Final Lab Report: Remote Locking System

Rahul Padhi and Emmanuel Agubata

Date: March 16, 2025

I. Description

Our project is a secure access control system designed to authenticate users using a combination of a keypad and an RFID scanner. The system is built around the CC3200 microcontroller and features an OLED display for user interaction, a servo motor for door locking and unlocking, and a buzzer for audio feedback. The system aims to provide a standalone, interactive, and efficient method of entry authentication.

A. System Overview

The access control system operates as follows:

1) The user enters a predefined PIN code on the keypad or scans an RFID card.
2) The input is processed by the microcontroller, which validates the credentials.
3) If the entered PIN is correct (e.g., ”1234D”) or the RFID tag is authorized, the system grants access.
4) Upon successful authentication, the servo motor rotates to unlock the door, and the buzzer sounds a confirmation tone.
5) If the entered credentials are incorrect, the OLED display notifies the user, and the buzzer sounds an error alert.
6) The system remains locked and prompts the user to re-enter the correct credentials.

B. Hardware Components

The key components of the system include:

- **CC3200 Microcontroller:** The central processing unit that handles authentication and controls peripheral devices.
- **Keypad:** Used to input the PIN code for authentication.
- **RFID Scanner:** An alternative authentication method that scans RFID cards.
- **OLED Display:** Provides real-time feedback to the user, displaying prompts and authentication status.
- **Servo Motor:** Controls the locking and unlocking mechanism of the door.
- **Buzzer:** Provides audio feedback to indicate success or failure of authentication.

C. Software and Communication

The microcontroller communicates with the peripherals using the following protocols:

- **I2C:** Used for communication with the OLED display.
- **GPIO:** Used for interfacing with the keypad, buzzer, and servo motor.
- **UART/I2C:** Intended for RFID scanner communication.

D. Standalone and Interactive Operation

The system is completely standalone, meaning it does not rely on an external computer for operation. It boots from flash memory and operates independently. The interactive nature of the project ensures that the user receives instant feedback through the OLED display and buzzer, making the authentication process seamless.

E. Current Limitations

While the system successfully implements keypad-based authentication and door control, certain functionalities, such as AWS IoT integration and full RFID authentication, were not fully realized. These features are planned for future iterations to enhance security and remote access capabilities.

Overall, our access control system effectively demonstrates a secure, user-friendly, and responsive authentication method that can be expanded with additional security features in the future.

II. Design

III. Functional Specification

The access control system follows a structured state machine model to handle user authentication and control the door lock mechanism. The system transitions between different states based on user input from the keypad or RFID scanner, verifying authentication credentials and providing feedback via an OLED display and buzzer.

A. State Machine Description

The state machine governing the system consists of the following states:

- **Idle State:** The system awaits user interaction. The OLED display prompts the user to enter a PIN or scan an RFID card.
- **Reading Input:** The system reads the entered PIN via the keypad or scans an RFID card. If using a keypad, the display updates with masked input (e.g., ”****”).
- **Validating Input:** The entered credentials are checked against the stored authentication database.

Rahul Padhi, UC Davis, Email: rpadhi@ucdavis.edu.
Emmanuel Agubata, UC Davis, Email: ebagubata@ucdavis.edu.

  - If the PIN or RFID is correct, the system moves to the **Access Granted** state.
  - If incorrect, it transitions to the **Access Denied** state.
- **Access Granted:** The OLED displays a success message, the buzzer sounds a confirmation tone, and the servo motor unlocks the door.
- **Access Denied:** The OLED displays an error message, the buzzer plays an alert tone, and the system prompts the user to retry.

The following diagram illustrates the state machine governing the authentication process:

B. High-Level Behavior

The high-level behavior of the system ensures secure access control through a combination of user input validation and real-time feedback mechanisms:

1) The system continuously displays a prompt on the OLED screen for the user to enter their PIN or scan their RFID card.
2) Upon input, the system checks the credentials and determines if access should be granted.
3) If the input is valid, the door unlocks and the system provides an audio-visual confirmation.
4) If the input is invalid, the system alerts the user and remains locked.
5) After an authentication attempt, the system resets and returns to the idle state, awaiting further input.

This structured approach ensures that the system operates efficiently, providing real-time user feedback while maintaining security.

IV. Implementation

V. Challenges

During the implementation of our project, we encountered several challenges that required careful debugging, problem-solving, and iteration. Below, we detail the key challenges we faced, our observations, and the steps we took to resolve them.

A. 1. Wi-Fi Connection Issues

One of the major challenges we faced was getting the Wi-Fi module to connect properly. Initially, we struggled with network configuration and debugging connection failures. We attempted various approaches, including checking firewall settings, modifying security protocols, and troubleshooting power supply inconsistencies. While we managed to establish partial connectivity, we were unable to fully integrate AWS IoT due to time constraints and API issues.

B. 2. RFID Scanner Integration

The RFID scanner posed another challenge. Initially, it was difficult to get consistent readings, as some tags were not being detected properly. We debugged this by testing different RFID modules and ensuring proper wiring and power supply. We also had to adjust the antenna positioning to improve detection range. Ultimately, while the RFID module functioned intermittently, we were unable to fully integrate it into the final system.

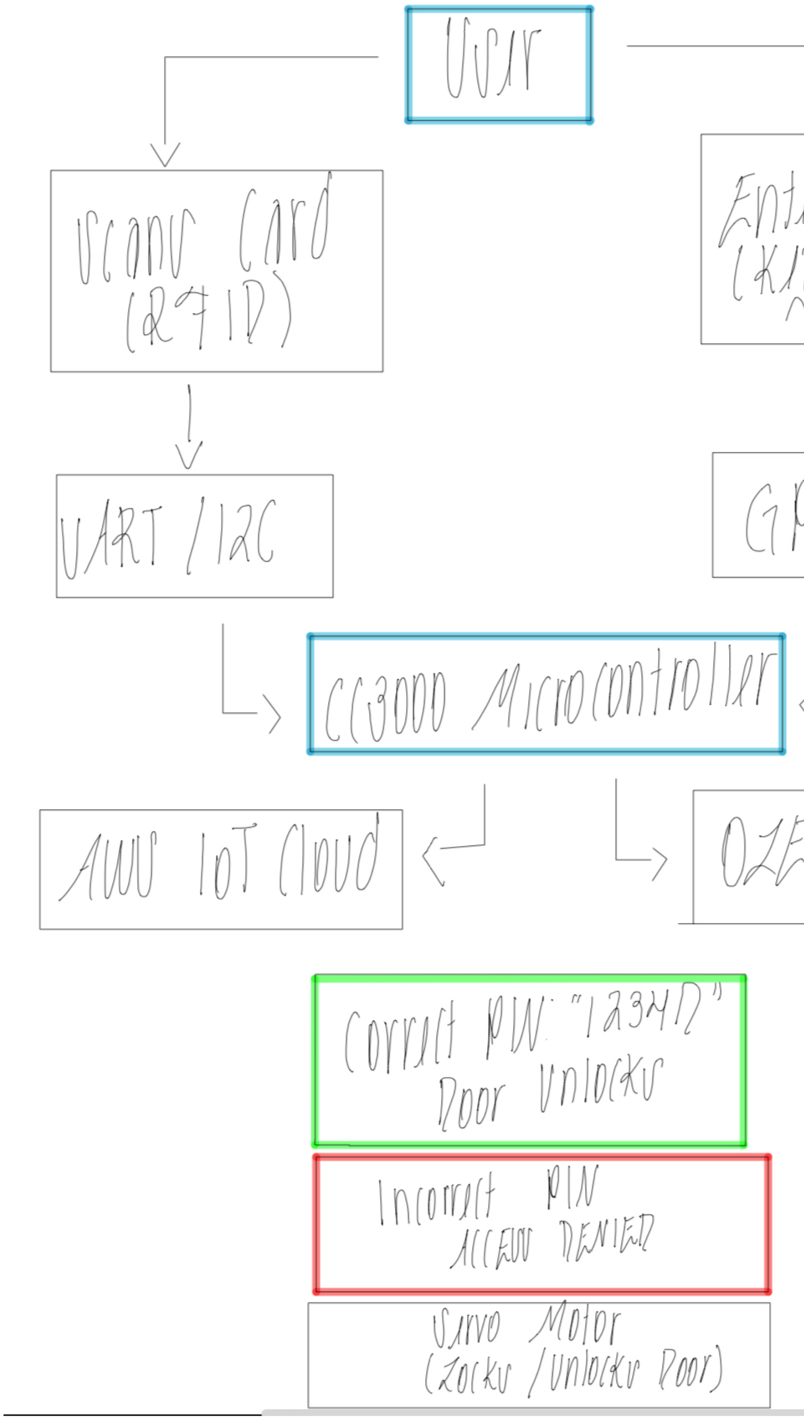

Fig. 1. State Machine Diagram for Authentication System

C. 3. Hardware Debugging

Several hardware-related issues slowed down our progress:

- **Unlocking Mechanism:** Finding a suitable mechanism to unlock the lock using a servo was a significant challenge. We explored different servo configurations and lock types before settling on a working combination.
- **Servo and Buzzer Coordination:** Initially, the servo motor did not unlock the door correctly, and the buzzer failed to trigger as expected. After adjusting the servo's

pulse width modulation (PWM) settings and refining our control logic, we achieved the desired functionality.
- **Keypad Input Handling:** We had difficulty reading user inputs properly from the keypad. Some keypresses were not registering correctly. By refining our debounce logic and testing different keypad libraries, we managed to improve input accuracy.
- **OLED Display Issues:** The OLED display did not light up initially due to incorrect wiring and an incompatible I2C address. After troubleshooting connections and verifying the correct library settings, we successfully initialized the display.

D. 4. Unresolved Issues

Despite our efforts, we were unable to fully implement AWS IoT and the RFID authentication system. While we successfully established partial connections, integration complexities prevented us from finalizing these components. Given more time, we would refine our approach to better incorporate cloud authentication and enhance RFID reliability.

Overall, through systematic debugging, testing, and iterative improvements, we successfully resolved most hardware and software challenges. The experience strengthened our problem-solving skills and deepened our understanding of embedded system development.

VI. Future Work

While our project successfully implemented a secure access control system using a keypad, OLED display, and servo motor, there are several enhancements we would like to introduce in future iterations. These improvements focus on increasing security, efficiency, and usability.

A. 1. Fully Implement AWS IoT and RFID Authentication

Currently, our AWS IoT and RFID authentication system is not fully functional. Future work will focus on debugging API communication, refining request handling, and ensuring seamless integration between RFID authentication and AWS IoT. A fully implemented cloud authentication system would allow for remote access monitoring and logging.

B. 2. Improve Security Features

Enhancing security is a key priority for future iterations. Some potential upgrades include:

- **Encrypting PIN inputs** to prevent unauthorized interception.
- **Multi-factor authentication (MFA)**, requiring both RFID and a PIN code for access.
- **Failed login attempt lockout** to temporarily disable access after multiple incorrect entries.

C. 3. Improve Hardware Efficiency and Reliability

Several optimizations can enhance the hardware's performance:

- **Low-power mode implementation** to reduce energy consumption when idle.
- **Optimizing servo motor response** by refining PWM control for smoother unlocking.
- **Replacing the servo with an electromagnetic lock** for increased durability and security.

D. 4. Expand the System's Connectivity

Expanding connectivity options would make the system more accessible:

- **Mobile App or Web Dashboard** to allow remote monitoring and control.
- **Bluetooth Backup Communication** as an alternative in case of Wi-Fi failures.

E. 5. Integrate Additional Sensors

Adding more sensors can improve security and functionality:

- **Motion Sensor (PIR or IR)** to detect nearby movement and trigger alerts.
- **Door Open/Close Sensor** to confirm if the lock successfully engaged.
- **Fingerprint Scanner** for biometric authentication.

F. 6. Enhance User Interface and Feedback

User experience can be improved by refining feedback mechanisms:

- **OLED Display Enhancements** to provide clearer status updates and error messages.
- **Audio Feedback** via a speaker or buzzer to announce access status.
- **LED Status Indicators** to visually indicate access granted (green) or denied (red).

By implementing these improvements, we aim to create a more secure, efficient, and user-friendly access control system.

VII. Bill of Materials

This is a comprehensive list of all components and materials that we used in the Smart Locker System prototype, including their costs and how we got them.

The Smart Locker System was built primarily using standard components available in EEC 172 Lab. The core microcontroller (CC3200 LaunchPad) and basic peripherals were provided by the EEC 172 lab, while specialized components such as the RFID scanner and locking mechanism were purchased separately. This design approach ensures that the prototype could be reproduced by anyone with access to similar lab resources for a total additional cost of approximately $38.00. With the total component cost of $38.00, our project falls well within the allocated budget of $50, demonstrating effective resource management while still achieving all functional requirements.

Component	**Quantity**	**Cost ($)**	**Source**
CC3200 LaunchPad	1	0.00	Provided in lab
OLED Display	1	0.00	Provided in lab
RFID Scanner	1	30.00	Purchased
Metal Lock	1	4.00	Purchased
Servo Motor	1	2.00	Purchased
4×4 Keypad	1	2.00	Purchased
Jumper Wires	Various	0.00	Provided in lab
Cardboard (housing)	1	0.00	Repurposed material
Metal Pick (for lock mechanism)	1	0.00	Repurposed from keyring
Total Cost		**$38.00**	

TABLE I

Smart Locker System Components and Materials