Multi-Party, Multi-Factor Authentication Lockbox

By

Shelby Doty

Noah Hill

Akshay Sundaram

Project Proposal for ECE 445, Senior Design, Fall 2022

TA: Zhicong Fan

14 September 2022

Project No. 17

Table of Contents

1 Introduction

1.1 Problem

Governments and government agencies, banks, hospitals, or companies may have rooms, safes, or vaults requiring controlled access to protect their contents. This may include sensitive information, security and surveillance equipment and their controls, critical facility infrastructure equipment for telecommunications or power distribution, or hazardous materials. Restricted areas may include server rooms, data centers, or rooms housing industrial control systems. These areas and their contents are prone to physical security attacks such as severance of critical cables, theft of communication equipment, or theft of data servers. Security attacks may be conducted by a malicious insider, resulting in devastating data breaches. According to IBM Security's "Cost of a Data Breach" report in 2020, 10% of malicious data breaches between August 2019 and April 2020 were the result of a physical security compromise while 7% were caused by a malicious insider. The 2021 "Cost of a Data Breach" report by IBM Security noted that the average time to identify and contain a breach caused by physical security compromise was 292 days while a breach caused by a malicious insider took on average 306 days to identify and contain. Existing methods to protect physical systems from malicious insiders include auditing, job rotation, and separation of duties. Auditing access to a restricted area is reactive and does not prevent unauthorized access from occurring. Job rotation and separation of duties only limit prolonged access to certain areas or physical systems.

1.2 Solution

Multi-factor authentication (MFA) is an electronic authentication method used to grant an individual access to an application or place only after successfully presenting multiple factors for verification purposes. Multi-party authorization (MPA) requires multiple individuals to authorize access to an application or place. An example of multi-party authorization usage occurs in banks when one accesses a lockbox. This requires both a bank official and the lockbox owner to act together to open the lockbox.

Our idea is to create an electronic lock mechanism that provides a proactive approach to physical access control by employing both MFA and MPA methods. Access is granted only when a configurable number of individuals (multi-party) successfully authenticate with an inherent factor and a disconnected software token received via SMS text (multi-factor). The inherent authentication factor will be a fingerprint. This locking mechanism would be applicable to a lockbox in a bank, for example, which already requires multiple parties to authorize access. However, the inherent authentication factor used for authentication in this design, the fingerprint, is not easily lost or misplaced as lockbox keys are.

1.3 Visual Aid

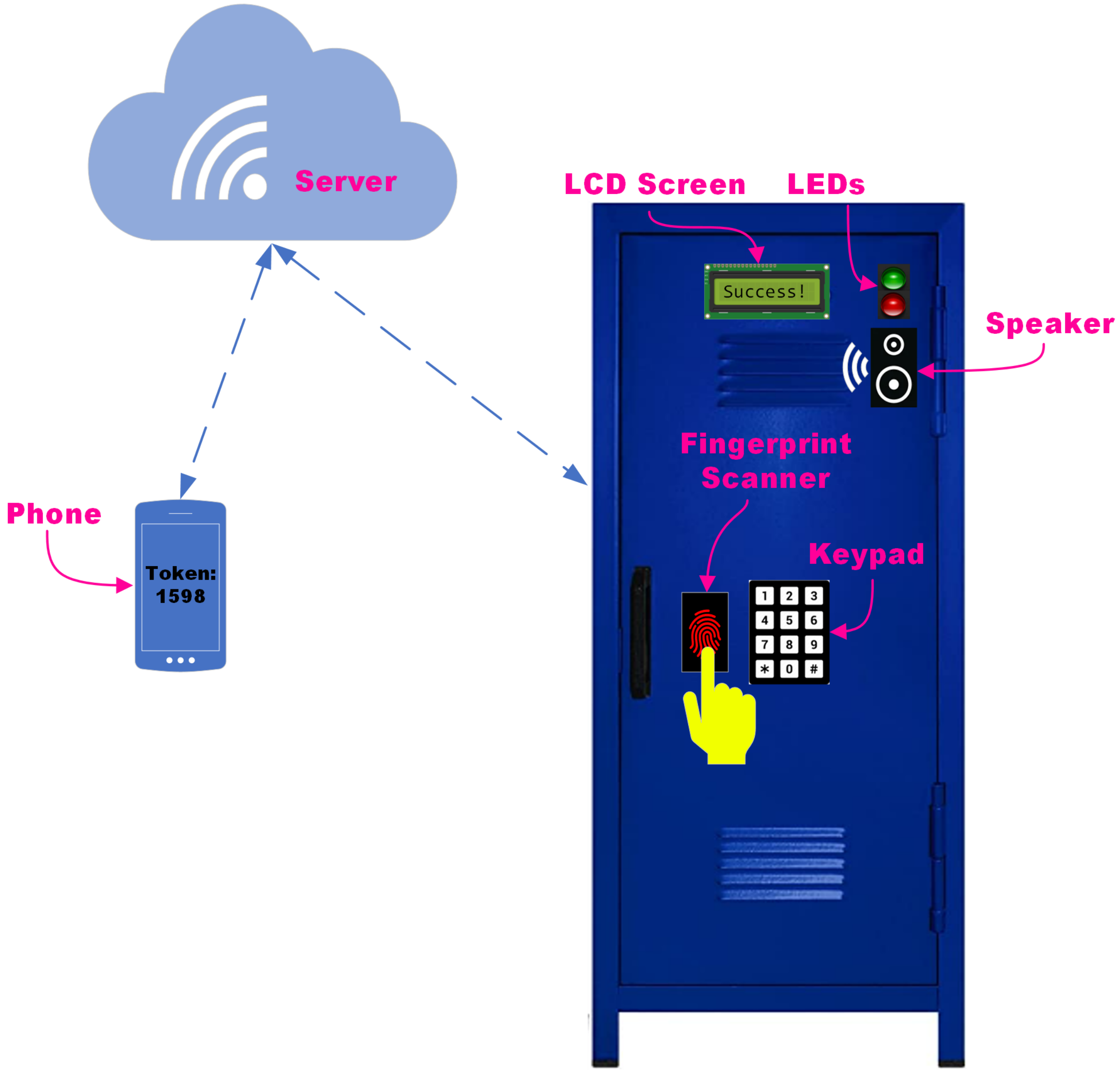

Figure 1: Visual Aid

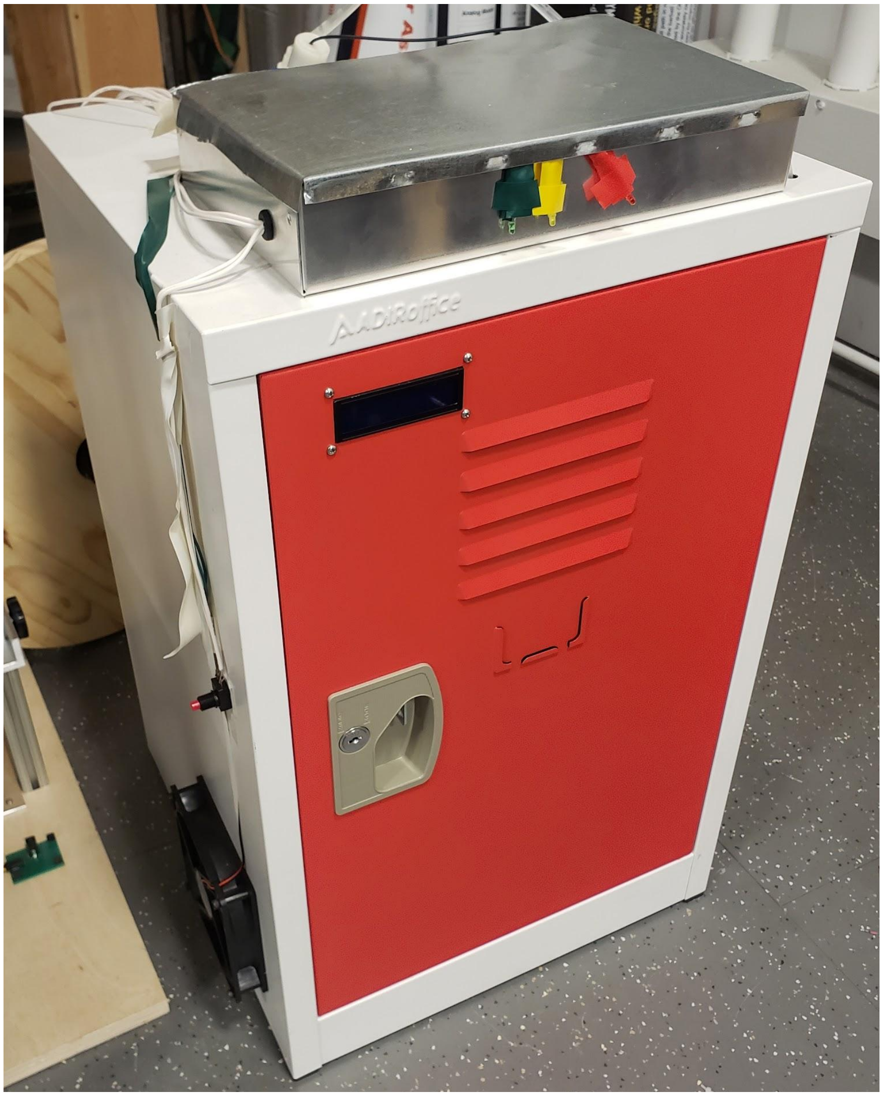

Figure 2: Project Locker (Used)

1.4 High-level requirements list

1. Authentication

Locking mechanism should unlock after verifying all users' fingerprints and confirming successful input of a one-time token from each. One-time token will be generated by a random-number generator and wirelessly sent to the user authenticating within reasonable time.

2. Wireless Connections

Send and receive messages via Wifi connection, link to TCP server, and then to someone's mobile device within a reasonable amount of time, <30 seconds.

3. Power

Powered by both wall outlet and back-up battery; Device can be powered by both conventional 120V AC wall outlet, or a DC power source such as the test bench power supply or a battery powered back-up.

2 Design

2.1 Block Diagram

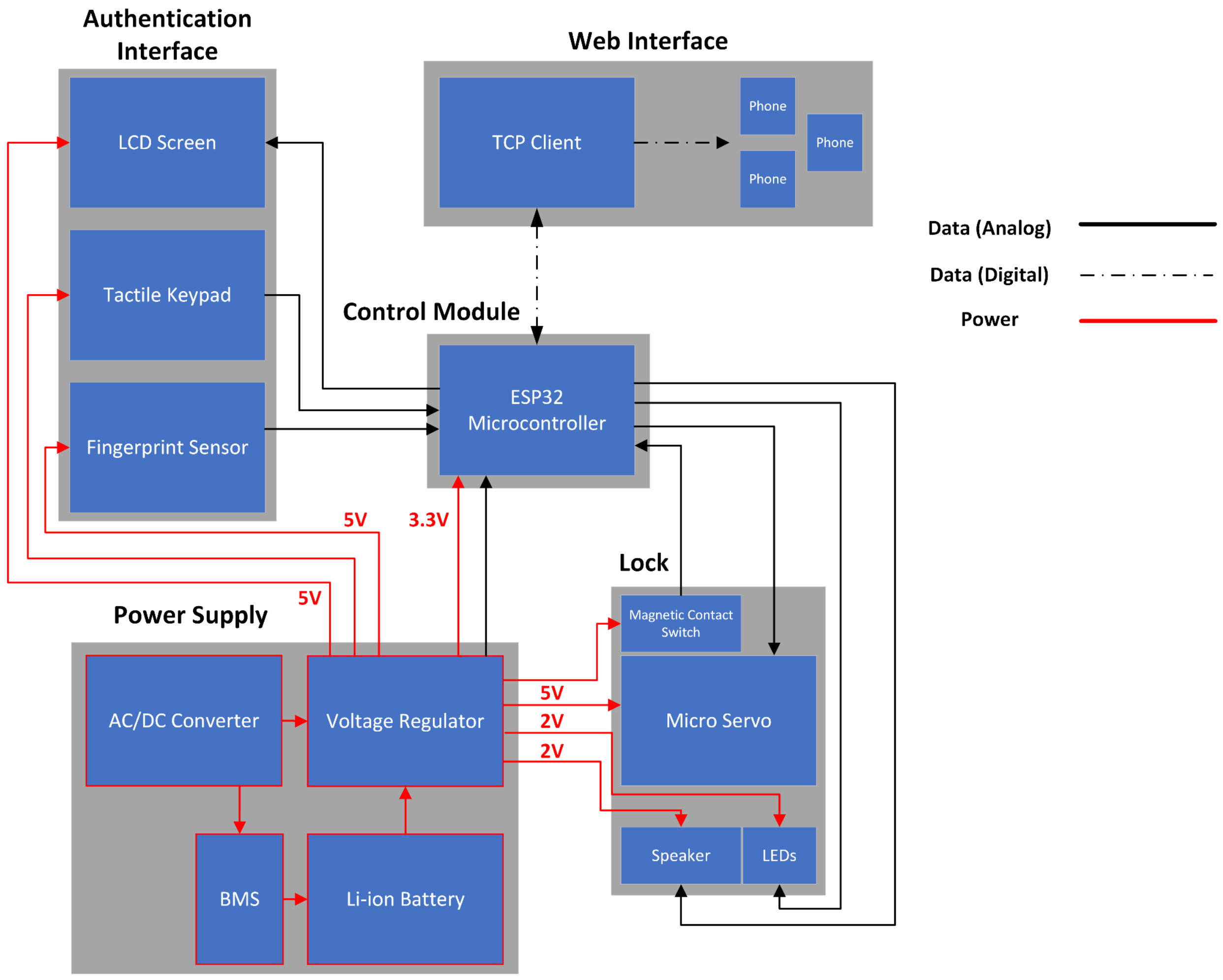

Figure 2: Block Diagram

The critical subsystems depicted in the block diagram include the power supply, control module, web interface, authentication interface, and lock. The power supply includes a battery-backup system, ensuring an uninterrupted source of power for all components in the event the system is unplugged from a regular utility power source. The control module is responsible for seamless communication between all other subsystems as it monitors the status of authentication attempts, engages and disengages the lock, and provides user feedback. The web interface allows the device to be easily connected to a wireless network and contains a client capable of generating and sending one-time tokens via SMS. The authentication interface consists of the devices utilized for authentication, including a fingerprint sensor and keypad for entering a one-time token. Lastly, the lock subsystem contains the lock hardware and status indicators for user feedback.

2.2 Subsystem Overview

2.2.1 Control Module

The control module receives data from the user interface subsystem via the fingerprint sensor and tactile keypad and sends data to the web interface subsystem over WiFi. The control module controls the LCD screen from the user interface and the servo/solenoid from the mechanical relay & lock status indicator for locking/unlocking. The control module consists of a microcontroller, the ESP32, which uses Wi-Fi connectivity and acts as a TCP client to provide the TCP server with data regarding user identity and authentication success/failure when an authentication attempt is made. Upon successful biometric authentication, the ESP32 microcontroller and the user authenticating receive a one-time token sent via SMS to be input on the tactile keypad. Access is granted/denied depending on whether the user inputs the correct token generated by the TCP server.

Requirements	**Verification**
1. Upon successful multi-factor authentication of all configured parties, the microcontroller must disengage the lock within 2 seconds.	1a. Engage lock 1b. Begin authentication process 1c. Once the last successful factor of authentication has been entered, begin a timer 1d. When the lock obtains a signal to disengage, stop the timer 1e. Ensure the time is less than 2 seconds
2. Upon successful biometric authentication, the microcontroller must transmit the identity of the party to the TCP server within 2 seconds.	2a. Begin biometric authentication process 2b. When a fingerprint scan is successfully matched to a template stored in the fingerprint database, begin a timer 2c. Stop the timer when the TCP server successfully receives the identifier 2d. Ensure the time is less than 2 seconds.

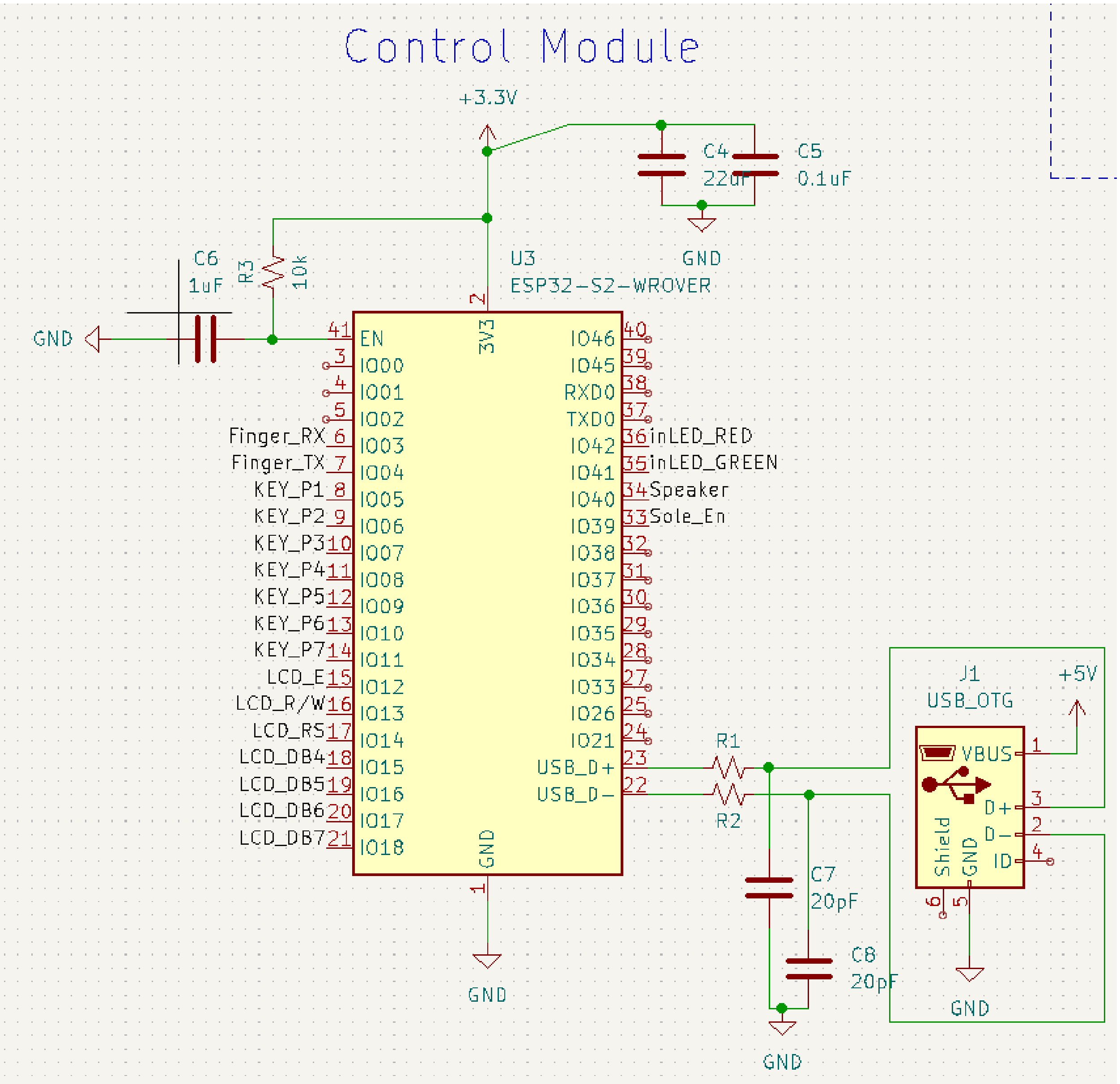

Figure 3: Control Module Schematic

2.2.2 User interface

This subsystem consists of the fingerprint sensor module for gathering biometric data, an LCD screen to display warnings and instructions, and a tactile keypad. The AS608 optical fingerprint sensor module stores biometric data, collects and renders fingerprint images, and matches fingerprint scans with those in storage. A LCD2004 character-type liquid crystal display provides user feedback regarding system status, authentication success/failure messages, remaining successful authentications before unlock, etc. The 3x4 tactile keypad allows users to enter a one-time token received via SMS.

Requirements	Verification
1. Tactile keypad buttons must be debounced after 100ms.	1a. Connect an oscilloscope to each output pin and press each of the 9 buttons while monitoring the voltage with respect to time 1b. Any button chattering will be visible and measurable 1c. Ensure chattering persists less than 100ms.
2. LCD displays each button press when typing in the 4 digit token.	2a. Visually verify that the correct numbers show up when pressed.

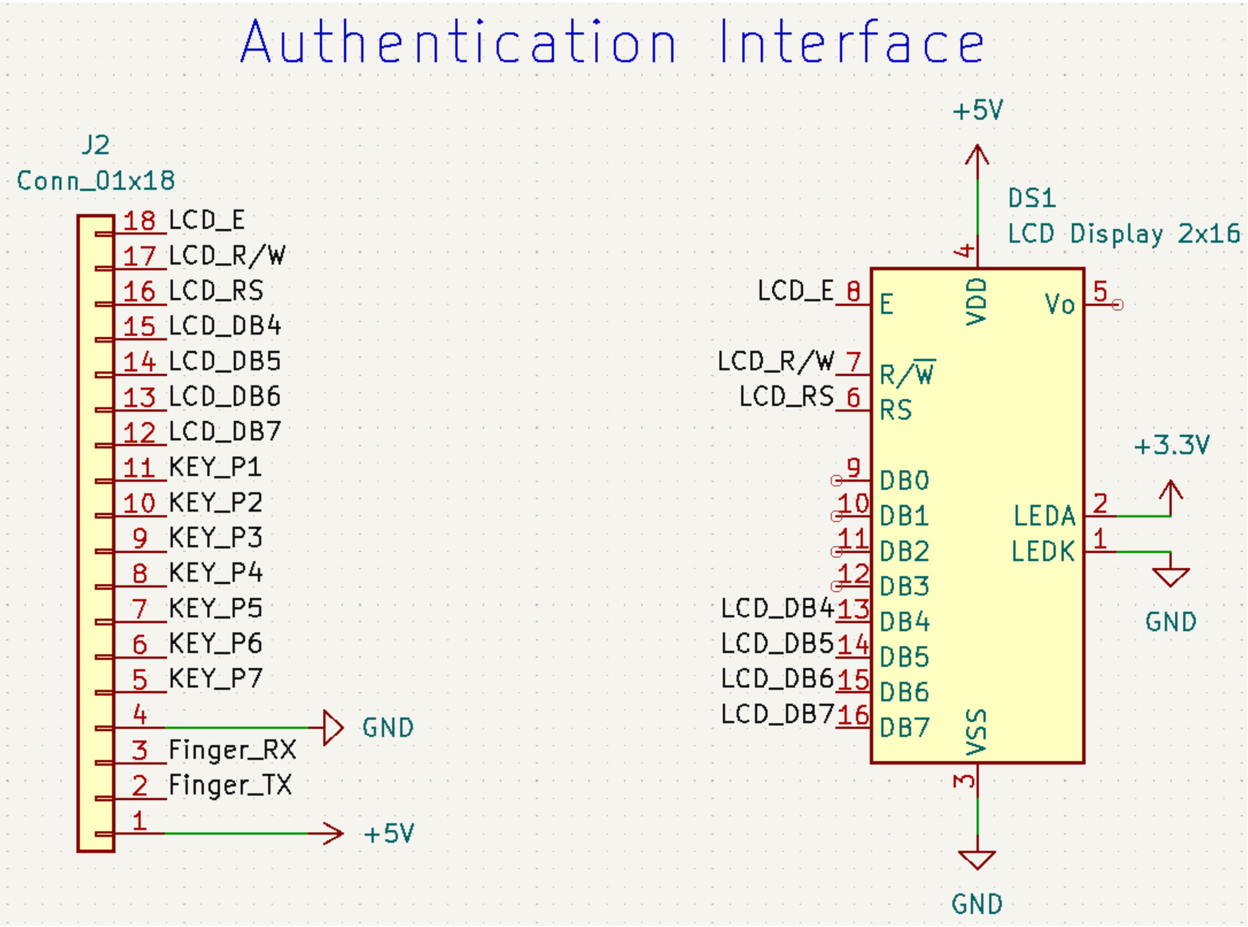

Figure 4: Authentication Interface Schematic

2.2.3 Mechanical relay & lock status indicator

This system will be controlled by the control unit and responsible for securely locking and unlocking the lockbox using a LD-20MG Digital Servo or a MP001162 Linear Solenoid.

LEDs indicate to the user when the lockbox is locked or unlocked. A speaker emits a beeping noise if the lockbox door is open longer than a predetermined amount of time. Both parts can be found in the ECE210 lab kit. A magnetic contact switch completes a closed circuit when the lockbox door is shut, sending a signal to the control module to engage the servo/solenoid lock. Each of these components were chosen because of their relatively cheap costs, and their ability to perform their function while not requiring an excessive amount of power to operate.

Requirements	Verification
1. Locking mechanism doesn't jam or get stuck open or closed.	1a. After attaching the linear solenoid to the inner part of the locker, fully close the door. 1b. Perform the unlocking sequence 1c. If the Solenoid doesn't cause enough linear motion to open the door readjust its positioning 1d. Repeat above steps until the lock never jams

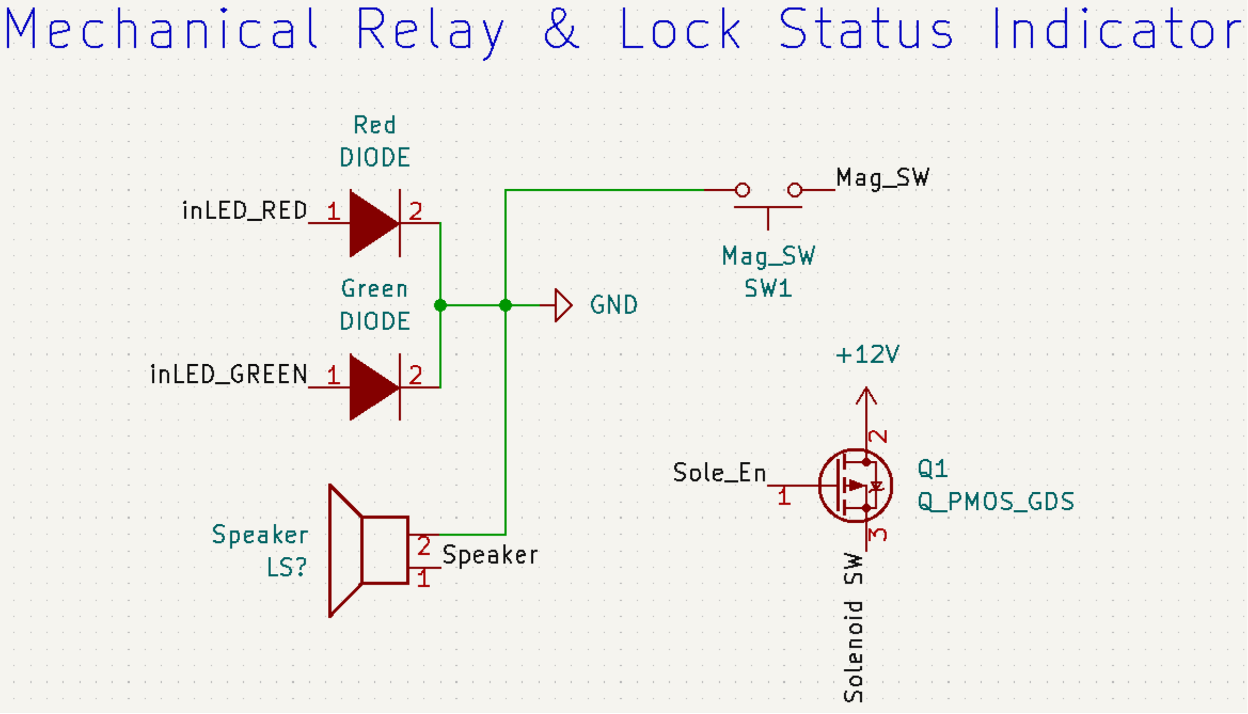

Figure 5: Mechanical Relay & Lock Status Indicator Schematic

2.2.4 Power Supply

The power subsystem plays a crucial role, powering the control unit, user interface, and the mechanical relay & lock status indicator subsystems. As stated previously in section 1.4, our lockbox will be primarily powered via an AC/DC wall outlet power supply, but also have a back-up battery so it remains functional if it loses power from the wall outlet. The Talent Cell 6000mAh 12V DC Li-ion battery pack can charge and power components at the same time. This functionality is compatible with our design because the lockbox must remain plugged in and while it is plugged in it should charge the backup battery and power all of the lockbox components. Included with the Talent Cell battery pack is a AC/DC 12.6 1A charger which satisfies our need to charge the battery pack, and/or power our other subsystems. Since the charger comes with the battery pack, there is no risk for us picking out the wrong one which could cause it to be damaged. Furthermore, the Talent Cell has a built in BMS with overcharge, discharge, and short-circuit protection.

The control unit needs to be powered with 3.3V while all of the other components need to be powered with 5V, excluding the linear solenoid which requires 12V. In order to achieve these voltages, we will need a voltage regulator. First, we will need to step down the 12V supply to 5V. To do this we will use a LM7805CT voltage regulator coupled with a 0.33uF and 0.1uF capacitors as stated by the datasheet [6]. To get the desired 3.3V to power the control unit, we will use an LM3940IT-3.3 voltage regulator to step down from 5V to 3.3V coupled with a 0.47uF and 33uF capacitors as stated by the datasheet [7].

Requirements	Verification
1. Battery remains within the rated temperature while operating under maximum possible load (~700mA)	1a. Connect an amp meter between the power source and the power input on the PCB 1b. Perform a routine opening and closing sequence 3 times in a row 1c. Use a laser thermometer gun to monitor the batteries w
2. The device must be able to remain powered even if unplugged from the wall outlet	2a. Connect a 1K resistor to the 12V, 5V, and 3.3V power rails and use a multimeter to monitor the current coming from the 12V source 2b. Connect an oscilloscope to monitor the voltages across the 1K resistor loads 2c. Unplug the wall outlet power supply and verify that all voltages remain present

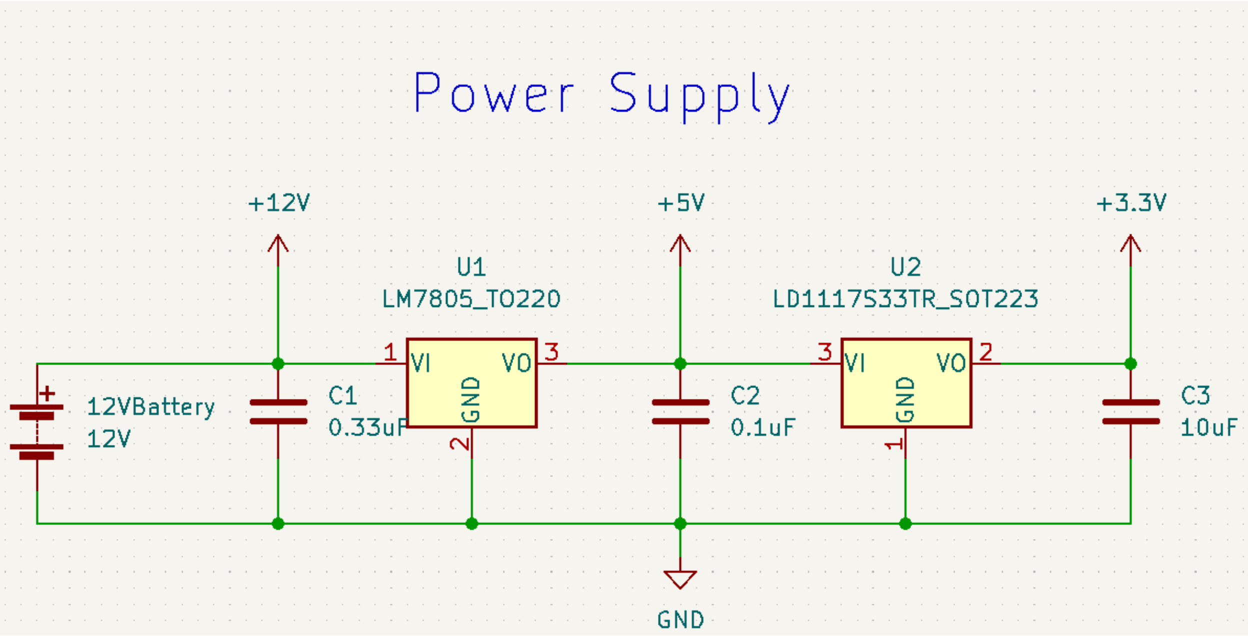

Figure 6: Power Supply Schematic

2.2.5 Web Interface

The ESP32 microcontroller will act as a TCP client and connect to the TCP server over Wi-Fi. On initial connection, the user configurations will be stored on the server. Each user configuration will include a signal alerting the server to a correct/incorrect fingerprint scan for that user and the user's phone number. This will be distinct for every user. On future connections, the TCP server will receive the signal from the TCP client and will then generate a software token containing a 4-digit randomized pin code. This TCP server will send this token to the ESP32 microcontroller over Wi-Fi and to the phones via SMS message. Phones will receive SMS messages from the TCP server with randomized 4-digit pin code to enter into the tactile keypad. Phones will also receive an alert from the TCP server if fingerprint scan is not correctly authenticated.

Requirements	Verification
1. Able to communicate with the ESP32 microcontroller over Wi-Fi at speeds over 5 Mbps.	1a. Write a script that searches for nearby Wi-Fi connections and displays a success message if securely connected. 1b. Write a script that provides a file with a predetermined size to the microcontroller and

	record the elapsed time. Then calculate Mbps to check the lower bound of 5 Mbps. 1c. Using the same method in 1B, calculate Mbps of a file sent from the microcontroller to the web application.
2. Able to securely store at least 3 distinct user configurations.	2a. Write a script that provides dummy configurations to the web application. Then check that those configurations can be accessed by the web application by displaying the dummy information.
3. Able to generate a software token containing a randomized 4-digit pin code.	3a. Display 4-digit pin code in web application and check with phones and microcontroller that all devices have the same 4-digit pin code sent to them.
4. Able to send accurate SMS messages to configured phone numbers in under 30 seconds.	4a. Write a script that sends SMS messages to the configured phone numbers and records and displays the time elapsed until the phone receives the message. 4b. Write a script that sends a fake fingerprint authentication failure signal to the web application and check that a SMS message is sent to the configured phone numbers with an alert.

2.2.6 User Software Flowchart

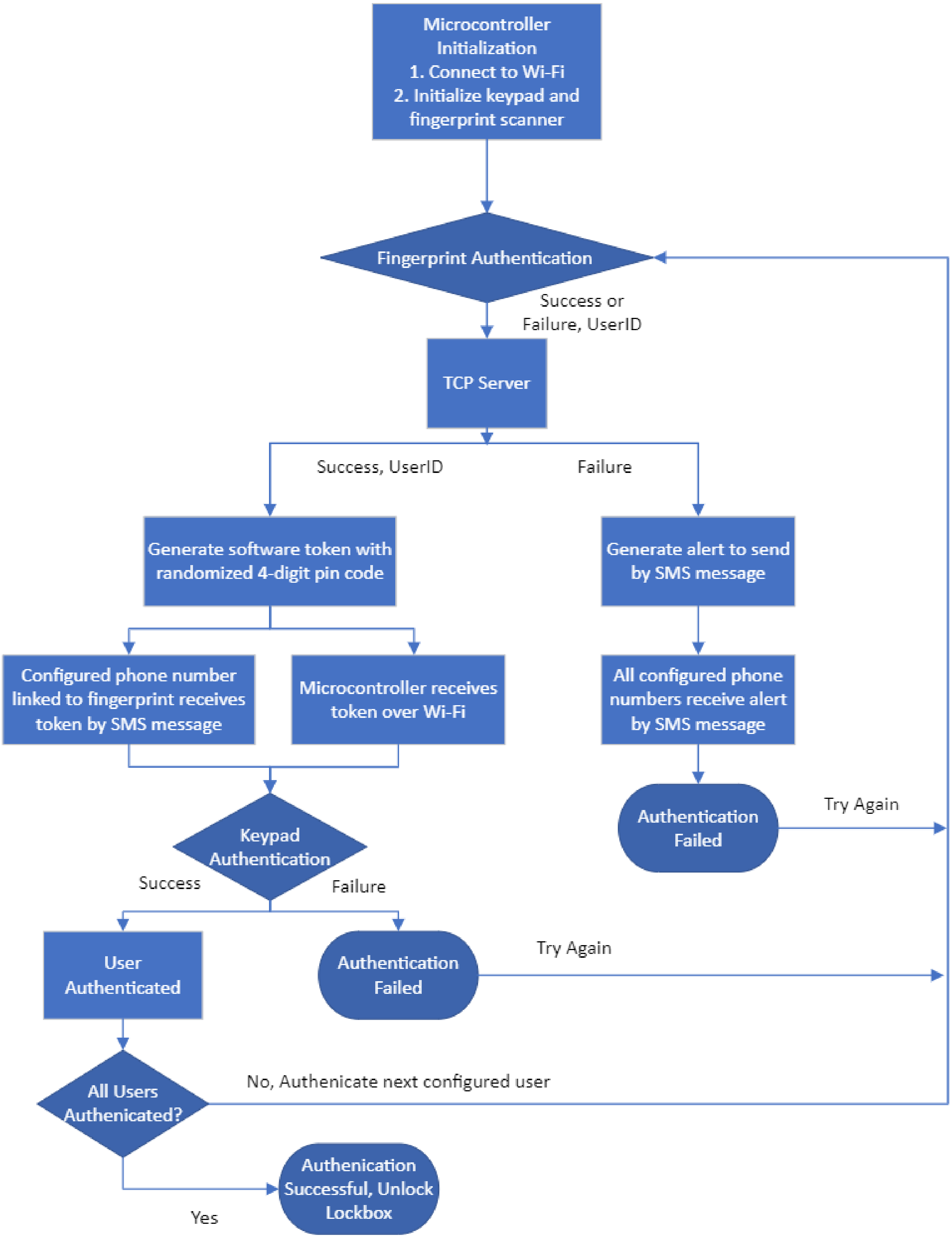
Microcontroller Initialization
1. Connect to Wi-Fi
2. Initialize keypad and fingerprint scanner
Fingerprint Authentication
Success or Failure, UserID
TCP Server
Success, UserID
Failure
Generate software token with randomized 4-digit pin code
Generate alert to send by SMS message
Configured phone number linked to fingerprint receives token by SMS message
Microcontroller receives token over Wi-Fi
All configured phone numbers receive alert by SMS message
Authentication Failed
Try Again
Keypad Authentication
Success
Failure
User Authenticated
Authentication Failed
Try Again
All Users Authenicated?
No, Authenicate next configured user
Yes
Authenication Successful, Unlock Lockbox

Figure 7: User Software Flowchart

2.2.7 Admin Software Flowchart

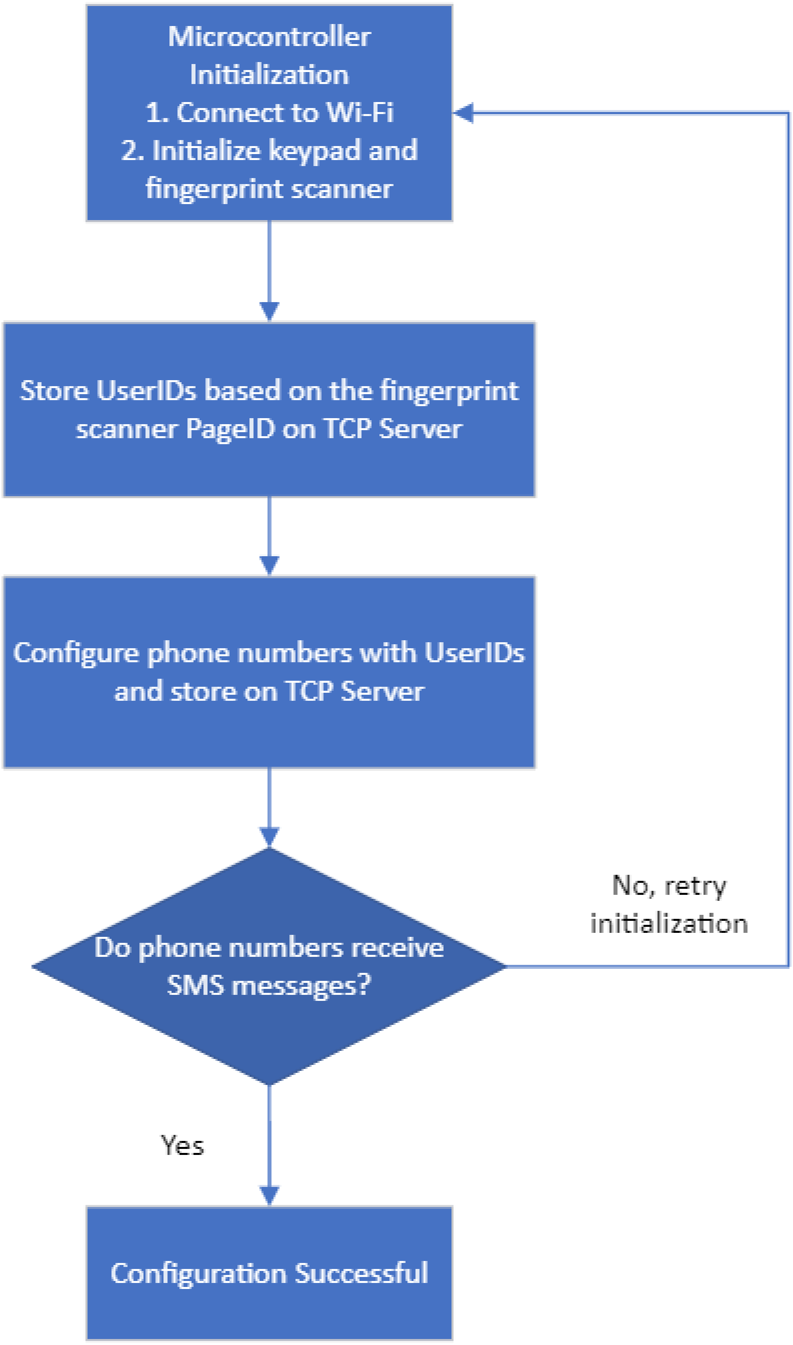
Microcontroller Initialization
1. Connect to Wi-Fi
2. Initialize keypad and fingerprint scanner
Store UserIDs based on the fingerprint scanner PageID on TCP Server
Configure phone numbers with UserIDs and store on TCP Server
Do phone numbers receive SMS messages?
No, retry initialization
Yes
Configuration Successful

Figure 8: Admin Software Flowchart

2.3 Tolerance Analysis

Supplying the system with adequate and uninterrupted power is imperative in ensuring the proper functionality of authentication methods, continuous communication with users, and preservation of biometric data. A standby uninterruptible power supply (UPS) will turn on to power the system when utility supply voltage has fallen below a predetermined level. When the UPS is not powering the system, a rectifier will convert AC to DC to charge the UPS.

The uninterruptible power supply will be composed of protected 18650 lithium ion batteries due to their high energy density and high voltage. To estimate the amount of power required to facilitate the lock system, a "worst-case" tolerance analysis was performed. Design components requiring power were placed at their tolerance limits to calculate the range of potential wattages demanded by the load.

Four key components were considered:

- AS608 optical fingerprint sensor module
- LCD2004 character-type liquid crystal display
- Micro DC motor / Push-pull solenoid
- ESP32-S2-MINI-1 microcontroller

Voltage requirements for the fingerprint sensor module range from 3.6 - 6.0V while current drawn ranges from 120 - 150mA.

Voltage requirements for the display range from 4.5 - 5.5V while current drawn ranges from 2 - 5mA.

Voltage requirements for the motor/solenoid vary from 6 - 12V while current ranges from 40 - 300mA.

The ESP32 microcontroller input voltage varies from 3.0 - 3.6V and current drawn varies from 68 - 310mA.

Using P = IV, the greatest and least possible load power consumptions by these components were determined. These components, at minimum, will consume 0.855W 20%. At most, they will dissipate 5.6435W 20%. The additional margins provide a more encompassing tolerance estimate regarding the variation of the necessary power supply, increasing the probability of continuous power in the presence of solenoid voltage spikes or lithium-ion self-discharging.

3 Cost and Schedule

3.1 Cost Analysis

3.1.1 Labor

As of Sep 20, 2022, the average hourly pay for an electrical engineering graduate in the United States is approximately $36.27 an hour [8]. It is estimated that each person on the team will work 15 hours per week for 10 weeks.

$$Labor\ cost\ per\ person\ =\ \frac{\$36.27}{hour} * 2.5 * 150\ hours\ =\ \$16,321.50$$

$$Total\ labor\ cost\ =\ \frac{\$16,321.50}{person} * 3\ people\ =\ \$48,964.50$$

3.1.2 Parts

Description	Manufacturer	Quantity	Cost/Unit ($)	Link
ESP32-S2-WROVER	Espressif Systems	1	3.95	Link
3X4 Matrix Keypad Module	SparkFun Electronics	1	4.95	Link
ZFM-20 Fingerprint Identification Module	Zhiantec	1	49.95	Link
LCD2004 Module	SunFounder	1	10.99	Link
6000mAh Li-ion Battery Pack	TalentCell	1	34.99	Link
LD-20MG Digital Servo	LewanSoul	1	15.98	Link
MP001162 Linear Solenoid	Multicomp Pro	1	5.56	Link
SW-MAG REED FLANGE MOUNT	NTE Electronics, Inc	1	4.11	Link
IC REG LINEAR FIXED POS STD REG	Fairchild Semiconductor	1	1.78	Link
LD1117AS33TR 5 to 3.3V Regulator	Stmicroelectronics	1	0.95	Link
Red 623nm LED Indication	Lite-On Inc.	1	0.36	Link
Green 568nm LED Indication	Kingbright	1	0.34	Link
BUZZER MAGNETIC 3V 12MM TH	CUI Devices	1	1.27	Link
1uF Capacitor	TDK	5	0.062	Link
10uF Capacitor	TDK	2	0.096	Link
22uF Capacitor	TDK	1	0.154	Link
0.1uF Capacitor	TDK	4	0.021	Link
20pF Capacitor	MURATA	4	0.002	Link
0.33uF Capacitor	TDK	2	0.397	Link
Total cost: $136.23				

3.1.3 Grand Total

$$Grand\ total\ =\ total\ labor\ cost\ +\ total\ parts\ cost$$
$$=\ \$48,964.50\ +\ \$136.23$$
$$=\ \$49,100.73$$

3.2 Schedule

Week	Project Component	Noah	Shelby	Akshay
9/26	Design Document	Finish draft of PCB design	Compile power supply & lock parts required	Database structures, Research python modules
10/3	Design Review PCB Reviews	Revise PCB design	Connect user interface module, test requirements	Web application development, Testing
10/10	PCB Order I Teamwork Evaluation I	PCB Order I design complete	Test power supply requirements with different locks	Web application development, Testing
10/17	Devise lock box layout	Plan out how to assemble all parts onto locker	Plan out how to assemble all parts onto locker	Wi-Fi connectivity, Fingerprint scanner data transfer to server
10/24	Revist Requirements & Verification	Verify components	Verify components	Debugging microcontroller connection
10/31	PCB Order II Individual Progress Reports	Assemble all components	Assemble all components	Review and optimize code, Debugging
11/7	Debugging and Finalization	Assemble all components	Assemble all components	Verify code works with ESP32, Debugging
11/14	Mock Demonstration			
11/21	**Fall Break**			
11/28	Final Demonstration	Prepare for	Prepare for	Prepare for

		demo	demo	demo
12/5	Final Presentation Final Papers Teamwork Evaluation II	Complete paper and evaluation	Complete paper and evaluation	Complete paper and evaluation

4 Ethics and Safety

We will make sure “to treat all persons fairly and with respect”[1] when conducting ourselves as a team both between ourselves and with all others. We will also be sure to “hold paramount the safety, health, and welfare of the public”[1] when designing our lockbox in accordance with the IEEE and ACM Code of Ethics.

Since this will be a lockbox that opens using biometric data, a fingerprint, it must be able to both secure the contents, but equally important it must keep the biometric data secure. In alignment with sections 1.6 and 1.7 of the ACM code of ethics and professional conduct which state, “Computing professionals should protect confidentiality except in cases where there is evidence of the violation of law, of organizational regulations, or of the Code. ”[2], we will make sure that data is transferred by secure methods and data is never made public in order to preserve the integrity of our lockbox. Fingerprint data will also be kept on the hardware instead of the web server to keep the biometric data more secure to cyber attacks.

Regarding our battery pack, we will need to be safe in the lab when working with this. Our battery pack will follow the guidelines from the General Battery Safety[3] document on the ECE445 course website. We will also look through the battery’s manuals for the proper safety and handling procedures. We have chosen to implement a prebuilt battery pack with a built in BMS to avoid costly mistakes that may happen when designing our own. Batteries have hazards such as battery acid burn, flammability, and electric shock. In order to prevent injuries to users, we need to make sure the battery is safely secured onto the lockbox. Additionally, we will practice proper wall outlet safety by purchasing an AC/DC Converter and avoiding overheating components.

5 References

[1] “IEEE Code of Ethics.” IEEE, IEEE Policies, Section 7 - Professional Activities (Part A - IEEE Policies), . [Accessed 15 September 2022]

[2] “ACM Code of Ethics and Professional Conduct.” Association for Computing Machinery, ACM, . [Accessed 15 September 2022].

[3] “General Battery Safety.” Safe Practice for Lead Acid and Lithium Batteries, [Online]13 April 2016, [Accessed 15 September 2022].

[4] IBM Security. (2020). *Cost of a Data Breach Report 2020.*

[5] IBM Security. (2021). *Cost of a Data Breach Report 2021.*

[6] Texas Instruments, “uA7800 Series Positive-Voltage Regulators”, LM7805 datasheet, May 1976 - Rev. May 2003, [Accessed 15 September 2022].

[7] Texas Instruments, “LM3940 1-A Low-Dropout Regulator for 5-V to 3.3-V Conversion ”, LM3940 datasheet, May 1999 - Rev. Feb. 2015, [Accessed 15 September 2022].

[8] ZipRecruiter, “Graduate electrical engineer salary.” [Online]. Available: https://www.ziprecruiter. com/Salaries/Graduate-Electrical-Engineer-Salary