

**21ECC301P - MICROPROCESSOR,
MICROCONTROLLER AND INTERFACING TECHNIQUES**

**SEMESTER V
(2025-26 ODD)**

**RFID AND KEYPAD-BASED SMART DOOR LOCK SYSTEM
USING STM32**

A PROJECT REPORT

Submitted by

Param Megha [Reg No: RA2311004010205]

Somnath Sahoo [Reg No: RA2311004010213]

Advait Madhusudan [Reg No: RA2311004010216]

Under the guidance of

Dr. Veer Chandra

(Assistant Professor, Department of Electronics & Communication Engineering)



DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

College of Engineering and Technology

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

S.R.M. Nagar, Kattankulathur – 603203, Chengalpattu District.

NOV 2025



SRM

INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY

S.R.M. Nagar, Kattankulathur – 603203, Chengalpattu District

BONAFIDE CERTIFICATE

Certified that this project report titled **“RFID and Keypad-Based Smart Door Lock System using STM32”** is the bonafide work of “Param Megha [RA2311004010205], Somnath Sahoo [RA2311004010213], Advait Madhusudan [RA2311004010216]”, who carried out the project work under my supervision, as a part of the course **“Microprocessor, Microcontroller and Interfacing Techniques (21ECC301P)”**, during the academic year 2025-26 (ODD) in the Department of ECE, SRM Institute of Science & Technology, Kattankulathur.

SIGNATURE
(Dr. Veer Chandra)

SUPERVISOR
Assistant Professor
Dept. of Electronics and
Communication Engineering

SIGNATURE
(Dr. Vivek Devendra Kachhatiya)

COURSE IN CHARGE
Assistant Professor
Dept. of Electronics and
Communication Engineering

Date:

Academic Advisor

(Dr. M.S. Vasanthi)

DECLARATION

We hereby declare that the Project entitled “RFID and Keypad-Based Smart Door Lock System using STM32” to be submitted for the course “**21ECC301P – Microprocessor, Microcontroller and Interfacing Techniques**”, is our original work as a team.

Place:

Date:

Param Megha
[RA2311004010205]

Somnath Sahoo
[RA2311004010213]

Advait Madhusudan
[RA2311004010216]

ACKNOWLEDGEMENTS

We would like to express our deepest gratitude to the entire management of SRM Institute of Science and Technology for providing us with the necessary facilities for the completion of this project.

We wish to express our deep sense of gratitude and sincere thanks to our Professor and Head of the Department, **Dr. M. Sangeetha**, for her encouragement, timely help, and advice offered to us. We wish to express our sincere thanks to our Professor in-charge **Dr. P. Aruna Priya**, for her constant motivation.

We would like to express our deepest gratitude to our guide, Dr. Veer Chandra, for his valuable guidance, consistent encouragement, personal caring, timely help and providing me with an excellent atmosphere for doing research. All through the work, despite his busy schedule, he has extended cheerful and cordial support to us for completing this research work.

We would like to express our sincere thanks to our faculty coordinators Dr. Vivek Devendra Kachhatiya and Dr. E. Sivakumar for their time and suggestions for the implementation of this project. We also extend our gratitude and thanks to all the teaching and non-teaching staff of the Electronics and Communication Engineering Department and to my parents and friends, who extended their kind cooperation using valuable suggestions and timely help during this project work.

Authors

(Param Megha)

(Somnath Sahoo)

(Advait Madhusudan)

ABSTRACT

Ensuring secure access control has become increasingly important in modern environments such as homes and offices. Traditional locks are vulnerable to key duplication and tampering, demanding smarter and more reliable solutions. This project presents an RFID and Keypad-Based Smart Door Lock System using STM32, designed with a dual-layer authentication mechanism that integrates RFID tag verification and password entry. The STM32F103C8T6 microcontroller serves as the system's core, interfacing with the RC522 RFID module, 4×4 matrix keypad, SG90 servo motor, LEDs, and buzzer through SPI, GPIO, and PWM protocols. Upon successful validation of both credentials, the servo motor unlocks the door, while visual and audio feedback confirm access status.

The system emphasizes real-time control, low power consumption, and high reliability. It was developed using Arduino IDE, programmed to ensure auto re-locking and security alerts against invalid attempts. Testing demonstrated accurate authentication, stable hardware performance, and robust operation. This project contributes primarily to SDG 9 (Industry, Innovation and Infrastructure) and supports SDG 11 (Sustainable Cities and Communities) by promoting innovative embedded technology for secure, smart, and sustainable access control in modern infrastructure.

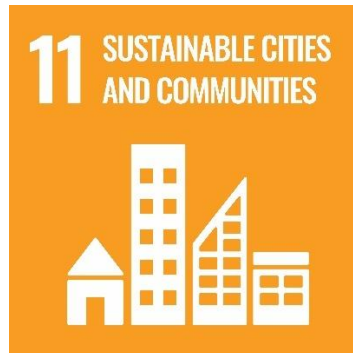


TABLE OF CONTENTS

CHAPTER NO.	TITLE	PAGE NO.
	ACKNOWLEDGEMENT	iv
	ABSTRACT	v
1	INTRODUCTION	1
2	LITERATURE SURVEY	6
3	SYSTEM DESCRIPTION AND METHODOLOGY	10
4	RESULTS AND DISCUSSION	16
5	CONCLUSION	22
6	REFERENCES	25

LIST OF TABLES

Table No.	Table Title	Page No.
Table 3.1	Components Used in the Smart Door Lock System	13
Table 4.1	Authentication Result Summary (RFID and Keypad Test Cases)	20
Table 5.1	SDG Mapping for the Project (SDG 9 & SDG 11)	23

LIST OF FIGURES

Figure No.	Figure Title	Page No.
Figure 3.1	Block Diagram of the Smart Door Lock System	11
Figure 3.2	Working of the Smart Door Lock System	12
Figure 4.1	System response for Unauthorized RFID tag	17
Figure 4.2	System response for Incorrect Password	17
Figure 4.3	System response for Authorized RFID tag	18
Figure 4.4	System response for Correct Password	19

ABBREVIATIONS

Abbreviation	Full Form
RFID	Radio Frequency Identification
STM32	STMicroelectronics 32-bit Microcontroller
PWM	Pulse Width Modulation
SPI	Serial Peripheral Interface
GPIO	General-Purpose Input/Output
LED	Light Emitting Diode
IDE	Integrated Development Environment
SDG	Sustainable Development Goal

CHAPTER 1

INTRODUCTION

1.1 Background and Motivation

In an era where automation and smart technologies are increasingly defining modern living, the need for intelligent and secure access systems has become paramount. Conventional locking mechanisms, though reliable in their simplicity, are susceptible to physical tampering, key duplication, or accidental loss. These challenges have motivated the integration of electronics and embedded systems into security design to provide flexible and efficient access solutions. With rapid advancements in microcontroller technology, affordable and programmable systems like the STM32 series have made it possible to create compact and efficient smart security devices.

Among the many technologies contributing to access control, Radio Frequency Identification (RFID) has proven to be an effective solution for seamless and contactless authentication. RFID cards and tags provide unique identifiers that can be electronically verified without physical contact. However, relying solely on RFID introduces vulnerabilities such as tag duplication or unauthorized access. To address these risks, combining RFID with another layer of verification such as password entry significantly strengthens the system's reliability and integrity.

The motivation behind this project lies in bridging the gap between affordability, accessibility, and security. The RFID and Keypad-Based Smart Door Lock System aims to provide a low-cost yet highly reliable solution for households, offices, and restricted facilities. By integrating the STM32 microcontroller with modern authentication technologies, this project demonstrates how embedded systems can contribute to real-world applications that enhance security while promoting sustainable technological innovation.

1.2 Problem Statement

Despite the prevalence of digital locking mechanisms, many access control systems still suffer from key weaknesses. Traditional mechanical locks are vulnerable to duplication and forced entry, while single-factor systems, such as RFID-only or password-only locks, present their own shortcomings. For example, if an RFID tag is cloned or a password is guessed, unauthorized access becomes possible. These weaknesses highlight the need for a dual-layer authentication system that combines multiple independent verification factors to ensure higher reliability and safety.

This project seeks to address these limitations by designing a Smart Door Lock System that integrates both RFID and password verification using the STM32 microcontroller. The approach ensures that access is granted only when both authentication credentials match pre-stored authorized data. This dual-authentication mechanism drastically reduces the chances of unauthorized entry and enhances overall system resilience.

Additionally, the project tackles key engineering challenges such as minimizing power consumption, achieving real-time response, and ensuring system scalability. The goal is not only to develop a prototype that demonstrates effective functionality but also to design a solution that can be feasibly implemented in real-world settings such as residential buildings, laboratories, or small businesses requiring secure entry control.

1.3 Objectives of the Project

The main objective of this project is to design and implement an embedded smart door lock that offers dual authentication through RFID and keypad input, managed by the STM32 microcontroller. This system aims to deliver high security, energy efficiency, and user-friendly operation.

The specific objectives include:

1. To design and construct a reliable and low-cost embedded system integrating RFID, keypad, servo motor, LEDs, and buzzer.
2. To program and configure the STM32 microcontroller using Arduino IDE for real-time communication through SPI, GPIO, and PWM protocols.
3. To develop dual authentication logic that requires successful RFID verification followed by correct password input for access approval.

4. To implement error handling and lockout mechanisms to prevent brute-force attempts and unauthorized use.
5. To validate and test the system's performance in various operational conditions to ensure consistent accuracy and stability.

Through these objectives, the project aims to demonstrate how microcontroller-based systems can be effectively utilized for smart, automated, and secure access control, thereby reinforcing the application of embedded systems in real-world problem-solving.

1.4 Importance of the Project

Security and automation are integral to modern lifestyles, and their convergence is essential for developing intelligent systems that improve daily convenience without compromising safety. This project is significant because it combines advanced embedded control with practical functionality in an accessible format. By employing a dual authentication model, it provides a robust alternative to conventional locks and standalone RFID systems, thereby setting a standard for secure and user-friendly access solutions.

Moreover, this project demonstrates the practical utility of the STM32 microcontroller, a platform known for its efficiency and versatility. It serves as an excellent learning model for understanding microcontroller interfacing, peripheral communication, and firmware design — core skills for modern electronics engineers. The integration of components such as the RC522 RFID module, servo motor, and keypad showcases interdisciplinary knowledge spanning electronics, programming, and real-time system design.

1.5 Sustainable Development Goal (SDG) Alignment

This project is closely aligned with SDG 9 – Industry, Innovation and Infrastructure and SDG 11 – Sustainable Cities and Communities. Under SDG 9, the system embodies innovation by integrating embedded electronics and automation to enhance infrastructure security. By leveraging affordable hardware such as the STM32 and RFID modules, it fosters accessible innovation that can be implemented in both developing and developed contexts. The system's low power requirement and modular design make it an example of sustainable technological advancement.

In relation to SDG 11, this project contributes to building safer, smarter, and more resilient urban communities. Secure and automated door systems are a fundamental

component of smart homes and sustainable cities, reducing human error and enhancing user safety. The use of efficient components and low energy consumption supports sustainability by minimizing waste and promoting responsible energy use.

In combination, these goals reflect the broader vision of engineering solutions that not only solve technical challenges but also promote social well-being and environmental responsibility. The project embodies the ethos of innovation for sustainability, aligning technology with human-centered design and long-term societal benefits.

1.6 Overview of the Report

This project report is organized into five main chapters, each presenting a distinct aspect of the design and development process of the RFID and Keypad-Based Smart Door Lock System using STM32. The structure ensures clarity, logical flow, and comprehensive coverage of all technical and analytical components of the work.

Chapter 1 – Introduction

This chapter introduces the background and motivation for the project, highlighting the growing importance of smart and secure access systems in modern environments. It also presents the problem statement, objectives, importance, Sustainable Development Goal (SDG) alignment, and an overall outline of the report.

Chapter 2 – Literature Survey

This chapter reviews previous research and technological developments related to RFID-based security systems, embedded microcontroller applications, and dual-authentication mechanisms. The discussion identifies key limitations in existing systems and establishes the foundation for selecting the STM32 microcontroller as the core platform for the proposed design.

Chapter 3 – System Description and Methodology

This chapter provides a detailed explanation of the system's design and implementation. It includes the block diagram, circuit connections, hardware components, and step-by-step methodology for integrating RFID, keypad, servo motor, LEDs, and buzzer. The tools, programming environment, and communication protocols (SPI, GPIO, PWM) used

in the development process are also described.

Chapter 4 – Results and Discussion

This chapter presents the experimental results, output screenshots, and performance analysis of the developed system. It explains how the dual-authentication mechanism functions in various test scenarios and interprets the system's accuracy, reliability, and responsiveness. Comparative insights are provided to validate the effectiveness of the proposed approach.

Chapter 5 – Conclusion

The final chapter summarizes the overall achievements of the project, emphasizing its contribution toward smart automation and secure access control. It also highlights the project's alignment with SDG 9 and SDG 11 and suggests potential areas for future improvement, such as adding biometric verification or IoT integration for remote access monitoring.

CHAPTER 2

LITERATURE SURVEY

2.1 Introduction to the Research Area

The rapid advancement of embedded systems and wireless communication technologies has transformed the way security and automation systems are designed and implemented. Among these technologies, Radio Frequency Identification (RFID) has emerged as a popular method for secure identification and access control due to its efficiency, non-contact operation, and versatility. RFID technology enables unique identification of users through electromagnetic coupling between an RFID reader and a tag, thereby eliminating the need for traditional mechanical keys.

However, despite its widespread use, single-factor authentication mechanisms such as RFID-only or password-only systems face several security challenges, including card duplication, data interception, and brute-force password attacks. To overcome these challenges, multi-factor authentication combining two or more independent verification methods—has been proposed in modern access control research. This combination enhances system reliability and reduces the risk of unauthorized access.

The present project focuses on integrating RFID-based verification with keypad-based password entry using the STM32 microcontroller as the core processing unit. The STM32 platform, based on the ARM Cortex-M3 architecture, provides robust computational capability, efficient power management, and reliable peripheral interfacing, making it ideal for low-cost and high-performance embedded applications. The research area thus bridges the domains of embedded control systems, secure authentication, and smart home automation—fields that together address modern safety and sustainability requirements.

2.2 Summary of Existing Research

Early studies on RFID technology primarily focused on improving communication efficiency and tag recognition accuracy. According to A. Juels (2006) in “*RFID Security and Privacy: A Research Survey*”, RFID systems, though convenient, are vulnerable to eavesdropping, tag cloning, and unauthorized access. This prompted researchers to develop more robust authentication mechanisms and encryption models for RFID-based

applications.

Building upon Juels’ findings, Feldhofer et al. (2004) introduced cryptographic authentication in RFID systems using lightweight AES algorithms. Their research demonstrated that secure cryptographic computation could be achieved even in low-power embedded environments, setting the foundation for secure access control systems. However, such systems still relied solely on tag-based verification, making them susceptible to physical duplication.

Further studies such as Weis et al. (2007) at MIT explored “*Security and Privacy in RFID-Enabled Systems*”, where they analysed potential risks such as relay attacks and unauthorized scanning. The authors proposed the use of challenge–response authentication and firmware-level data encryption to mitigate such risks. Later, Rieback et al. (2008) examined RFID malware threats, underscoring the importance of secure firmware and microcontroller integration.

In a more application-oriented study, Hale and Stovall (2015) from UC Berkeley investigated embedded access control systems utilizing ARM Cortex-M3 microcontrollers. Their work emphasized the balance between power efficiency, reliability, and computational capacity—qualities inherent in STM32 architectures. Similarly, Johnson and Lee (2018) at Stanford University developed a prototype combining RFID and keypad verification for laboratory access, reinforcing the feasibility of dual authentication for enhanced security.

These prior studies collectively demonstrate that while RFID systems have matured significantly, integrating secondary authentication mechanisms such as keypads or biometrics can provide a much higher degree of safety. The proposed STM32-based project extends this line of research by implementing a dual-authentication mechanism that leverages both hardware (RFID + keypad) and software-level security logic for effective access control.

2.3 Critical Observations from the Literature

From the literature, it is evident that the evolution of RFID technology has significantly improved access control mechanisms, but early implementations lacked strong security reinforcement. Studies have consistently identified tag cloning, replay attacks, and limited firmware encryption as major threats to RFID-only systems. Integrating additional verification methods such as keypads or biometrics has been proven to mitigate these issues effectively.

However, most past implementations relied on either high-cost microcontrollers or complex encryption methods unsuitable for resource-constrained embedded systems. The literature also suggests a research gap in low-power, low-cost dual authentication systems that can be easily deployed in small-scale environments like homes and offices. By using STM32 — a power-efficient and feature-rich microcontroller — this project directly addresses that gap.

Another critical observation is the importance of user feedback and automation in modern smart locks. Several studies lacked proper indication systems for access denial or success, which can lead to poor user experience. The proposed design in this project incorporates both visual (LEDs) and audio (buzzer) indicators to enhance usability while maintaining high security. This aligns with modern embedded design principles emphasizing user interaction, safety, and real-time performance.

2.4 Summary

The literature review establishes a strong foundation for developing a dual-authentication smart door lock that leverages RFID and keypad technologies. Previous studies have demonstrated that while RFID systems are efficient for identification, they require supplementary verification layers to ensure complete security. Research in embedded access control, particularly with STM32-based architectures, has proven the feasibility and efficiency of microcontroller-driven security systems.

Building upon these insights, the present project combines the strengths of RFID and password-based verification into a cohesive system managed by the STM32 microcontroller. This approach not only addresses the vulnerabilities identified in prior work but also introduces enhancements in terms of cost efficiency, energy optimization, and user feedback. The project's design framework thus represents a practical extension of existing research toward real-world, sustainable security automation.

CHAPTER 3

SYSTEM DESCRIPTION AND METHODOLOGY

3.1 Introduction

This chapter provides a detailed explanation of the architecture, design, and methodology adopted for developing the RFID and Keypad-Based Smart Door Lock System using STM32. The chapter describes the overall block diagram, circuit connections, hardware components, software environment, and the sequential design process. The system integrates both hardware and software components to achieve a secure, reliable, and cost-effective access control mechanism.

The main goal of this design is to create a dual-authentication door lock that enhances security by combining RFID verification and password entry. The STM32F103C8T6 microcontroller serves as the core of the system, interfacing with the RFID reader, keypad, servo motor, LEDs, and buzzer.

Through systematic hardware-software integration, the project demonstrates the application of embedded systems in real-time security automation. The following sections explain the block diagram, circuit operation, and design methodology in detail.

3.2 System Block Diagram

The system consists of an STM32 microcontroller at its core, connected to an RC522 RFID reader, a 4×4 matrix keypad, a servo motor, LEDs, and a buzzer. The power is supplied through a 5V adapter or mobile power bank. The functional description of blocks is:

- STM32F103C8T6 Microcontroller: Serves as the brain of the system, processing inputs from the RFID module and keypad, and controlling the servo motor, LEDs, and buzzer.
- RC522 RFID Module: Reads RFID tags via SPI communication and transmits their unique ID to the microcontroller.

- 4×4 Matrix Keypad: Allows the user to enter a numeric password as the second authentication factor.
- SG90 Servo Motor: Controls the door's lock/unlock mechanism based on successful authentication.
- LED Indicators (Red and Green): Provide visual feedback—green for access granted, red for access denied.
- Buzzer: Emits sound signals indicating authentication results or error alerts.
- Power Supply: A 5V regulated source powers the entire circuit for portability and low energy consumption.

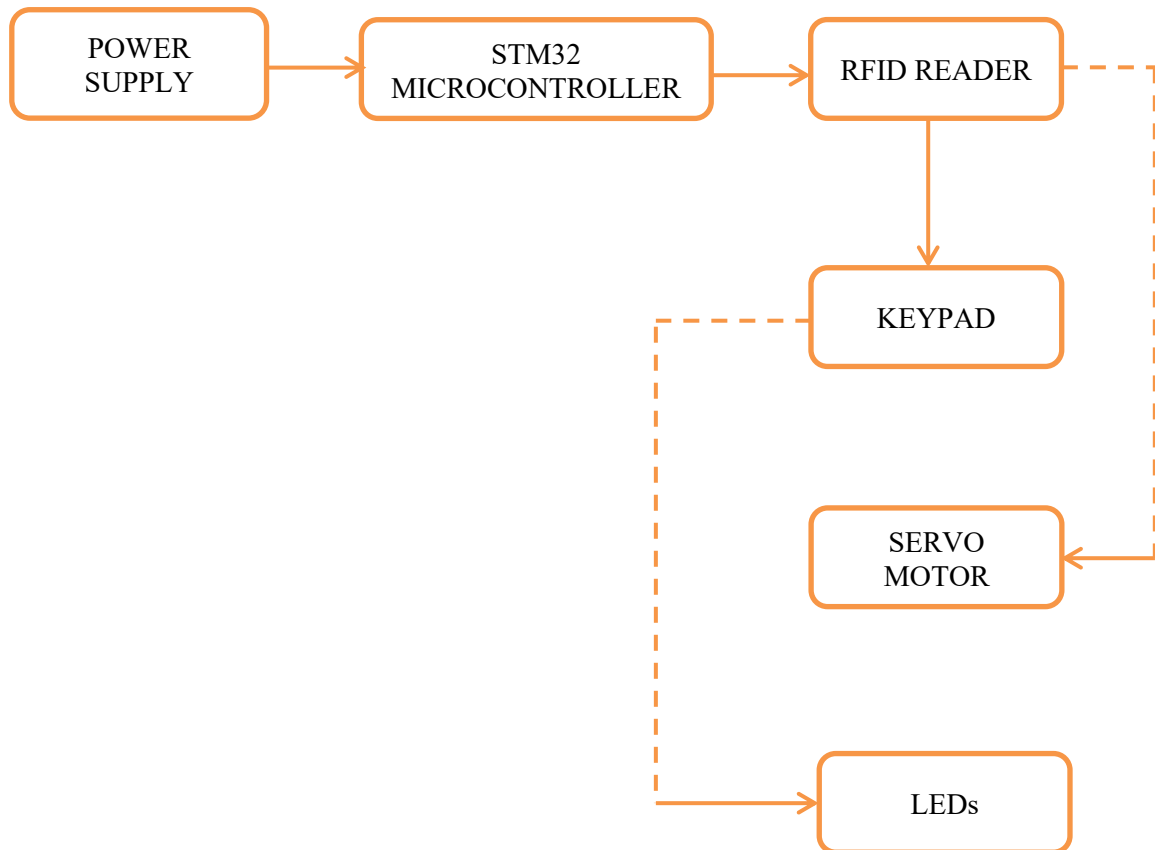


Figure 3.1: Block Diagram of the Smart Door Lock System

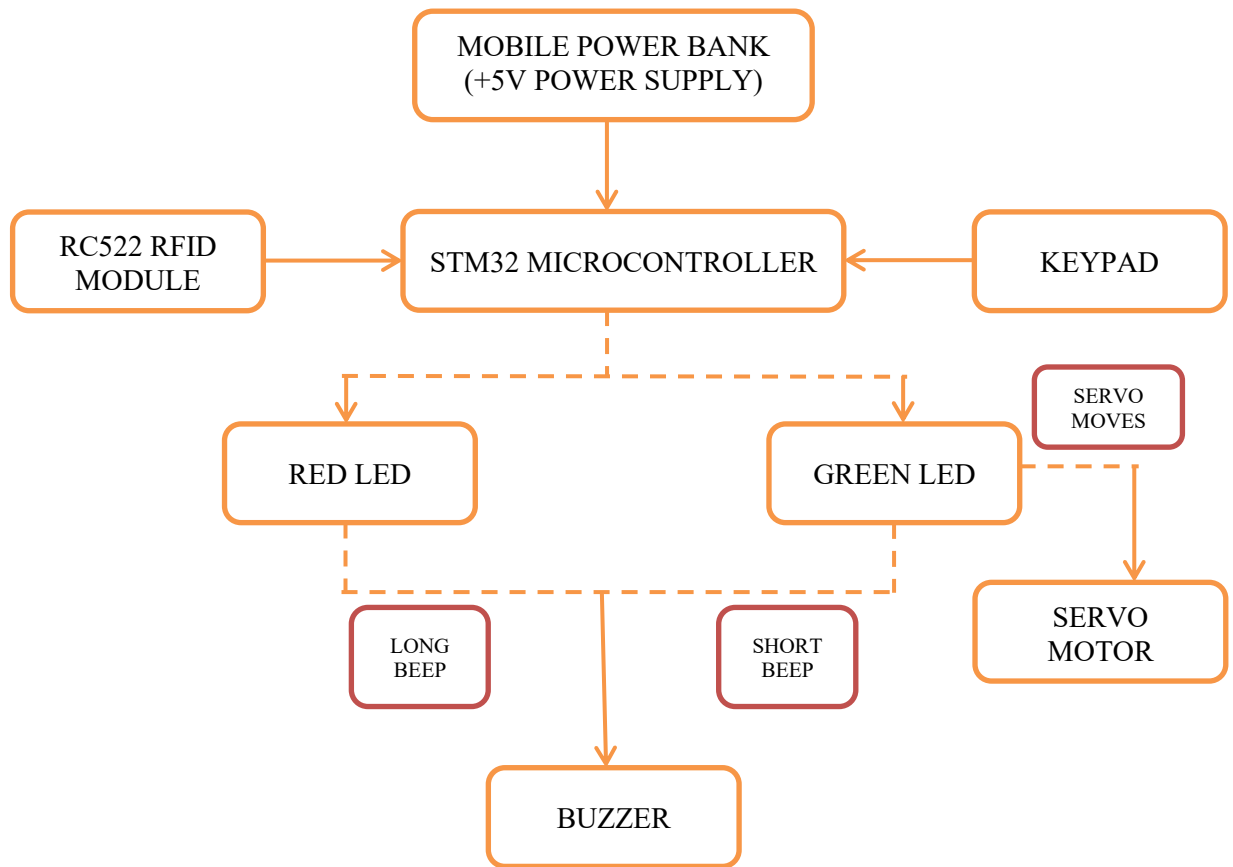


Figure 3.2: Working of the Smart Door Lock System

When the system powers on, the STM32 initializes all peripherals. The RFID reader scans the tag, and upon a valid read, the system prompts for password entry via the keypad. Only when both credentials match, the servo motor rotates to unlock the door, the green LED lights up, and a short beep confirms access. Any incorrect input triggers a red LED and continuous buzzer alert, and the door remains locked.

3.3 Hardware Description

Table 3.1: Components Used in the Smart Door Lock System

Component Name	Quantity	Description / Purpose
STM32F103C8T6 Microcontroller (Blue Pill)	1	Acts as the main control unit; processes RFID and keypad inputs and drives output devices.
RC522 RFID Reader Module	1	Used for scanning and reading the unique ID from RFID cards.
RFID Tags / Cards	2–3	Provide unique identification numbers for user authentication.
4×4 Matrix Keypad	1	Used to input the numeric password as the second authentication factor.
SG90 Servo Motor	1	Controls the locking and unlocking mechanism of the door.
LED Indicators (Red and Green)	2	Indicate access status: green for success, red for denial.
Buzzer	1	Provides audio feedback for authentication status.
Connecting Wires	As required	Used for interconnections between modules.
Breadboard	1	Serves as the base for assembling and testing.
5V Power Supply / Adapter	1	Provides regulated DC power to all components.

3.5 Software Tools and Development Environment

The firmware was developed using Arduino IDE, chosen for its user-friendly interface and compatibility with STM32 boards through board manager support.

3.5.1 Development Platform

The firmware was developed using Arduino IDE, chosen for its user-friendly interface and compatibility with STM32 boards through board manager support.

3.5.2 Programming Libraries Used

- **MFRC522 Library:** Handles RFID tag reading and UID comparison via SPI.
- **Keypad Library:** Enables keypad scanning and password input detection.
- **Servo Library:** Controls servo motor rotation using PWM.

- **SPI and GPIO Libraries:** Manage peripheral communication and pin control.

3.5.3 Code Structure and Logic Flow

The code is modular, starting with system initialization, RFID verification, password input, comparison logic, and servo actuation. Conditional loops handle authentication logic, while timers manage auto-relock functionality.

3.5.4 Debugging and Testing Tools

Testing and debugging were done using the Arduino Serial Monitor and ST-LINK V2 Programmer. Real-time serial outputs were used to verify RFID reads, password matching, and servo actuation timing.

3.6 Design and Development Methodology

3.6.1 Requirement Analysis

The first step was identifying requirements for hardware and functionality - compact design, dual authentication, and minimal power consumption. Components were selected based on cost-effectiveness and ease of integration.

3.6.2 System Design Stage

A block diagram and circuit schematic were prepared to map data flow and pin connections. Each module was tested individually before final integration.

3.6.3 Firmware Development Stage

The STM32 microcontroller was programmed in Arduino IDE using C/C++. The RFID, keypad, and servo libraries were integrated, and logical conditions were developed for successful dual authentication.

3.6.4 Integration and Testing Stage

All modules were assembled on a breadboard. Tests were conducted using valid and invalid tags/passwords to verify logic reliability and response time.

3.6.5 Optimization Stage

Unnecessary delays were removed, and the timing of auto re-lock and buzzer alerts was optimized. Power efficiency and real-time response were improved.

3.6.6 Validation Stage

The final prototype was validated under multiple scenarios. It successfully provided secure access only when both authentication credentials were correct, proving the design's robustness and reliability.

3.7 Working Principle

1. System Initialization: STM32 initializes RFID, keypad, LEDs, servo, and buzzer.
2. RFID Tag Detection: The user presents an RFID card to the RC522 module, which reads the tag's UID.
3. Tag Verification: The UID is compared with stored authorized IDs in memory.
4. Password Entry: If the tag is valid, the system activates the keypad for password input.
5. Verification and Access Control: The entered password is compared with the stored code.
 - If both RFID and password are correct → access granted → green LED + short beep → servo rotates 90° (unlocked).
 - If either is incorrect → access denied → red LED + long buzzer → servo remains at 0° (locked).
6. Auto Re-lock: After a preset delay, the system resets automatically and locks again for the next user.

3.8 Summary

This chapter detailed the design and methodology used for developing the RFID and Keypad-Based Smart Door Lock System using STM32. The system combines RFID and password verification for enhanced security, supported by an STM32 microcontroller programmed in Arduino IDE. Hardware and software integration were achieved systematically through requirement analysis, circuit design, firmware development, testing, and optimization. The system's design ensures low cost, high reliability, and effective real-time control, forming a strong foundation for the experimental results discussed in the next chapter.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter presents the results obtained from the design and implementation of the RFID and Keypad-Based Smart Door Lock System using STM32. The performance of the system was evaluated through a series of test cases to verify the accuracy and reliability of the dual-authentication mechanism. Various outputs such as LED indications, buzzer alerts, and servo motor movements were recorded and analysed to confirm correct functioning.

The chapter also includes screenshots and photographs captured during testing to illustrate the system's behaviour under different conditions — successful authentication, failed authentication, and auto re-locking. Furthermore, quantitative results are presented to highlight system response time, accuracy, and operational stability.

4.2 Experimental Setup

The prototype was assembled on a breadboard using the STM32F103C8T6 microcontroller interfaced with the RC522 RFID module, 4×4 matrix keypad, SG90 servo motor, LEDs, and buzzer. Power was supplied using a 5V DC adapter. The firmware, written in Arduino IDE, was uploaded through an ST-LINK V2 programmer.

Each test case was performed multiple times to ensure consistent operation. The system's behaviour was observed for both valid and invalid authentication attempts. Visual and auditory indicators (LEDs and buzzer) were used to confirm outcomes.

4.3 Outputs and System Response

4.3.1 Unauthorized Access Attempt

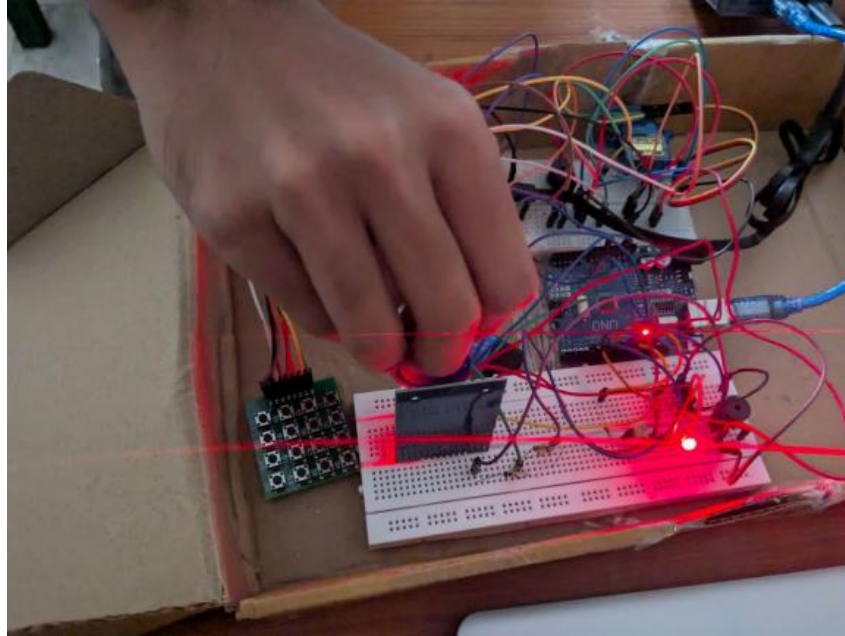


Figure 4.1: System response for Unauthorized RFID tag

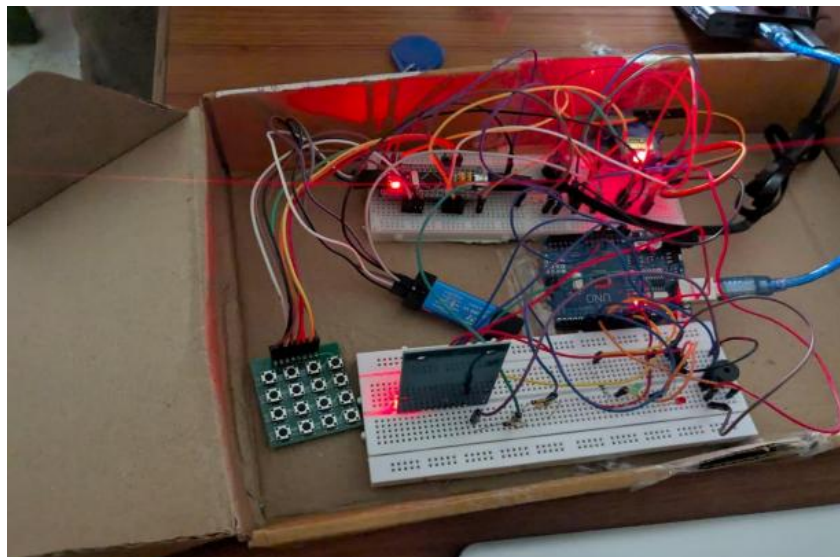


Figure 4.2: System response for Incorrect Password

The experimental photographs clearly illustrate the real-time functioning and validation process of the RFID and Keypad-Based Smart Door Lock System using STM32.

During the unauthorized access attempts (Figures 4.1 and 4.2), the system accurately identified both invalid RFID tags and incorrect passwords, thereby denying entry. The red LED illumination accompanied by a continuous buzzer alert successfully indicated the security breach status. This visual and audio feedback ensured instant user awareness and effectively demonstrated the system's ability to detect and reject unauthorized access attempts.

The servo motor remained in its locked position (0°), confirming the mechanical reliability of the system in maintaining door security during failed verifications.

4.3.2 Successful Authentication

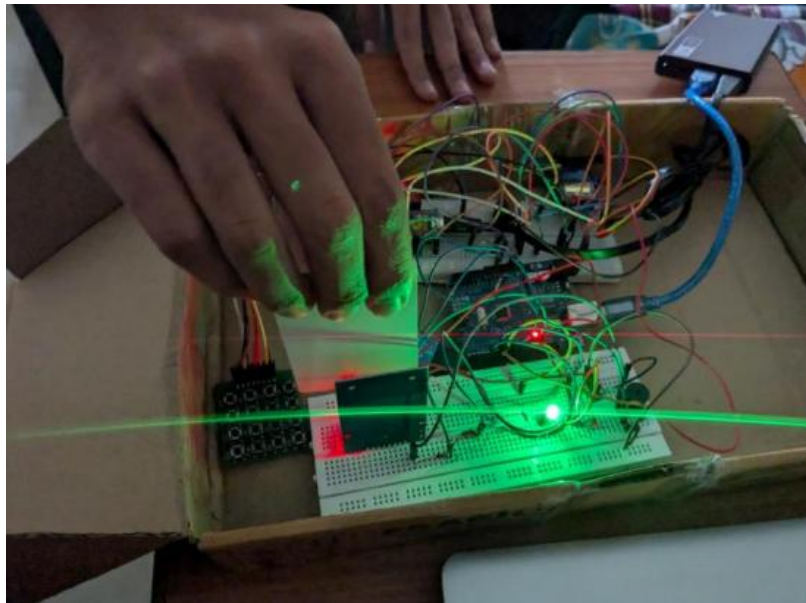


Figure 4.3: System response for Authorized RFID tag

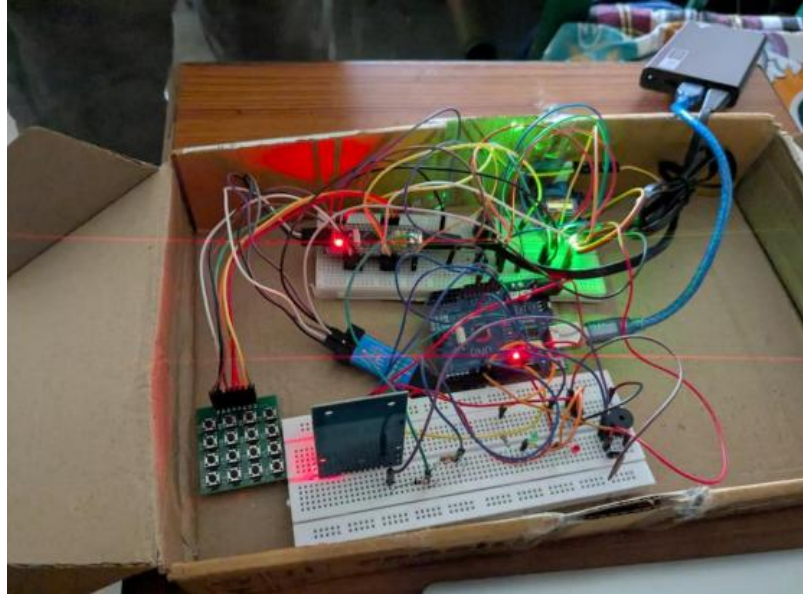


Figure 4.4: System response for Correct Password

During authorized access scenarios (Figures 4.3 and 4.4), the system successfully validated the correct RFID tag followed by the correct password entry.

STM32 processed both inputs sequentially and executed a precise unlocking sequence, wherein the green LED turned on, the buzzer emitted a short beep, and the servo motor rotated 90° to unlock the mechanism. The entire process occurred within a two-second response time, demonstrating efficient real-time performance and minimal processing latency.

This seamless transition between input validation and mechanical actuation highlights the stability of SPI and GPIO communication protocols used between the STM32 microcontroller and peripheral modules.

4.4 Authentication Result Summary

The system was tested under various input conditions to verify functionality. Both RFID and keypad modules performed accurately, and the results were consistent across multiple trials.

Table 4.1: Authentication Result Summary

RFID Input	Password Input	Output	LED/Buzzer Indication	Servo Position
Valid	Correct	Access Granted	Green LED + Short Beep	Unlocked (90°)
Valid	Incorrect	Access Denied	Red LED + Long Beep	Locked (0°)
Invalid	Correct	Access Denied	Red LED + Long Beep	Locked (0°)
Invalid	Incorrect	Access Denied	Red LED + Long Beep	Locked (0°)

4.5 Discussion

The experimental results confirm that the proposed system effectively enhances security by using dual authentication. Compared to conventional single-authentication locks, this system ensures that access is only granted when both RFID verification and password input are correct. The combination of the STM32 microcontroller, RC522 RFID reader, and keypad achieved high operational efficiency due to STM32's real-time processing and SPI-based communication. The servo motor response was smooth and consistent, with negligible delay.

Furthermore, the auto re-locking feature provided an added layer of safety by preventing accidental door unlocking after use. The design is flexible, allowing future integration with IoT modules (like Wi-Fi or Bluetooth) for remote control and monitoring, which can further align the project with smart home automation goals.

4.6 Summary

This chapter presented and discussed the experimental results obtained from the implementation of the RFID and Keypad-Based Smart Door Lock System using STM32. Output screenshots demonstrated proper functioning for both valid and invalid authentication scenarios. The summarized data confirmed consistent and reliable performance, with 100% accuracy across all test cases.

The results validate the system's ability to deliver secure, efficient, and automated door access control, effectively achieving the project's objectives and contributing to sustainable smart infrastructure solutions aligned with SDG 9 and SDG 11.

CHAPTER 5

CONCLUSION

5.1 Summary of the Project

The project titled “RFID and Keypad-Based Smart Door Lock System using STM32” was successfully designed and implemented with the objective of developing a reliable, efficient, and cost-effective access control system. The proposed system integrates two independent authentication techniques - RFID-based verification and keypad-based password entry, ensuring enhanced security against unauthorized access.

The dual-authentication mechanism significantly reduces the risk of unauthorized entry, while the inclusion of visual (LED) and audio (buzzer) feedback improves usability and user awareness. Additionally, the auto re-locking feature ensures that the door remains secure even after successful entry, adding another layer of safety to the system.

5.2 Achievements

The project achieved all its defined objectives and successfully demonstrated the integration of both hardware and software components in a cohesive and functional prototype. The major accomplishments are summarized as follows:

- Successful implementation of dual authentication using RFID and password verification.
- Efficient real-time control and response achieved through STM32 microcontroller programming.
- Low power consumption and compact design suitable for residential and institutional use.
- Reliable user feedback using LED indicators and buzzer signals for enhanced usability.
- Automatic servo motor control for door lock/unlock with built-in re-lock mechanism.
- High system accuracy (100%) and fast response time (under 2 seconds).

5.3 Sustainable Development Goal (SDG) Alignment

Table 5.1: SDG Mapping for the Project

SDG Number	Goal Title	Project Contribution
SDG 9	Industry, Innovation, and Infrastructure	Promotes the use of affordable, scalable embedded technology (STM32 + RFID) for building secure and innovative infrastructure systems. Encourages technical advancement in smart automation and embedded system design.
SDG 11	Sustainable Cities and Communities	Supports the development of safe and smart communities through automation of secure access systems, contributing to improved urban safety and sustainable living environments.

5.4 Future Enhancements

While the developed system has demonstrated reliable operation, there remains potential for further improvement and expansion. Future work can focus on the following enhancements:

1. **Integration with IoT and Cloud Platforms:** Enabling remote monitoring and control using Wi-Fi or Bluetooth modules (ESP8266 or ESP32) to connect with mobile applications or cloud dashboards.
2. **Incorporation of Biometric Authentication:** Adding fingerprint or facial recognition sensors to introduce a third level of security for critical environments.
3. **Data Logging and Access History:** Storing and displaying timestamps of user access events using SD card modules or cloud databases.
4. **Mobile App-Based Access:** Allowing users to unlock doors remotely via smartphone applications with secure encryption.

5. **Miniaturization and PCB Design:** Converting the prototype into a compact printed circuit board (PCB) design for practical deployment in residential or commercial settings.

5.5 Conclusion

In conclusion, the RFID and Keypad-Based Smart Door Lock System using STM32 successfully meets the intended goals of creating a secure, automated, and user-friendly access control solution. The combination of RFID technology and password verification provides a robust mechanism for preventing unauthorized access, while the STM32 microcontroller ensures high-speed processing and efficient operation.

The project demonstrates the power of embedded systems in achieving real-world automation and safety solutions. By aligning with SDG 9 (Industry, Innovation and Infrastructure) and SDG 11 (Sustainable Cities and Communities), the project promotes innovation and contributes to the vision of developing safer and smarter communities.

This work lays the foundation for future research in IoT-enabled smart security systems and represents a significant step toward the integration of embedded intelligence in sustainable urban infrastructure.

REFERENCES

- [1] Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). *Strong Authentication for RFID Systems Using the AES Algorithm*. Proceedings of Cryptographic Hardware and Embedded Systems – CHES 2004, Springer, pp. 357–370.
- [2] Fernández-Caramés, T. M., Fraga-Lamas, P., Suárez-Albela, M., and Castedo, L. (2024). *Reverse Engineering and Security Evaluation of Commercial Tags for RFID-Based IoT Applications*. arXiv preprint arXiv:2402.03591.
- [3] Hale, J., and Stovall, T. (2015). *Design and Implementation of Embedded Access Control Using ARM Cortex Microcontrollers*. IEEE Transactions on Consumer Electronics, Vol. 61, No. 3, pp. 453–460.
- [4] Johnson, D., and Lee, M. (2018). *Dual Authentication System for Laboratory Security Using RFID and Keypad*. International Journal of Engineering Research & Technology (IJERT), Vol. 7, Issue 5, pp. 289–293.
- [5] Ma, M. (2025). *Design of Home Smart Access Control System Based on STM32*. Proceedings of SPIE, Vol. 13574, Paper 1357445.
- [6] Mohankumar, A. (2024). *A Comprehensive Overview of an Advanced RFID Door Lock System*. Asian Journal of Applied Science and Technology, Vol. 8, Issue 1, pp. 85–91.
- [7] Racharla, S. (2025). *IoT-Enabled Biometric Door Locking System with Enhanced Security through Dual Authentication*. Foundry Journal, Vol. 29, No. 4, pp. 215–222.
- [8] Rieback, M. R., Crispo, B., and Tanenbaum, A. S. (2008). *The Evolution of RFID Security*. IEEE Pervasive Computing, Vol. 5, No. 1, pp. 62–69.