University of Central Florida

Department of Electrical and Computer Engineering

Initial Project and Group Identification Document

Divide and Conquer, Version 2.0

Dr. Lei Wei

Smart Door Security System

Group 15:

Adam Stefanik, Electrical Engineering
Moisess Rodriguez, Computer Engineering
Reham Hammad, Electrical Engineering
Zachary Jachovich, Computer Engineering

1. Project Narrative

1.1. Motivation

As people continue to incorporate advanced technology in their homes, smart locks become one of the many things people want to have. With all the high-tech products we have in our homes, we surely want to protect them. Our motivation is to enhance the traditional way of entering homes by integrating advanced and secure technology into a door locking system, while still maintaining easy availability.

A smart door with a built-in security system, gives us the ability to lock/unlock a house door without a physical key. For any door with a traditional lock, this technology will be helpful. Using the smart door system, a new form of authentication will be in use, and keys will no longer be required.

1.2. Goals & Objectives

The goal of this project is to incorporate multiple features to develop a two-factor authentication system. If validation is successful, the system will unlock a door and send real-time updates to the user's mobile devices. This system will prevent unauthorized users from entering the building and notify users of the attempt. Photographic evidence of the unauthorized person will be collected.

1.3. Functionality

The functionality of this project involves improving standard electronic door locks by leveraging two-factor authentication. This system will be controlled by a Raspberry Pi, which will collect data from the sensors and process it before making the decision to unlock the door. The sensors will include voice, image, and a touchscreen keypad. The authentication will include any two of the following: voice recognition, facial recognition, pin entry on keypad.

This feature will reduce hassle for the user, while enhancing security. The project functionality will also include multiple colors of LED lights to display how many factors are authenticated. The LED will display white while waiting for user input. A red light will be displayed if validation is denied, then it will turn yellow if one factor is authenticated. When two factors are authenticated, the light will turn green and the door will unlock. A speaker will be used to welcome the user home once passed the authentication check. Upon closing, the door will lock itself back.

2. Project Requirements & Specifications

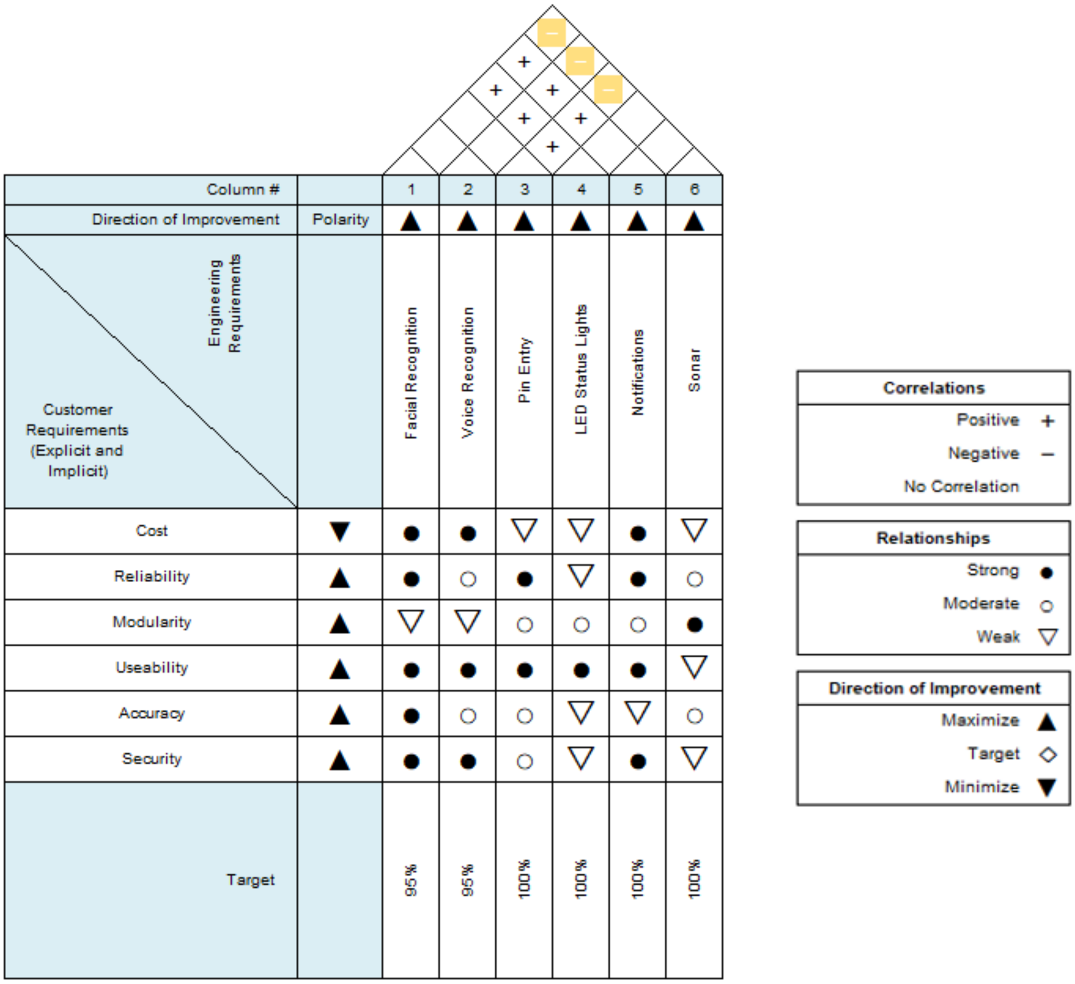
The system shall have a variety of requirements and specifications which will ultimately provide quality assurance as well as guaranteed functionality. At a high level the door must open when all requirements are satisfied, and the process shall be performed efficiently. Table 1 shows additional requirements and specifications for this security system. Figure 1 shows the relationship between our requirements in a House of Quality diagram

ID	Specification	Metric	Showcased in Expo
01	Facial Recognition	Shall recognize authorized users 95% of the time. A user will approach the system 10 times, the system shall recognize the users face at least 9 times.	**Yes**
02	Voice Recognition	Shall recognize authorized users 95% of the time. A user will vocally command the system 10 times, the system shall recognize the user voice at least 9 times.	**Yes**
03	PIN entry	Shall recognize PIN 95% of the time. A user will enter a PIN 10 times, the system shall recognize the PIN at least 9 times.	**Yes**
04	Unlock	The door shall unlock 95% of the time if and only if two out of the three authentication methods are validated. If the system is tested 100 times, then the door shall unlock at least 95 times.	N/A
05	LED Status lights	Shall indicate correctly 95% of time. If the system is tested 100 times, then the LEDs shall display the correct sequence of lights at least 95 times.	N/A
06	Notifications	Shall be sent upon sensing an unauthorized person 95% of time. If the system is tested 100 times, then notifications shall be sent to the user at least 95 times.	N/A
07	Sonar	Shall take the system out of sleep upon sensing movement 95% of time. If the system is tested 100 times, then the Sonar sensor shall wake the system up 95 times.	N/A
08	Speaker System	Speakers shall announce a greeting message 95% of the time. If the system is tested 100 times, then the speaker system shall announce a greeting message at least 95 times.	N/A
09	Auto relock	The door shall relock upon closing 95% of the time. If the system is tested 100 times, then the door shall relock automatically at least 95 times.	N/A

Table 1: Design Specifications

Demonstration:

For the demonstration we will be preforming a series of 10 tests. The system shall recognize a user's face, voice command, and PIN entry at least 9 out of the 10 times. Once one of these features are recognized then a message will be displayed on a screen stating so. Since the other features are integrated into to the system they will be running sequentially. Such as LED status lights changing and the door unlocking once two out of the three authentication methods are validated.



Column #		1	2	3	4	5	6
Direction of Improvement	Polarity	▲	▲	▲	▲	▲	▲
Engineering Requirements Customer Requirements (Explicit and Implicit)		Facial Recognition	Voice Recognition	Pin Entry	LED Status Lights	Notifications	Sonar
Cost	▼	●	●	▽	▽	●	▽
Reliability	▲	●	○	●	▽	●	○
Modularity	▲	▽	▽	○	○	○	●
Useability	▲	●	●	●	●	●	▽
Accuracy	▲	●	○	○	▽	▽	○
Security	▲	●	●	○	▽	●	▽
Target		95%	95%	100%	100%	100%	100%

Correlations	
Positive	+
Negative	–
No Correlation	

Relationships	
Strong	●
Moderate	○
Weak	▽

Direction of Improvement	
Maximize	▲
Target	◇
Minimize	▼

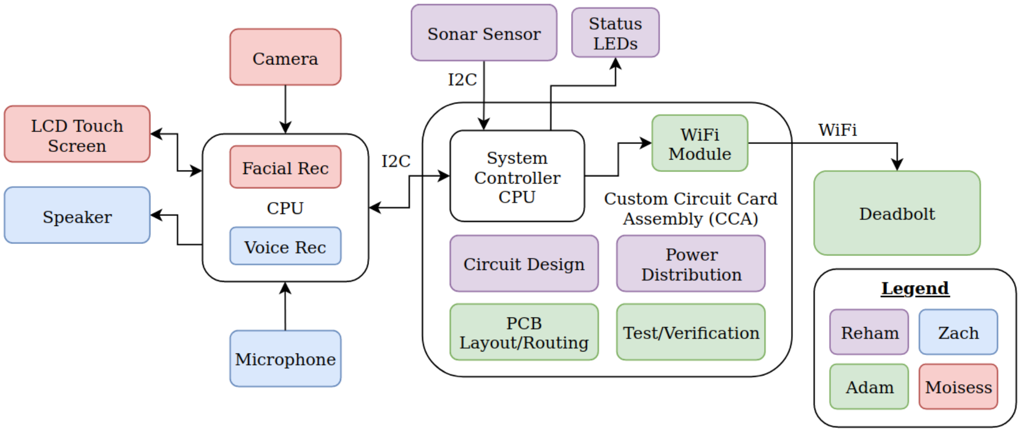
Figure 1: House of Quality Chart

Hardware and Software Diagrams

Diagram Status:

The blocks are currently still being researched, since we are still in the planning phase ideas or concepts may change. None of the bocks are purchased yet, we are still designing and researching components. Until we are comfortable with a design, we will not be purchasing anything. Also, none of the blocks are being prototyped. The development process is still very early, so we are not currently at a prototyping phase.

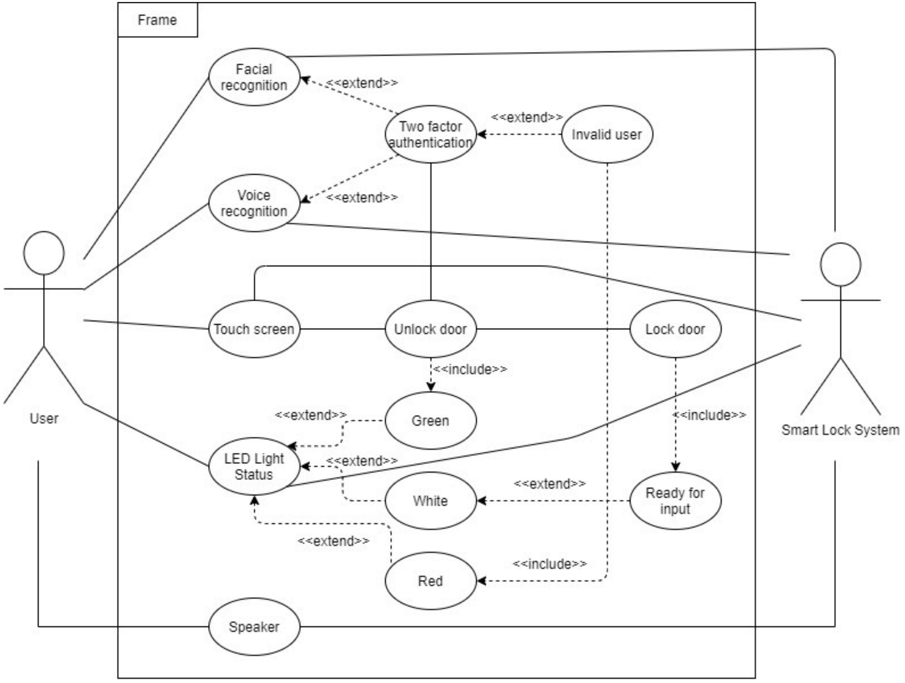
Hardware Diagram:



Hardware Diagram Description:

In the block diagram we can see a high-level representation of the system's different components. Essentially there will be multiple microcontrollers (MCUs) that will control various functions. In the diagram proposed there will be a high level MCU with the facial and voice recognition software loaded onto it. A camera and microphone will also be connected to this microcontroller via usb chords. This MCU will be connected to the system controller, or central MCU via an I2C communication protocol. Additionally, there will be an external sonar sensor and LED status lights which will be controlled by the main MCU. An external LCD touch screen keypad will be connected to a processor which will take user inputs as well as display messages/prompts to the user. A speaker will also send verbal messages/prompts to the user. Lastly the deadbolt will be controlled by the central MCU using a WiFi connection.

Software Diagram:



Software Diagram Description:

A use case diagram is provided which displays multiple options for a user while interacting with the system. They will be able to use facial recognition, voice recognition, a touch screen keypad to unlock the door, and LED status lights will be visible. If the two-factor authentication protocol is validated then the door will unlock and the LED light will turn green. If it is not validated then the door will not unlock, and the LED will turn red. If a password is provided by the keypad then the door will unlock and toggle the LED. A speaker will allow the system to greet the user if they are authenticated. Once the door is unlocked the user will open the door, close it, the door will lock, and the LED will revert back to white symbolizing that it is ready for new inputs.

3. Research and Investigation

This section describes the research process that was conducted in order to develop this project. Existing products on the market with similar features were studied to successfully design a working system prototype.

3.1. Existing products

In spite of the fact that smart locks have already been produced by many companies and have been available on the market for a couple of years, our team believes that trying to design our own lock is a great learning opportunity. Investigating some existing products can help us learn about the involved technology and shine the light on the system flaws. This could inspire us with great solutions and lead us into creating better designs. For the purpose of this project research, multiple products were reviewed. We're to focus on three products similar to our idea.

3.1.1. US:E Camera Smart Lock by Elecpro Group Inc.

The US:E Camera Smart Lock allows the user to access the door in multiple ways, smartphone, password, figure print, key fob, physical key and facial recognition. The company created two version for this lock. The user can choose either the password or the facial recognition option. For the facial recognition version, the lock comes with a built-in infrared 3D recognition technology and 4 AI recognition levels, which guaranties face recognition in daylight or night and allow the user to unlock the door with a look to the camera. US:E has the capacity to store up to 100 faces, and can't be tricked by photos or videos. The facial recognition version supports palmprint recognition as well. As in many other smart locks, US:E lock uses a mobile app which allows remote control of the lock, and also helps monitor the surroundings.

The password version has a wonderful security feature, which gives the user the freedom to type any random combination before or after the correct code and the door lock would still recognize the password and opn the door as long as it was typed in the right order. This feature is great to use when theuser have company

and doesn’t want to reveal the passcode to others. This lock also comes with fingure print scanner, and a double verification mode where the door can only be unlocked when two unlocking methods are verified.
The release of this lock is coming up in May 2021 which will take smart locks to a different level of security.

3.1.2. Camera Smart Lock by Gate labs

The Camera Smart Lock is an all in one security system. It replaces smart doorbell, lock, and security cameras. The camera has a motion sensor for activation, which only start videotaping whenever the sensor detects a movement around the door. The system also includes a two-way audio which allows the owner to interact with someone at the door. The lock has a built in Wi-Fi which can be connected to the house network for allowing automatically updating the system and also upload the recorded videos.

The system also includes a phone application which allow remote access to the door to lock/unlock as needed while the owner is away. It also could be used to create individual passcodes to grant authorized people access to the house. In addition, the lock sends notifications through an app whenever a movement around the door is detected.

The Camera Smart Lock has an easy installation process, it can easily replace any traditional lock and it fits all standard exterior and interior doors. After installation the user only has to download a mobile app and connect the mobile with the smart lock.

3.1.3. FL1000 by ZKT ECO

FL1000 was the world’s first smart lock to use facial recognition technology. It has four unlocking mechanisms face, password, card, and a traditional key which can be used to override the door in case of emergencies. The lock comes with a 3-inch capacitive touch screen, camera, home button, power button, key cap, reset button and emergency power connector.

The touch screen provides higher security than a regular keypad since a touchscreen prevents fingerprint code detection which is possible on a button keypad. The system is capable of recognizing up to 100 faces, storing 100 password and RFID cards and has a log capacity of 30000. This lock has a smart alarm feature which notifies the owner in case of unauthorized activities or if the battery is running low. The lock also supports time zone management which allow visitors to enter only at specific times chosen by the owner. FL1000 smart lock is powered by the building, but also have an emergency power connector which can draw power from 9V battery in case of losing power.

ZKT ECO also produces ZM100 which is a smart lock with hybrid biometric recognition technology. Which provides two unlocking mechanisms. Face and fingerprint. It comes with a 2.8 inches capacitive touch screen and SilkID fingerprint sensor that can perform a live fingerprint detection. Equipped with a double HD camera that uses ZK face algorithm, The lock performs 3D face scan for high speed verification, and an accurate recognition at the dark. ZM100 uses a rechargeable lithium battery which can last up to a year when fully charged, but also has an external terminal to draw power from 9 volts battery.

3.2.Similar Designs

To advance our team knowledge, research for similar designs on UCF senior design website was conducted. Two similar projects were found and studied in order to develop a better understanding of the performance for these types of smart locks.

3.2.1. Smart Lock Fall 2019

From the graduating class of fall 2019, group 6 designed a smart lock system. Their goal was to come up with a system that replaces security cameras and help provide better protection to homes and business with a reasonable price. The smart lock was designed to grant the user access by facial recognition, mobile app, backlit LCD touchscreen, RFID and Fingerprint identification.

The facial recognition feature was only enabled when all the other authentication methods fails. A camera connected to the system would capture the person attempting to gain entry and compare it with the authorized people pictures uploaded to a database. If access permeation were denied the camera will then take a photo of the person and send it to a mobile app. Once a picture is received on the app; the user can then choose to unlock the door or keep it locked.

A backlit touch screen was used to allow users to key in their password, the screen lights at night to allow clear vision of the digits. Passive RFID and a fingerprint reader were used to allow fast access by swiping a card or simply place the thump on the scanner. A temporary password can be created through the mobile app and can be used by any authorized user. The team suggested to keep other ways of entry specified to the household members. The system is capable of storing the date of a 100 user so multiple people access doesn't overwhelm the system.

Smart lock is user friendly; installation time is estimated under 2 hours. The lock is also power efficient, where all authentication methods were set to low power mode for low power consumption purposes.

3.2.2. Keyless Entry Fall 2019

In the same graduating year of Fall 2019, another group worked on the same idea of smart locks. Group 11 goals were to provide a competitive design for a smart lock that increases security and accessibility to homes while keeping the cost to minimum.

Keyless entry smart lock provided different access methods. RFID, fingerprint, keypad, and a mobile app. These were all methods that doesn't require the user to use a traditional key, which was the aim of this project. The used RFID sensor operates at 13.56MHz which is a secure frequency that is used for financial transactions. The capacitive fingerprint reader provides another secure way of entry since it's immune to photo impersonation of fingerprints. A keypad and mobile app were also used as in the discussed previous products.

An accelerometer was also used to serve as another way to gain entry by using a sequence of door knocks, but also provides a safety feature by notifying the primary user in case of forced entry. Because of size constrains the team choose four AAA batteries to power the lock, these batteries are recyclable and easy to replace. A record of the door lock activities is available on the mobile app and can be used to better monitor the lock.

3.3. Related Technology's

In this section we're to discuss the different technologies related to our project and justify the reason to pick one technology over the other.

3.3.1. Bluetooth Vs Wi-Fi

Bluetooth uses short-range radio waves to transmit signals within paired devices and does not require internet access. Wi-Fi also uses radio, but it connects to the internet using a router. Generally, Bluetooth has lower power consumption than Wi-Fi, but it is less secure. Bluejacking attacks and Bluesnarfing attacks can transmit and receive data without permission. Wi-Fi can support more users at the same time and it has a longer range than Bluetooth, but modern Wi-Fi uses a higher frequency.

3.4. Components Research

In this section we're to discuss the components used in our project and the research that was done in order to pick the right parts. The work was divided between the team members and each member conducted their own research.

3.4.1. Occupancy Sensor

Different technologies are used to detect the presence or absence of an object in a space. The two main types of motion sensors are active and passive sensors. The active sensors are a radar-based motion sensor. They radiate a radio wave or microwave across the area and wait for the signal to be detected upon reflecting after the wave hits an object. The sensor mechanism is basically to detect the frequency shift in the returning wave which indicates that the wave did hit a moving object. After that the sensor sends an electrical signal to the operating device such as a light or an alarm system. On the other hand, passive sensors, simply detect the infrared energy emitted by a living being. These sensors can be set to detect the motion of an object within some level of emitted heat to avoid triggering the alarm when an animal is moving within the detection area.

Passive infrared (PIR), ultrasonic and many other sensors are all methods to spot a moving object within a specified range. Acoustic detection is also used in some sensors. A comparison between the different technologies was conducted in order to select the right sensor for our project needs.

Microwave sensors use Doppler radar to detect motion. The sensor generates and electromagnetic field between the transmitter and receiver creating a hidden volumetric detection zone. A continuous wave of microwave radiation and phase shift is emitted in the reflected microwave due to the motion of an object which results in a change in the signal at low audio frequency.

Ultrasonic sensor is a good example for the active sensors, it sends out an ultrasonic wave into a medium and measure the speed needed for the wave to return in order to detect the presence of a person. This sensor can cover the entire space and doesn’t need a line of sight which allows it to detect people behind an object. Ultrasonic sensor is very sensitive to motions, which makes it suitable for applications in open spaces since the ultrasonic sensor doesn’t require a line of sight.

Tomographic Motion sensors detect the change in radio waves as they travel from node to another in a mesh network. This sensor emits radio waves at a frequency able to pass through walls, which makes it very valuable in application that needs to scan large areas since its able to sense the presence of a person behind walls or large objects.

Passive infrared sensor (PIR) works by sensing the difference between the heat emitted by a moving person with respect to the background heat. It’s called passive because the sensor doesn’t emit energy. For PIR sensor, line of sight between the sensor and the object is essential which can be problematic for some applications. This sensor is suitable for applications in enclosed places, where low level of motion is needed.

While PIR sensors are good in detecting a general movement, they can't provide any other information about the object. To gain more information active infrared sensors are used. Active infrared sensor works by using a dual beam transmission as structure. Where the transmitter is responsible for shooting an infrared Ray (light beam) to an in-line receiver, the receiver sees the IR beam and send a motion detection signal if the beam gets interrupted. Some active IR sensors uses a transmitter and receiver facing the same direction, and very close to each other which allow the receiver to detect a reflection of the object in the monitored area.

Video Camera software is another method used for motion detection purposes. This method is highly valuable when the application purpose is to record a video after being triggered by a movement in the monitored area. the output of the camera can be used to detect motion using software. Video camera software can be used with infrared illumination to detect movements in the dark.

Dual technology motion sensors, combining multiple technologies into one sensor can help reducing false triggers but it comes at the cost of increasing vulnerability.

4. Project Budget & Financing

Currently our group does not have any funding from a sponsor, we will be funding the project out of our own pockets. Below shows a preliminary/rough estimate of our budget that will be fluid throughout the first semester during Senior Design 1. We tried to overestimate costs so that we can come in under budget.

Equipment	Cost
MCU's (possibly more than 1)	$200
Camera	$30
Keypad	$20
Broken "August" Lock	$40
Custom/Populated Circuit Card Assembly	$50
General Jumper Wires for Peripherals	$20
Speaker	$30
Microphone (x2)	$50

Total:	**$440 - $110/member**

5. Initial project Milestone for both Semesters

The milestone section is divided into two parts, the first part is to be concluded in senior design 1 (Spring 2021), and the second part is to be continued in senior design 2 (Summer2021). In order to meet the deadlines for our Smart Door Security System, milestones were set at the beginning of the semester as shown in the two tables below. According to the class syllabus, specific dates were set to ensure our project design gets finished on time. Since each group member is required to write at least 30 pages, setting deadlines can help us keep track of our progress and can be used as a guideline for weekly goals to be met.

Number	**Task**	**Duration**
	Senior Design 1	
1	Creating Groups	Jan 11 – Jan 17
2	Brainstorming	Jan 18- Jan 22
3	Initial Doc- Divide and Conquer 1	Jan 23- Jan 29
4	Research & Documentation	Jan 30- Feb 6
5	Initial Doc- Divide and Conquer 2	Feb 7 -Feb 12
6	60 pages Draft	Due Apr 2
7	100 pages Draft	Due Apr 16
8	Final Document	Due Apr 27
	Senior Design 2	
10	Build Prototype	May 21-June 4
11	Test & Redesign	July 10-July 24
12	CDR Presentation	June 25
13	Final Presentation	July 25
14	Final Report	July 30
10	Build Prototype	May 21-June 4

While still in senior design 1, the exact days for senior design 2 are not known yet. This table is to be updated once the deadline requirements for senior design 2 are set.

References

[1] [Online]. Available: https://www.kickstarter.com/projects/1624790698/us-e-camera-equipped-smart-lock-with-facial-recogn
[2] [Online]. Available: https://smartlocksguide.com/best-smart-lock-with-camera/
[3] [Online]. Available: https://www.zkteco.me/product-details/fl1000
[4] [Online]. Available: https://www.zkteco.me/product-details/zm100
[5] [Online]. Available: https://www.ojismart.com/product/zm100-face-fingerprint-lock-copper/
[6] [Online]. Available: http://www.ece.ucf.edu/seniordesign/projects.php
[7] [Online]. Available: https://www.thomasnet.com/articles/instruments-controls/all-about-motion-sensors/
[8] [Online]. Available: https://www.frontpointsecurity.com/blog/best-motion-sensor-for-home-security#:~:text=Unlike%20active%20sensors%2C%20which%20detect,signals%20radiated%20from%20living%20beings.
[9] [Online]. Available:
[10] [Online]. Available:
[11] [Online]. Available:
[12] [Online]. Available: