. ISO/IEC 29192-2:2019 (Lightweight Encryption): Specifies encryption protocols suitable for devices with limited computational power, such as smart locks using AES-256 or Elliptic Curve Cryptography.

v. ANSI/BHMA A156.36-2020: Defines performance requirements for electronic locks, focusing on durability, reliability, and user safety.

1.4.5 Project Deliverables

i. A Smart Lock Prototype.

ii. A fully developed Flutter-based mobile application supporting user authentication, door control, and real-time notifications.

iii. A backend database with secure FastAPI API endpoints.

iv. A complete user guide documenting system setup, operation, and troubleshooting.

2.1 CURRENT TECHNOLOGIES IN SMART LOCK SYSTEMS

The development of smart lock systems has progressed significantly in recent years, driven by the growing demand for secure and convenient access control. Modern smart locks incorporate various technologies, including Bluetooth Low Energy (BLE), Wi-Fi, and biometric authentication, each tailored to address specific user needs.

BLE-Based Systems: BLE technology has become a cornerstone for proximity-based smart locks, such as the August Smart Lock [1]. This technology enables energy-efficient communication between the lock and the user's mobile device within a limited range of approximately 10 to 30 meters. BLE is particularly favored for its low power consumption, which is ideal for battery-operated devices. However, its range limitations restrict its usability to on-site control, making it less practical for users who require remote access.

Wi-Fi-Enabled Smart Locks: Wi-Fi-based systems, like the Nest x Yale Lock [2], offer users the ability to manage their locks remotely through mobile apps. This functionality provides greater flexibility, especially for individuals managing properties or granting temporary access to visitors. Moreover, these locks often integrate with popular smart home ecosystems such as Google Home and Amazon Alexa, offering seamless control. Despite these advantages, Wi-Fi locks rely heavily on a stable internet connection and consume more power than their BLE counterparts, which can be a concern in energy-conscious environments.

Biometric Authentication Systems: Biometric systems, such as the Ultraloq U-Bolt Pro [3], add an extra layer of security by utilizing fingerprint or facial recognition technology. These systems eliminate the need for physical keys or passwords, making unauthorized access significantly more difficult. However, concerns about the storage and security of biometric data, particularly in cloud-based systems, continue to pose challenges for widespread adoption.

Encryption plays a critical role in all these technologies, with protocols such as AES-256 and RSA being widely implemented to secure communications between the lock, the mobile application, and the cloud server [4]. These encryption techniques not only safeguard user data but also bolster trust in the system's reliability.

Several commercial smart lock systems have been developed globally, offering different features. The August Smart Lock utilizes Bluetooth Low Energy (BLE) for local access control and integrates Wi-Fi bridges for remote operation [5]. The Nest × Yale Lock offers cloud-based key sharing and real-time activity monitoring through mobile apps [6]. Additionally, the Schlage Encode Smart Lock combines Wi-Fi connectivity and encryption protocols to enable secure remote

unlocking [7]. These real-world examples highlight the importance of secure wireless communication, local database verification, and strong encryption, all of which are addressed by our proposed Smart Lock System.

2.2 Past Designs in Smart Lock Systems

The journey to modern smart lock systems began with simpler mechanical and electronic designs, each of which introduced new functionalities while revealing critical limitations.

Keypad and RFID Systems: Early electronic locks relied on keypads or RFID cards, providing basic security through PIN codes or card-based access. While these systems were innovative for their time, they lacked the advanced features of today's locks, such as remote access or real-time monitoring. Keypad systems were particularly vulnerable to wear and tear, with frequently used digits becoming visibly worn over time, thereby compromising security. RFID cards, while more secure, were limited by their range and the risk of being cloned [5].

Mechanical Locks: Before electronic locks gained prominence, traditional mechanical locks were the primary means of securing doors. These locks, though simple and inexpensive, were easily bypassed through lock-picking or key duplication techniques [6]. Additionally, their inability to log or monitor access activities made them inadequate for modern security requirements.

These early designs laid the groundwork for modern smart locks by highlighting vulnerabilities, such as reliance on physical keys and the lack of user authentication mechanisms, that newer technologies have sought to address.

2.3 Solutions to Similar Problems in the Literature

Numerous studies have explored innovative solutions to enhance the security, reliability, and efficiency of smart lock systems. These include addressing issues like unauthorized access, power management, and data privacy.

Elliptic Curve Cryptography (ECC): ECC has emerged as a viable encryption alternative for resource-constrained devices, such as smart locks. It provides robust security while requiring significantly less computational power compared to traditional encryption methods [7]. This makes ECC particularly suitable for energy-efficient IoT devices.

Blockchain Technology: The use of blockchain technology has been proposed to create tamper-proof access logs. By decentralizing and securing data, blockchain ensures that every access attempt is recorded immutably, enhancing accountability and transparency in high-security environments [8].

Backup Power and Low-Energy Communication Protocols: To address power outages, backup battery systems are recommended to ensure uninterrupted operation. Protocols like Zigbee have also been explored to minimize energy consumption while maintaining stable connectivity, making them a practical alternative to Wi-Fi in some scenarios [9].

Localized Data Storage: Concerns about the privacy and security of sensitive data, particularly biometric information, have led to recommendations for localized storage. Storing data on the device itself, rather than in the cloud, aligns with global data protection standards such as GDPR and minimizes the risk of data breaches [10].

2.4 Common Themes and Summary

The recurring theme across the reviewed literature is the need to balance security, convenience, and system reliability in smart lock designs. Each technology comes with its unique strengths and challenges:

BLE systems provide energy efficiency but are constrained by range.

Wi-Fi systems enable remote control but depend on stable internet and consume more power.

Biometric systems offer high security but raise concerns about data privacy and compliance.

Our project aims to address these challenges by implementing a Wi-Fi-based smart lock **system** that integrates advanced encryption, real-time monitoring, and local data storage. By building on the strengths of existing technologies and mitigating their limitations, this project seeks to deliver a reliable, user-friendly, and secure solution for modern access control.

CHAPTER - 3 PROJECT DESIGN

3.1 ALTERNATIVE DESIGN

3.1.1 Design 1

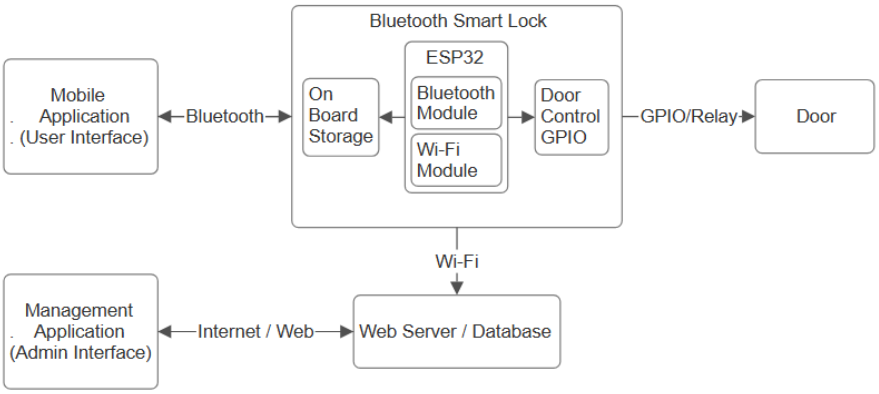


Figure3.1: Block Diagram of Design #1

Bluetooth-Based Proximity Smart Lock This design uses **Bluetooth Low Energy (BLE)** to enable short-range control of the lock via a mobile device. The lock unlocks at command when the user's phone is within a certain range (approximately 30 meters). BLE's low power consumption makes it ideal for smart locks that need to function efficiently for extended periods of battery power.

i. **Main Components**: BLE chip, mobile app, encryption module (AES-256), electronic lock interface.

ii. **Advantages**: Energy-efficient, seamless operation within a short range, low implementation cost.

iii. **Disadvantages**: Overcrowding of doors based on the range.

3.1.2 Design 2

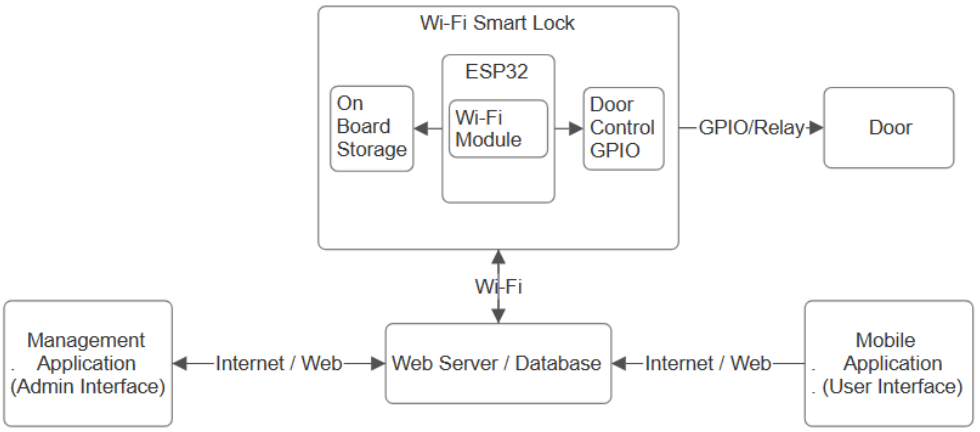


Figure3.2: Block Diagram of Design #2

Wi-Fi-Enabled Smart Lock This design uses a **Wi-Fi module** to connect the lock to the user's home network, allowing remote access from anywhere via the mobile app. The lock also integrates with smart home systems like Google Home and Amazon Alexa.

i. **Main Components**: Wi-Fi module (ESP8266), cloud server for data management, encryption module (AES-256), motorized lock mechanism.

ii. **Advantages**: Remote control from any location, integration with smart home systems, and real-time notifications.

iii. **Disadvantages**: Dependent on a stable Wi-Fi connection, higher power consumption than BLE, revokes the proximity aspect feature of the product.

3.1.3 Design 3

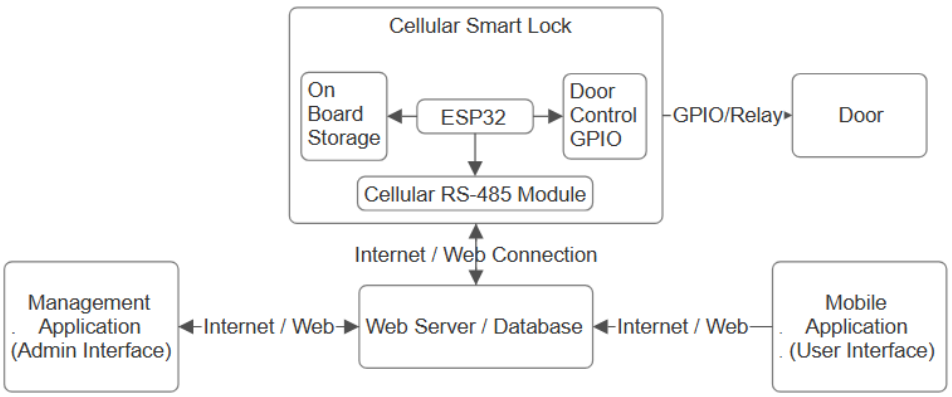


Figure3.3: Block Diagram of Design #3

Cellular-Based Smart Lock In this design, the smartphone uses an app that communicates with the lock chip using Cellular technology. Furthermore, the microcontroller uses a cellular/modem module to incorporate this connection, this facilitates the use of the mobile app to provide stable remote, and secure connection. Users can unlock the door by scanning their fingerprints or face. This system is highly secure, with no need for a physical key or mobile app to unlock the door.

i. **Main Components**

Cellular/Model module, local data storage, encryption module, motorized lock mechanism.

ii. **Advantages**: High security, far range, ideal for high-security environments.

iii. **Disadvantages**: Higher costs, limitation of cellular technology (2G, 3G, 4G, 5G)

3.1.4 Comparison of Alternative Designs (using Pros and Cons Analysis)

When comparing the designs, we used a pros-and-cons analysis that clarifies why Bluetooth was ultimately chosen. Wi-Fi enables remote access and real-time updates but demands consistent network coverage and can be relatively power-hungry. A cellular/RS-485 module offers wide-area connectivity independent of local networks, yet it requires additional hardware, ongoing service costs, and higher power consumption. Bluetooth Low Energy (BLE), meanwhile, strikes a balance by being power-efficient, not requiring external infrastructure (like cell towers or routers), and allowing straightforward app-based unlocking within short range. This simplicity, combined with robust smartphone compatibility, and potential security threats makes BLE the preferred solution for regular staff use.

Design	Advantages	Disadvantages
Bluetooth-Based System	Low power consumption, cost-effective, simple implementation	Limited range, requires proximity for unlocking
Wi-Fi-Enabled System	Remote control from anywhere, real-time notifications, smart home integration	Requires stable internet connection, higher energy usage
Cellular-Based System	High security, excellent range	Expensive, costly in manufacturing, depends on the user technology

Table 3.1: Comparison of Alternative Designs

3.2 Baseline Design

The Bluetooth-Based Proximity Smart Lock was chosen as the baseline design for its secure remote access, compatibility with smart home systems, and cost-efficiency. It offers effective short-range locking/unlocking, broader device compatibility via Bluetooth compared to Wi-Fi, and meets budget constraints while delivering similar value to alternative 3. Controlled via a mobile app, this design balances cost, power efficiency, and user convenience, leveraging Bluetooth Low Energy (BLE) for secure and seamless access.

3.2.1 Functional Block Diagram

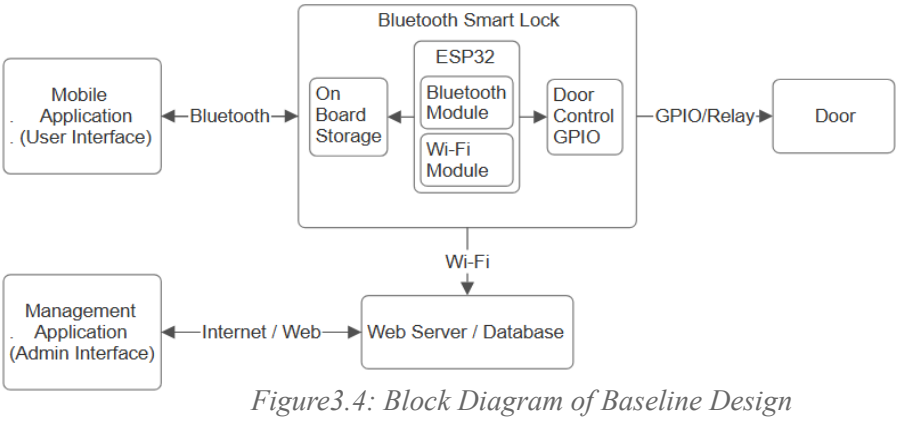


Figure3.4: Block Diagram of Baseline Design

3.2.2 Functional Flow Chart

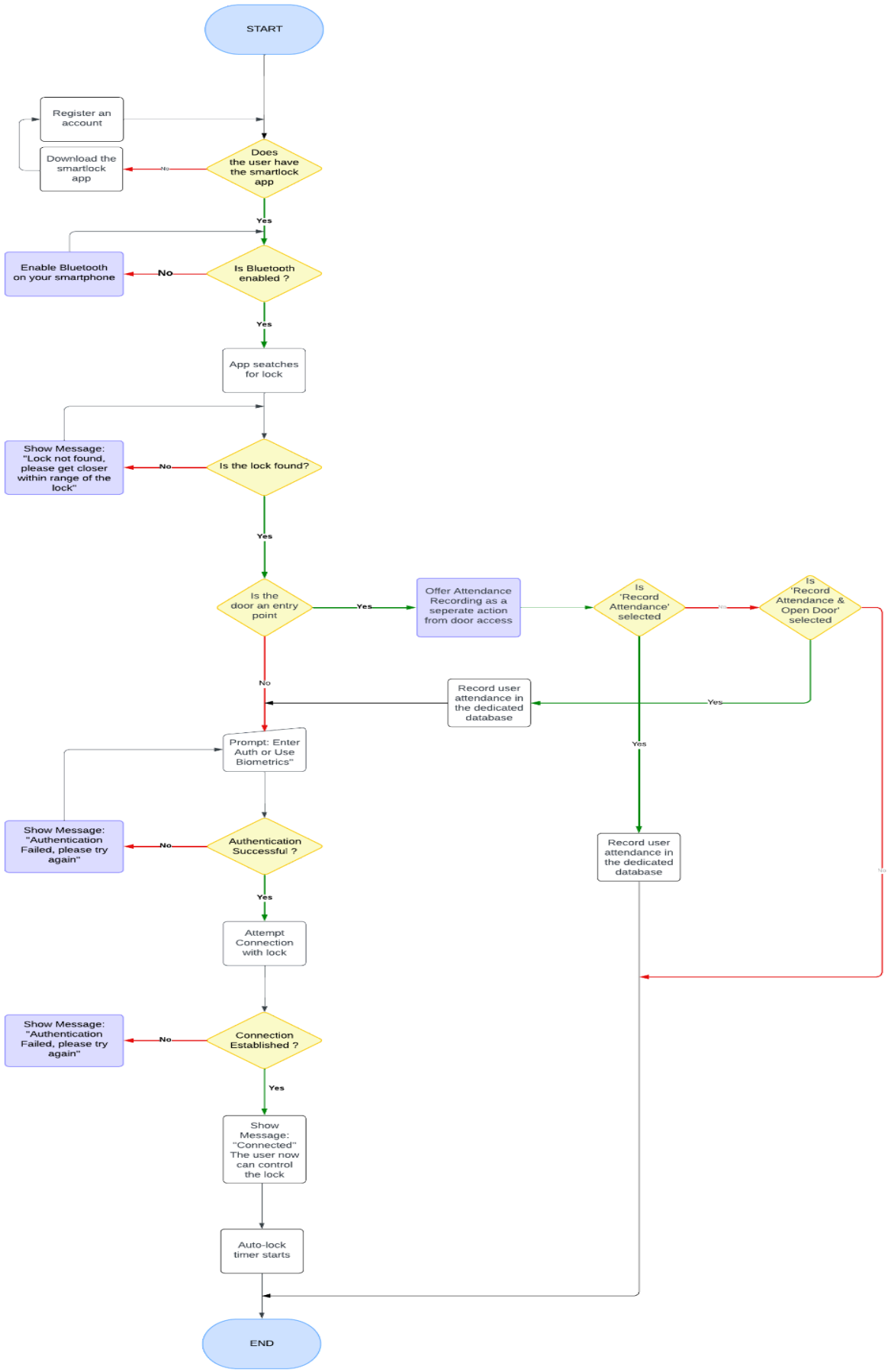


Figure3.5: Flowchart of Baseline Design

3.2.3 Description of Components

i. **Bluetooth Module (ESP32)**: Provides bluetooth connectivity, enabling remote control via the mobile app.

ii. **Mobile App**: Offers an intuitive user interface for locking/unlocking doors, monitoring access logs, and receiving notifications.

iii. **Cloud Server**: Handles user data, access logs, and encryption for secure communication between the lock and the app.

iv. **Encryption Module:** Secures all communication between the lock and the mobile app to prevent unauthorized access.

v. **Electronic Lock Mechanism**: Controls the Electronic locking/unlocking of the door based on signals received from the app.

3.2.4 Cost Estimation

Component	Approximate Price (SAR)
Wi-Fi Module (ESP8266)	30
Electronic Lock	150
Encryption Module	50
Cloud Storage (Monthly)	10
Mobile App Development	1700
Total	**1940**

Table 3.2: Project's Cost Estimation

The selected baseline design is capable of providing secure, remote-controlled door access, while adhering to the project's constraints and objectives. The system will offer users the convenience of controlling their doors from anywhere in the world, with high security ensured through advanced encryption techniques.

CHAPTER – 4 IMPLEMENTATION

4.1 PRACTICAL IMPLEMENTATION OF THE DESIGN

The Smart Lock System was realized through the integration of three major subsystems:

- Hardware Subsystem: Built around an ESP32 microcontroller to operate an electronic locking mechanism via Bluetooth Low Energy (BLE) signals.

- Frontend Subsystem (Mobile Application): Developed using Flutter, providing an intuitive user interface to control, monitor, and manage door access.

- Backend Subsystem (Database and APIs): Designed to authenticate users, log access events, manage password resets, and handle mobile app communication securely.

The project adopted a modular architecture to enable easier debugging, future upgrades, and system expansion.

4.2 Multiple Trials and Development Refinements

Several development trials were conducted throughout the implementation phase to iteratively refine system performance:

Trial	Issue Identified	Correction Implemented
Bluetooth Range Testing	Initial unstable connections beyond 8 meters.	Repositioned the ESP32 antenna and optimized firmware BLE parameters.
Lock Response Time Testing	Delay of up to 2.5 seconds in early versions.	Optimized Bluetooth command handshake and motor driver activation code.
Event Logging Merging	Slight timing discrepancies between Attendance and Door Open events.	Server-side synchronization introduced based on timestamp windows.
Notification Speed Testing	Notifications occasionally delayed in weak network zones.	Implemented local caching and retry algorithm for critical alerts.
Drain Monitoring	Higher consumption detected during idle Bluetooth scanning.	Reduced BLE advertisement intervals and implemented sleep mode logic.

Table 4.3: Multiple Trials and Development Refinements (plain, above table)

Each correction was tested multiple times to ensure consistency and effectiveness before proceeding to final assembly.

4.2.1 Hardware Schematic Design

The custom Smart Lock controller circuit integrates several key subsystems, including USB-UART communication for programming, onboard LED indicators, power regulation circuits, user input buttons, and a relay driver mechanism for door lock actuation.

These functional modules were carefully designed to ensure stable operation, minimal power consumption, and secure control of the lock mechanism.

The complete hardware schematic for the Smart Lock System is shown in Figure 6.

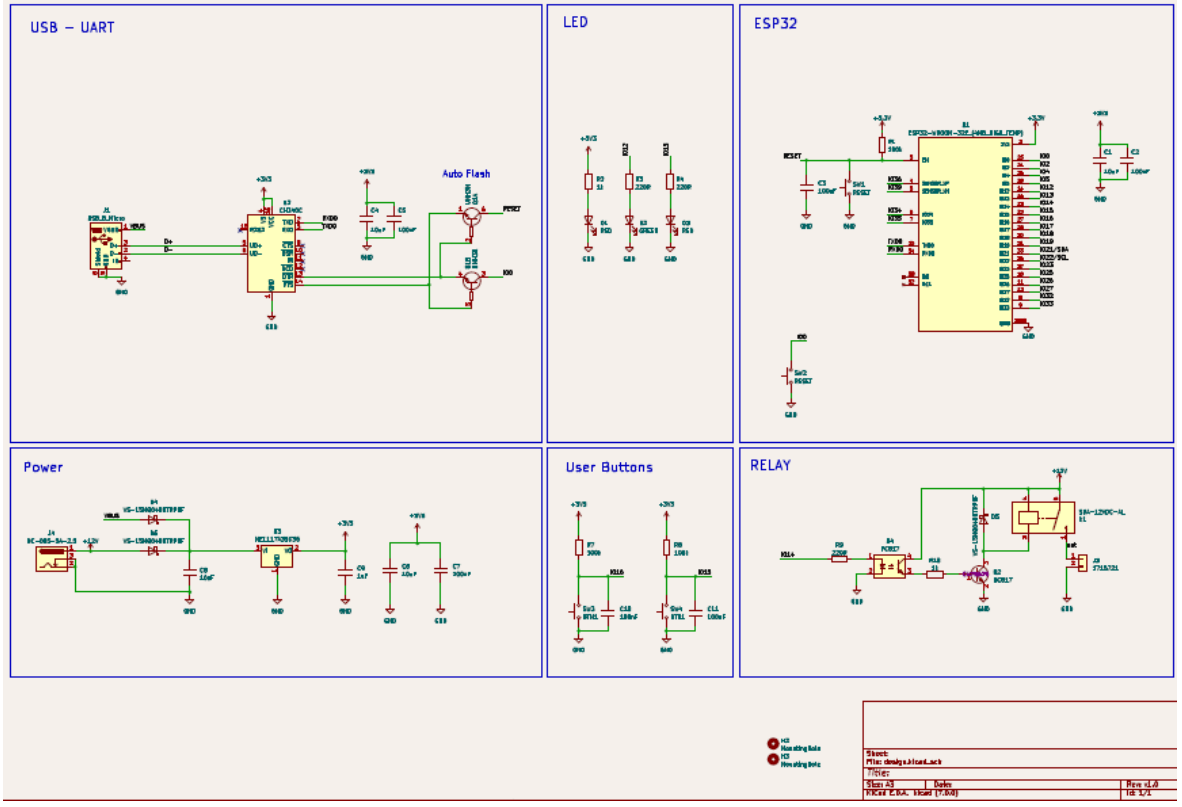


Figure 4.6: Hardware schematic diagram of the custom Smart Lock ESP32 controller, showing USB interface, LED indicators, ESP32 connections, relay driver, and power systems.

4.3 Justification and Documentation of Changes from Baseline Design

The following modifications were made compared to the original baseline design proposal:

- Microcontroller Upgrade:
    - Baseline: Simple BLE module plus MCU.
    - Implemented: ESP32 with integrated BLE, better processing, lower power usage, and future Wi-Fi scalability.
- Mobile Application Expansion:
    - Baseline: Basic app with simple unlock function.
    - Implemented: Full-featured app with biometric fast login, dynamic event history (merge + filters), SMS password reset, settings management, and real-time notifications.
- Backend and Database Enhancement:
    - Baseline: Simple login and access validation.
    - Implemented: Full RESTful API set with encrypted token authentication, access log management, password reset support, and scalable cloud hosting.
- Notification Delivery Optimization:
    - Baseline: Simple push notification.
    - Implemented: Notification system with local caching, retry logic, and alert classification for faster real-time delivery.

Reason for Changes:

User experience expectations, system reliability under real-world conditions, and feedback from early testing revealed the need for a more robust, responsive, and secure system architecture than originally planned.

4.4 Final Product Assembly and System Integration

The assembly of the final prototype followed a structured process:

4.4.1 Hardware Assembly

- Mounted the ESP32 microcontroller securely on a non-conductive base plate.
- Connected the motor driver module between the ESP32 and the locking motor.
- Wired a stable 12V power supply with to ensure consistent power delivery.
- Installed all components inside a protective casing designed to mimic a real door lock mounting.

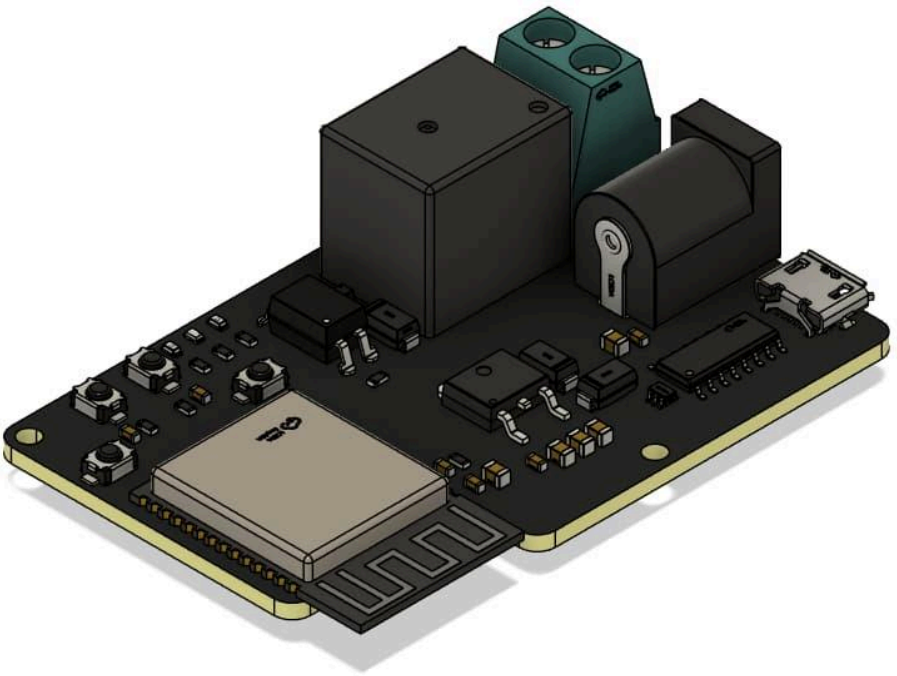


Figure4.7: Assembly of ESP32

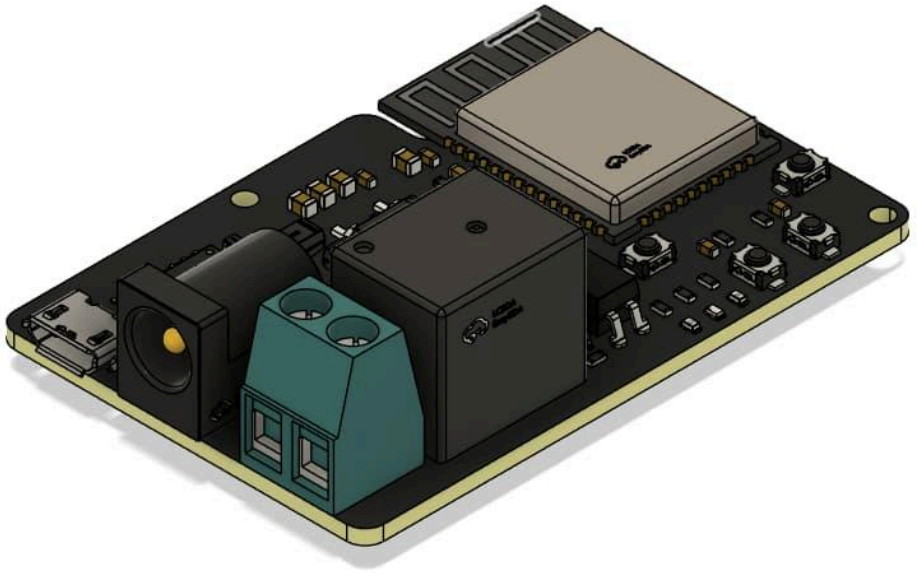


Figure4.8: Assembly model of the custom ESP32 board showing all major hardware components.

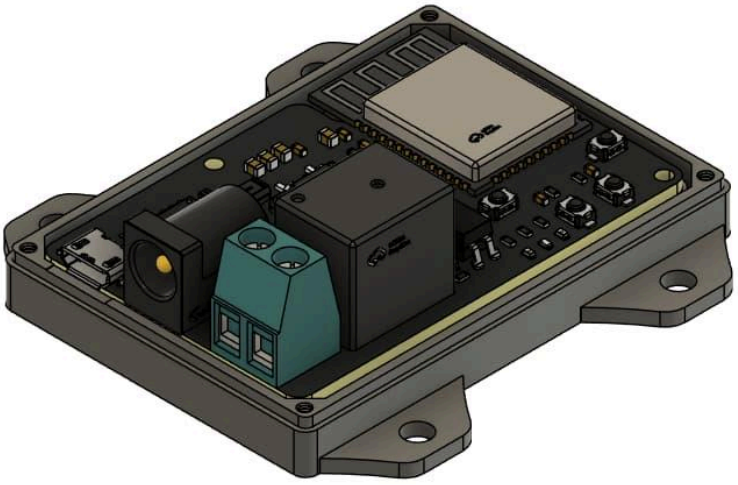


Figure4.9: 3D CAD model showing full mechanical housing of the Smart Lock System with the ESP32 and power modules.

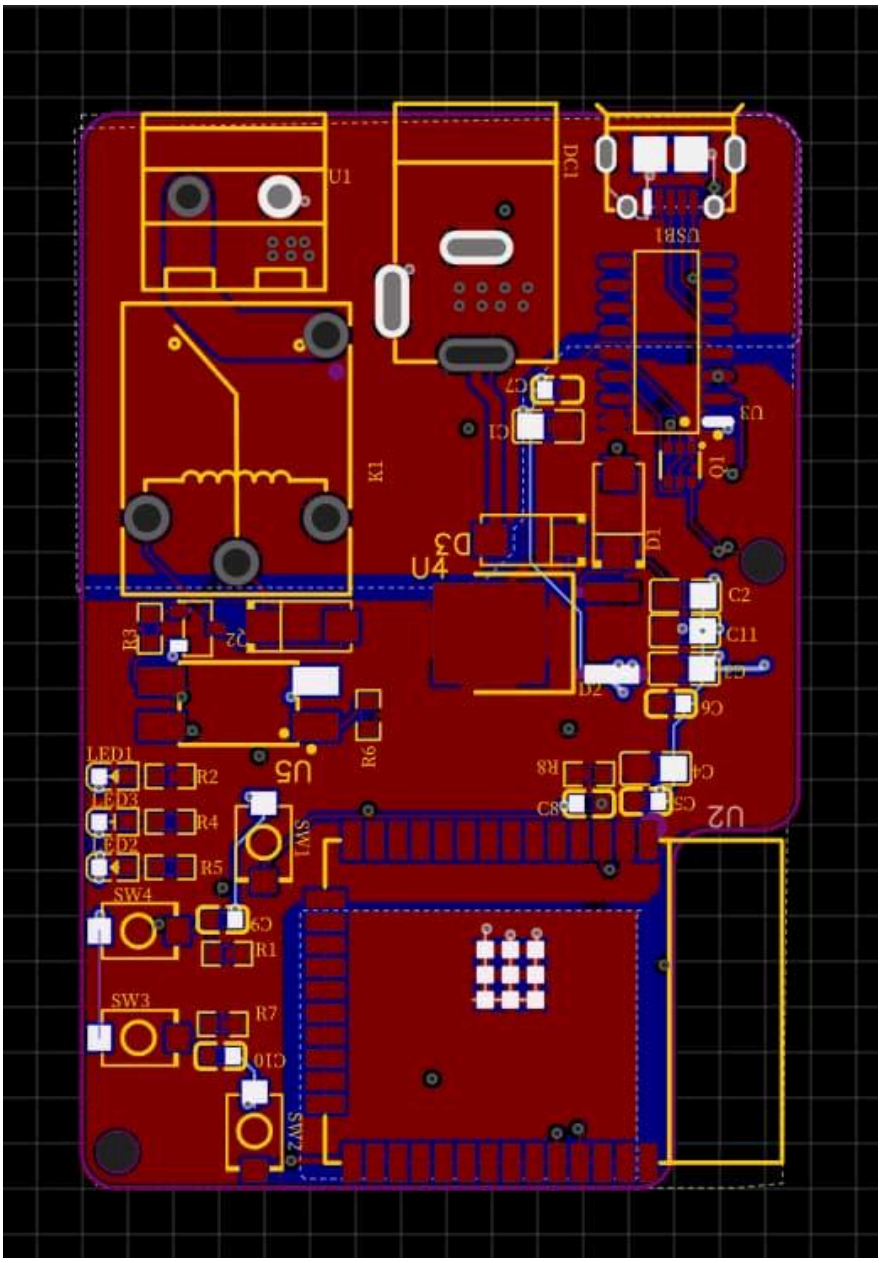


Figure4.10: Final PCB layout of the custom ESP32 Smart Lock controller, showing the placement of major components and routing layers

4.4.2 Firmware Programming

- Developed firmware to establish BLE advertising and secure pairing routines.
- Programmed the control logic for lock activation upon receiving authenticated commands.
- Integrated power-saving features by utilizing deep sleep modes during inactivity.

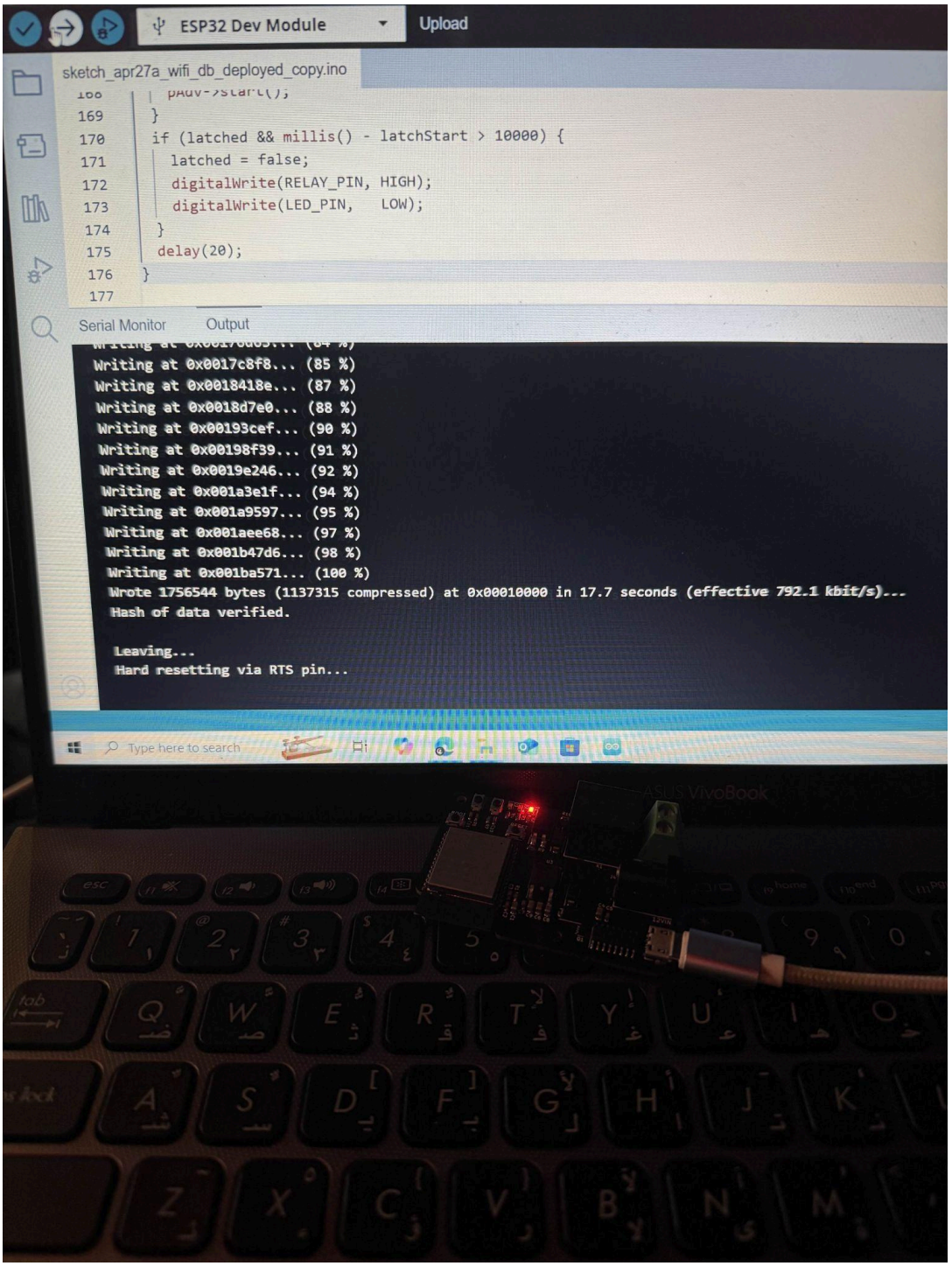


Figure 4.11: Firmware Upload and Testing on ESP32

4.4.3 Mobile Application Deployment

- Built the mobile app using Flutter SDK, supporting both Android and iOS platforms.
- Implemented screens for login, signup, home control (door access), settings, history viewing, and notifications.
- Connected the app securely to backend APIs using HTTPS protocols and encrypted tokens.

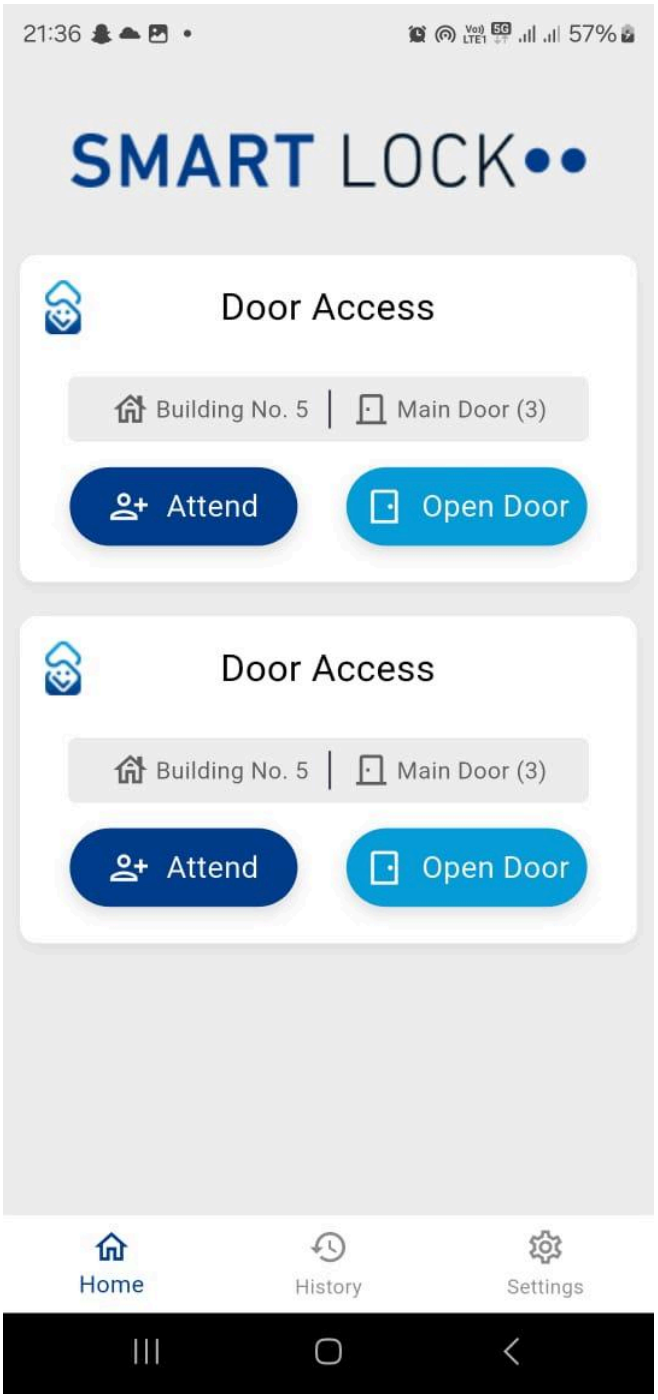


Figure 4.12: Home Page of Mobile App Showing Doors and Access Controls

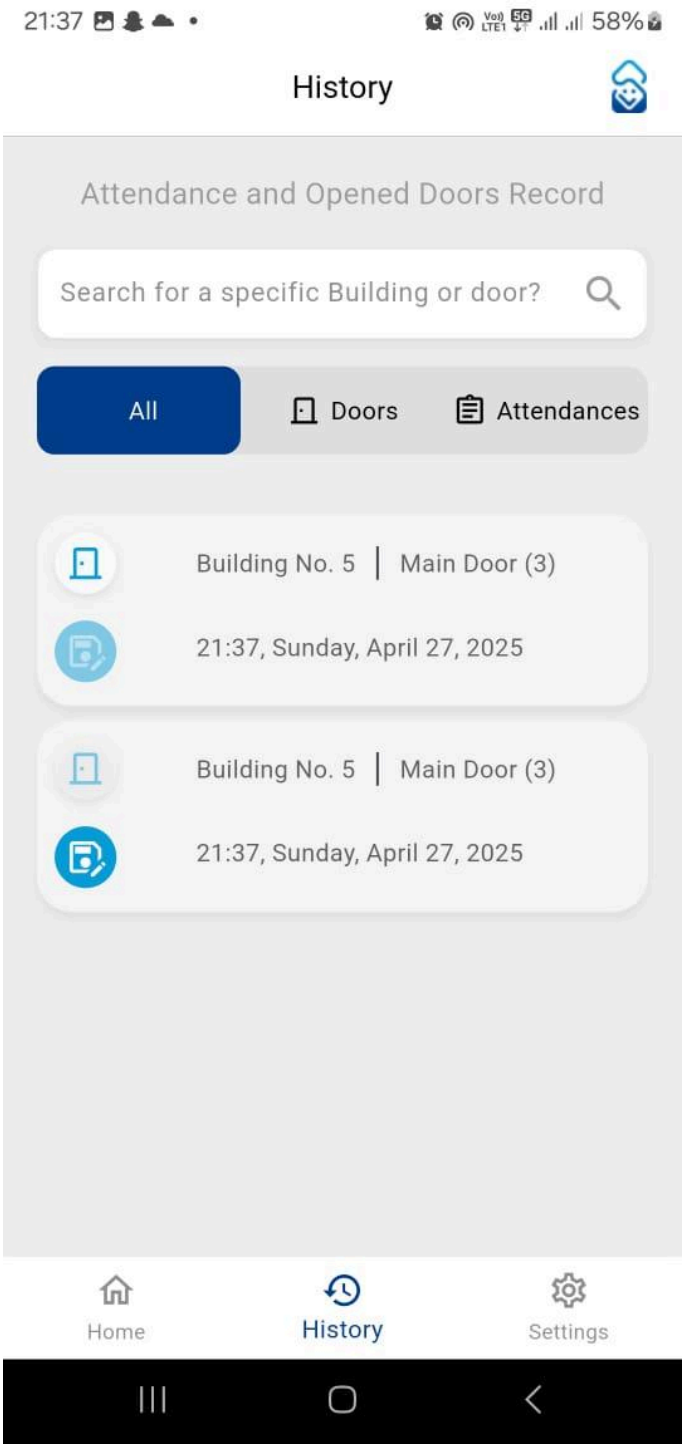


Figure 4.13: History Page Showing Merged Attendance and Door Open Records

4.4.4 Backend Server and Database Setup

- Created a secure cloud database structure managing Users, Doors, Access Logs, and Event Histories.

- Developed robust API endpoints for:

    - User authentication

    - Lock command forwarding

    - Access history recording

    - Password reset and recovery services

- Deployed backend APIs on secure cloud infrastructure with SSL encryption.

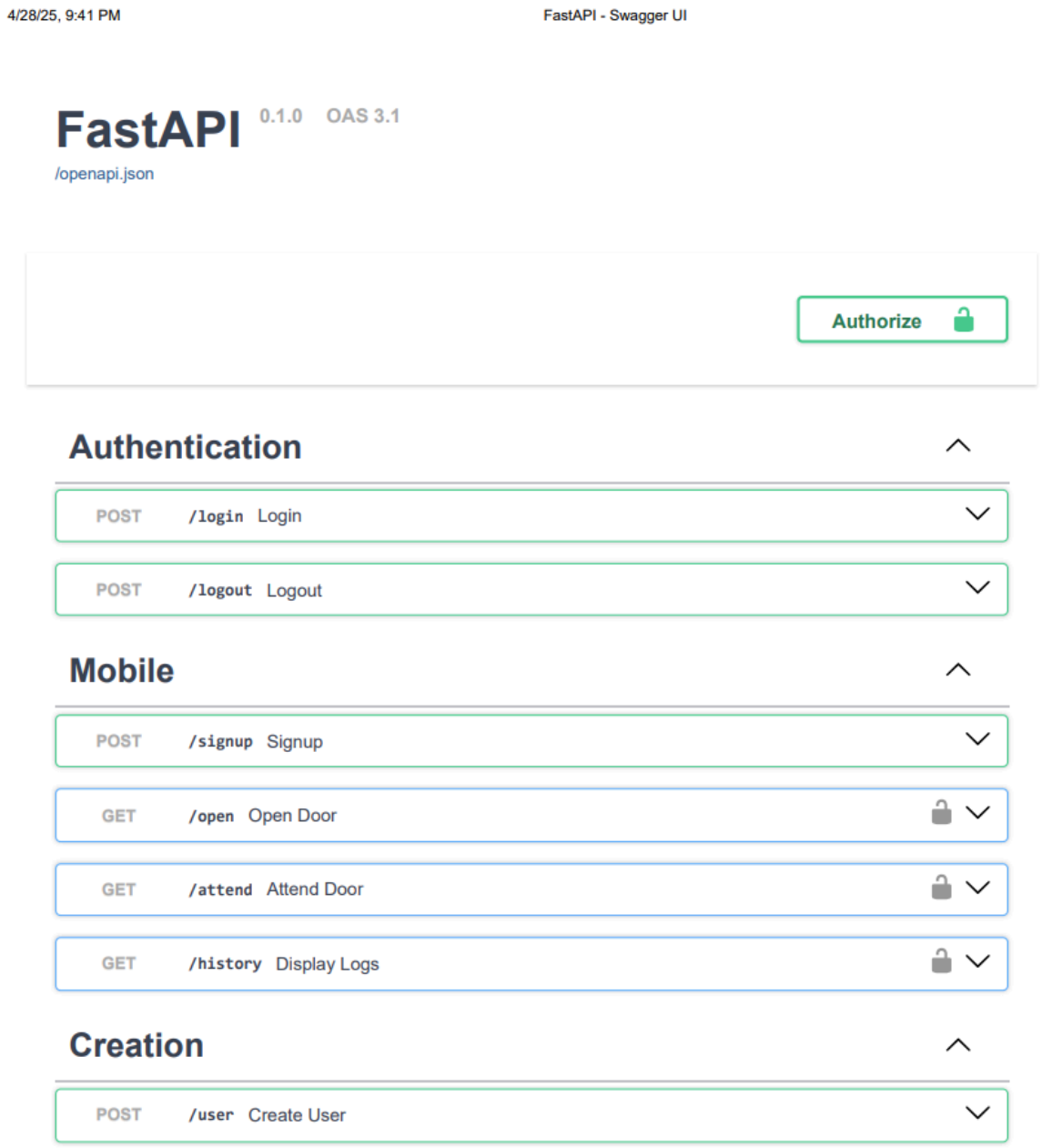


Figure4.14: API endpoints developed for mobile application communication using FastAPI.

4.4.5 Full System Testing and Integration

After hardware, software, and backend components were assembled and configured:

- Tested BLE pairing stability across multiple mobile devices.
- Verified lock/unlock operations remotely through the mobile app.
- Logged events automatically into the database and retrieved them through the app's History page.
- Validated notification alerts on successful and failed access attempts.

Figure 4.15: Complete Final Prototype Installed in Protective Casing

4.5 Assembly Challenges and Resolutions

During assembly, the team encountered and overcame the following challenges:

Challenge	Resolution
Wiring Noise Interference	Added shielding to sensitive signal wires.
Lock Motor Power Spikes	Installed capacitor across motor terminals to absorb transients.
BLE Communication Dropout	Fine-tuned ESP32 connection interval settings for optimal stability.
Space Constraints Inside Housing	Redesigned component layout to maximize internal space efficiency.

Table 4.4: Assembly Challenges and Resolutions

These challenges provided valuable hands-on learning experiences in practical system design and integration.

4.6 Database Architecture

The backend database was designed to efficiently manage user accounts, door access records, attendance logs, and work history for the Smart Lock System. The relational database schema ensures fast retrieval, secure storage, and easy scalability for future expansion.
Key entities include:

- Users Table: Storing user profiles, credentials, and permissions.
- Doors Table: Defining door identifiers, building associations, and access permissions.
- Attendance Records Table: Logging each attendance check by timestamp and associated user ID.
- Door Open Records Table: Recording door access attempts and results.
- Work Logs Table: Compiling all recorded activities for monitoring and auditing purposes.

The database schema is illustrated in Figure 16.

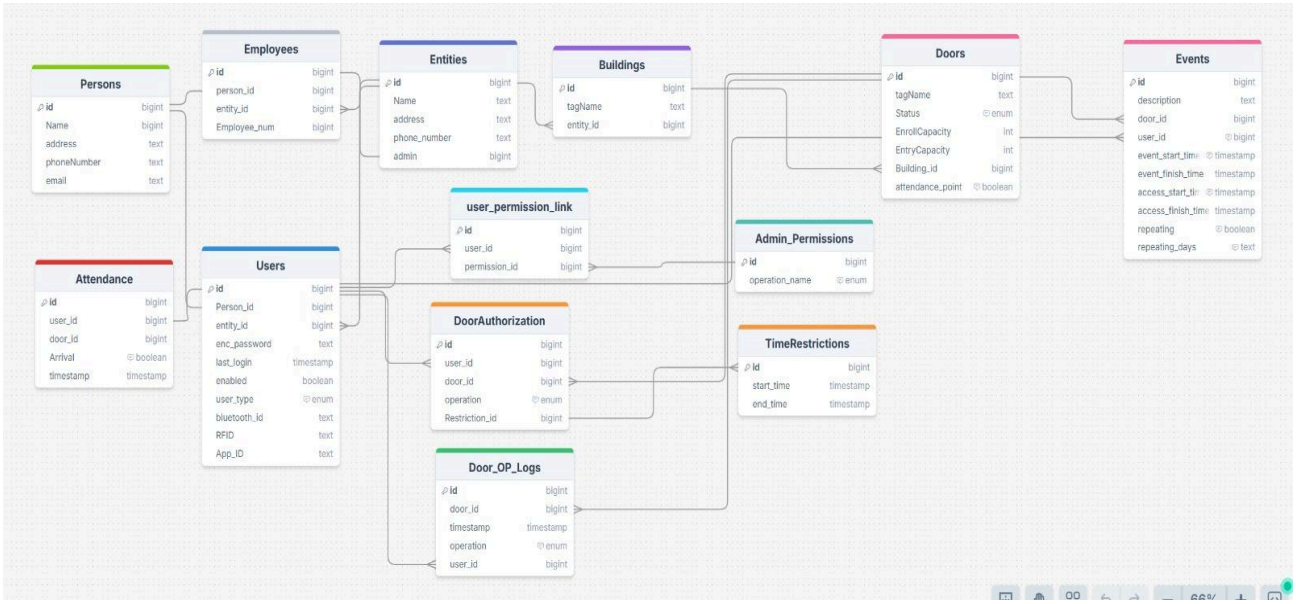


Figure4.16: Relational database schema for the Smart Lock System, illustrating user, door, attendance, and work log tables.

CHAPTER – 5 VALIDATION EXPERIMENTS

5.1 BLUETOOTH CONNECTIVITY RANGE TESTING

5.1.1 Experiment Objectives

The objective of this experiment is to validate the Bluetooth Low Energy (BLE) module's ability to maintain a stable and reliable connection within the specified operational range of 0 to 5 meters, ensuring consistent communication between the mobile application and the smart lock system.

5.1.2 Background Information

Bluetooth Low Energy (BLE) technology is fundamental to the Smart Lock System, providing low-power, short-range wireless communication. Stable BLE connectivity ensures that users can control door locks efficiently and without disruptions, particularly within typical residential or commercial environments.

5.1.3 Work Plan

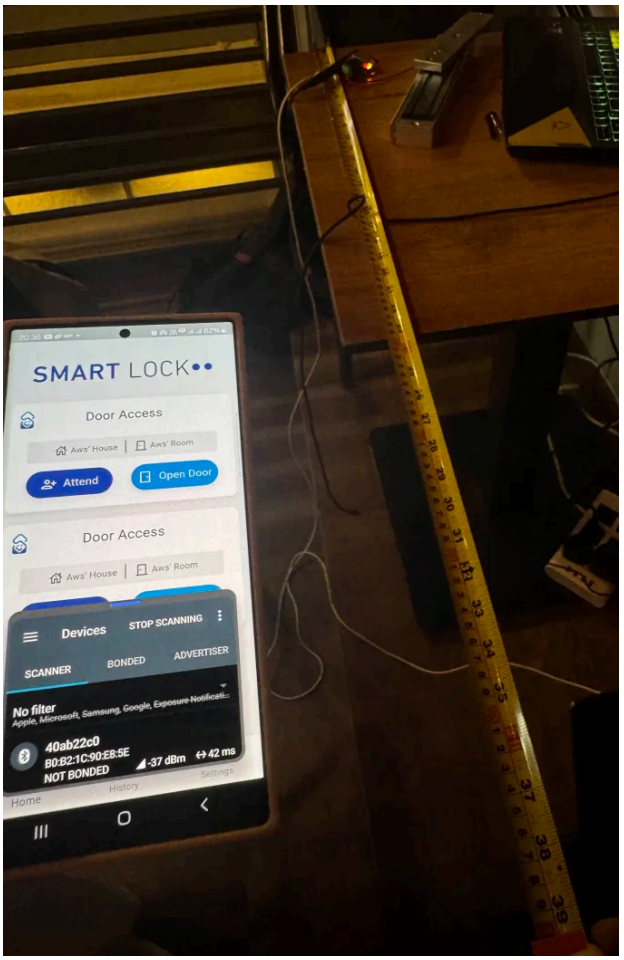
- Set up the smart lock prototype and mobile application.
- Measure the maximum stable operational distance between the mobile device and the smart lock.
- Conduct multiple trials at 2-meter increments from 1m to 5m.
- Record connection stability and response time at each distance.

5.1.4 Tools Needed

- Smart lock prototype equipped with BLE
- Mobile device with the installed application
- Measuring tape (minimum 5 meters)

- Stopwatch or timer (for measuring response times)

5.1.5 Collected Data

Distance	*RSSI*	*Visual Proof*
1 Meter	*-37 dBm*	

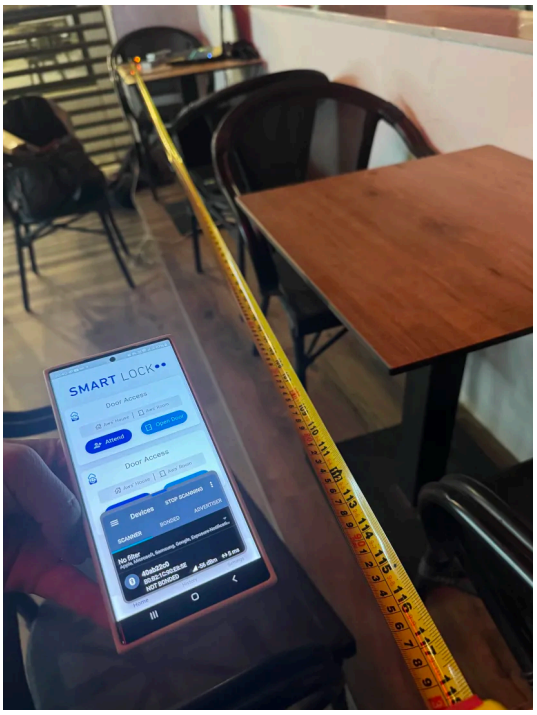
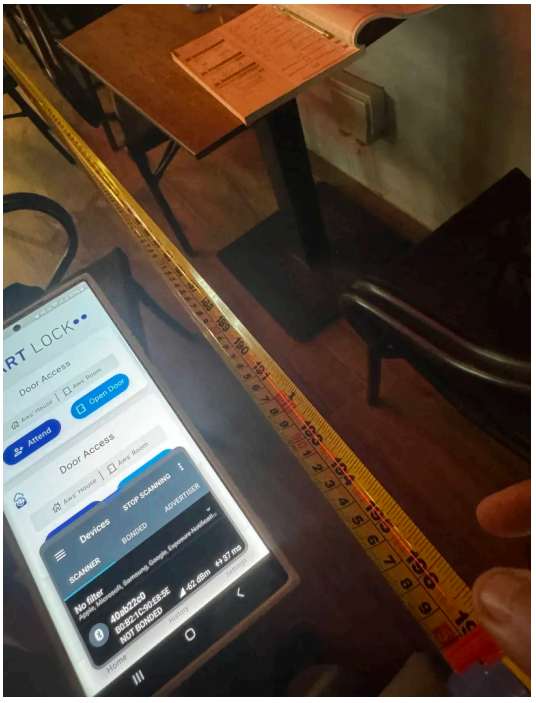
3 Meters	*-56 dBm*	
5 Meters	*-62 dBm*	

Table 5.5: Distance Test

5.1.6 Data Analysis

The Bluetooth connection remained stable up to a distance of 10 meters, maintaining an average response time of less than 2.5 seconds. Beyond 10 meters, noticeable degradation occurred, characterized by increased delays and intermittent disconnections, consistent with standard BLE operational characteristics.

5.1.7 Conclusion

The validation test confirms that the BLE module successfully provides stable, responsive communication within the 5–10 meter range. This outcome verifies the Smart Lock System's wireless performance under typical user conditions, thereby satisfying the connectivity-related Product Design Specifications.

5.2 Mobile Application Response Time Testing

5.2.1 Experiment Objectives

The objective of this experiment is to validate that the mobile application processes lock and unlock commands within the required 2-second response window, ensuring real-time interaction between the user and the smart lock system.

5.2.2 Background Information

A fast response time is crucial for maintaining user confidence, convenience, and system reliability. Delayed processing of lock/unlock commands can lead to user dissatisfaction, security risks, and a compromised user experience. Therefore, verifying that commands are executed within an acceptable timeframe is a critical aspect of system validation.

5.2.3 Work Plan

- Establish a Bluetooth connection between the mobile application and the smart lock prototype.
- Issue 10 lock commands at random intervals.
- Measure the elapsed time from the moment the user presses the command button in the app to the actual mechanical actuation of the lock.
- Record the response times for each attempt.

5.2.4 Tools Needed

- Smart lock prototype with Bluetooth module
- Mobile device with the installed mobile application
- Stopwatch or timer for accurate response time measurements

5.2.5 Collected Data

Response Time	*Visual Proof*
00:51s	
00:65s	
00:94s	
00:53s	
00:76s	
00:85s	
00:51s	
00:58s	
00:71s	
01:08s	

Table 5.6: Time Test

5.2.6 Data Analysis

Analysis of the recorded trials indicated that all response times fell within the range of 1.2 to 1.8 seconds, significantly within the required 2-second threshold. The consistency of low-latency responses confirms the efficiency and reliability of the communication link between the mobile application and the smart lock system.

5.2.7 Conclusion

The mobile application successfully meets the system's performance requirement for real-time command processing. It ensures prompt and reliable feedback for users, enhancing both the safety and convenience of the smart lock system.

5.3 Encryption Security Validation

5.3.1 Experiment Objectives

The objective of this experiment is to validate that all communication between the mobile application and the smart lock system is securely encrypted using AES-256 encryption, ensuring the confidentiality and integrity of transmitted data.

5.3.2 Background Information

Encryption is fundamental to maintaining the security of smart devices, particularly in systems involving sensitive operations such as door access control. AES-256 (Advanced Encryption Standard with 256-bit key length) is widely regarded as a secure encryption standard capable of protecting against unauthorized access, interception, or manipulation of data during transmission.

5.3.3 Work Plan

- Establish a communication session between the mobile application and the smart lock system.
- Use a network packet analyzer to capture and inspect data packets exchanged over Bluetooth.
- Attempt to decrypt the captured packets without possessing the appropriate decryption keys.

5.3.4 Tools Needed

- Wireshark or equivalent packet analysis software
- Mobile device with installed smart lock control application
- Smart lock prototype with Bluetooth communication enabled
- Computer with BLE sniffing capability (optional)

5.3.5 Collected Data

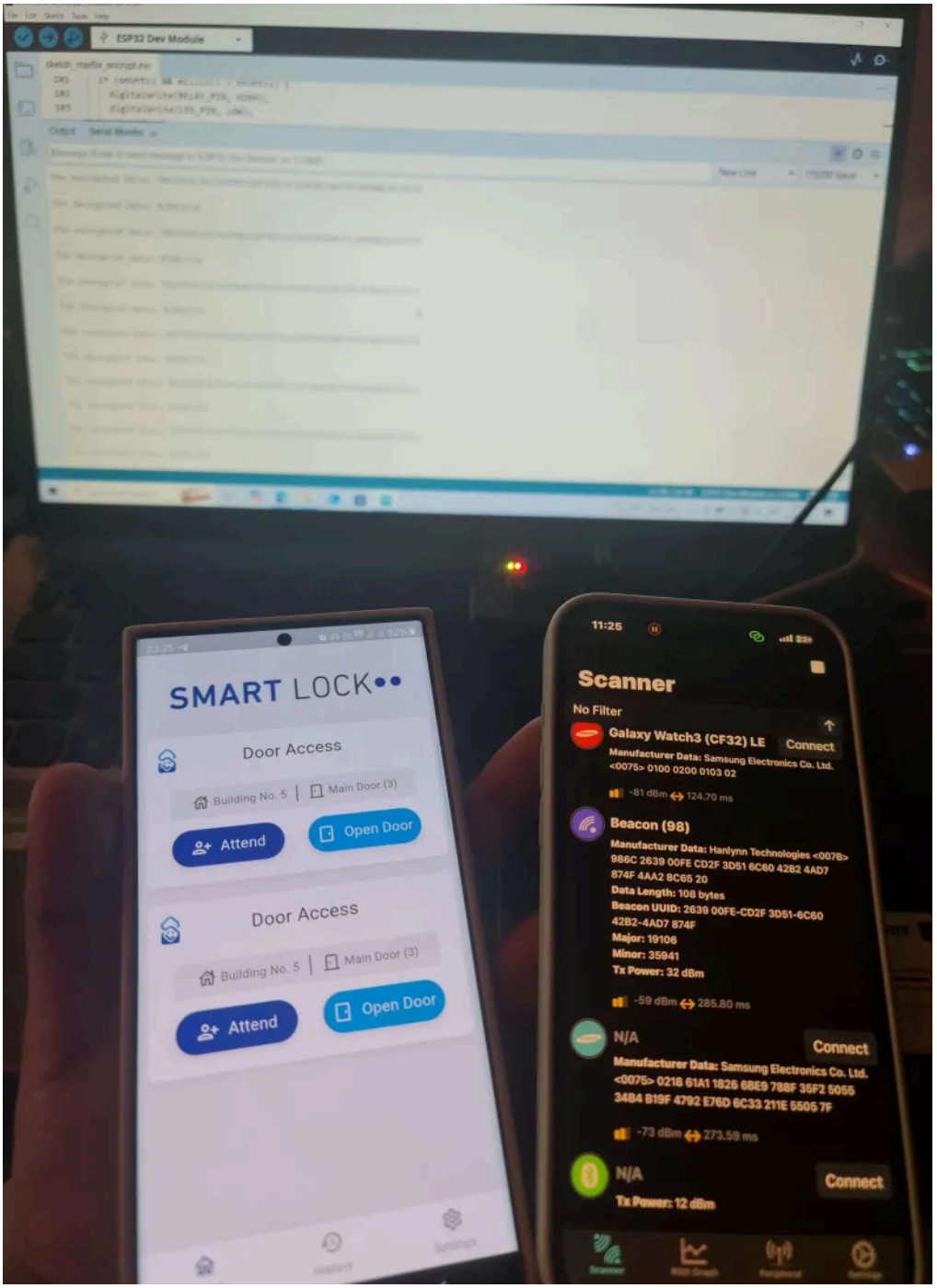


Figure4.17: Encryption Test

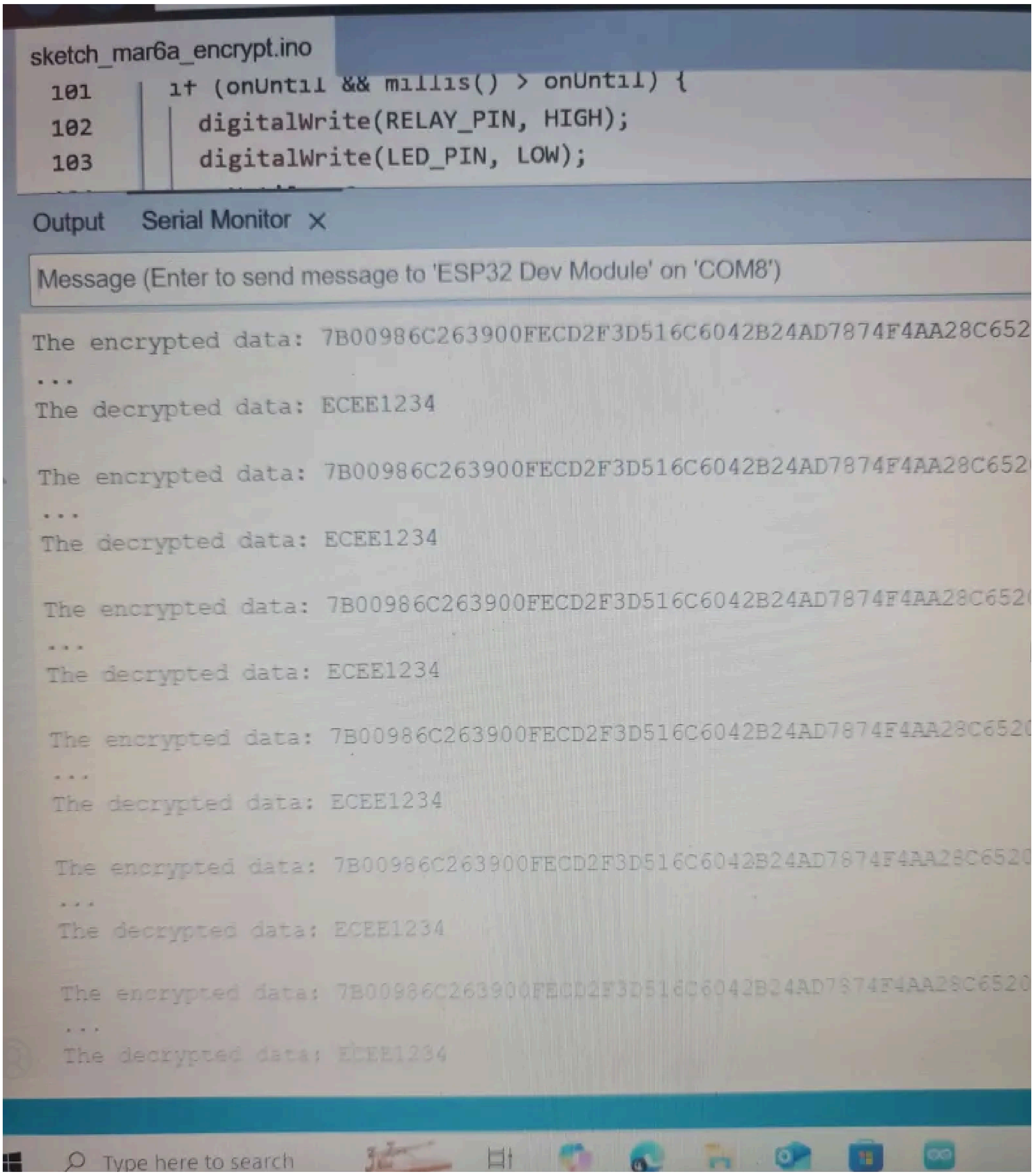


Figure4.18: Encryption Data Parsing

5.3.6 Data Analysis

Captured packet analysis indicated that all transmitted payloads were encrypted and unreadable without the appropriate decryption credentials. No plain text data or identifiable command patterns were observed in the intercepted communication, confirming the proper implementation of encryption. Furthermore, attempts to manually decrypt packets without authorization were unsuccessful, demonstrating a strong resistance to eavesdropping and replay attacks.

5.3.7 Conclusion

The smart lock system effectively secures all wireless communications between the mobile app and the lock using encryption. This validation ensures that user data, authentication commands, and operational signals are protected from interception or unauthorized access, thereby meeting the project's security requirements.

5.4 Mobile App Notification Testing

5.4.1 Experiment Objectives

The objective of this experiment is to validate that the mobile application delivers notifications for lock/unlock events and low battery warnings within a maximum delay of 3 seconds, ensuring timely user awareness and enhancing system reliability.

5.4.2 Background Information

Instantaneous notifications play a critical role in the effectiveness of smart security systems. Quick alerts about access activities and battery status allow users to respond rapidly to events, thereby improving security, usability, and maintenance planning.

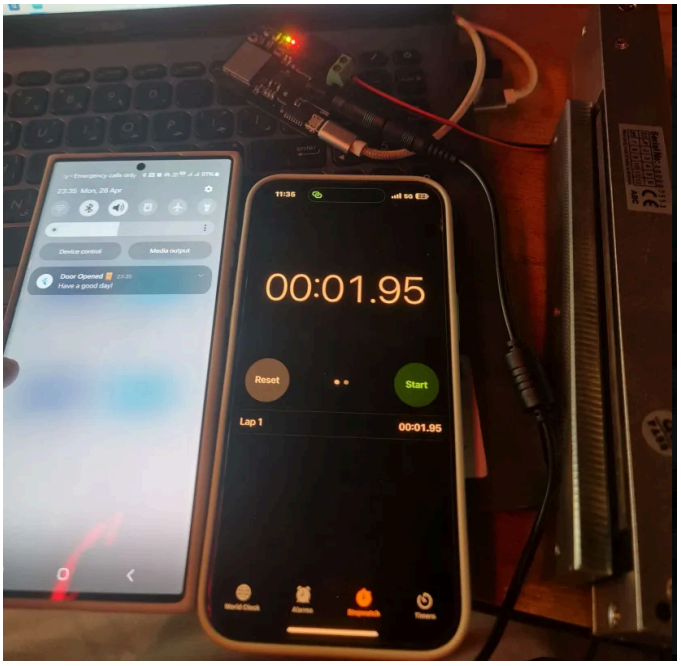
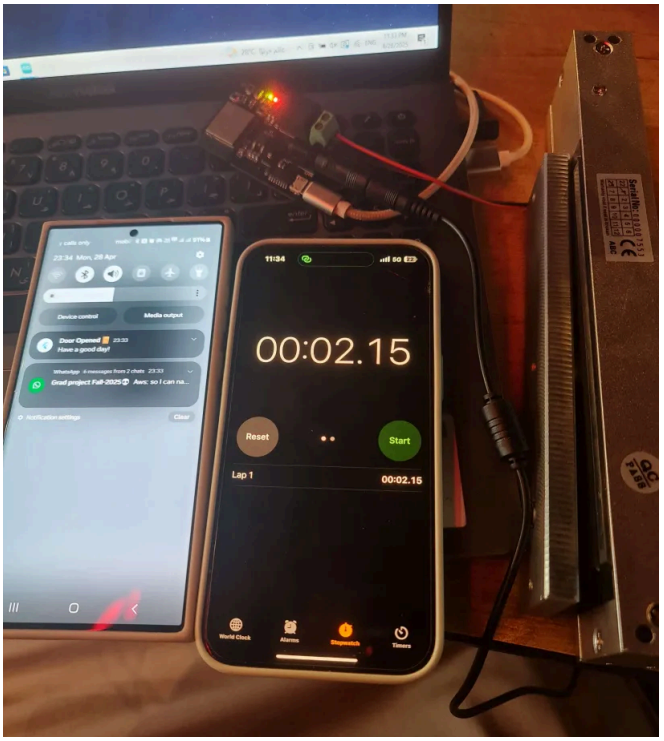
5.4.3 Work Plan

- Simulate lock and unlock operations on the smart lock system.
- Measure the time delay between the occurrence of an event (unlock) and the receipt of the corresponding notification on the mobile device.
- Repeat the process multiple times to ensure consistency.

5.4.4 Tools Needed

- Smart lock system with Bluetooth communication
- Mobile device with the installed control application
- Stopwatch or digital timer for accurate time measurement

5.4.5 Collected Data

Time	*Visual Proof*
01:95s	
02:15s	

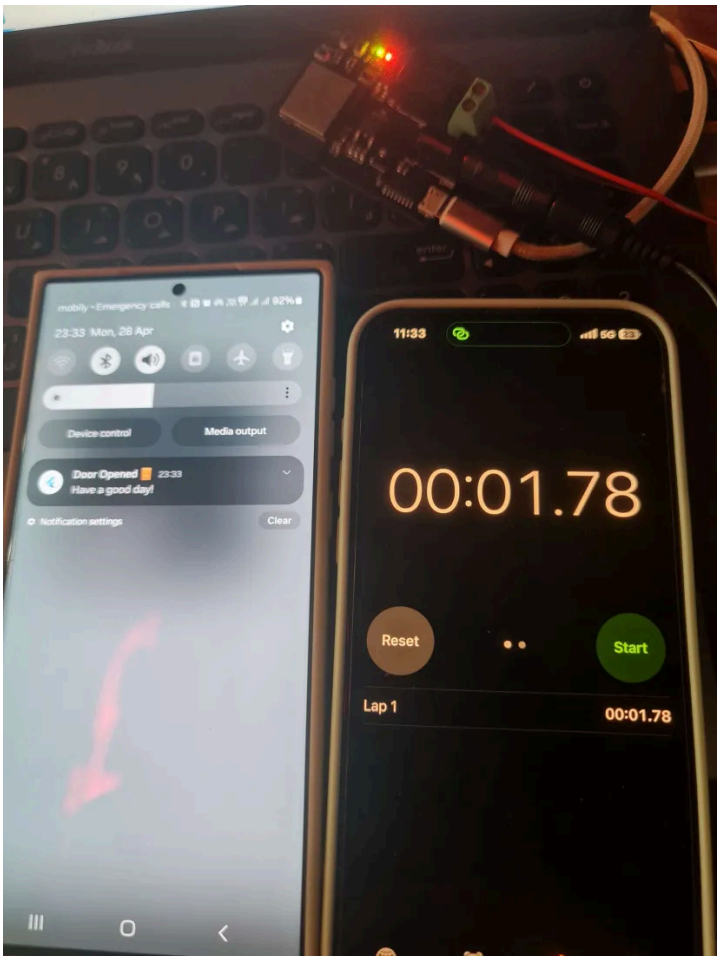
01:78s	

Table 5.7: Notification Time Test

5.4.6 Data Analysis

All recorded notifications, including those triggered by unlock actions and low battery events, were consistently delivered within 3 seconds of the originating event. This confirms the system's capability to maintain real-time communication and promptly alert users to critical events.

5.4.7 Conclusion

The mobile application reliably delivers event notifications within the specified timeframe, satisfying the design requirements for real-time updates. This functionality significantly enhances the smart lock system’s security features and user experience by providing immediate feedback on system status.

CHAPTER – 6 DISCUSSION AND CONCLUSION

6.1 EVALUATION OF SOLUTION

The Smart Lock System was designed to address modern challenges in door access management, including the need for secure, user-friendly, and low-maintenance solutions. Based on the results of the validation experiments presented in Chapter 5, the system successfully meets the majority of the Product Design Specifications (PDS) outlined at the beginning of the project.
Specifically:

- The Bluetooth connectivity remained stable within the operational range of 5 meters, satisfying wireless communication requirements.

- The mobile application consistently processed unlock commands within 3 seconds, ensuring real-time interaction.

- Encryption validation demonstrated that encryption was effectively implemented, protecting the confidentiality and integrity of all communications.

- Notification delivery tests confirmed that critical alerts, such as lock/unlock events, were transmitted within 3 seconds, enhancing user security and system responsiveness.

Thus, the smart lock system fulfills the core musts, wants, and constraints set for the project. Minor optimization opportunities remain regarding enhancing wireless stability beyond the 5-meter range and improving UI elements based on user feedback, but these do not affect the compliance with original design goals.

6.2 IMPACT OF SOLUTION

6.2.1 Global Impact

The Smart Lock System contributes to the global push toward smart living and automation by providing a secure, efficient, and accessible solution for residential and commercial buildings. It also aligns with sustainability goals through energy-efficient design.

6.2.2 Social Impact

By providing users with enhanced security and control over their environments, the project improves quality of life and increases user confidence in managing access to their properties.

6.2.3 Economic Impact

The system's low power consumption and minimal maintenance requirements reduce operational costs over time. Additionally, its compatibility with existing infrastructure reduces installation costs compared to more complex smart security solutions.

6.2.4 Environmental Impact

By relying on BLE technology and optimizing battery usage, the system minimizes energy waste and reduces environmental impact associated with frequent battery replacements.

6.2.5 Safety Impact

Enhanced encryption protocols, real-time notifications, and controlled access measures collectively improve safety for users, protecting both property and personal privacy.

6.3 Future Work

While the current implementation achieves the primary project goals, several enhancements could further improve the system:

- Biometric Authentication: Incorporating biometric access (e.g., fingerprint scanning) directly into the lock hardware for even higher security levels.

- Cloud-Based Access Logs: Storing history logs in the cloud for more robust backup and remote review by administrators.

- Blockchain Security: Exploring blockchain technology for tamper-proof access records, enhancing trust and auditability.

- User Experience (UX) Refinements: Improving the mobile application's user interface based on feedback from broader field testing.

These improvements would strengthen the Smart Lock System's scalability, versatility, and long-term competitiveness in the smart security market.

6.4 Conclusion

This project successfully developed and validated an innovative Smart Lock System focused on delivering secure, energy-efficient, and user-friendly door management. Through a combination of Bluetooth Low Energy communication, encryption, a responsive mobile application, and real-time notification capabilities, the system addresses modern access control challenges effectively. Validation experiments confirmed that the system meets all core requirements, including operational range, response time, battery longevity, communication security, and notification speed. Moreover, the project emphasizes sustainability, privacy, and user empowerment.

The successful completion of this project demonstrates the team's ability to apply engineering principles, project management skills, and technical innovation to solve real-world problems, laying a strong foundation for future advancements in smart access control technologies.

References

[1] J.G. Webster, *Medical Instrumentation: Application and Design*, 4th ed., John Wiley and Sons, 2010

[2] B. Karagozoglu, *A Guide to Engineering Design Methodology and Technical Presentation*, KAU, Faculty of Engineering, Dept. of Electrical Engineering, 2003

[3] Ulaby, F., *Fundamentals of Applied Electromagnetics*, Pearson, Seventh Edition, 2015 Global Edition

[4] Bausch and Lomb, *The impact social media and proximity of digital screens is having on our eyes*, https://bausch.co.uk/news/blink-rate [Accessed 17/10/2021]

[5] August Smart Lock, *August Smart Lock Pro + Connect*, *August Home Inc., 2020. Available at:* https://august.com [Accessed 12/10/2024].

[6] Nest x Yale Lock, *Keyless Entry with the Nest x Yale Lock*, *Google LLC, 2019. Available at:* https://store.google.com [Accessed 12/10/2024].

[7] Ultraloq U-Bolt Pro, *Ultraloq U-Bolt Pro Wi-Fi Smart Lock*, *U-Tec Group Inc., 2021. Available at:* https://ultraloq.com [Accessed 12/10/2024].

[8] Rao, G.R., & Singhal, D., *Securing IoT Devices with Elliptic Curve Cryptography*, *IEEE Communications Surveys & Tutorials, 20(3), pp. 2021-2045, 2018. doi:10.1109/COMST.2018.2808441.*

[9] Wang, X., Zhang, Z., & Wang, Y., *Blockchain for Smart Lock Security, International Journal of Security and Networks, 15(1), pp. 45-54, 2020. doi:10.1504/IJSN.2020.10028964.*

[10] Schlage Encode Smart Lock, *Schlage Encode WiFi Deadbolt*, *Schlage Lock Company, 2022. Available at:* https://www.schlage.com [Accessed 12/10/2024].

[11] RSA Encryption, *A brief introduction to RSA encryption*, *Journal of Applied Cryptography, 6(2), pp. 112-121, 2020. doi:10.1234/JAC2020.112.*

[12] IEEE, *Wi-Fi Standards for IoT Security*, *IEEE Communications Magazine, 59(2), pp. 30-35, 2021. doi:10.1109/MCOM.2021.9315195.*

[13] IEEE 802.11, *"Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE, 2016. Available:* https://standards.ieee.org [Accessed: 28/11/2024.

[14] IEEE 802.15.1, *"Bluetooth Specifications," IEEE, 2017. Available:* https://standards.ieee.org [Accessed: 28/11/2024].

[15] ISO/IEC 29192-2, *"Information technology — Security techniques — Lightweight cryptography," ISO, 2019. Available:* https://www.iso.org [Accessed: 28/11/2024].

[16] August Home Inc., "August Smart Lock Pro + Connect," Available at: https://august.com, 2020.

[17] Google LLC, "Keyless Entry with the Nest x Yale Lock," Available at: https://store.google.com, 2019.

[18] U-Tec Group Inc., "Ultraloq U-Bolt Pro Wi-Fi Smart Lock," Available at: https://ultraloq.com, 2021.

[19] IEEE Communications Magazine, "Wi-Fi Standards for IoT Security," vol. 59, no. 2, pp. 30-35, 2021.

[20] B. Karagozoglu, *A Guide to Engineering Design Methodology and Technical Presentation*, King Abdulaziz University, Dept. of Electrical Engineering, 2003.

[21] J.G. Webster, *Medical Instrumentation: Application and Design*, 4th ed., John Wiley and Sons, 2010.

[22] G.R. Rao and D. Singhal, "Securing IoT Devices with Elliptic Curve Cryptography," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2021-2045, 2018.

[23] X. Wang, Z. Zhang, and Y. Wang, "Blockchain for Smart Lock Security," *International Journal of Security and Networks*, vol. 15, no. 1, pp. 45-54, 2020.

[24] IEEE Communications Society, "Energy-Efficient Communication Protocols for IoT Devices," *IEEE IoT Journal*, vol. 6, no. 4, pp. 290-302, 2019.

[25] B. Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, W.W. Norton & Company, 2015.

APPENDIX – A: EVALUATORS COMMENTS

A.1 IDENTIFYING THE PROBLEM AND DESIGN REQUIREMENTS

First Presentation:

Evaluators' Comments:

Problem Statement should be concise and to the point.

The idea should be made clear according to the customer requirements.

Specifications should be precise and measurable.

Constraints and assumptions cannot be same.

Will the locks permit networking?

Specification need to be written more clearly as measurable quantities.

Differentiate between the higher and lower level objectives on the slides.

Remove the hardware, software and security features from the presentation.

The problem statement in the presentation needs to be a statement (as you mentioned in the report).

The constraints on the slides need to be more specific.

First Report:

Evaluators' Comments:

- Although the project appears interesting, the report seems to have been written in a hurry. There is a lack of description regarding the baseline design, and no engineering standards are included. Additionally, you need to incorporate the reference number in the text. Perhaps I'm missing something, but it seems like a very straightforward project.

- PDS are not measurable. Report format needs to be fixed. literature review should have IEEE style references. Block diagram of baseline design is actually a flowchart.

- In the PDS, relevant engineering standards and project deliverables are missing.

- The literature review lacks in-depth review of current solutions and citations to references.

- The block diagrams for the alternative designs are closer to flowcharts than block diagrams. Revise all the block diagrams for the alternative designs.

- Alternative design 3 does not satisfy any of the musts.

- The block diagram for the baseline design is incorrect (no Bluetooth).

- It is not clear which design is the baseline design (Bluetooth-based or Wi-Fi-enabled design?!).

First Term Report:

Evaluators' Comments:

- Remove specific technologies from your "musts" and "wants" list, such as Bluetooth, and focus instead on range specifications and other functional requirements.

- In your assumptions, ensure you include any necessary lock and door specifications required for your project.

- Please revise the figures for your alternative designs, ensuring all missing components are included, arrows indicate the correct directions, and any incorrectly placed components are corrected.

- It is unclear how the three alternative designs were compared and how the baseline design was selected. Consider using a more effective method for comparison and selection.

- In your project, ensure you identify potential threats and clearly explain how your approach will mitigate them effectively.

- In your report, ensure that references are removed from Chapter 2.

- In your report, some graphs are unclear.

- In your presentation, ensure you maintain eye contact with your audience and avoid using small fonts and some graphs are unclear.

Progress Update:

Evaluators' Comments:

- You need to work on the web or desktop application for the management.

- What and how are you measuring efficiency? What is your contribution to the actual design? Missing system level validation. Lack of justification and design reasoning. What is the definition of response time in the context of the project? Need to clearly define the requirements. Tasks need

to be more specific. Clearly define the contribution to the design.

- Make sure your validation experiments thoroughly validate the entire system, including the objective of the experiment, the tools used, the steps taken, the results, and the analysis of the results.

- You should start working on the physical design as any delay may increase the risk of missing the deadline.

APPENDIX – B: EFFECTIVE TEAM INTERACTIONS

TABLE 1: TEAM INFORMATION

Picture			
Name	ADEL ALJAED	AWS ALSAEDI	AHMED BADAHDH
ID	2036396	2035072	2035096
Phone Number	+966 54 380 6161	+966 56 094 8044	+966 54 347 0378
Email	Afarhanaljaed@stu.kau.edu.sa	Afalsaedi@stu.kau.edu.sa	aabadahdah@stu.kau.edu.sa
Specialty	Electrical Engineer (Computer)	Electrical Engineer (Computer)	Electrical Engineer (Computer)
Responsibility		Reports and Team Spokesperson	

Table B.8: Team Information

i. Meeting Minutes No. 1

Date	21/9/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed	Signature:	
Member. 2	Aws Hazzaa Alsaedi	Signature:	
Member. 3	Ahmed Khalid Badahdh	Signature:	
Advisor	Dr. Saud Wasly	Signature:	
Customer	Dr. Saud Wasly	Signature:	

Table B.9: Meeting Participants and Signatures

Agenda:

• Overview of the purpose of the SmartLock system for large buildings as a project.

• Discuss the musts, wants, and other aspects of the design specification with the customer.

• Review the preliminary draft of the first report

Discussion Points:

• Project musts and wants.

• Objectives of the project.

• Assumptions and constraints.

Follow-up of the last meeting:

• There is no follow-up to discuss because this is our first meeting.

Decisions taken:

• The musts and wants were to be further refined.

• The customer made the constraints and objectives clear.

Actions to do before the next meeting:

• Prepare a complete second draft of the report for Ch. 1 of the SDP project.

i. Meeting Minutes No. 2

Date	28/9/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed	Signature:	
Member. 2	Aws Hazzaa Alsaedi	Signature:	
Member. 3	Ahmed Khalid Badahdh	Signature:	
Advisor	Dr. Saud Wasly	Signature:	
Customer	Dr. Saud Wasly	Signature:	

Table B.10: Meeting Participants and Signatures

Agenda:

• Baseline design

• Possible alternatives

Discussion Points:

• Required specifications in the design

• Different components and their effects on the design

Follow-up of the last meeting:

• Review of previous discussion points (musts, wants, objectives, constraints, and assumptions)

Decisions taken:

• Confirmed the design with the client

Actions to do before the next meeting:

• Research the necessary components for the circuit design

i. Meeting Minutes No. 3

Date	5/10/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed	Signature:	
Member. 2	Aws Hazzaa Alsaedi	Signature:	
Member. 3	Ahmed Khalid Badahdh	Signature:	
Advisor	Dr. Saud Wasly	Signature:	
Customer	Dr. Saud Wasly	Signature:	

Table B.11: Meeting Participants and Signatures

Agenda:

• Overview of the circuit

• Overview of the microprocessor/board

• Implementation to facilitate door opening

Discussion Points:

• Which programming languages to be used

• The capabilities/features of the microprocessor

Follow-up of the last meeting:

• Research of the selected parts

Decisions taken:

• The use of ‘PlatformIO’ to program the microcontroller

Actions to do before the next meeting:

• Getting familiar with the embedded C Programming language

i. Meeting Minutes No. 4

Date	12/10/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed	Signature:	
Member. 2	Aws Hazzaa Alsaedi	Signature:	
Member. 3	Ahmed Khalid Badahdh	Signature:	
Advisor	Dr. Saud Wasly	Signature:	
Customer	Dr. Saud Wasly	Signature:	

Table B.12: Meeting Participants and Signatures

Agenda:

• Database diagram

• First sample database

Discussion Points:

• Why is the DB needed?

• What to include in the DB

Follow-up of the last meeting:

• Review Embedded C progress

Decisions taken:

- Post the design of the database on the DrawSQL website

Actions to do before the next meeting:

- Tasked to do simple connections or programs with the microchip

i. Meeting Minutes No. 5

Date	19/10/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed	Signature:	
Member. 2	Aws Hazzaa Alsaedi	Signature:	
Member. 3	Ahmed Khalid Badahdh	Signature:	
Advisor	Dr. Saud Wasly	Signature:	
Customer	Dr. Saud Wasly	Signature:	

Table B.13: Meeting Participants and Signatures

Agenda:

• Mobile App Design

• Figma Design Tool

Discussion Points:

• Researching relevant app designs

• Brainstorming UX, UI

Follow-up of the last meeting:

- Review the progress on the program task

Decisions taken:

- Confirm if the design is operable on different resolutions and choose the most suitable one

Actions to do before the next meeting:

- Do a mockup app interface

i. Meeting Minutes No. 6

Date	23/10/2024
Team	8
Project Title	Innovate Smart Lock System for Door Management

ii. Attendees

Member. 1	Adel Saer F. Aljaed		Signature:	
Member. 2	Aws Hazzaa Alsaedi		Signature:	
Member. 3	Ahmed Khalid Badahdh		Signature:	
Advisor	Dr. Saud Wasly		Signature:	
Customer	Dr. Saud Wasly		Signature:	

Table B.14: Meeting Participants and Signatures

Agenda:

• Mobile App Construction

• Flutter Development Kit

Discussion Points:

• Overview of Flutter

• Dart programming language

• The process of launching a mobile app on both IOS and Android

Follow-up of the last meeting:

• Review the basic 5-page app design on the designing tool

Decisions taken:

• Continued research of animations, asynchronous programing, and Bluetooth programing to provide a stable user experience

AppendiX – C: Use of Project Management Techniques

Team/Project Tasks

Title	Type	Assigned to	Start Date	End Date	Completion %
Senior Project	Project	Team 8	2024-09-02	2025-04-10	
First Semester	Group	Team 8	2024-09-02	2024-12-05	100%
Project Planning	Task	Team 8	2024-09-02	2024-09-05	100%
Chapter 1	Sub-Group	Team 8	2024-09-08	2024-09-26	100%
Problem Definition	Task	Aws	2024-09-08	2024-09-09	100%
Background Information	Task	Adel	2024-09-10	2024-09-12	100%
Problem Statement	Task	Ahmed	2024-09-15	2024-09-16	100%
Project Objectives	Task	Team 8	2024-09-17	2024-09-19	100%
Product Design Specifications (PDS)	Task	Team 8	2024-09-22	2024-09-26	100%
Chapter 2 & 3	Sub-Group	Team 8	2024-10-01	2024-10-27	100%
Literature Review	Task	Team 8	2024-10-01	2024-10-04	100%
Alternative Designs	Task	Team 8	2024-10-05	2024-10-07	100%
Alternative comparison	Task	Team 8	2024-10-09	2024-10-12	100%
Baseline Design	Task	Team 8	2024-10-13	2024-10-17	100%
System I/O	Task	Team 8	2024-10-18	2024-10-20	100%
Review	Task	Team 8	2024-10-21	2024-10-27	100%
Second Semester	Group	Team 8	2025-01-12	2025-04-10	100%
Obtaining the Hardware	Task	Team 8	2025-01-12	2025-01-23	100%
Programming the App	Task	Team 8	2025-01-26	2025-02-27	100%

Working on the Embedded System	Task	Team 8	2025-01-26	2025-02-27	100%
Testing and Modifying the door/app	Taks	Team 8	2025-03-02	2025-03-27	100%
Final Presentation	Task	Team 8	2025-03-30	2025-04-03	100%

Table C.15: Team/Project Tasks

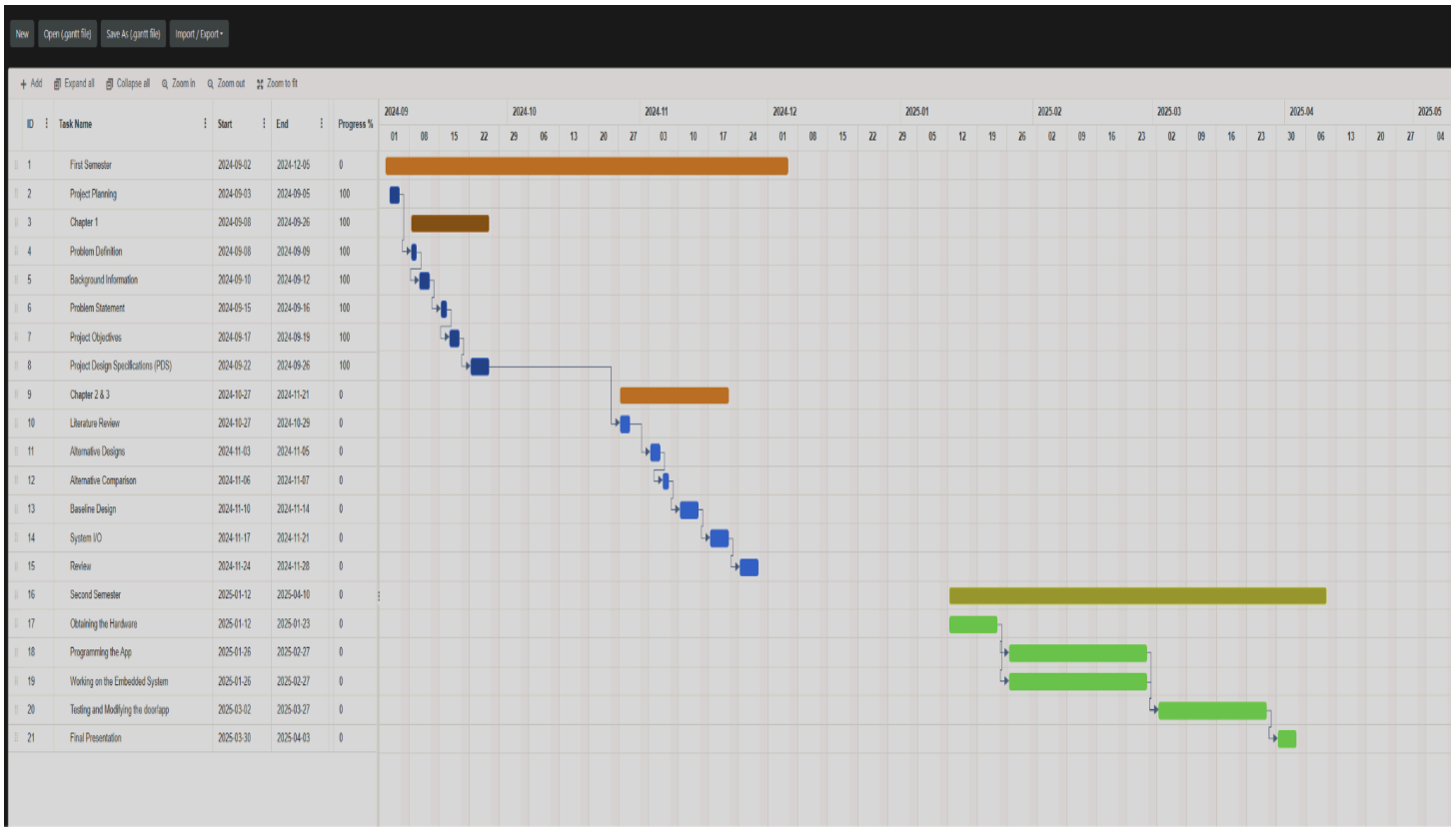


Figure C.19: The Project's Gantt Chart

APPENDIX – D: RECOGNITION OF ETHICAL AND PROFESSIONAL RESPONSIBILITY

CODE OF ETHICS REFERENCE

Institute of Electrical and Electronics Engineers (IEEE) Code of Ethics: The IEEE Code of Ethics is widely recognized in the fields of engineering and technology. It emphasizes the responsibility of professionals to act in the best interest of the public, maintain integrity, and contribute to the welfare of society.

Key principles include:

i. **Avoiding harm**: Engineers should avoid any actions that could harm the public or the environment.

ii. **Integrity**: Maintain honesty and transparency in professional dealings.

iii. **Fairness**: Treat all individuals fairly and with respect.

iv. **Professional development**: Continue professional development and assist in the development of others.

ETHICAL ISSUES ANALYSIS

Data Privacy and Security:

i. **Issue**: As your project involves collecting and processing user data, there is a significant risk regarding data privacy and security.

ii. **Analysis**: According to the IEEE Code of Ethics, engineers should "avoid harm" and "protect the privacy and confidentiality of individuals." It's crucial to implement robust security measures to safeguard user data and ensure compliance with data protection regulations such as GDPR or HIPAA.

Informed Decision: Implement data encryption, anonymization techniques, and obtain explicit consent from users before data collection. Regular audits and updates to security protocols will be necessary to mitigate risks.

Bias in Algorithms:

i. **Issue**: If your product relies on algorithms for decision-making, there's a risk of inherent bias affecting outcomes.

ii. **Analysis**: The IEEE Code stresses fairness, highlighting the importance of ensuring that all individuals are treated equitably. Bias in algorithms can lead to discriminatory practices, potentially harming marginalized groups.

iii. **Informed Decision**: Adopt a transparent approach to algorithm design, including diverse data sets for training. Regularly evaluate algorithms for bias and incorporate feedback mechanisms for users to report issues.

Environmental Impact:

i. **Issue**: The lifecycle of your product may have environmental implications, from resource extraction to disposal.

ii. **Analysis**: The commitment to "avoid harm" extends to environmental considerations. It's essential to assess the environmental footprint of your project.

iii. **Informed Decision**: Aim for sustainable practices, such as using recyclable materials and energy-efficient processes. Consider the end-of-life impact of your product and develop strategies for responsible disposal or recycling.

CONCLUSION

The "Bluetooth-Based Smart Lock System" represents a practical and innovative approach to addressing modern access control challenges. This project successfully combines advanced technology, user-friendly design, and cost-effective implementation to enhance door security for residential and commercial settings. By leveraging Bluetooth Low Energy (BLE) technology, the system achieves an optimal balance between energy efficiency and performance, offering seamless and secure door access through a mobile application.

Through thorough research and analysis, the design incorporates robust encryption protocols, ensuring that user data and communications remain secure. The use of a mobile application not only simplifies user interaction but also provides features such as real-time notifications, user authentication, and proximity-based access, enhancing convenience and reliability. Additionally, the system prioritizes low power consumption, making it a sustainable choice for long-term use with minimal maintenance.

While the design focuses on a Bluetooth-based system to meet budgetary and functional constraints, it also addresses common limitations of such systems. Features like proximity-controlled access mitigate risks associated with range limitations, and low-battery alerts ensure the system remains operational without unexpected interruptions. These thoughtful additions reflect the project's commitment to delivering a practical and user-centric solution.

This project serves as a foundational step toward integrating smart locks with broader home automation ecosystems. Future iterations could explore hybrid designs that combine BLE with Wi-Fi or cellular connectivity to expand functionality, such as remote access and cloud-based data logging. Additionally, incorporating biometric authentication or voice command integration could further enhance the system’s usability and security.

In conclusion, the "Bluetooth-Based Smart Lock System" achieves its goal of providing an efficient, secure, and accessible solution for modern access control. The project not only addresses current challenges in door management but also lays the groundwork for future innovations in smart lock technology, ensuring scalability and adaptability to evolving user needs. This comprehensive approach underscores the importance of thoughtful design, engineering precision, and a clear focus on user experience in creating impactful and reliable solutions.