UNIVERSITY OF TEXAS AT ARLINGTON

EMBEDDED SYSTEM II

Fall 2025

TERM PROJECT PROPOSAL

(Two Step Verification Lock)

Title and Introduction

Title: Two-Step Verification Lock with an RFID key and Multiplexed Key Pad.

Team Names:

1.) **Rezwana Karim Roza**
2.) **Andrew Weiler**
3.) **Juliet Cuin**

Problem:
Conventional key-based locking mechanisms face several limitations, including the risk of lost or stolen keys, unauthorized duplication, and the inability to monitor or log access attempts. These issues reduce overall security and convenience, especially in multiple-user environments.

Motivation:
With the growing emphasis on innovative and IoT-enabled security solutions, there is a strong demand for secure and user-friendly systems. RFID-based locks address this need by offering contactless authentication, reduced reliance on physical keys, and the ability to scale across various settings such as dormitories, laboratories, and offices. Having the RFID-based lock enable a multiplexed keypad will allow for extra security.

Objective:
The primary objective of this project is to design and implement an embedded RFID-based smart lock and multiplexed keypad system that authenticates users through RFID tags, controls access to a secured area, and maintains a log of entry events for monitoring and auditing purposes.

Background and Relevance

Context
Embedded systems are widely used in computer engineering to integrate hardware and software for real-world applications. In access control, they enable compact, low-cost, and reliable solutions that connect RFID readers, keypads, and microcontrollers to provide secure entry systems. By combining multiple input methods, embedded platforms can implement stronger authentication schemes similar to modern digital security practices..

Literature
Rahman et al. (2021) presented an *RFID-Based Digital Door Locking System* that used an Arduino Uno, MFRC522 RFID module, and a servo motor to control access. The system successfully demonstrated contactless authentication and user registration features, along with visual and audio indicators (LEDs and buzzer). While effective as a prototype, the study noted limitations in scalability and lacked advanced features such as event logging or protection

against RFID card cloning. Building on this foundation, our project introduces a two-step verification approach, requiring both a valid RFID key and a correct PIN entered on a multiplexed keypad. This design enhances security by reducing reliance on a single factor and provides a more robust embedded access control system.

Innovation

Rahman et al. (2021) demonstrated the feasibility of an RFID-based door lock using an Arduino Uno, but our project advances this idea in two significant ways. First, we adopt the STM32 Nucleo platform in place of the 8-bit Arduino. Built on a 32-bit ARM Cortex-M architecture, the STM32 offers higher clock speed, more memory, and broader peripheral support. These improvements enable faster and more reliable real-time processing, smoother integration with multiple peripherals, and greater scalability. In practical terms, this allows us to implement advanced features such as event logging, timeout safeguards, and secure communication without overloading the system.

Second, our design introduces a two-step verification mechanism by combining an RFID key with a multiplexed keypad for PIN entry. This dual-factor approach enhances security by requiring both possession (RFID card) and knowledge (PIN), significantly reducing the risk of unauthorized access through lost, cloned, or stolen tags. Together, the STM32 platform and two-step verification create a more secure, scalable, and professional-grade embedded access control system than prior single-factor prototypes.

Reference

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

Methodology

System Design

The proposed access control system consists of an MFRC522 RFID reader, a multiplexed keypad, an STM32 Nucleo microcontroller, a servo motor, and LEDs with a buzzer for feedback. The RFID reader communicates with the STM32 via the SPI bus, sending the UID of scanned tags, while the keypad is interfaced through GPIO to capture PIN input. The STM32 verifies both factors by first checking the UID against a stored whitelist and then validating the entered PIN. Only when both conditions are satisfied does the system trigger the servo motor through PWM to unlock the lock, light the green LED, update the LCD with an “Access Granted” message, and log the event via USART to a connected PC. If either the RFID tag or the PIN is invalid, the red LED and buzzer are activated, the LCD “Access Denied,” and the lock remains

engaged. The yellow LED indicates system readiness, while UART logging provides real-time monitoring of access attempts.

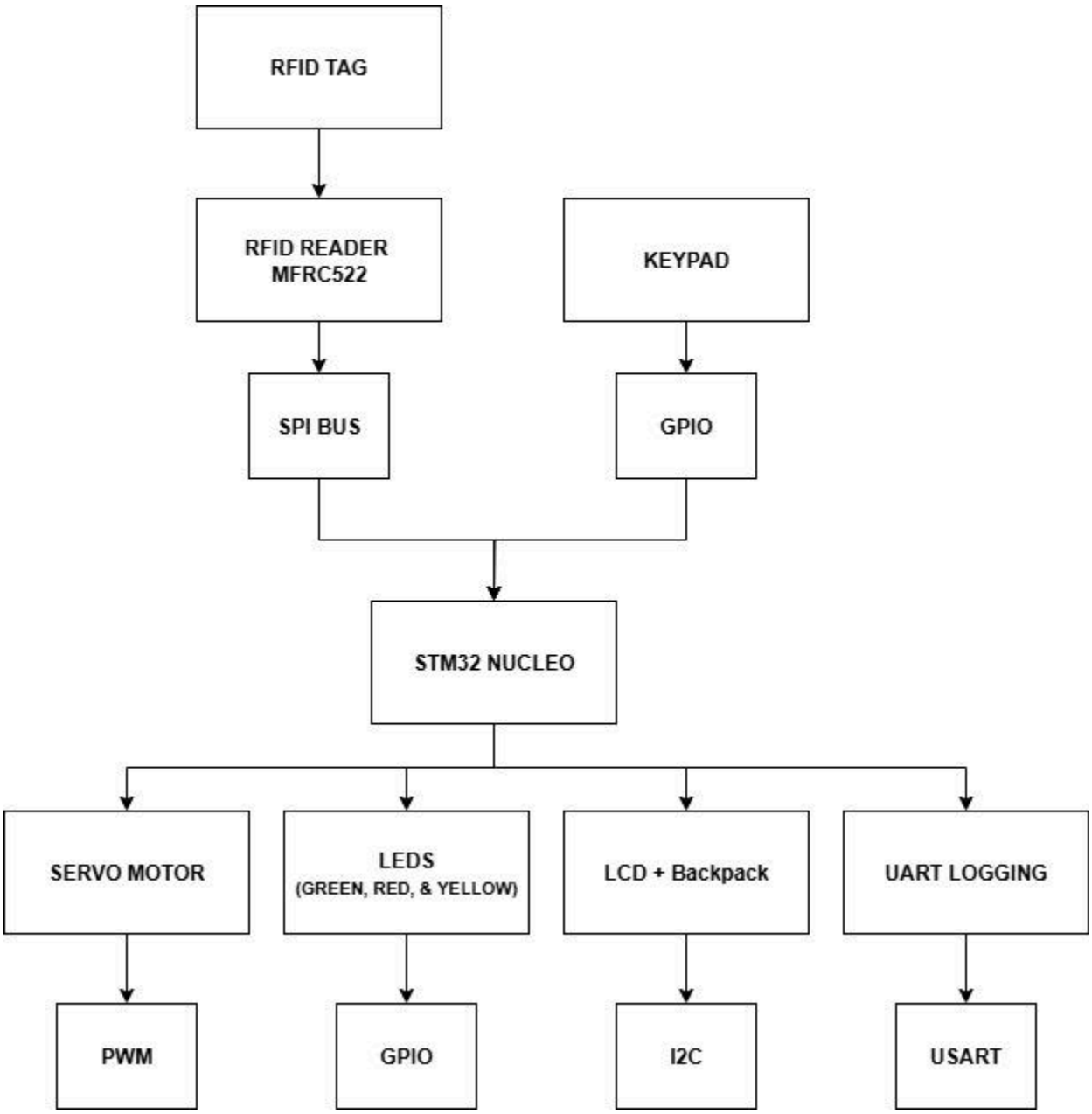

Fig 1: Block Diagram for The System Design

Tools

Hardware: STM32 Nucleo-F446RE (32-bit Cortex-M4F), MFRC522 RFID module, Multiplexed Keypad (4×4 matrix), 16×2 LCD with I²C Backpack, SG90 Servo Motor, LEDs (Green, Red, Yellow), Active Buzzer, Regulated 3.3 V/5 V rails, Power supply.
Software: Keil (version 2.17.0), STMcube Programmer, CMSIS device headers, and direct peripheral register access.

Plan

We will complete the project in three phases: design, prototyping, and testing. In the design phase, the RFID reader (MFRC522) will be connected to the STM32 Nucleo via SPI, and a multiplexed keypad will be interfaced through GPIO for PIN entry. The servo motor, LEDs, and buzzer will be controlled with PWM and GPIO outputs, while an I²C 16×2 LCD will display system messages. USART will handle event logging to a PC.

In the prototyping phase, firmware will be developed to initialize the RFID module, read tag UIDs, and compare them against a whitelist. If a valid RFID tag is detected, the user must also enter the correct PIN. Only then will the system unlock the servo, light the green LED, sound the buzzer, display "Access Granted," and log the event. Invalid input from either the RFID tag or PIN will trigger the red LED and buzzer, display "Access Denied," and keep the lock engaged.

Finally, testing will evaluate system performance by measuring the time between scanning and response, verifying reliability across repeated scans, and confirming correct timeout and re-lock behavior.

Timeline and Resources

Timeline

Week 1-2	Researching our RFID reader, completing a circuit design with all components (sketch and wiring diagrams) assemble all components on a breadboard, breadboard testing.
Week 3-5	Code development for RFID integration, Keypad Matrix Scanning, and passcode logic.
Week 6-7	System integration: combine RFID and keypad code. Building full flow.
Week 8-9	Final System testing, checking multiple tags and pin inputs, observing lock behavior.
Week 10-11	Final integration: refining code and improving stability. Finalizing prototype. Preparing and completing report documents.

Resources

Hardware:

STM32 Nucleo board – $20
MFRC522 RFID Reader Module – $10
RFID Tags/Cards – $12 for 2 of them
SG90 Servo Motor – $10
16×2 LCD with I²C Backpack – $12
LEDs, Buzzer, Resistors, Wires – $5
Power Supply (5 V adapter/battery) – $10
Multiplexed Keypad (4×4) – $8

Software

STM32CubeIDE (free)
Serial terminal (PuTTY)

Estimated Total: ≈ $88

Risks

Several factors could impact the progress of this project. Hardware delivery delays, such as late arrival of the RFID reader or keypad, may slow development. There is also a risk of component failures, including the reader, buzzer, or servo motor. An inadequate power supply could cause unstable operation, especially when driving the servo and peripherals simultaneously. Finally, time constraints pose a challenge, as debugging and integration may take longer than anticipated and limit the completion of all planned features.

Expected Outcomes

Deliverables

Expect a fully functional prototype of a 2-step verification locking system using RFID and a keypad multiplexor. The system will first verify access using RFID tags and then require a valid PIN entered via a matrix keypad. A coordinating LED and buzzer will provide real-time user feedback for access granted, denied, or system errors. Additionally, expect a clean, well-documented source code, a comprehensive report covering research, design, and implementation, and a live demo of the complete locking system.

Evaluation

The system will be evaluated based on metrics such as RFID tag recognition accuracy, system responsiveness and latency, and keypad input reliability. The target is to achieve 95% uptime and consistent, accurate behavior from both RFID and keypad subsystems during repeated and varied test conditions.

Impact

This project will enhance practical skills in embedded systems, including peripheral integration, GPIO management, real-time input processing, and multistage access control logic. It provides hands-on learning with RFID technology, matrix keypad scanning, and the STM Nucleo microcontroller platform. Ultimately, this will serve as a valuable addition to a personal portfolio, demonstrating a clear ability to integrate hardware and software into real-world, security-focused applications.