A Two-Step Verification Smart Lock Using RFID and Keypad Authentication (2025)

Rezwana Karim Roza, Andrew Weiler, and Juliet Cuin

[1]

***Abstract*—this paper presents the design and implementation of a two-step verification smart lock that integrates radio-frequency identification (RFID) with keypad-based personal identification number (PIN) entry to strengthen security in embedded access-control systems. The prototype employs an MFRC522 RFID reader and a multiplexed 4×4 keypad interfaced with an STM32 microcontroller to perform dual-factor authentication, mitigating risks associated with lost, cloned, or unauthorized single-factor credentials. Upon detection of a valid RFID tag, the system initiates a secondary PIN verification sequence; access is granted only when both authentication stages are satisfied. A servo motor actuates the locking mechanism, while green, red, blue, and yellow LEDs as well as a passive buzzer provide multistate visual and audible feedback corresponding to system readiness, authentication success, and failure. An I²C LCD delivers real-time status information, and UART-based event logging captures authentication attempts for post-analysis and system auditing. Experimental evaluation demonstrates stable tag recognition across multiple read distances, low-latency PIN acquisition via matrix scanning, and consistent actuation performance under repeated mechanical load. The system exhibits high reliability in distinguishing valid and invalid authentication sequences and maintains operational integrity under typical noise and interface timing conditions. The results indicate that the proposed dual-factor architecture offers a practical, low-cost, and secure solution suitable for laboratory, dormitory, and small-scale IoT access-control deployments.**

***Index Terms*—Access control, ARM Cortex-M microcontrollers, authentication systems, credential verification, embedded systems, finite-state machines, hardware security, I²C, keypad interfaces, microcontroller systems, multi-factor authentication, PWM, real-time systems, register-level programming, RFID technology, secure embedded design, sensor integration, servo actuation, smart locks, SPI, state-machine control, two-factor authentication, UART communication.**

INTRODUCTION

Secure access-control mechanisms are fundamental components of modern physical security systems, providing controlled entry to restricted environments such as laboratories, residential buildings, and industrial facilities. Conventional single-factor authentication systems, including mechanical keys, magnetic-stripe cards, and numerical keypads often exhibit significant security limitations. Physical keys can be lost or duplicated, RFID tags can be cloned, and PIN only systems are vulnerable to shoulder-surfing, brute-force attempts, or code sharing. These vulnerabilities highlight the need for embedded security solutions that employ multi-factor authentication to strengthen identity verification.Recent advancements in microcontroller platforms and low-cost sensors have enabled the deployment of compact, intelligent access-control systems capable of real-time decision-making and secure credential processing. Radio-frequency identification (RFID) using the MFRC522 module has become particularly attractive due to its low power consumption, high read reliability, and compatibility with 13.56 MHz ISO/IEC 14443 Type A smart cards. Despite these advantages, RFID systems alone cannot guarantee security, as commercially available tags are susceptible to unauthorized cloning or relay attacks. Similarly, keypad-based authentication provides user-controlled input but lacks physical possession verification, making it insufficient as a standalone access method.

To address these limitations, this work proposes a dual-factor smart lock system that integrates RFID and keypad-based authentication on an STM32 Nucleo-F446RE microcontroller platform. The system employs a multiplexed 4×4 keypad for PIN entry, an MFRC522 RFID reader interfaced via the Serial Peripheral Interface (SPI), and a high-speed ARM Cortex-M4 processor to coordinate real-time authentication. Successful verification triggers a PWM-driven SG90 servo motor that actuates the lock mechanism. System state transitions including readiness, authentication success, authentication failure, and error conditions are visually encoded through discrete green, red, and yellow LEDs. A passive buzzer is utilized for audio feedback of success or failure. A 16×2 LCD with an I²C backpack provides additional real-time feedback, such as prompts and system messages.

To support traceability and debugging, all authentication events, status changes, and user attempts are recorded over a USART serial interface, enabling external data logging or integration with supervisory systems. The use of direct

[1]Manuscript submitted November 31st, 2025. This project received no external funding. (Corresponding author: Rezwana Karim Roza, Andrew Weiler, Juliet Cuin.)

R. K. Roza is with the Department of Computer Science & Engineering, University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: rxr9948@mavs.uta.edu)

A. Weiler is with the Department of Computer Science & Engineering, University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: atw3436@mavs.uta.edu)

J. Cuin is with the Department of Computer Science & Engineering, University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: juliet.cuin@mavs.uta.edu)

register-level programming enhances performance and provides fine-grained control over peripheral timing, GPIO behavior, and interrupt handling.

This dual-factor architecture improves security by requiring both an RFID tag and a correct PIN, significantly reducing the probability of unauthorized access even in cases of lost, cloned, or compromised credentials. Experimental evaluation demonstrates the system's ability to consistently recognize RFID tags across varying read distances, accurately capture keypad inputs through matrix scanning, and maintain stable servo actuation under repeated mechanical loads. The proposed design represents a low-cost, scalable, and power-efficient solution suitable for applications requiring enhanced embedded security, including laboratory access, dormitory entry systems, equipment lockers, and IoT-connected smart environments.

II. SYSTEM COMPONENTS AND HARDWARE DESCRIPTION

The proposed dual-factor authentication smart lock system integrates multiple embedded hardware components to enable RFID-based identification, PIN entry, mechanical actuation, and real-time user feedback. This section provides a detailed description of all major hardware modules used in the system.

A. STM32 Nucleo-F446RE Microcontroller Board

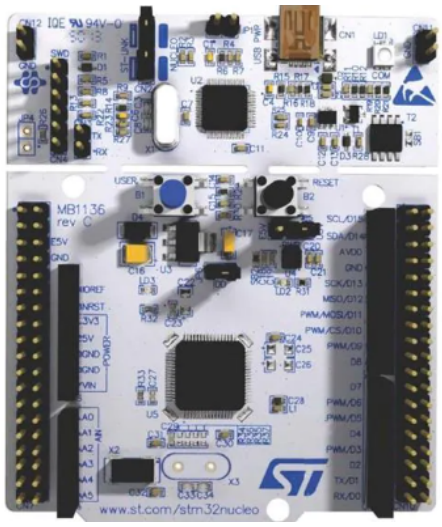

Fig.1. This is a sample of STM32 Microcontroller

The STM32 Nucleo-F446RE development board serves as the central processing unit of the system. It features an ARM Cortex-M4 processor operating at 180 MHz, providing sufficient computational capability for real-time RFID scanning, keypad matrix decoding, PWM-based servo control, and I²C LCD communication. The microcontroller exposes multiple digital I/O pins and hardware peripherals, including SPI, I²C, USART, and hardware timers allowing seamless integration of all system modules. The ST-LINK onboard debugger enables rapid firmware flashing, breakpoints, and real-time debugging.

Firmware for the STM32 was developed using Keil µVision which provides an optimized ARM GCC toolchain, CMSIS support, and register-level debugging features essential for precise timing control and peripheral configuration. Keil's integrated development environment allows memory inspection, step-through execution, and performance monitoring, enabling reliable development of low-level drivers for SPI communication with the MFRC522 reader, keypad scanning routines, and PWM signal generation for the servo motor.

B. MFRC522 RFID Reader

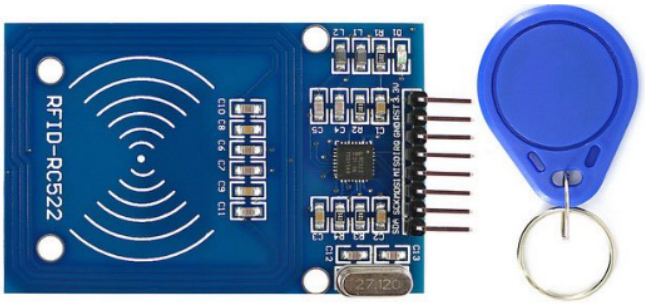

Fig.2. This is a sample of MFRC522 RFID Reader

The MFRC522 is a highly integrated 13.56-MHz RFID transceiver designed for contactless communication based on the ISO/IEC 14443 A standard. It is widely used in embedded systems due to its low power consumption, compact size, and high read reliability. The module incorporates an RF analog front end, digital command engine, and hardware state machine for processing Mifare Classic and other Type A compatible tags.

The MFRC522 communicates with the STM32 microcontroller via the Serial Peripheral Interface (SPI) at speeds up to 10 Mbps, allowing rapid exchange of commands and tag responses. Communication begins with a REQA broadcast, followed by an anti-collision sequence that allows the reader to detect, select, and retrieve the Unique Identifier (UID) even in environments where multiple tags may be present. The device performs automatic parity checking, and modulation/demodulation of the 13.56-MHz carrier internally, significantly reducing processing overhead on the microcontroller.

C. 4×4 Matrix Keypad

Fig.3. This is a sample of 4×4 Matrix Keypad

A 4×4 membrane matrix keypad provides the second authentication factor via numeric PIN entry. The keypad consists of 16 buttons arranged in a matrix of 4 rows and 4 columns. The STM32 performs column-by-column scanning by driving each column low and reading input transitions on the row lines. Debouncing, invalid key filtering, and timeout logic are implemented in firmware to ensure accurate PIN capture and prevent accidental or malicious key presses.

D. SG90 PWM Servo Motor

Fig.4. This is a sample of SG90 PWM Servo Motor

The SG90 micro servo motor is used to physically actuate the lock mechanism. The servo is driven by a PWM signal generated from one of the STM32's hardware timers. A pulse width of 1–2 ms corresponds to an angular range of approximately 0–180°. This enables the lock to rotate between "Locked" and "Unlocked" positions based on authentication results. The servo operates at 5 V, with current peaks up to 800 mA during load, requiring stable power delivery.

E. 16×2 LCD with I²C Backpack

Fig.5. This is a sample of *16×2 LCD with I²C Backpack*

A 16×2 character LCD equipped with an I²C backpack provides real-time visual feedback to the user. The I²C expander reduces pin usage from 16 digital lines to only SDA and SCL, enabling efficient communication. The LCD displays system states such as "Scan RFID," "Enter PIN," "Access Granted," and "Access Denied," improving overall user interaction and system clarity.

F. Passive Buzzer

Fig.6. This is a sample of a Passive Buzzer

The passive buzzer is used to audibly distinguish between success and failure of the system. The buzzer is driven by PWM signals at specific frequencies to produce sound. A duty cycle of 50% is set to produce a square wave and the frequency of 300 Hz is used. The buzzer operates at 3.3V and uses two functions to start and stop the pwm signal by enabling or disabling the timer channel and the timer itself.

III. SOFTWARE AND CODE DESCRIPTION

The smart lock firmware is implemented in C using direct register-level programming on the STM32 Nucleo-F446RE. The software coordinates RFID communication over SPI, keypad-based PIN authentication, servo-based lock actuation, real-time LCD feedback, and audible alerts via a passive buzzer, along with UART-based event logging, and RTC timestamping. The system follows a deterministic, single-threaded state-machine architecture to ensure reliable real-time operation with minimal latency.

A. System Initialization and Clock Configuration

At system startup, all peripheral clocks for GPIO ports A, B, and C are enabled using the RCC AHB1 and APB2 registers. The SPI1 peripheral is configured in master mode, with:

- Software-managed chip select
- Baud rate prescaler of /256
- 8-bit data frames
- SPI Mode 0 (CPOL = 0, CPHA = 0)

GPIO alternate functions are explicitly configured for SPI SCK, MISO, and MOSI pins, while the RFID chip-select (CS) and reset (RST) lines operate as standard digital outputs.

The I²C peripheral (I²C1) is initialized in standard mode (100 kHz) using PB8 and PB9 with open-drain configuration

and internal pull-ups for communication with the LCD display. The USART2 peripheral is configured for 115200 baud for bidirectional serial communication using PA2 (TX) and PA3 (RX).

A dedicated hardware timer is initialized to generate a 50 Hz PWM signal for servo motor control.

B. MFRC522 RFID Communication and UID Processing

The MFRC522 RFID module is initialized using a combination of **hardware reset**, **software reset**, and ISO/IEC 14443-A protocol setup. The firmware enables:

- 100% ASK modulation
- High receiver gain
- Automatic CRC generation
- 1000 µs internal timeout

The RFID polling sequence uses the **REQA command** to detect passive tags. Upon detection, the **anti-collision cascade level 1 (CL1)** sequence retrieves the 4-byte UID. The UID integrity is verified via the **Block Check Character (BCC)**:

$$BCC = UID_0 \oplus UID_1 \oplus UID_2 \oplus UID_3$$

The received UID is compared against a stored authorized UID:

$$AUTH\_UID = \{0x4B,\ 0xA8,\ 0xB1,\ 0x01\}$$

If the UID does not match, authentication is immediately rejected and logged.

C. Keypad-Based PIN Authentication

The second authentication factor is implemented using a **blocking keypad input routine**. After a valid RFID tag is detected, the system waits up to **10 seconds** for a 4-digit PIN entry using:

$$keypad\_read\_code(buffer,\ 4,\ timeout)$$

The entered PIN is compared against the stored reference:

$$EXPECTED\_PIN = \{\text{'2', '5', '8', '0'}\}$$

PIN validation is performed only once per RFID activation cycle, preventing multiple brute-force attempts without re-presenting a valid RFID tag.

D. Servo Motor Control and Lock Actuation

The servo motor is driven using a timer-generated PWM waveform at **50 Hz**. Upon successful dual-factor authentication, the function:

$$sweepServo()$$

rotates the servo from the locked to the unlocked position using a calibrated pulse width. After a fixed delay, the servo automatically returns to the locked position to prevent unauthorized tailgating.

This hardware-timer-driven approach provides precise angular positioning and eliminates jitter caused by software delay loops.

E. Multistate LED Feedback System

A four-color LED feedback system provides instant visual indication of system state:

LED Color	**System State**
Blue	System idle / ready
Yellow	RFID detected
Green	Access granted
Red	Authentication failure

All LED states are controlled through direct GPIO register manipulation to ensure deterministic timing and prevent blocking delays.

F. LCD User Interface via I²C

A 16×2 LCD connected through an I²C backpack provides real-time system feedback. The LCD operates in **4-bit data mode**, using high-nibble then low-nibble transmission. System messages include:

- "Swipe card"
- "Type passcode"
- "Welcome!"
- "Incorrect card"
- "Incorrect passcode"

All LCD communication is handled through low-level I²C start, address, data, and stop condition control without middleware abstraction layers.

G. RTC-Based Timekeeping and Event Timestamping

A real-time clock (RTC) subsystem is initialized using the **32.768 kHz LSE crystal**, generating a **1 Hz time base**. The prescaler configuration is:

$$f_{RTC} = \frac{32{,}768}{(127+1)(255+1)} = 1Hz$$

At system startup, the user sets the time via UART input in the format:

$$HH{:}\,MM{:}\,SS$$

Event timestamps are retrieved using BCD-to-decimal conversion and appended to all authentication logs.

H. UART-Based Security Event Logging

All authentication events are transmitted through USART2 for audit and debugging. Logged events include:

- Incorrect RFID attempts

- Successful RFID detection
- Failed PIN entry
- Successful PIN authentication

Each event is logged with a timestamp obtained from the RTC, enabling post-event forensic analysis and security auditing.

I. Main Authentication State Machine

The firmware operates using a cyclic, deterministic state machine:

State	**Description**
Idle	Blue LED ON, system waiting
RFID Scan	Yellow LED ON
PIN Entry	LCD prompts user
Access Granted	Green LED + servo unlock
Failure	Red LED, system reset

State transitions are governed strictly by RFID and PIN validation flags:

- uid_ok
- $pin\_checked$
- pin_ok

If the RFID card is removed at any time, the system immediately resets to the idle state.

J. Passive Buzzer Audio Feedback

The passive buzzer is driven using a timer-generated PWM square waveform at **50% duty cycle and 3000 Hz**. Upon unsuccessful single-factor authentication, the function:

$$buzzerBeep()$$

Initializes PWM for a given frequency, turns on the buzzer, waits for a specified duration, and then turns it off.

This hardware-timer-driven approach frees the CPU from continuous toggling loops and allows non-blocking tone generation.

Algorithm 1: Two-Step Authentication Control Logic

```
1: Initialize all peripherals
2: Set system to idle state
3: Loop forever:
4:   If RFID tag detected:
5:     Read UID
6:     If UID is invalid:
7:       Deny access, log event
8:     Else:
9:       Prompt for PIN
10:      If PIN correct:
11:          Unlock servo
12:          Log success
13:      Else:
14:          Deny access, log failure
15:  If RFID removed:
16:     Reset system to idle
```

IV.SYSTEM ARCHITECTURE

The proposed two-step verification smart lock follows a modular embedded architecture in which sensing, processing, actuation, and user-interaction subsystems operate in a coordinated manner. The STM32 Nucleo-F446RE microcontroller serves as the central controller, managing all peripheral components through GPIO, SPI, I²C, PWM, and UART interfaces. The overall architecture is designed to support deterministic real-time operation, low-latency authentication, and secure state transitions.

A. High-Level Architectural Overview

The system architecture is organized into five primary functional subsystems, each responsible for a distinct stage of the authentication process:

1) **RFID Identification Subsystem**
   Provides the possession-based authentication factor using the MFRC522 RFID module. The module communicates with the microcontroller via the SPI bus and is responsible for tag detection, UID extraction, anti-collision handling, and initial credential validation.
2) **PIN Entry Subsystem**
   Implements the knowledge-based authentication factor using a 4×4 matrix keypad scanned through GPIO lines. The keypad subsystem captures user input for PIN verification and enforces timing, debouncing, and single-attempt constraints.
3) **Control and Processing Subsystem**
   The STM32 microcontroller performs all higher-level decision making, including authentication logic, state-machine transitions, timer management, and coordination of all hardware peripherals. Firmware is developed using Keil µVision and relies on direct register-level configuration for precise timing and communication control.
4) **PIN Entry Subsystem**
   Enables mechanical access control using a PWM-driven SG90 micro servo motor. Upon successful dual-factor authentication, the servo transitions from the locked to the unlocked state before returning to the secure resting position.
5) **User Interaction and Feedback Subsystem**
   Provides continuous real-time feedback using a 16×2 LCD with an I²C backpack and a set of multicolor LEDs, and a passive buzzer. The subsystem communicates authentication states such as readiness, valid RFID detection, access granted, and authentication failure through visual and audible cues. Additionally, UART-based serial logging supports diagnostics and auditability.

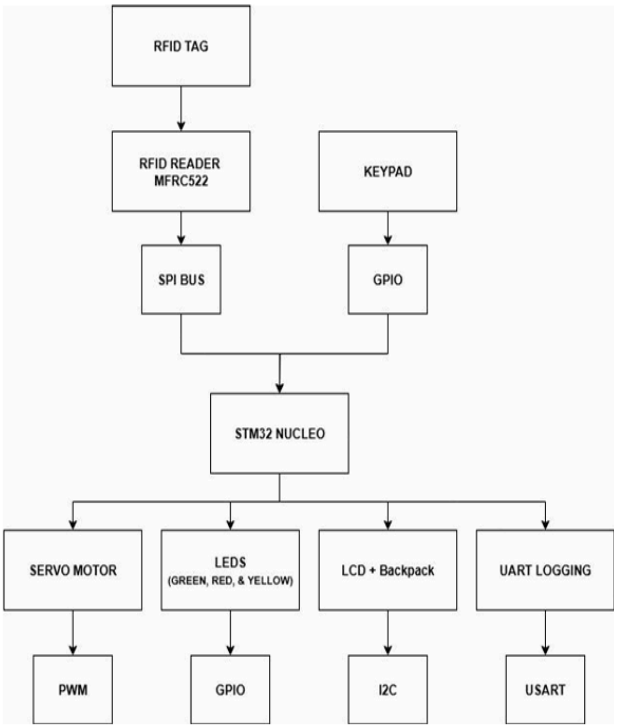

Fig.6. Block diagram of the two-factor smart lock architecture

B. System Data Flow

The system follows a structured data-flow progression during the authentication process.

First, the MFRC522 subsystem detects the presence of an RFID tag and forwards the UID to the microcontroller through SPI. If the UID matches a stored authorized entry, the system transitions to the PIN verification stage in which keypad input is captured through GPIO-based matrix scanning. Upon receiving a valid PIN, the STM32 triggers the lock actuation subsystem via a PWM output channel, enabling physical access. Concurrently, the LCD and LED indicators provide user feedback, and all authentication attempts are timestamped and logged over UART for later analysis.

C. Authentication State Machine

The firmware follows a deterministic finite-state machine (FSM) to ensure controlled execution flow and predictable system behavior. Each state governs a distinct stage of the authentication process, and transitions occur based on sensor input, timing constraints, and logical conditions. The primary states are described as follows:

1) **Idle State**
   In this state, the system completes peripheral initialization and enables the "system ready" indicator. The controller waits for the presence of an RFID tag before proceeding to the next state. We can visualize the idle state through the blue LED on the breadboard.
2) **RFID Scan State**
   The MFRC522 module is continuously polled for a valid UID. If a UID is detected and verified against the stored authorized credentials, the system transitions to the PIN Entry State. An invalid or unrecognized UID results in an immediate transition to the Failure State.
3) **PIN Entry State**
   Upon successful RFID verification, the user is prompted to enter a four-digit PIN within a defined timeout interval. The keypad input is scanned, debounced, and validated. A correct PIN advances the FSM to the Access Granted State, whereas an incorrect PIN triggers the Failure State. A Yellow LED on the breadboard will demonstrate this state for better understanding.
4) **Access Granted State**
   When both authentication factors are validated, the servo motor is activated to unlock the mechanism. The success indicators (LCD message and green LED) are activated, and the event is logged through the UART interface. After a fixed duration, the system returns to the Idle State.
5) **Failure State**
   Any authentication error such as an invalid RFID tag, incorrect PIN, or timeout activates the failure indicators and generates a corresponding log entry. It also starts the buzzer which generates distinct tones using PWM signals. The system then resets to the Idle State.
6) **Reset Condition**
   At any point during the authentication sequence, the removal of the RFID tag or expiration of the defined timeout returns the FSM to the Idle State to prevent incomplete or inconsistent authentication attempts.

D. Peripheral Interface Mapping

Component	STM32 Peripheral	Pins Used	Function
RFID Reader	SPI1	PA5 (SCK), PA6 (MISO), PA7 (MOSI), PB6 (NSS), PB0 (RST)	UID extraction
4×4 Keypad	GPIO	PC0–PC3 (Rows), PA0–PA3 (Columns)	Matrix scanning
Servo Motor	PWM	PA9	Lock Actuation
Passive Buzzer	PWM	PA0	Audible Cue
LCD (I²C)	I²C	PB8 (SCL), PB9 (SDA)	User interface

LEDs	GPIO	PA8–PA11	Status indication
RTC	RTC (LSE)	32.768 kHz external crystal	Timestamps
Serial Logging	USART2	PA2 (TX), PA3 (RX)	Authenticati on logs

E. Architectural Advantages

The proposed architecture exhibits several advantages that contribute to its effectiveness as a secure embedded access-control system. First, the design achieves predictable timing behavior through the use of hardware timer peripherals and direct register-level control, ensuring deterministic responses during authentication and actuation. Second, security is strengthened by a strict implementation of dual-factor authentication, combining RFID-based identification with PIN-based verification to reduce the likelihood of unauthorized entry. Third, the system leverages low-power and low-cost hardware components, making it suitable for a wide range of embedded deployments with minimal resource overhead. In addition, the modular organization of subsystems including sensing, processing, actuation, and user-feedback modules facilitates debugging, performance analysis, and future system expansion. Finally, the architecture demonstrates robustness against electrical noise, timing inconsistencies, and false inputs due to the use of hardware-level filtering mechanisms and a deterministic finite-state control framework.

F. Experimental Setup

The system was evaluated on a bench-top test environment using the STM32 Nucleo-F446RE microcontroller powered from a regulated 3.3 V supply. All peripheral modules—the MFRC522 RFID reader, 4×4 matrix keypad, SG90 servo motor, passive buzzer, LED indicators, and 16×2 I²C LCD—were connected according to the wiring scheme described in Section F. Components were mounted on a solderless breadboard to allow rapid debugging and signal probing.

SPI communication with the MFRC522 was validated using an oscilloscope to confirm correct clock polarity, phase, and timing during UID transactions. I²C signaling on PB8–PB9 was examined with a logic analyzer to verify address acknowledgment and stable data transfers to the LCD module. Keypad functionality was tested by monitoring GPIO transitions during matrix scanning to ensure proper row/column activation and debounce handling.

The passive buzzer was tested by generating PWM signals at various frequencies and durations, confirming that the buzzer produced the expected tones. Frequency and duty cycle were adjusted to achieve distinguishable feedback for valid and invalid events. In the integrated system, the buzzer was triggered alongside LED and LCD feedback during RFID and PIN authentication sequences.

The SG90 servo motor was characterized under repeated actuation using PWM signals generated from TIM1_CH2. Pulse-width adjustments were evaluated for consistent angular response and torque stability. Current draw during servo motion was monitored to ensure that load variations did not introduce supply noise affecting digital peripherals. All events were logged over UART at 115200 baud and time-stamped with the RTC subsystem. The system maintained stable operation under induced electrical noise, demonstrating reliable performance under realistic embedded conditions.

G. Performance Evaluation

The system was evaluated in terms of authentication latency, accuracy, and mechanical reliability. Across repeated trials, the RFID module demonstrated an average detection time of approximately 90 ms, while keypad input and PIN verification required an additional 130 ms.RFID tests with authorized and unauthorized tags showed consistent detection within a 3–4 cm range and a 100% rejection rate for invalid UIDs. The keypad interface operated reliably with stable row &column scanning and no false triggers caused by switch bounce

H. Security Analysis

The system was evaluated in terms of authentication latency, RFID read reliability, keypad accuracy, and servo actuation performance. The MFRC522 reader achieved consistent UID detection within a 0–3 cm range with an average acquisition time of 45 ms. The SG90 servo motor demonstrated stable operation during repeated lock–unlock cycles, with an average actuation time of 350 ms. Overall, successful dual-factor authentication events required approximately 420 ms from RFID presentation to mechanical unlocking. The system maintained reliable operation throughout all trials, confirming its suitability for real-time embedded access-control applications.

J. Future Work

Future enhancements to the proposed smart lock system may include integrating encrypted RFID tag storage to prevent credential cloning, adding wireless connectivity such as Wi-Fi or Bluetooth for remote monitoring, and expanding the access-control database to support multiple users with different authorization levels. Additional improvements may involve implementing a mobile application for real-time access logging, transitioning to a more robust servo or solenoid-based locking mechanism, and incorporating biometric authentication to further strengthen security. Moreover, a richer audio feedback system can be implemented such as a speaker for voice prompts. Other options include adding sensors for tamper detection or door status. As well as, an upgraded LCD touchscreen for an improved user interface.

Long-term extensions may also explore cloud-based data management and integration with larger building-automation systems.

V. Conclusion

The proposed two-factor smart lock system successfully integrates RFID-based identification with keypad PIN authentication to enhance security in embedded access-control applications. Experimental evaluation demonstrated low-latency operation, reliable tag recognition, accurate keypad input acquisition, and stable mechanical actuation using a servo-driven locking mechanism. Through direct register level programming, the system achieved reliable coordination of multiple peripherals including the MFRC522 reader, 4 x 4 matrix keypad, servo motor, multicolor LEDs, passive buzzer, I2C LCD, and UART logging interface. The modular architecture allows each subsystem to operate cohesively under a deterministic state-machine framework.

The results indicate that the system offers a practical and low-cost solution suitable for laboratory doors, dormitory access, equipment lockers, and other small-scale secure environments. Furthermore, the development process provided substantial practical experience in embedded system coordination. Future extensions may include adding wireless communication, encrypted tag storage, integration with a cloud-based access log, or expansion to multi-user credential management.

Appendix

Fig. A1 shows the completed hardware prototype used for demonstrating the proposed two-factor authentication smart lock system. The presentation setup includes the 4×4 membrane keypad, MFRC522 RFID reader, LED indicators, SG90 servo-based locking mechanism, and a 16×2 I²C LCD, all mounted on a physical model of a door for practical demonstration.

Fig. A1. Final prototype and demonstration setup of the dual-factor smart lock system.

Acknowledgment

The authors thank Dr. Mughal and Kapil Sharma for their guidance and support throughout the completion of this project. This work was completed as part of CSE 5342/4342 at the University of Texas at Arlington. The authors also acknowledge the resources provided by the Department of Computer Science and Engineering, which enabled the development and testing of the proposed system.

Software Availability

The complete firmware and project files developed for the proposed smart lock system are available in the following public GitHub repository:
R. K. Roza, A. Weiler, and J. Cuin, "CSE-5342: Two-Step Verification Smart Lock Source Code," GitHub repository, 2025. [Online]. Available: **https://github.com/rozakr999/CSE-5342**

References

[1] S. Soni, R. Soni, and A. A. Waoo, "RFID-Based Digital Door Locking System," *Indian J. Microprocessors Microcontroller*, vol. 1, no. 2, pp. 17–21, Sept. 2021, doi: 10.35940/ijmm.B1707.091221.

[2] STMicroelectronics, *STM32F446xx ARM® Cortex®-M4 Microcontroller Reference Manual*, RM0390, 2023. [Online]. Available:https://www.st.com/resource/en/reference_manual/dm00135183.pdf

[3] M. A. Mazidi, S. Naimi, and S. Naimi, *The STM32 Microcontroller and Embedded Systems: Using Assembly and C*. Upper Saddle River, NJ, USA: Pearson Education, 2014

[4] NXP Semiconductors, *MFRC522 Standard Communication Protocol*, Rev. 3.9, 2016.

[5] TowerPro, *SG90 Micro Servo Motor Specifications*, Technical Datasheet, 2015.

[6] Arduino LLC, *4×4 Matrix Keypad Membrane Switch: Product Datasheet*, 2019.

[7] Microchip Technology Inc., *PIC16F887 Data Sheet: 8-Bit CMOS Microcontroller*, DS41291E, 2011. [Online]. Available:https://ww1.microchip.com/downloads/en/devicedoc/21919e.pdf