Final Documentation

The SMOCK Lock

University of Central Florida
Department of Electrical and Computer Engineering

Dr. Lei Wei
Senior Design I

Group 39
Kenneth McDonald – Computer Engineering
Gabriel Couto – Computer Engineering
Matthew Navarro – Computer Engineering
Eric Sayegh – Computer Engineering

Table of Contents

1.0 Executive Summary:

The lock will have many functionalities, allowing for multiple tiers of security. The lock will have a regular key which would provide access in case of a network or power failure, facial recognition, as well as a fingerprint scanner. Depending on the level of security the owner wishes to use, it can require one or more methods of verification, such as a key and fingerprint scan being required for entry. This will all be configurable in an app that communicates with the lock. The app will not only let users configure the level of security, but also provide a way to designate other people who are authorized to unlock the lock (such as family members, or close friends). The app will also provide notifications to the owner regarding important events, such as an unrecognized person who is attempting to enter. In order to ensure a customer's safety, the door can be set to auto-lock after it has been unlocked and can be set by the customer using the locks app.

Essentially the process of how the SMOCK Lock would start would be like this: A visitor/guest will approach the door, the some type of Infrared Sensor will detect motion and provide power to all the other parts, if it's the visitor/guests first time being seen by the SMOCK Lock the app will not be able to determine who is at the door, but will still send a notification to the homeowner that someone is at the door. Since this is the visitors first time seeing the SMOCK LOCK the fingerprint scanner would not be able to allow access for the visitor.

If necessary, the homeowner can inform the visitor to leave the premises without actually having to be home, with the use of the Speaker inside of the lock casing. After letting a visitor/guest that the homeowner recognizes and knows he now has the option of giving the them access to the lock app and could even add him as an owner-level account. With this the new smart lock member can add their fingerprint so that the scanner recognizes their fingerprint. The database/server will take care of all the necessary computation, the only thing the microcontroller will have to do is get the feedback from the database/server and act accordingly, if there are no matches keep the door locked, if there is a lock notify the homeowner or allow access to the home.

The idea is to have the app very customizable and give the homeowner all the power when it comes to adding and removing new members. The homeowner will essentially be granted a Master Key with their fingerprint and facial features. The homeowner also has the chance of holding onto a electronic key that will be able to provide access to the home.

The SMOCK Lock should provide easy to use and secure technology that will allow people to feel safe at their homes, travels, or commercial properties.

2.0 Project Description

The purpose of this section is to provide a detailed description of this project. This section will describe our motivation, goals, objectives, hardware and software requirements, the house of quality diagram, and our project block diagram. This will speak upon why we want to design a lock, and what we hope to provide/achieve. This section speaks about what some of the requirements for our hardware and software are such as what we need to achieve our goals and objectives. The house of quality diagram speaks on our values and what we deem quality parts and a quality product. The project block diagram will show who worked on what part of the project.

2.1 Project Motivation and Goals

The motivation behind our project is that we as a group value safety in our homes. With this lock we would essentially provide that. The lock would contain a camera that can provide us a view of the visitor. After the user evaluates who is at the door, the user is then able to accept or deny entry into the home. This can even be done if the user is not home. The lock would be connected to the home network and with the use of an app the user can communicate with our lock from anywhere. Through the speakers, the user would be able to hear instructions if they were to be sent auditorily. We hope to use this lock in any scenario whether it be hotels, commercial properties, or a private residence.

The goal of our project is to create a lock that provides multiple secure ways of entry. The lock would provide owners an option to allow visitors entry to their home without the need of having to be there personally, all of this could be done from any location as long as you have your phone and are given owner privileges in the app. We are aiming to create a reasonably priced lock that includes biometric features to unlock such as face recognition, and fingerprint scanning. We also want to allow for the lock to communicate with the owner. An app would be required that would provide access to the lock via Wi-Fi, that can be downloaded onto a mobile device to configure settings and provide notifications to the owner.

2.2 Project Objectives

The objectives for the project would be to design a lock that would provide a homeowner with a secure lock that would allow you to allow access to anyone to your home from anywhere as long as they have the homeowner’s approval. We want to make a lock with many security features that would still be affordable to most homeowners, with an app that would simplify everything there is to do. The quality of the lock would still be very great, however there are many ways we think that we could separate ourselves from the rest of the locks out there. Our product along with our app would be very easy to install and set up. Instructions will be very clear, and the homeowner will be pleased with the extra security that our lock provides.

2.3 Requirements:

Listed below are all the requirements that are required and set by the group to design and build a smart lock.

The overall size of the casing is going to limit the size of all the other parts, which is the reason we have to carefully decide what size casing we will use. It must be able to be mounted on a door, we are hoping to keep the size of the system and casing to 10”x6”x4”. It must be easy to use to all homeowners, especially because there are many homeowners who are not comfortable with operating technology.

The power consumption must be able to be powered by a 9V battery. We’ve decided to use batteries instead of using electricity from the house because we want our product to have no wires. A wire would also cause a potential tripping hazard. We are also hoping to use a some type of Infrared Sensor in conjunction with a low power mode from our micro controller, which will allow us to only have the Infrared Sensor powered until it detects motion. This would allow us to save a lot of power, considering we wouldn’t have to power all of our biometric features constantly.

Network Capability is a must, without the network capability the lock won't be able to function properly. We must be able to connect to the internet so that the camera can send images to our database/server which then process the visitors face to determine who it is. That would imply the visitor has been seen before and has been given a name on the app. A speaker will be included in our SMOCK LOCK which will be used to communicate with the owner as well as potentially greeting the visitor upon their arrival.

A Fingerprint Scanner makes up another one of our biometric features, which will be able to match a person's fingerprint on the database to deny/allow access to the home for the visitor if they are registered with the homeowner. A neat feature which will allow guests to come and go without the need of a key.

Another requirement that we have set is that in case of a power failure, the lock will go into a low power mode where the only thing that is powered is our RFID sensor, which will be able to unlock and lock the door.

The table below provides a more brief overview of our hardware requirements.

Table 1.1: Hardware Requirements

#	Requirement	Description
1.1	Size	The system shall be able to fit into a to be designed casing that will be mounted on a door. Targeted at 10”x6”x4”.
1.2	Ease of Use	The system shall be user friendly so that anyone can use the lock, set up time should be less than 10 minutes (not including installation of actual lock).
1.3	Power Usage	The system shall provide power for at least 2-3 months. Output Power Targeted for 10W.
1.4	Network Capability	The system shall be able to communicate with server through network module
1.5	Relay	The system shall have a relay to be used for supplying power to the lock mechanism
1.6	Camera	The system shall have a camera to identify a person's face
1.7	Speaker	The system shall include a speaker to welcome the visitor as well as to hear the owner of the lock.
1.8	Fingerprint Scanner	The system shall include a fingerprint scanner to be used to unlock the door by accepted fingerprints (95% accuracy)
1.9	Back-Up Key	The system shall include a key to be used to unlock the door in case of network or power failure.
1.10	Power Supply	The system shall include a power supply capable of holding charge that will allow us to not need recharging or replacing for at least 2-3 months.
1.11	Microcontroller	The system shall include a microcontroller to communicate with each hardware component as well as to supply power to them.
1.12	Casing	Big enough to fit all the components of the lock. Targeted at 10”x6”x4”.

Some of the software requirements that we have set are that we must use a server that would communicate between the app and the microcontroller. This will serve as the bridge between them, The microcontroller will communicate with the server which will then update/view the database. The database will contain facial scans, audio filles, fingerprints, names, access level, and a few more features.

Our implementation of Computer vision should allow for an accuracy of at least 75%, it will compare pictures of the returning guest compared to an image that has been previously saved. Our Fingerprint detection shall be able to read fingerprints and be at least 95% accuracy. The fingerprints can be registered with the app to a specific user if the homeowner would like to do so. The SMOCK Lock would require a simple and easy to manage app, homeowners should be pleased with the quality of the application and the fast and easy process required to manage and customize their lock.

Table 1.2: Software Requirements

#	Requirement	Description
2.1	Server	The software shall include a server to communicate between the app and the microcontroller.
2.2	Database	The software shall include a database to store data like facial scans, audio files, fingerprints, names, etc.
2.3	Computer Vision	The software shall include a computer vision module to allow for facial recognition with an estimated accuracy of at least 75%
2.4	Fingerprint Detection	The software shall include a fingerprint detection module to scan and detect users fingerprints with an estimated accuracy of 95%.
2.5	App	The software shall include an app that will allow the user to manage and customize their SMOCK

2.4 Specifications

In this section we will discuss the specifications that this project has, such as power, safety, Wi-Fi, Mobile Application Features, Facial Recognition Camera, Fingerprint Biometric.

2.4.1 Power Specification

The primary source of power that will be supplied to the lock will be batteries. Most likely a 9V battery will be used but we are still exploring other options. We would have liked to use a direct power source, but we determined it would be inconvenient for a user to install a wire going across the door to hook up to the lock. Using a direct power source would also limit some users from purchasing the lock since some houses do not have outlets right next to the door. We also would've needed to design some sort of cable management system for when the door opens so it wouldn't pull the cable out of the wall. We also plan to use a backup battery incase the power is loss from the batteries. If the batteries are low, we plan to have the app alert the user, so they know when to change the batteries.

2.4.2 Safety Specification

Our lock will have a casing so no exposed wires will be shown. This will help prevent any electrical or mechanical injuries that could be a result of any electrical problem that can arise. Each component will be mounted to the casing so that there will be no free moving parts. The lock will contain the lighting needed to be able to see at night. Most of the circuit configuration will be printed on a PCB that will be mounted to the enclosing. The enclosing will be designed by us and will be produced by 3D printing. The door lock will consist of two pieces where each piece will be attached to each side of the door.

We have several other safety features that will have their own designated specification section such as Facial Recognition Camera, and Fingerprint Biometric which both play a crucial role in the security of the lock.

2.4.3 Wi-Fi Specification

The lock will upload pictures to the server via Wi-Fi. Once the camera takes a picture of a user or a snapshot of a live feed, it will directly upload the image to the server over Wi-Fi. The other components such as the fingerprint sensor will be connected to the microcontroller and will be upload via Wi-Fi through the controller. The controller and the server will communicate to and from each other over Wi-Fi. The mobile app will also communicate to and from the server over Wi-Fi. The security of theses Wi-Fi connections will be determined based on the user’s home Wi-Fi security. We recommend using WPA2 for a Wi-Fi network security protocol. As it is arguably the most secure internet protocol.

2.4.4 Mobile Application Feature Specification

We intend for our mobile application to be ran on the two largest mobile operating systems in the US, Android and iOS. The mobile application will allow for users to create an account. With an account, a user can set up a facial scan, fingerprint scan, and other configurable settings. The user is also able to add guest passes to their account that they are able to send to guest to use for entry. There will be tiers of security that can be set up. For example, the owner can require a facial recognition along with the RFID scan to allow entry. Data will be communicated between the database and application through a server in the form of JSON packages.

2.4.5 Facial Recognition Camera Specification

One of the security authentication methods is facial recognition. The user at the door will need to stand in front of the camera. From there the camera will either use live feed video or take a picture of the person and will detect a face of the users in the video or picture. From there the detected faces will be compared with saved faces that are stored in the database. If a match is found, the door will unlock, and the user will be entered. If a match is not found, the picture will be sent to the owner of the household through the mobile application and the owner will need to determine if the user can enter. If so, the picture will be stored in the database. We hope to implement a feature where the database will store the best 10 facial images of a person, and if better facial data is found when entering, the worst facial data will be removed from the database

2.4.6 Fingerprint Biometric Specification

Another form of security authentication that is to be included with our lock will be fingerprint recognition. The fingerprint sensor will read a user's fingerprint, process the data into an image and will send the data to the microcontroller. From the microcontroller the data will be sent to the server to be compared with the stored fingerprints in the database. If a match is found, the door will unlock, and the user will be entered. If a match is not found, the owner will be alerted through the mobile application that there is someone at the door who entered a fingerprint that is not in the database. If the owner wants to let this user in, the fingerprint will be saved to the database to be used for comparisons in the future.

Table 2.1: Specifications Description

Specification Number	Specification	Description
2.4.1	Power	A 9V will be used to power the system.
2.4.2	Safety	The casing will leave no wires exposed.
2.4.3	Wi-Fi	The Wi-Fi module must be able to allow the camera to upload pictures to the server/database
2.4.4	Mobile Application Feature	The app will be accessible for both iOS and Android, as well provide an interface to manage all the security features for the homeowner.
2.4.5	Facial Recognition Camera	The Facial Recognition Camera will upload a video or series of images to the database which will then be used the following visit to compare the visitor with previous visitors.
2.4.6	Fingerprint Biometric	This security feature will read a person's fingerprint process the data into an image and will send the data to the server through the use of our microcontroller.

2.5 House of Quality:

The House of Quality resembles what we value in a Smart Lock. Such as Safety, Installation, Cost, Accuracy with Biometric features, and Power Efficiency.

With safety, we decided to break it up into three different sections, the Auto-Lock Feature, Back-Up Key, and Software Security. Each of these three we value highly, the auto-lock feature is something we find very important. Sometimes people forget to lock their doors, it's reassuring to know that your lock will automatically lock if you forget to do so. A back-up key is also very important, and we believe it’s the most important safety feature, if for some reason a component fails, or the lock gets stuck in power mode, or the battery is dead you will still be able to gain access into your home. Software security is also very important, you would not want someone hacking into your smart lock and gaining access into your home.

Installment Ease with the Smart Lock is another category we looked at, and we broke it up into three categories: Size, Setup Time, Easy to Use App. We value these relatively high as well but not compared to our earlier section Safety. The size should be relatively small, however big enough to house all of our components. At the end of the day I'd value my safety higher than the size of the lock. The Short Setup Time is something we value as well, but it's a little harder to scale due to the large variations in people who would be using our lock. Some people might not be good with tools, and it will still take long, however we would hope that are setup time is under 30 minutes. That includes removing the old lock, as well as installing the app and setting up all the security features. The Easy to Use App is probably our highest rated section in this category, we think it's very important to be able to have people who are not comfortable with electronics to still be able to feel secure and know how to get around the app.

Our next category is Cost, this category we feel is pretty universal. Everyone would like for the product to be less expensive, and we feel the same way. We want homeowners to feel like it was worth the price, whatever that price may be set to.

Accuracy is without a doubt our highest rated category. It's important that all of the biometric features involved in the Smart Lock are all as accurate as possible so as to not provide access to people who are not registered to the home. The Facial Recognition is very important, the camera is intended to be able to name the visitor at the door. The Fingerprint scanning is another biometric feature that needs to be very accurate, with the owners fingerprint the door will be unlocked.

The Power Efficiency category can be summed up into two sections, a long life cycle and low power consumption. Those two go hand in hand however we hope to provide a long life cycle as to not have the owner constantly replacing the batteries. With a low power consumption comes a longer life cycle, we believe however that low power consumption is not highly desired. However a lower power consumption would imply that the components are not constantly being used/overworked which would provide the components to have a longer life span as well.

Now something to consider when creating a House of Quality is how these categories and their sections relate to each other. Such as Cost and Accuracy the products with better accuracy cost more. When a product is higher in price an assumption is made that the product must use great technology or is simply a great product. Cost and Safety, the more secure and safe the product is the more the product would be worth. Safety and Accuracy, the safer the product would also imply that their security features are more accurate. Power Efficiency and Accuracy, The more accurate the features are the more power they will require. Installment Ease and Cost, when someone pays for a product that's expensive the last thing people would want to deal with is a product that is difficult to assemble.

We are aiming to have an output power of 10W, a Size of 10”x6”x4”, an app that is both compatible with iOS and Android, a Facial Recognition that is at least 75% accurate, a Fingerprint Scanner that is 95% accurate or above, a cost of less than $200, and an Installment Time of less 30 minutes, along with a Power Efficiency greater than 50%.

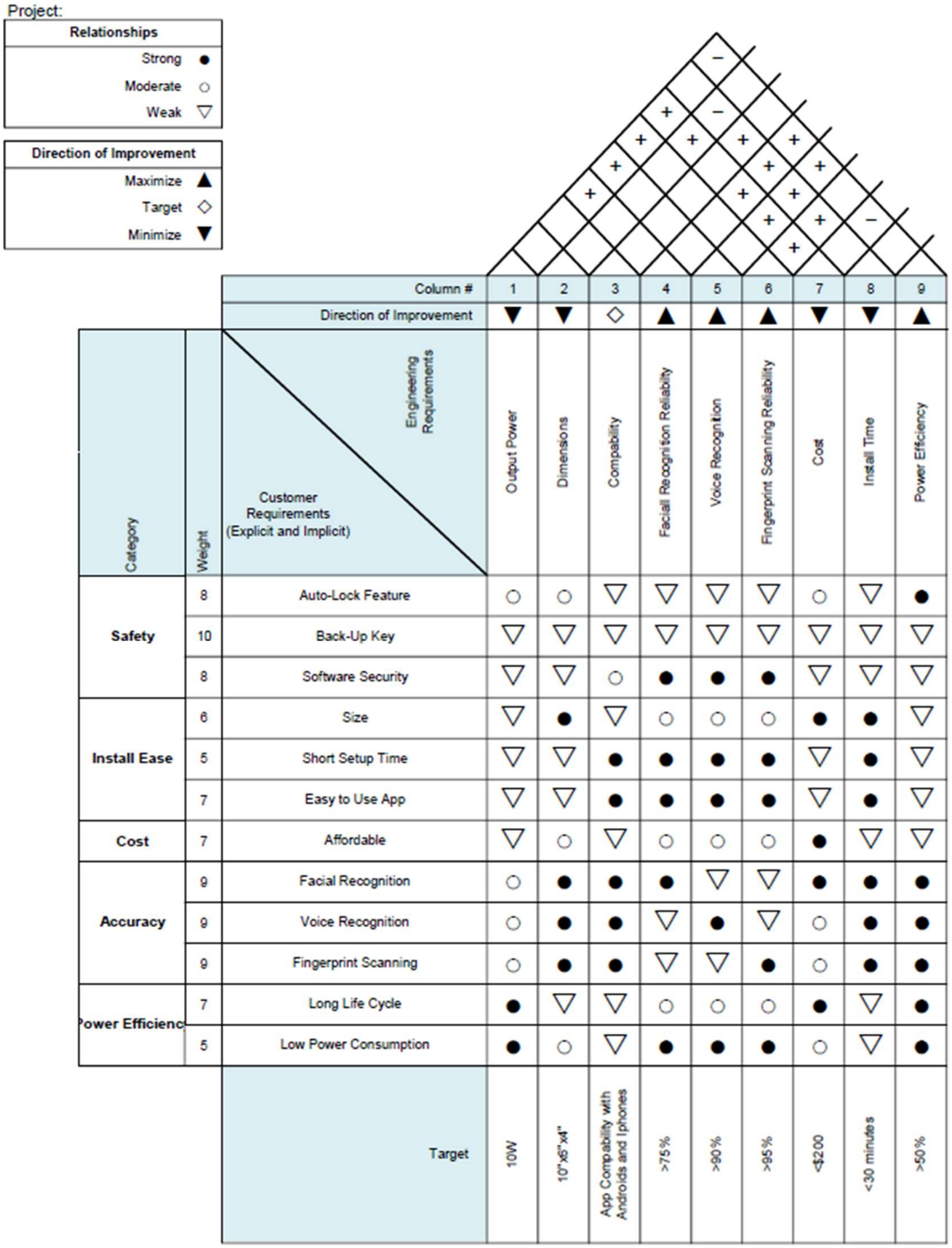
A Figure of the House of Quality is in the following page.

2.6 Project Block Diagrams:

Our group is composed of four Computer Engineers: Eric Sayegh, Kenneth McDonald, Gabriel Couto, and Matthew Navarro. We have decided to divide our project into two parts Hardware and Software and have designated components/software application to our group members.

Eric will be leading the research of the power supply unit, the power supply unit must be able to power the microcontroller, motion sensor, Camera, Speaker, Fingerprint Scanner, Network Adapter, as well as the Infrared Sensor. The motion sensor must be able to properly detect when someone approaches the door in order for low power mode. He is also going to be the lead developer of our easy to use and highly functional app that is compatible with both iOS and Android. Along with the app development he will also be developing the software used in the microcontroller.

Figure 1: House of Quality



Project:

Relationships	
Strong	●
Moderate	○
Weak	▽

Direction of Improvement	
Maximize	▲
Target	◇
Minimize	▼

Category	Weight	Column #	1	2	3	4	5	6	7	8	9
		Direction of Improvement	▼	▼	◇	▲	▲	▲	▼	▼	▲
		Engineering Requirements / Customer Requirements (Explicit and Implicit)	Output Power	Dimensions	Compability	Faciall Recognition Reliability	Voice Recognition	Fingerprint Scanning Reliability	Cost	Install Time	Power Efficiency
Safety	8	Auto-Lock Feature	○	○	▽	▽	▽	▽	○	▽	●
	10	Back-Up Key	▽	▽	▽	▽	▽	▽	▽	▽	▽
	8	Software Security	▽	▽	○	●	●	●	▽	▽	▽
Install Ease	6	Size	▽	●	▽	○	○	○	●	●	▽
	5	Short Setup Time	▽	▽	●	●	●	●	▽	●	▽
	7	Easy to Use App	▽	▽	●	●	●	●	▽	●	▽
Cost	7	Affordable	▽	○	▽	○	○	○	●	▽	▽
Accuracy	9	Facial Recognition	○	●	●	●	▽	▽	●	●	●
	9	Voice Recognition	○	●	●	▽	●	▽	○	●	●
	9	Fingerprint Scanning	○	●	●	▽	▽	●	○	●	●
ower Efficienc	7	Long Life Cycle	●	▽	▽	○	○	○	●	▽	●
	5	Low Power Consumption	●	○	▽	●	●	●	○	▽	●
		Target	10W	10"x6"x4"	App Compability with Androids and Iphones	>75%	>90%	>95%	<$200	<30 minutes	>50%

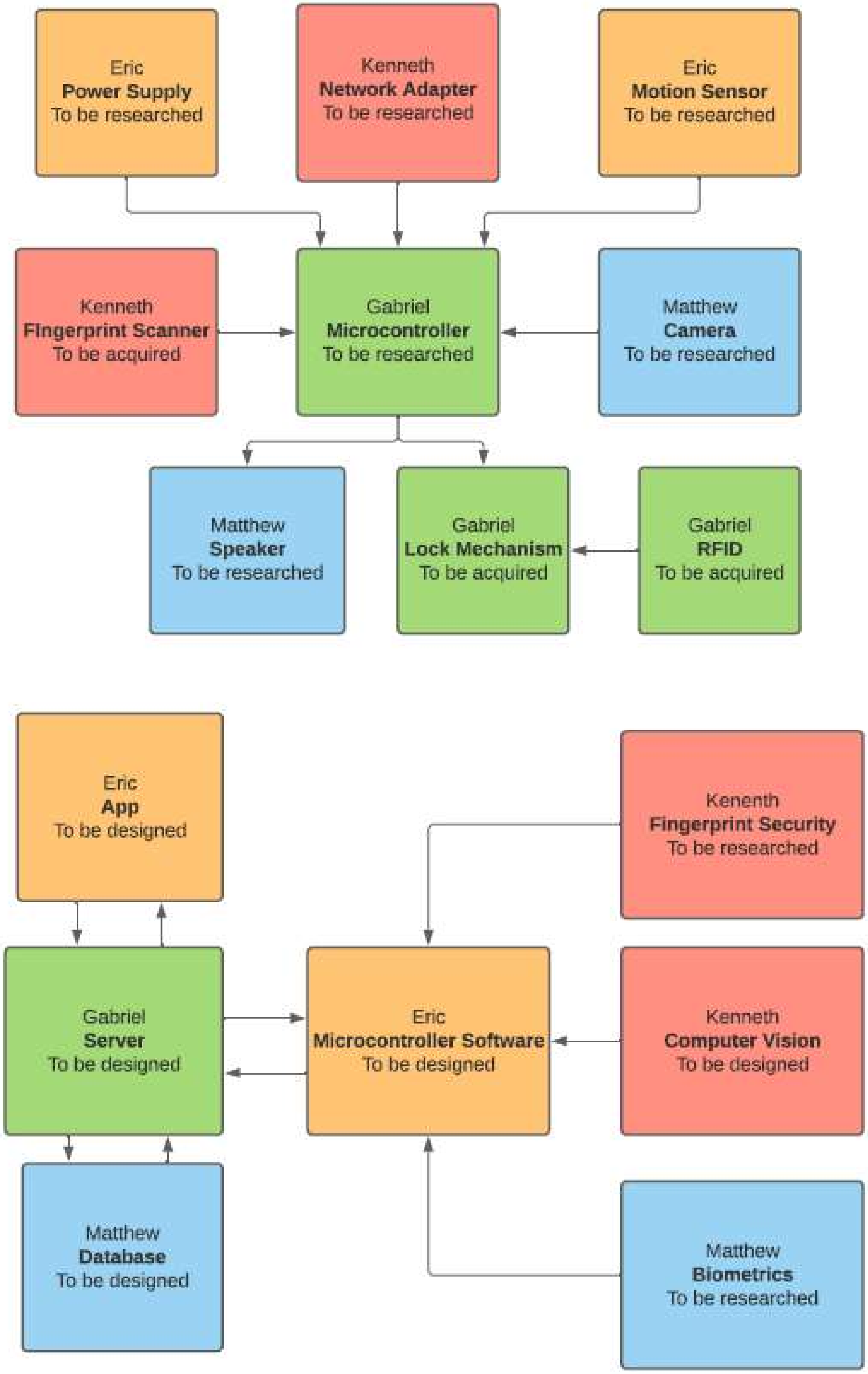
Kenneth will be researching the Network Adapter, we must be able to communicate with the server, at a relatively quick speed. The fingerprint scanner is to be required and tested as well, a sensor that will be accurate and able to send results to the microcontroller which will then send those results to the server. In the software section, Kenneth will be designing and implementing the computer vision needed for the smart lock to function as intended.

Gabriel will be researching which microcontroller provides a simple to use yet complex decision making, that will be able to regulate ample power to the components used in this lock. Gabriel will also require our lock and RFID, as to the software section, Gabriel will take the lead in designing a server that will be able to handle the requests made from the microcontroller as well as providing the microcontroller with responses to those requests.

Matthew will be researching the Camera necessary to provide the microcontroller or server directly with images so that they can be processed, the speaker is something else that must be researched, this will allow the visitor at the door to be able to hear the owner. In the software section, Matthew will be leading the development of the Database as well as researching the necessary biometrics, such as how to implement the necessary fingerprint accuracy as to not allow an incorrect finger to unlock the door.

For a figure explaining this section please look at Figure 2.

Figure 2: Project Block Diagram



3.0 Research Related to Project Definition

In this section we will be discussing Existing Similar Projects and Products, Relevant Technologies, Part Selection and Comparison, and Part Selection Summary.

3.1 Existing Similar Projects and Products

In this section will be discussing the iView FL400 a Facial Recognition keyless smart door lock, the eufy Security Smart Lock which is a Smart Lock that has very similar features to the SMOCK LOCK, The ROMIX 5 in 1 Smart Keyless Door Lock, the ULTRALOQ UL3 BT 2nd Generation Smart Lock, and the Lockly PGD728FSN smart lock. After researching all the existing products, we feel that as long as our smart lock is priced under $200.00 we will be providing a great product for a low price compared to the competition.

3.1.1 iView FL400

The iView FL400 Facial Recognition keyless smart door lock is a deadbolt lock that includes a built-in infrared camera to conduct facial recognition as well as provide nighttime vision. The lock includes multiple unlocking modes including facial recognition, id card, passcode, and key card. Backup keys are also provided as a failsafe in case other methods of entry fail. The facial recognition process also includes checks for unauthored users attempting entry through photos or videos of an authorized person. This is done through an infrared illumination check, which will be used to detect if a screen is Infront of a camera. It also includes a liveliness detection check to prevent the use of printed images. Up to 100 users and 50 faces can be stored in the lock. The lock claims a battery life of up to 1 year in standby mode. The iView FL400 is available for $229.99.

3.1.2 eufy Security Smart Lock

The eufy Security Smart Lock makes use of 4 methods of entry. The main method of entry advertised is the fingerprint biometrics. eufy states that the door lock can recognize your fingerprint in 0.3 seconds and can unlock the door in 1 second. They store fingerprint data locally instead of on the cloud for increased security and to keep personal information safe and private. They also state the elderly and young children should not make use of the fingerprint detection due to the changes our fingerprints go through during these life stages. The second form of entry is through the use of the keypad. They do not provide much documentation on keypad entry but it is safe to assume that you can program a combination of keys to unlock the door. The third form of entry is through the eufy security app. This app seems to provide a simple interface with controlling your door lock. You can also unlock your door through the app as long as you are connected through Bluetooth and within 150 feet of the lock. The fourth form of entry is a back-up key.

The front of the lock has a cover that blocks the keyhole and can be moved when needed. The lock also consists of an automatic locking feature with a built in sensor that detects when your door is closed and locks it automatically. This lock is priced at $250.

3.1.3 ROMIX 5 in 1 Smart Keyless Door Lock

The ROMIX 5 in 1 smart keyless door lock is a smart lock that has 5 methods of entry. These include facial recognition, fingerprint, password, mechanical key, and smart IC cards. This lock can store up to 100 facial captures, fingerprints, and IC cards. It can hold up to 5 passwords as well. The lock has a mode that allows for any length of code to be put in and as long as it contains the correct passcode embedded in the string it will unlock. This was implemented to prevent people looking at the wear and tear of the numpad to determine the code. There is a mechanical key available in case of power failure or any other issues. The lock uses 8 AA batteries and is said to last from 3-6 months. This lock is priced at $188.

3.1.4 ULTRALOQ UL3 BT 2nd Generation Smart Lock

The ULTRALOQ UL3 BT 2nd Gen Smart Lock utilizes Bluetooth, fingerprint, and keypad as methods of unlocking. It also includes a mechanical key in case of power failure. This lock includes many features through such as smartphone control, knock to open, shake to open, temporary access codes or ekeys, and an auto locking feature. The knock to open uses Bluetooth and requires the user to knock on their phone 4 times to unlock. Shake to open also operates in a similar way. 128-bit AES is used for data encryption. The lock is powered by 3 AA batteries. The lock is priced at $169.99.

3.1.5 Lockly PGD728FSN

The Lockly PGD728FSN is a smart lock that utilizes a fingerprint scanner, keypad, and digital eKeys. This lock utilizes a unique patented keypad with 4 keys that include 3 digits per key. Pressing a key multiple times changes the digit that will be used for the code. This is done to prevent unauthorized users from guessing a passcode based off of wear and tear. The lock includes an app that is able to store access history, grant codes, or digital eKeys. The lock uses 4 AA batteries and is said to last up to 1-year on normal use. The lock is priced at $223.09.

3.1.6 Similar Existing Products Summary

Please reference Table 3.1: Similar Existing Products for a detail summary of other smart locks we have reserched.

Table 3.1 - Similar Existing Products

Product	Price	Battery Life	Features
iView FL400	$229.99	Up to 1 year in standby mode	- Facial Recognition - Night vision - Backup key - Fraud protection
eufy Security Smart Lock	$250	Up to 1 year	- Finger print Scanner - Bluetooth - Electronic keypad - Backup Key - All weather protection - Stores information locally
ROMIX 5 in 1 Smart Keyless Door Lock	$188	Up to 3 – 6 months	- Facial Recognition - Fingerprint - IC cards - Backup Key
ULTRALOQ UL3 BT 2nd Generation Smart Lock	$169.99	Up to 1 year	- Bluetooth - Fingerprint - Code - Knock to open - Shake to open - Backup Key
Lockly PGD728FSN	$223.09	Up to 1 year	- Fingerprint - Digital eKeys - Keypad - Application to configure lock features

3.2 Relevant Technologies

The technologies used for the SMOCK LOCK are discussed in this section, they are Facial Recognition, Fingerprint Scanner, RFID Scanner, PIR Sensors, Application Development, API, Database, Server, Computational Configuration, Microcontrollers, Single Board Computers, Lock Mechanisms, and Relevant Software.

3.2.1 Facial Recognition

One of our main forms of security authentication for our lock is facial recognition. This requires the use of a camera module. This camera module will communicate an image or live feed of someone in front of the lock trying to access the door. The data will be sent over Wi-Fi to an encrypted server that will process the images and run a facial recognition software and return the results back to the microcontroller of the lock instructing it to either keep the door lock or open the door if a match is detected. Facial recognition is a massive and continuously researched technology in the modern age. Facial recognition used as a means of authentication requires a high level of accuracy and reliability. There have been many algorithms that have been developed since the introduction of the technology in the mid-60s, building upon each other with their own strengths and weaknesses. In this section we will compare some of the most popular algorithms that have been developed over the years and discuss their pros and cons.

3.2.1.1 Principal Component Analysis Normalizer

Principal Component Analysis is the process of turning an initial unfiltered image to an image focused on a real coordinate space. The real coordinate space consists of a sequence of unit vectors, also called Eigenvectors, where the vector is in the direction of the best fit line. The vectors are also orthogonal to the previous vector making the space orthonormal. Principal Component Analysis shows a covariance matrix that can be written as C = AA where A and A are the indices of the matrix that represents the initial image. The image once placed in the matrix can then be used to find the Eigenvectors that are associated with the Eigenvalues set. Once the Eigenvectors are found the normalization process is complete and allows for the algorithms to consistently derive the correct focal points.

3.2.1.2 Eigenfaces

Eigenfaces is a focal based traditional approach on facial recognition that attempts to view the whole face instead of breaking the face down into individual components. Eigenfaces is the first full-fledged version of facial recognition that was recognized as an algorithm that could be used in authentication reliably and effectively and is now normally used as a baseline for comparison. The Eigenfaces are created by first recognizing Eigenvectors obtained through the normalization process of Principal Component Analysis. Then these vectors are set in a subspace of user defined space called the “face space” for comparison and computation. As the face space consists of the initial image the image in a database can also be compared to it and allows for easy face detection as it can detect the slight image similarities. Once the face is detected some computations are made to compute the Euclidean distance which is the similarity distance and is how the algorithm determines the comparison of the face.

3.2.1.3 Fisherfaces

Fisherfaces is an evolution of the previous algorithm Eigenfaces and solves some of the problems associated with it. Mainly the age of the algorithm shows that it struggles on images that are even slightly distorted and only handles head displacement well. The vectors are also found through the same method as the Eigenfaces which is Principal Component Analysis. Also, as the later algorithm is linear, Fishers algorithm is nonlinear and attempts to conform the shape of the scatter into a class scatter matrix. This matrix allows for the computation of the difference of classes which is essentially the same as the Euclidean distance for

Eigenfaces. so the confirmation of faces is validated by comparing a predetermined threshold to the difference of classes. If the value is to lower the image is denied and retested as a different scatter, greater and the image is validated.

3.2.1.4 LBPH

Local binary Patterns Histograms take a different approach than the previous two algorithms. Eigenfaces and Fisherfaces treat facial image data as a vector in a high-dimensional image space. This means it requires a lot more computational power to conduct these algorithms. LBPH avoids this by using only local features of an object keep things in a low dimensionality. This is done by comparing each pixels with its neighborhood and setting it to either a 1 or a 0 based on the intensity of the center pixel being greater or equal to a threshold when compared to its neighbors. This process uses something called an LBP operator and it is able to detect a spot, spot/flat, line, edge, or corner of an image. After an image has been transformed through this process, it can be split up into local regions. From here, we can extract a histogram of each region and concatenate the histograms from each region to form one large histogram that describes the facial image. This can be used to accurately compare facial images. LBPH provides a simpler approach to facial recognition than the other algorithms and would be less computationally expensive.

3.2.1.5 Multilinear analysis of Tensorfaces

A multilinear analysis of Tensorfaces can be used to conduct facial recognition. Tensorfaces create an ensemble of an image that includes a facial image data tensor D. This facial image data tensor is made up of a core tensor Z, which governs the following 5 mode matrices. U_{People} is a people matrix parameter. U_{Views} is the view matrix parameter, U_{Illums} is the matrix parameter of illumination, $U_{Express}$ is the matrix parameter of expression, and finally U_{Pixels} is the matrix of pixels that span the space of the image. This can be seen as an evolution of eigenfaces as conducting a multilinear analysis of Tensorfaces maps all images of a person regardless of viewpoint, illumination, and expression to the same coefficient vector. Eigenfaces and traditional PCA would represent each image of a person with a different coefficient vector. Thus, using a multilinear analysis of Tensorfaces would provide our facial recognition software the ability to withstand differences and be more accurate in cases where illumination, expression, or viewpoint differ from time to time. Tensorfaces still requires a front facing view however to operate with its highest accuracy. Tensorfaces is would also require more work to implement as we would have to build our own implementation of this algorithm. Unlike, the other algorithms listed which have already been implemented in an open source library called openCV.

3.2.1.6 Artificial Neural Networks

Artificial neural networks can be used to implement an accurate facial recognition process. Face Recognition is a library available on python that is built using dlib's deep learning models to build a face recognition model that is reported to have an accuracy of 99.38% on the Labeled Faces in the Wild benchmark. This provides an extremely simple way to implement facial recognition using a deep learning architecture. Using this package, implementing facial recognition simply requires us to uses the built-in methods provided by the package to encode and compare facial images.

3.2.2 Fingerprint Scanner

Another form of security authentication that will be integrated into our smart lock is fingerprint biometrics. The three most popular forms of fingerprint scanners are capacitive scanners, optical scanners, and ultrasound scanners. Capacitive scanners create an image by means of a small electric charge generated by miniature built-in capacitors that can store electricity. When a finger touches the scanner, the capacitors get discharged. The scanner measures the difference of discharges and determines the pattern. Optical scanners light up the finger through a prism and the sensor reads the information and converts it into an image. Ultrasound scanners make use of an ultrasound signal instead of light. Due to this, the scanner does not need to be in contact with the finger so it can be covered by a screen. The scanner records the echo generated by ridges and valleys of the fingerprint. It also records the echoes of edges that are farther away from the sensor, so the image generated is closer to 3-dimensional. This allows for detection of fakes such as printing a fingerprint on a sheet of paper. For our project, we will mainly be looking at capacitive and optical sensors due to price and simplicity to implement.

3.2.3 RFID Scanner

The last form of authentication technology that will be used is an RFID system. RFID systems are a way to collect data and detect objects through radio waves. Depending on the use different frequency of waves can be used. Low frequency systems range from 30 – 300 kHz, have a very short-read range, and are good for low-data transmissions. RFID systems usually consist of an RFID reader, RFID tags, and antennas. The RFID tag is comprised of an antenna and RFID chip. The chip holds information such as the tags ID. Low Frequency RFID tags will not have a battery and are powered through the energy received from the reader through transmissions. The RFID reader is the part that transmits and receives radio waves to communicate with the RFID tags.

3.2.4 Passive Infrared Radiation (PIR) sensors

To avoid the lock operating at full power, even when there is no use for it. A low power mode has to be introduced. In order to do this, the lock can operate in a low power mode until a person is detected in range. Thus, a passive infrared sensor (PIR) sensor would allow for this functionality. PIR sensors detect movement through sensing infrared radiation. PIR sensors usually have two slots that both contain a material that is sensitive to IR. These slots both detect the same amount of IR when idle. When a warm body such as a human walks in range, one of the slots will experience a positive differential change, and when it leaves the range of the sensor, it will experience a negative differential change. These changes are what indicates a warm body is present in the sensor.

Table 3.2 - Types of RFID Scanners and their applications

	Primary Frequency Range	Contact Range	Applications
Low Frequency RFID	125 - 134 kHz	10 Centimeters	Animal Tracking, Access Control, etc.
High Frequency RFID	13.56 MHz	30 Centimeters	Library Books, poker chips, DVD Kiosk, etc.
Active RFID	433 MHz	30 - 100+ Meters	Vehicle Tracking, mining, asset tracking
Passive RFID	860 - 960 MHz	Near Contact - 25 Meters	Manufacturing, Inventory Tracking

3.2.5 Relay

In order to have control over our lock, we will need to have a component that can control when power is supplied to the mechanism. A relay will solve this since it's a basically an electric switch that opens and closes circuits by receiving electrical signals from outside sources. In this section we will discuss the different types of relays.

3.2.5.1 Electromagnetic Relays

Electromagnetic Relays are designed by using a magnetic field that is created by a powered coil. This field allows for a moving piece to complete the circuit that maintains the connection for the relay. While the physical aspect of the relay allows for a constant and guaranteed flow of electricity, it does have a reduced close and open time for the lock. For the locks purposes though it has the highest reliability and for the purposes of starter projects normally the best.

3.2.5.2 Solid State Relays

Solid State Relays are designed to use a low power signal to generate an optical semiconductor signal that acts as an electrical switch that toggles the output pin of the relay. The newest developed of the relays utilizes all the new technology from semiconductors, hence the name solid state as there are no moving parts. These relays are much more complex than other relays and require more manufacturing and cost a great deal more and unlike electromagnetic relays these cannot handle higher voltages or shorts. However, for established and higher end products the speed and consistency of the Solid-State relay cannot be beat. Also, as there are no moving parts the relay is completely silent unlike electromagnetic relays.

3.2.5.3 Reed Relays

Reed Relays are designed to use a solenoid that creates a magnetic field that push and pull a switch, called the “reed”, into to place to create the pathway. The reed is a magnetic strip that is sealed in a gaseous tube to prevent decay and corrosion. Due to the magnetic nature of the relay you need to place a protective circuit in order to not short out the relay. The advantages of this relay compared to the others are the comparatively low power cost to run and the fastest switch speed. The disadvantages of the relay is the inability to handle high voltage loads and have a lower reliability in comparison to the other relays.

3.2.5.4 Selection

We have decided to go with an SRD electromagnetic relay as they are usually cheaper, and they have the highest reliability for household applications which in our case would be a door lock.

3.2.5 Application Development

The SMOCK lock will need an application to configure and operate the lock. There are a few design choices that could be made regarding the development of an application. To start off with, the application could be developed in a native language, using Objective C or Swift for iPhone development, and Java or Kotlin for Android development. The downside of using a native code to develop our app is we will have to make two separate code bases in order to have support for both iPhone and Android users. There are cross-platform technologies to develop an app with one code base and run natively for both platforms. Some of these options include native react, flutter, and Xamarin. Native react uses the widely used JavaScript language as well as the ability to use Java, Swift, or C when needed. Flutter uses its own object-oriented language called dart. Xamarin utilizes C# in order to compile native applications for both platforms. There are pros and cons to choosing to develop natively or using a cross-platform framework. Coding natively often results in a more responsive app, and access to take full advantage of the platforms hardware, at the cost of developing separate code bases. Choosing to use cross-platform development can allow for faster development due to the single code base at the cost of less responsiveness as well as limited functionality.

3.2.6 API

API allows for communication between the backend and the frontend of the application. There are three forms of API protocol REST, RPC, and SOAP The representational state transfer (REST) architecture, or REST API are stateless and store no data between requests. They operate in a client/server approach and act as a sort of mailman between the frontend and backend. REST API is by far the most popular and offers flexibility in implementation. It is coded in JSON or XML but The Remote Procedural Call (RPC) protocol often invokes executable actions or processes and provides a way to send parameters and receive results. RPC can be coded in JSON or XML. SOAP API is highly structured and contains up to 4 components: envelope, header, body, and fault (error handling). SOAP is usually coded in XML. All the APIs can be coded in languages that handle parsing of JSON and XML packages such as JavaScript and Php.

Table 3.3 - Forms of API Protocol

Form of API Protocol	Description
Representational state transfer (REST)	A stateless approach, easy to setup, flexible
Remote Procedural Call (RPC)	Invokes executable actions or processes.
Simple Object Access Protocol(SOAP)	Highly structured API, useful for secure development.

3.2.7 Database

There are two main types of databases that can be used NoSQL and SQL. The two databases that will be spoken about are: MongoDB, and MySQL. MySQL is an SQL based database management system that is open source. If we decide to go with MySQL, we will most likely go with a LAMP Stack which would use a Linux Server, Apache Web Service, MySQL for the database, and PHP/Python for the coding language. MongoDB is a NoSQL database. If we go with MongoDB, we will most likely go with a MERN Stack which consists of MongoDB for the database, Express JS which is a Node.js web framework, React JS is a client-side JavaScript framework, Node JS which is the web server.

Below is a table of different databases please reference Table 3.4: Databases, for a summarized version.

3.2.7.1 MySQL

MySQL is a relational database management system based on SQL. MySQL is able to store a wide variety of data and offers high scalability. MySQL is often considered the most popular database management system used today. MySQL is used by large organizations such as Facebook, twitter, and YouTube.

3.2.7.2 MongoDB

MongoDB is a document-oriented database system. It is considered a NoSQL database system. MongoDB stores data in JSON-like documents and was developed using C++, JavaScript, and python. MongoDB supports both JSON and BSON data formats. Since a BSON-document size limit is 16MB, MongoDB uses a convention, GridFS, to store and retrieve files larger than this size limit.

MongoDB offers a modern approach to databases and is considered to be simpler and easier to use than relational databases such as MySQL. MongoDB is used by large organizations such as Google, EA, and Verizon.

3.2.7.3 PostgreSQL

PostgreSQL is an object-oriented relational database management system. It is considered a more advanced relational database system when compared to others such as MySQL. PostgreSQL offers support for partial, bitmap, and expression indexes. It also provides materialized views as well as table inheritance. It also provides support for advance data types such as arrays and user defined types. These are all big advantages over SQL which only supports simple data types and does not offer the other features mentioned.

3.2.7.4 Firebase

Firebase is a NoSQL cloud-based database management created by Google that offers unique features. Firebase allows creators to build, monitor, release, and engage with their database. Firebase also offers a large library of extensions that are useful for application development.

3.2.7.5 DynamoDB

DynamoDB is a fully managed, serverless, key-value NoSQL database by Amazon that offers support for an application of any scale. DynamoDB provides built in features such as security, continuous back-ups, in-memory caching, and data export tools. DynamoDB is one part of the Amazon Web Service (AWS). AWS free tier offers 25 Gigabytes of storage and up to 200 million free read and write request. Large companies such as Disney, Snapchat, and Zoom user AWS service to power their programs.

3.2.7.6 Apache Cassandra

Apache Cassandra is an opensource NoSQL distributed database management system. Cassandra has very fast read times at O(1) time, and provides very high writing scalability. A downside of Cassandra is it only supports JSON data format and does not have support for BSON data formats. Cassandra is used by large companies such as Instagram, Hulu, and Reddit.

Table 3.4: Databases

Database Name	Database Type
MySQL	SQL
MongoDB	NoSQL, document-oriented database system
PostgreSQL	Relational Database Management System, Written in C
Firebase	NoSQL, cloud-hosted database

Table 3.4.5: Databases Continued

Database Name	Database Type
DynamoDB	NoSQL, key-value document data structures
Apache Cassandra	NoSQL, Written in Java

3.2.8 Server

The server that will be used depends on the stack that is used. If we decide to use a LAMP stack, the server that will be used is an Apache HTTP server. The Apache web server is maintained by the efforts of the Apache HTTP server project. Apache is an open source HTTP server. If we decide to use a MERN stack the web server framework that would be used is Express.js

3.2.9 Cloud Computing Solutions

Cloud computing services offer on demand compute resources such as storage and processing power over the cloud.

3.2.9.1 Amazon Web Service (AWS)

Amazon web services is a broadly adopted cloud platform that offers over 200 fully-featured services. AWS offers the ability to lower costs, become more agile, and create faster. AWS offers things such as computing power, storage, databases, machine learning, artificial intelligence, analytics, and much more. There is also a variety of different databases offered that are targeted to specific applications. Amazon claims to have a large community, offers secure services, and global support.

Table 3.5 - Amazon Web Service Featured Products

Service	Description	Pricing
Amazon Elastic Compute cloud (Amazon EC2)	A secure and resizable compute capacity to support virtually any workload. Provides control of computing resources and is run on Amazon's computing environment.	AWS free tier includes 750 hours of Linux and windows t2.micro instances. On Demand Rates: t3.micro - $0.0104/hour t3.small - $0.0208/hour t3.medium - $0.0416/hour
Amazon Simple Storage Service (Amazon S3)	An object storage services with scalability, data availability, security, and performance.	Storage – First 50 TB / Month at $0.023 per GB Request and Data Retrieval – range from 0 - $0.0005 per 1000 request. Data Transfer – All data in is free, Data out from Amazon S3 up to 1.

Table 3.5.5: Amazon Web Service Featured Products Continued

Service	Description	Pricing
		GB / month is free, after the next 9,999 TB / month is $0.09 per GB
Amazon Aurora	MySQL and PostgreSQL-compatible relational database built for the cloud.	Db.t4g.medium - $0.073 per hour Db.t4g.large - $0.146 per hour Db.t3.medium - $0.082 per hour Db.t3.large - $0.164 per hour
Amazon DynamoDB	A fully managed, serverless, key-value, NoSQL database designed for high performance at any scale.	Storage: First 25GB – Free After 25GB - $0.25 per GB Write/Read request: First 200 million read/write request - Free Write request units per million – $1.25 Read request units per million - $0.25 Backups: Continuous backups - $0.20 per GB per month On-demand backup - $0.10 per GB per month Restoring a table - $0.15 per GB DynamoDB streams: First 2.5 million stream read request are free for each month. $0.02 per 100,000 stream read request after.
Amazon Relational Database Service(RDS)	Provides the ability to set up, operate, and scale a relational database in the cloud.	AWS free tier: 750 hours of Amazon RDS single-AZ db.t2.micro instance per month 20 GB of General purpose DB storage. 20 of storage for automated backups. RDS on VMware: Db.mv11.medium - $0.084 per hour Db.mv11.large - $0.168 per hour

Table 3.5.10 Amazon Web Service Featured Products Continued

Service	Description	Pricing
AWS Lambda	Runs code without the need to provision or manage servers or clusters.	X86 Price: $0.0000166667 per GB-second $0.20 per 1 million request Arm Price: $0.0000133334 per GB-second $0.20 per 1 million request
Amazon Virtual Private Cloud (VPC)	Gives complete control over a your virtual networking environment, including resource placement, connectivity, and security.	Pricing varies based on resources used. AWS prcing Calculator can be used to determine price based on required resources
Amazon Lightsail	Preconfigured cloud resources including a virtual private server, containers, storage, databases and more.	AWS Free Tier – 3 months free Pricing varies based on resources used including VPS, containers, storage, and databases.
Amazon SageMaker	A broad set of capabilities built for machine learning to help build, train and deploy ML models.	Pricing varies based on resources used.

3.2.9.2 Google Cloud

Google Cloud is a suit of cloud computing services offered by Google. It is used by many large companies and even by google itself to power things such as YouTube, Google Drive, Google Search, etc. The following services are included in the services offered by google.

Table 3.6: Google Cloud Featured Services

Service	Description	Pricing
Compute Engine	Secure and customizable compute service that lets you create and run virtual machines on Google's infrastructure.	General purpose machine (e2-micro instance) offered for free.
Cloud Storage	Object storage, able to store any amount of data and retrieve it as often as you like.	Standard storage starts at $.02 per GB per month.
Cloud SDK	Tools and libraries for interacting with google cloud products.	Available at no charge for users with a Google Cloud account.

Table 3.6.5 – Google Cloud Featured Services Continued

Service	Description	Pricing
Cloud SQL	A fully managed relation database service for MySQL, PostgreSQL, SQL Server. Also, includes rich extensions collections, configurations flags, and developer ecosystem, without the need for self-management.	Pricing varies depending on how much storage, memory, and CPU required.
Google Kubernetes Engine	Googles Kubernetes Engine is a managed services for running Kubernetes, a portable extensible open source platform for managing containers. Makes it easy to create clusters, balance loads, auto scale, and more.	One autopilot cluster per billing account is free. After, a $0.10 per cluster/hour applies.
BigQuery	Serverless, highly scalable, and cost-effective multicloud data warehouse designed for agility.	Storage - $0.02 per GB, per month Streaming Inserts - $0.01 per 200 MB Loading, copying, or exporting data - Free
Vision AI	Offers insights from images stored in cloud using either AutoML vision, or pre-trained vision API models. Able to detect objects, faces, handwriting, emotion, and more.	Pricing varies based on which Vision AI product is used. For the first 1000 units, vision API is free to use after, most of the APIs are about $1.50 for each 1000 units.
Cloud Run	Develop and deploy highly scalable containerized application on a fully managed serverless platform.	CPU – 180,000 vCPU-seconds per month for free. $0.000024 per vCPU-second after. Memory – 360,000 GiB-seconds per month for free. $0.0000025 per GiB-seconds after. Requests – 2 million request per month for free. After, $0.40 per million request.

Table 3.6.10: Google Cloud Featured Services Continued

Service	Description	Pricing
Cloud Functions	Scalable pay-as-you-go functions to run your code without the need for server management.	Pricing is based on how long your function runs, how many times it is invoked, and how many resources you need for the function
Anthos	Anthos offers management of infrastructure and applications with a Google Cloud-backed control plane for operation at scale. Offered for major public clouds such as Google Cloud, AWS, and Azure.	Pricing is estimated to be at about $6 per month per vCPU with a subscription.

3.2.9.3 Microsoft Azure

Microsoft Azure is a public cloud platform that offers a large collection of services including virtual machines, managed database service capabilities, and much more.

Table 3.7: Microsoft Azure Featured Products

Service	Description	Pricing
Virtual Machines	Azure virtual machines offer up to 416 vCPUs and 12 TB of memory. Can scale from one to thousands of VM instance in minutes. Able to choose between Linux or windows operating systems.	Pricing varies based on the amount of vCPUs, RAM, temp storage, and processor needed.
Azure Virtual Desktop	Azure Virtual Desktop allows for secure remote work, on a Windows 11 os. Includes the option for multi-session experience and can use existing eligible windows licenses.	Pricing includes User access rights, as well as Azure infrastructure cost. Pricing varies depending on products used.
Azure SQL	Azure SQL cloud databases provide high flexibility and help the developer choose the best option based on needs.	Pricing varies depending on products used.
Azure Cosmos DB	Azure Cosmos DB offers a fully managed NoSQL database service. As well as, guaranteed single-digit millisecond response times and 99.999-percent availability. Includes open-source APIs for MongoDB and Cassandra.	1,000,000 serverless request units offered at $0.25.

Table 3.7.5: Microsoft Azure Featured Products Continued

Service	Description	Pricing
Azure Kubernetes Service (AKS)	Azure Kubernetes Service (AKS) offers the ability to deploy and manage containerized applications.	Pricing varies depending on resources required.
Azure Cognitive Services	Azure Cognitive services offers a collection of API calls to integrate AI into a developers application.	Pricing varies depending on which API is used and the required task.
App Service	App Service allows for developers to easily create enterprise-ready web and mobile apps, deploy, and scale on a reliable cloud infrastructure.	Pricing varies depending on the required resources.
Azure Functions	Executes event-driven serverless code.	$0.000016 per GB-s (first 400,000 GB-s are free per month) $0.20 per million executions (first 1 million executions are free)

3.2.9.4 DigitalOcean

Digital Ocean is a cloud hosting provider that offers developer a variety of cloud computing services. Developers can host websites, build web apps and API backends, and deploy container-based apps with managed Kubernetes similar to the services offered by Google Cloud and Azure. Digital Ocean gives users a predictable cost without the need for a complex calculator like some of its competitors in AWS and Azure. Users can buy droplets which are virtual machines that can be set up for basic, general, CPU-optimized, or memory-optimized configurations.

Table 3.8: DigitalOcean Products

Services	Description	Pricing
Droplets	Droplets are cloud based virtual machines. Digital oceans offers droplets that are priced based on the computing power they offer. The beginning tier of a basic droplet has 1GB of RAM, 1 intel CPU, 25GB of SSD, and up to 1000GB to transfer. This can be upgraded to increase the computing power. Droplets are also offered to be CPU optimized,	Pricing varies depending on the computing power required but is simply stated under their pricing tab.

Table 3.8.5: DigitalOcean Products Continued

Services	Description	Pricing
	memory optimized, or storage optimized depending on needs.	
Managed Kubernetes	DigitalOcean offers a free control plane for their Kubernetes unlike other competitors. They also provided the option to upgraded for more availability.	Free tier available. High availability feature available for $40/month.
App Platform (PaaS)	The app platform offered by DigitalOcean has three tiers the starter, basic, and professional with varying features.	Starter – free Basic - $5/month Professional - $12/month
Managed Databases	Digital ocean offers fully managed databases with varying computing power. MongoDB, MySQL, Redis, and PostgreSQL database engines are available.	Pricing varies depending on the required resources.
Spaces Object Storage	A simple and scalable s3-compatible object storage with a built-in content delivery network.	$5 per month
Volumes (Block Storage)	Block storage that is available in three levels of storage capacity.	100GB - $10 / month 500GB - $50 / month 1000GB - $100 / month
Load Balancers	Scale applications and improve availability, security, and performance by spreading traffic across compute resources.	$10 per month per node
Container Registry	Store and manage private container images with a registry that integrates with DigitalOcean Kubernetes	Free tier Basic - $5/month Professional - $20/month

3.2.9.5 Heroku

Heroku is a container-based cloud platform as a Service (PaaS). Using Heroku, developers can deploy, manage, and scale apps with ease. Heroku offers dynos which are lightweight, isolated Linux containers to run an app. Heroku offers developers a domain as well which takes away the need to find another third-party domain host, which would need to be done if something like Digital Ocean is used.

Table 3.9 - Heroku Products

Containers (dynos)	Description	Pricing
Free	Heroku offers a free tier of dynos. This offers 550 – 1000 dyno hours per month. It allows users to deploy with Git and Docker, custom domains, container orchestration, as well as automatic OS patching	Free
Hobby	The hobby level gives users everything included in the free tier, free SSL, automated certificate management, and never sleeps	$7 per dyno per month
Standard 1x/ Standard 2x	The standard level offers 2 different levels. This includes all the features from the Hobby tier, as well as a horizontal scalability, app metrics, prebook, zero-downtime deploys, and unlimited background workers. The Standard 1x and standard 2x offers more computing power with either more RAM or CPU power as needed.	Standard 1x - $25 per dyno per month Standard 2x - $50 per dyno per month
Performance M/ Performance L	The performance level includes all features from the standard level, predictable performance for highest traffic applications, dedicated resources, autoscaling, and can mix with standard dynos. The M offer 2.5GB RAM. The L offers high concurrency and parallelism for max throughput and comes with 14GB of RAM.	Performance M - $250 per dyno per month Performance L - $500 per dyno per month
Private / Shield	The private and shield level are extremely high-end with full network isolation, dedicated runtime environment, private network, and data services. The shield offers higher level security with PCI compliance, keystroke logging, space level log drains, and strict TLS enforcement.	The private and shield level require contact with the sales team at Heroku for custom pricing.

Heroku is fully managed, which means developers do not need to worry about maintaining their servers, hardware, or infrastructure. They offer support to troubleshoot 12 hours, 5 days a week for free. With a premium plan you can receive 24/7 support to troubleshoot.

Table 3.10 - Summary Comparison of Cloud Computing Solutions

Cloud Computing Solution	Summary
Amazon Web Service (AWS)	Amazon provides a unique suite of services that features a serverless computing solution. Amazon offers high scalability and a pay as you go payment structure. If quick and easy scalability was necessary for our SMOCK lock Amazon Web Services would be a good option.
Google Cloud	Google Cloud offers a large suite of services similar to AWS and Microsoft Azure including database, powerful server side computing, and high scalability. A unique service offered by is their vision AI which offers a robust library of computer vision API.
Microsoft Azure	Microsoft offers a large suite of services like AWS and Google cloud. It provides a unique virtual desktop that makes it easy to manage your server. Azure offers fixed rates as well as pay as you go. Like the previous two options, this would be a good option for quick and easy scaling.
Digital Ocean	The services offered by Digital Ocean are not as robust as AWS, Google Cloud, and Azure. They offer a simple and flexible payment structure allowing for a more CPU, RAM, or Storage based plan based on needs. This would be a good option for the SMOCK lock due to its simple pay structure and flexibility for computing power.
Heroku	Heroku offers a cloud platform as a service. It does not have as wide a variety of services as offered by the other computing solutions. However, it offers a simple payment structure and wide support for other tools that will be used for the SMOCK LOCK.

3.2.10 Computational Configuration

For our project we there are a few ways we can configure our set up. One is through the use of a microcontroller such as an Arduino board, and the other is through the use of single board computer such as a Raspberry Pi.

For our project there are a few ways we can configure our set up. We have the option of using either Microcontrollers, Single board computers, or Field Programmable Gate Arrays. These all have their advantages and disadvantages related to our needs.

3.2.10.1 Microcontrollers

A microcontroller is a small form simple computer with the primary goal of accessing and interacting with other hardware. Since microcontrollers can only run one program at a time, they usually have very few resources in terms of CPU and RAM. Also, since microcontrollers can only run one program at a time, they cannot support the use of an operating system such as Windows 10 and Ubuntu. Due to the small number of resources on the board, this allows for low power consumptions and the “availability of real-time, fine-grained processing of connected hardware. Microcontrollers are also much cheaper than other types of boards since they are very simple and have the minimal number of resources.

3.2.10.2 Single board Computers

A single board computer, also known as systems-on-a-chip, are basically miniature computers. The components they consist of include microprocessors, memory, input/output (I/O) component connections, and other features that a usual computer can support. Unlike a normal desktop computer, SBC’s do not rely on expansion slots for peripheral functions or expansions. While SBC’s do not rely on these slots, some SBC’s can support the use HAT (Hardware Attached on Top) expansions which can allow for other functionality that usually wouldn’t come standard on the board.

3.2.10.2 Field Programmable Gate Arrays (FPGA)

Field programmable Gate Arrays are semiconductor devices that are built on a matrix of configurable logic blocks. This means that unlike traditional development on something like a microcontroller. Development requires the use of a hardware description language such as Verilog or VHDL. Field programmable gate arrays have the advantage of giving the develop a blank canvas. Thus, they have the power to give the developer total control of how the hardware operates.

3.2.10.2 Application Specific Integrated Circuits (ASICs)

Application specific integrated circuits are microchips designed for a specific task. Unlike other chips such as microcontroller that are general purpose, these are designed with a specific task in mind and meant to optimize the chip to conduct such a task.

Table 3.11: Computational Configuration Comparison

Part	Description
Microcontrollers	Small form simple computer meant to complete simple tasks. Microcontrollers do not have a full general-purpose operating system. They are often used for specialized tasks. Such as an IoT of things, where it controls multiple sensors. Microcontrollers are not as powerful as single-board computers. For this reason, a microcontroller would be used if powerful processing operations are not needed to be done on the board itself such as facial recognition. Microcontroller Features: • Single-core CPU • Limited RAM • Extremely small Flash storage • Requires external interfacing chipsets • Requires the use of electronic interfaces such as IIC, SPI, UART. • Runs with no operating system, no drivers, little complexity • Low power consumption • Cheap but limited functionality • Require interrupts if to run parallel operations
Single Board Computers	Miniature Computer that is used for task that require a greater amount of processing power. Single board computers are small full-fledged computers. Where microcontrollers require external interfacing chipsets and extra hardware, Single Board Computers have these built in. A popular Single Board Computer brand is Raspberry Pi Single Board Computer Features: • Powerful CPU • RAM • Storage • Higher power consumption • Supports peripherals through standard USB • Have an operating system • Simple task can be more complex

Table 3.11.5: Computational Configuration Comparison Continued

Part	Description
Field Programmable Gate Arrays (FPGA)	Field Programmable gate arrays are not programmed the same way as microcontrollers or single board computers. FPGAs require the use of a hardware description langue such as Verilog to configure the FPGA's internal circuitry. FPGA Features: • Developer has complete control of hardware • Able to handle parallel I/O without the need for interrupts • Can be very fast
Application Specific Integrated circuits (Asic)	Application specific integrated circuits are microchips that can be special ordered from a company to conduct a specific task. ASIC Features: • Built with specific application in mind

3.2.10.3 Computational Configuration Selection

We have decided to go with microcontrollers for our SMOCK lock. These give us enough flexibility to conduct all the required operation for our lock, while also keeping the price low. Microcontrollers also consume low power allowing us to design our lock with a longer battery life in mind.

3.2.11 Serial Communication with Microcontroller

In this section we will discuss the different types of Serial Communication, along with their advantages and disadvantages. For a brief but detailed understanding, please reference Table 3.12: Serial Communication

3.2.11.1 Inter-Integrated Circuit (I^{2}C)

I2C was first developed by Phillips for some of their chips, now it is commonplace in most microcontroller boards. The bus of I2C is made with two lanes the Serial Data and Serial Clock, this way multiple masters can act on the same bus. The bus drivers act as open drains in which they can call low signals but cannot make them high. This allows for less power drain in total and through the use of pull up resistor's components can still read high. As the systems doesn't allow high signals from signals, voltage regulation is easy between components and a sperate converter is only required when the voltage difference is much greater than normal, around 5V.

3.2.11.2 Serial Peripheral Interface (SPI)

A synchronous serial communication type that specializes in single lane transmissions. It also uses the master-slave architecture but only allows 1 master at a time thus cannot run multi layered systems. SPI normally runs in four lanes making it the worst in taking up lanes on the physical board. However, the board is the fastest in terms of communication at 10Mhz per second and has no data overhead making it the best in communication from microcontroller to any number of devices, but is unable to run in multi controller setting.

3.2.11.3 Universal Asynchronous Receiver-Transmitter (UART)

UART is a computer hardware device for asynchronous serial communication where the data format and the transmission speed are configurable. During communication, the transmitting UART converts parallel data from a controlling device, and then transmits it in serial to the receiving UART. The receiving UART then converts the serial data back into parallel data for the receiving device. Due to this conversion of data, only 2 wires are needed to transmit data, usually the TX and RX pins.

Table 3.12: Serial Communication

Type	Advantages	Disadvantages
I2C	Only uses 2 board lines Can use multiple controllers communicating on the bus Easy to implement into existing software.	Middle of the pack in terms of data transfer speeds A small overhead that leads to extra data per transmission. Most complex to modify.
SPI	The fastest form of serial communication at 10Mhz per second Simplest to implement into existing software.	4 Board Lines are used for every connection limiting the number of devices that can be used. Only Allows one master controller per bus.
UART	Most used form of Serial Communication An actual physical circuit and not a communication line. Simplest to implement in the hardware	The ports are asynchronous, thus the components must both agree on a similar clock rate. Slowest of the 3 in transmission rate at only recognized Baud rates Only suited for 2 devices, 3 or more is possible but not recommended.

3.2.12 Lock Mechanism

There is various lock mechanism that we can incorporate into our smart lock. In this section we will discuss these methods and how they work.

3.2.12.1 Gear Based Turning

A few basic smart locks make use of a gear based turning method to allow for manually turning of a lock through the use of a key while maintaining the ability to turn electronically without damaging the motor. The configuration consists of a DC motor, a worm gear, a reduction gear, a big gear, a switch pusher, and snap action switches. It makes use of the normal deadbolt construction but adds onto the thumb turn shaft. When the lock is told to unlock, the DC motor spins the worm gear since it is attached to the motor shaft. From there the worm gear drives a reduction gear which then rotates the big gear. The big gear spins the switch pusher and the thumb turn. When you manually lock or unlock, the switch pusher's square corners overpower the leaf springs to open/close the bolt. The big gear and reduction gear do not move during this which allows for the motor to be untouched while still allowing for manual locks and unlocks.

3.2.12.2 Electric Solenoid

An electric solenoid lock consists of a plunger and a latch that locks or unlocks when the solenoid is supplied with a current. It makes use of the principle of electromagnetism. The electromagnets turn on and off through the supply of current. The electromagnet is on when there is current. The electromagnet is off when there is no current. The electromagnet pulls the plunger in to unlatch, and when removed, a fail-safe spring re-engages the lock.

3.2.12.3 Gate lock

A gate lock can be used in turn with a servo motor. When power is supplied to the motor, the motor will turn 180 degrees in one direction, and when the motor is attached to the lock through the use of arms and a connector, it will pull the lock back and therefore unlock it. When power is resupplied again, the motor will turn 180 degrees in the opposite direction and will relock the gate.

Table 3.13: Lock Mechanism Comparison

Lock Mechanism	Description
Gear Based Turning	Allows to manually turn the lock with the use of the key while not damaging the motor. It will also allow for a motor to electronically unlock the door.
Electric Solenoid	When the solenoid is supplied with current it could unlock/lock the door depending on what it was set to in the off position.

Table 3.13.5: Lock Mechanism Comparison Continued

Lock Mechanism	Description
Gate Lock	The gate lock which is the simplest and least secure type of lock available for us to use, would be the simplest to implement a locking and unlocking mechanism for. However we would not be able to unlock the door in case of a power failure

3.2.12.4 Fail Safe Locks

Fail safe locks are known as locks that unlock when power is removed. The default state is unlocked. In order to keep it locked, power must be applied. At any time that power is loss then the lock automatically unlocks. This would also mean that we'd have to power the lock constantly for the door to be locked, which would require us to have a large supply of power. The lock would be drawing power constantly throughout the day with little breaks scattered throughout whenever the door gets unlocked.

3.2.12.5 Fail Secure Locks

Fail safe locks are known as locks that lock when power is removed. The default state is locked. In order to unlock, power must be applied. At any time that power is loss then it automatically locks. If we were to apply this to the SMOCK Lock, the battery being drained would not be difficult at all. The lock would need to be powered to unlock, however we could very easily instruct the lock to auto lock after a few seconds. This would save power ultimately, because the lock wouldn't require power constantly throughout the day.

3.2.13 Relevant Software for our System of Hardware Components

There are a few ways to test and use our components with software. Those being Eagle, Python, Code Composer Studio, Arduino IDE. In this section we will discuss how to use the software and which software will be used for which purpose.

3.2.13.1 EAGLE

EAGLE is an Autodesk product, it is also an electronic design automation (EDA) software that lets printed circuit board(PCB) designers to connect schematic diagrams, component placement, and a few more features. Essentially it allows our group to design our PCB, which we will need to do once we've decided what board and components we will use for the project. You will see in later sections what those components are.

EAGLE has a great tool named schematic editor, which allows us to test ideas and validate circuit performance, drag and drop reusable design blocks, rule checking which validates a schematic design with a complete set of electronic rule checks.

EAGLE also has a PCB layout editor that provides you with a multitude of different tools and ways to easily edit your PCB. Some of those tools allow you to arrange and order PCB design objects with alignment tools. It also has obstacle avoidance routing which allows you to easily route complex PCB layout.

3.2.13.2 Python

Python first appeared 30 years ago and is an interpreted high level general-purpose programming language. Over the years Python grew along with their user population. The purpose of implementing Python into our project, would be to program a Raspberry Pi single board computer. There is also a way to incorporate Python into our Arduino through the use of some open-source libraries, a prime example of the way Python has grown, which makes it possible to code in Python inside of the Arduino IDE. Alongside with the fact that the Python Language is a lot simpler and easier to understand and write.

Our main objective when trying to incorporate Python with our Microcontroller or Single Board Computer is to design the board so that it can power on certain components when necessary as well as serving as a bridge to the server. Which allows our components to update the database. The server would then send information back to the board, such as supplying power to then unlock or lock the door.

3.2.13.3 Code Composer Studio

The Code Composer Studio software is an integrated development environment or IDE. It is used to develop applications for Texas Instruments embedded processors. We will discuss about a microcontroller made by Texas Instruments that we may use for this project.

Code Composer Studio includes a C and C++ compiler, source code editor, debugger, and a project build environment, etc. With Code Composer Studio we will be able to provide a way for our board to power on different components as well. Essentially Code Composer Studio will allow us to do what Python could do but in this case it would be for Texas Instruments components specifically.

3.2.13.4 Arduino IDE

The Arduino IDE is used as a text editing program to program an Arduino board which as you will read later, is one of the board types that we are researching. Arduino code is written in C++ with an addition of special methods and functions.

We can also download a library that will allow us to use Python in the Arduino IDE. With the Arduino IDE we would be able to power on certain components such as a Wi-Fi module. It can also be used to configure components like the Wi-Fi module to connect to a network and provide internet.

Table 3.14: Relevant Software for System of Components Summary

Software	Application
EAGLE	Used to Design PCB Layouts
Python	Used to program Raspberry Pi Boards as well as Arduino Boards
Code Composer Studio	Used to program Texas Instruments embedded processors
Arduino IDE	Used to program Arduino Boards

3.2.14 Relevant Software for Application Development

In this section we will be elaborating on the different software's that are necessary for certain application development. We will talk about different coding languages, source code editors, and mobile app development platforms.

3.2.14.1 Php

PHP is a general-purpose scripting language that is useful for web development. It was created in 1994 as one of the first server-side languages that could be embedded into html. PHP has a syntax that is easy to remember and has a vast number of frameworks.

3.2.14.2 Python

Python is a powerful high-level language as mentioned earlier. Python could be used to create the necessary APIs for operation of the lock. If a LAMP stack was to be implemented PHP or Python could be used for API.

3.2.14.3 JavaScript

In the below sections we will be discussing how we intend to implement JavaScript runtime environments, frameworks, and libraries into the design of the SMOCK Lock App.

3.2.14.3.1 Node.js

Node.js is an open-source, cross-platform, JavaScript runtime environment that operates JavaScript code outside of a browser. It uses Chrome's V8 JavaScript engine. Node.js is a powerful tool to create APIs and scripting for a server. If a

MERN stack was implemented Node.js is a good option for server scripting and APIs.

3.2.14.3.2 Express.js

Express.js is a prebuilt Node.js framework that helps with creating APIs and server-side applications. It is one of the most popular libraries in Node.js.

3.2.14.3.3 React.js

React is a free and open-source front-end library. React makes offers an intuitive approach to creating interactive UIs using components and states. React is able to render on mobile applications as with React Native.

3.2.14.4 C

C is a general-purpose procedural coding language. C is one of the most popular coding languages used today. C offers great control to the user in terms of memory management and garbage collection. C offers efficient programs and can handle low-level coding. Arduino code and mobile application are supersets of C such as C++ and Objective C.

3.2.14.5 Objective C

Objective-C is based on C, provides object-oriented principles, and a dynamic runtime. Objective-C is used to code mobile applications. Objective-C offers support to older generation IOS devices as a middle-level, general-purpose language. However, Apple has developed a new language, Swift, that Apple claims is 2.6 times faster than Objective C.

3.2.14.6 Swift

Swift, a coding language, was engineered by apple and has many open-source contributions that make it fast and safe to use. Swift has many useful features such as variables always being initialized before use, array indices are checked for out of bound errors, integers are checked for overflow, memory is managed automatically, and has robust error handling. Swift is very quick and would be great for iOS development. Choosing Swift would require having 2 codebases if Android support is desired.

3.2.14.7 Java

Java is a high-level, object-oriented language, that is used for the development of Android applications. Java ensures safety since many of its libraries are managed by companies such as Google and Apache. Java would support the requirements needed for the operation of our lock. This option would be chosen if development is targeted at Android users as it would require a separate code base for iOS development.

3.2.14.8 Kotlin

Kotlin is a newly created language that is based off Java. Kotlin application deployment is faster to compile, lightweight, and prevents applications from increasing in size. Kotlin code is much smaller than java code. Like Java, choosing to develop in Kotlin would be targeted at android audience and would require a second code based if iOS support is desired. Kotlin also has less community support than Java.

3.2.14.9 Android Studio

Android Studios is an integrated development environment for the android operating system. It's built on IntelliJ IDEA software and designed specifically for android development. Android studio can be used to code in Java, Kotlin, C++, or Dart. It is a powerful environment with plenty of plugins to help development.

3.2.14.10 Xcode

Xcode is a mobile application development environment for macOS used to develop software macOS, iOS, watchOS, and tvOS. Xcode provides an easy-to-use graphical interface to construct simple to complex apps. Xcode is exclusive to the macOS, which means we would not be able to code an Android app with it. Essentially if we choose to use Xcode we would be forced to code two different apps.

3.2.14.11 Visual Studio Code

Visual Studio Code is a source-code editor made by Microsoft for Windows, Linux, and macOS. There are features that support debugging, syntax highlighting, intelligent code completion, code refactoring, embedded Git, and few others. Programming Languages supported are: JavaScript, HTML, Java, CSS, TypeScript, Python, C, and many others. Visual Studio Code also has an Extensions section which allows you to download extensions such as a Live Server to locally test CSS and HTML based websites.

3.2.14.12 Xamarin

Xamarin is a Microsoft-owned free and open-source mobile app platform to build cross-platform native apps in iOS, Android and other OS in C#. Xamarin seems to be not as popular as other cross platform development frameworks.

3.2.14.13 React Native

React Native is a combination of native development with React.js. React native is very flexible and can be used on projects coded in other languages. Develop on iOS and Android is simple with only needing to maintain one code base. React Native is a great tool to make good looking native apps for both platforms.

3.2.14.14 Flutter

Flutter is Google's UI toolkit for building natively compiled applications for mobile, web, desktop, and embedded devices in a single codebase. Flutter contains dart native compilers to incorporate platform differences. Flutter is a great tool for cross-platform development. It googles own coding language Dart.

3.2.14.15 Dart

Dart is a language optimized for productive development of app. Dart can be compiled to ARM and x64 for mobile, desktop, and backend. It can also compile to JavaScript to run on the web. The language is optimized for building user interfaces with features such as sound null safety.

3.2.14.16 Stacks

Stacks are collections of software required for Web/App Development. The stacks often if not always contain the Operating System, Programming Language, Web server, and Database Server. Some types of stacks may be necessary to implement our app properly. Some of the different type of stacks will be summarized in one of the tables below.

Table 3.15: Coding Languages

Languages	Description
Php	Tool to develop APIs.
Python	Can be used to develop APIs.
JavaScript	Can be used for all aspects of development with wide community support and open-source projects.
NodeJS	Tool to develop APIs / Server-side scripting.
Express.js	NodeJS framework that make developing APIs quick and easy.
React.js	Library for front end development
React Native	React for Mobile development
C	Procedural code, very popular, capable of low-level programming.
Objective C	Superset of C, used for iOS mobile development. Supports older iOS devices.
Swift	Apple made language, faster than Objective C.
Java	Can be used to develop application for Android operating system.
Kotlin	Improved lightweight version of Java
Dart	Code used for flutter cross platform development.

Table 3.15.5: Coding Languages Continued

Languages	Description
Xamarin	Cross-platform toolkit, little support

Table 3.16: Development Environments

Development Environments	Description
Android Studios	Development environment capable of handling C++, Java, Kotlin, and Dart.
Xcode	IOS development environment. Apple OS preferred for development.
Visual Studio Code	Powerful development environment great for any project.

Table 3.17: Stacks

Stack Name	Stack Components
MEAN Stack	MongoDB, Express, AngularJS, and Node.js
LAMP Stack	Linux, Apache, MySQL, and PHP
MERN Stack	MongoDB, Express, ReactJS, and Node.js
Django Stack	Django, python, and MySQL
Ruby on Rails	Ruby, PHP, and MySQL

3.3 Part Selection and Comparison

In this section we will be selecting and comparing parts for our SMOCK LOCK. We will write about the different types of Microcontrollers that we have taken a look at, along with Cameras, Speakers, RFID Scanners, PIR Sensors, Fingerprint Sensors, Displays, Relays, Step-Up Boosters and Wi-Fi Modules.

3.3.1 Microcontroller

In this section we will be looking at Microcontrollers, this will allow all of our components to be able to communicate with each other as well as our database/server. We won’t be needing a chip that is capable of handling hard tasks, most of those tasks will be handled by the server. What we will need is something that is compatible with our sensors.

3.3.1.1 ATmega328P

The Atmel ATmega328P is part of the megaAVR family developed by Atmel. It’s based on the AVR enhanced RISC architecture, that is capable of executing powerful instructions in a single clock cycle.

Features:

- 8-bit AVR RISC CPU On-chip 2-cycle multiplier
- Up to 1 MIPS/MHz
- 32 8-bit general purpose working registers
- 32K bytes of in-system programmable flash with read-while-write capabilities
- 1K bytes EEPROM
- 2K bytes SRAM
- 23 I/O lines
- 3 flexible Timer/Counters with compare modes
- Internal and external interrupts
- A serial programmable USART
- A byte-oriented 2-wire serial interface (Phillips I^{2}C compatible)
- SPI serial port
- A 6-channel 10-bit ADC
- Watchdog timer with internal oscillator
- 5 power saving modes
- Operating Voltage 2.7V to 5.5V
- 0 to 8MHz at 2.7 to 5.5V
- 0 to 16 MHz at 4.5 to 5.5V.
- Active mode: 1.5mA at 3V – 4MHz
- Power-down mode: 1µA at 3V
- Price ≈ $ 2.82

3.3.1.2 ATmega4809

The ATmega4809 is part of the megaAVR 0-series, which uses the AVR processor with hardware multiplier which runs at up to 20 MHz. This series uses the latest technologies from Microchip with a flexible and low-power architecture. This includes the Event System and SleepWalking. This part is used in the Arduino Uno REV 2.

Features:

- 8-bit AVR RISC CPU, Single-cycle I/O access, Two-level interrupt controller, two-cycle hardware multiplier
- Up to 1 MIPS/MHz
- 32 8-bit registers directly connected to the ALU
- 48 KB In-system self-programmable Flash memory
- 256B EEPROM
- 6KB SRAM
- 41 Programmable I/O lines
- Watchdog Timer (WDT) with Window mode, with a separate on-chip oscillator

- External interrupt on all general-purpose pins
- A 16-bit Timer/Counter type A (TCA) with a dedicated period register and three compare channels
- Up to four 16-bit Timer/Counter type B (TCB) with input capture
- One 16-bit Real-Time Counter (RTC)
- Master/slave Serial Peripheral Interface (SPI)
- One-10bit 150 ksps Analog-to-Digital Converter (ADC)
- Five selectable internal voltage references: .55V, 1.1V, 1.5V, 2.2V, and 4.3V
- 0-5 MHz @ 1.8V – 5.5V
- 0-10 MHz @ 2.7V – 5.5V
- 0-20 MHz @ 4.5V – 5.5V
- Price ≈ $3.08

3.3.1.3 MSP430FR6989

The MSP430 series uses the ultra-low-power (ULP) 16-bit MSP430 CPU, the ULP architecture showcases seven low-power modes. These modes are optimized to achieve extended battery life in energy-challenged applications.

Features:

- Embedded Microcontroller, 16-Bit RISC Architecture up to 16-MHZ Clock
- 32-Bit Hardware Multiplier (MPY)
- 16, 16-bit registers
- Up to 83 I/O pins
- Ultra-Low-Power Ferroelectric RAM (FRAM) with up to 128KB of Nonvolatile memory.
- 2 KB SRAM
- Five 16-Bit Timers With up to 7 Capture/Compare Registers Each.
- eUSCI_A0 and eUSCI_A1 Support: UART with Automatic Baud-Rate Detection, Serial Peripheral Interface (SPI), IrDA Encode and Decode
- eUSCI_B0 and eUSCI_B1 Support: I^{2}C With Multiple-Slave Addressing, Serial Peripheral Interface (SPI).
- Low-Power Low-Frequency Internal Clock Source (VLO)
- 32-kHz Crystals (LFXT)
- High-Frequency Crystals (HFXT)
- 12-Bit Analog-to-Digital Converter (ADC) With Internal Reference and Sample-and-Hold and up to 16 External Input Channels
- Integrated LCD Driver with Contrast Control for up to 320 Segments
- Active Mode: Approximately 100 µA/MHz
- Standby: 0.4 µA
- Real-Time Clock (RTC): 0.35 µA
- Shutdown: 0.02 µA
- Price ≈ 10.00 to $11.00

3.3.1.5 Microcontroller Selection

We decided to choose the ATmega328P, the hardware specifics are relatively close, and we intend to have our server doing most of the computation, the biggest factor in our selection of the ATmega328P was the overwhelming open-source support. It is compatible, with all of the sensors we intend to use, and since the ATmega328P chip is cheaper and used more often, there's a significant number of tools and documentation on what the 328P is able to run. For a Comparison table please reference Table 3.16.

Table 3.18: Microcontroller Comparison

	ATmega328P	ATmega4809	MSP430FR6989
Price	≈ $ 2.82	≈ $3.08	≈ 10.00 to $11.00
CPU	8-bit AVR RISC CPU On-chip 2-cycle multiplier	8-bit AVR RISC CPU, Single-cycle I/O access, Two-level interrupt controller, two-cycle hardware multiplier	Embedded Microcontroller, 16-Bit RISC Architecture up to 16-MHZ Clock, 32-Bit Hardware Multiplier (MPY)
Operating Voltage	2.7V to 5.5V	1.8V to 5.5V	1.8V to 3.6V
ADC	8-channel 10-bit ADC in TQFP and QFN/MLF package	10-bit 150 ksps Analog-to-Digital Converter (ADC)	12-bit SAR
Flash Memory	32 KB	48 KB	N/A
SRAM	2 KB internal	6 KB	2 KB
EEPROM	2 KB	256 Bytes	N/A
FRAM	N/A	N/A	Up to 128KB non-volatile memory
I^{2}C	Byte-oriented 2-wire serial interface (Phillips I^{2}C compatible)	2-wire interface (Phillips I^{2}C compatible)	I^{2}C With Multiple-Slave Addressing
SPI	Yes	Yes	Yes
UART	Yes	Yes	Yes

Table 3.18.5: Microcontroller Comparison Continued

	ATmega328P	ATmega4809	MSP430FR6989
Registers	32 8-bit general purpose working registers	32 8-bit registers	16, 16-bit registers

I/O Pins	23 I/O lines	41 Programmable I/O lines	Up to 83 I/O pins

3.3.2 Camera

The purpose behind this section is to justify and decide which camera we shall use for the SMOCK Lock. The use of the camera will be to analyze a visitors face and use computer vision to inform the owner, or any other owner-level members, who is at their door. If the camera recognizes an owner, the lock will allow access to the home. That means that the camera needs to be able to be attached to our microcontroller/single board computer so that we may process that information. The camera should also be small, it needs to be able to take up very little space in our already relatively small casing.

3.3.2.1 OV2640

The OV2640 CameraChip image sensor is a low voltage CMOS device that is capable of providing the full functionality of a single-chip UXGA (1632xx1232) camera and image processor in a small footprint package. It is capable of operating at up to 15 fps in UXGA resolution.

Features:

- High sensitivity for low light operation
- Operating Voltage: ~1.2-3.3V
- Image Sizes: UXGA, SXGA, SVGA, any size scaling down from SXGA to 40x30
- Video or Snapshot operation
- Image Transfer Rate: 60-FPS (CIF size), 30-FPS(SVGA), 15-FPS(UXGA,SXGA)
- Supports LED and Flash Mode
- Automatic Image Control Functions: Exposure Control (AEC), Gain Control (AGC), White Balance (AWB), Band Filter (ABF), Black Level Calibration (ABLC)
- 2 Megapixels
- Image Quality Controls: Color Saturation, Gamma, Sharpness, Lens Correction, White Pixel Cancelling, Noise Canceling, 50/60 Hz luminance detection
- Supports Compression
- Lens Size: 1/4”
- Price: ~$1 - 5

3.3.2.2 OV7670

The OV7670 CameraChip image sensor is a low voltage CMOS device that unlike the OV2640 which is capable of running at UXGA is a VGA camera. Its capable of operating at up to 30 fps in VGA. Which would give us a lower image quality but smoother experience.

Features:

- High sensitivity for low light operation
- Operating Voltage ~1.8 - 3.3V
- Image Sizes: VGA, CIF, any size scaling down from CIF to 40x30
- Snapshot Operation
- Image Transfer Rate: 30 FPS (VGA)
- Supports LED and Flash mode
- Automatic Image Control Functions: Exposure Control (AEC), Gain Control (AGC), White Balance (AWB), Band Filter (ABF), Black Level Calibration (ABLC)
- Image Quality Controls: Color Saturation, Hue, Gamma, Sharpness, Anti-Blooming
- 656x488 pixels
- Auto adjust functions: Flicker (50/60 Hz), Saturation Level, De-noise level, edge enhancement level.
- Lens Size: 1/6”
- Price: ~ $5 - 10

3.3.2.3 OV5642

The OV5642 image sensor is a low voltage, high-performance, ¼-inch 5 megapixel CMOS image sensor that is capable of providing the full functionality of a single chip 5 megapixel (2592x1944) camera using OmniBSI technology in a small footprint package. It is capable of operating at up to 15 fps in 5 megapixel resolution.

Features:

- Ultra High Performance
- Operating Voltage: ~1.8 - 3.3V
- Automatic Image Control Functions: Exposure Control (AEC), Gain Control (AGC), White Balance (AWB), Band Filter (ABF), Black Level Calibration(ABLC), 50/60 Hz luminance detection
- Programmable controls for frame rate, AEC/AGC 16-zone size/position/weight control, mirror and flip, scaling, cropping, windowing, and panning
- Image Quality Controls: color saturation, hue, gamma, sharpness (edge enhancement), lens correction, defective pixel canceling, and noise canceling
- Image Sizes: 5 Megapixel, any arbitrary size scaling down from 5 MP
- Auto Focus Control
- Snapshot and Video Operation

- Image Transfer Rate 15 fps(5MP), 30fps(1080p), 60fps(720p,VGA), 120fps(QVGA)
- 5 Megapixel
- Support for LED and flash mode
- Embedded TruFocus light for extended depth of field
- Price: ~$30.00

3.3.2.4 Camera Selection: OV2640

We decided to go with the OV2640 camera since it is very low price, supports video and photo operation modes, gives us a reasonable transfer rate, and can accomplish facial recognition using all the image sizes it provides. The OV5642 would be the best quality camera to go with but since the price is about 5x more than the OV2640, we ultimately decided against it.

An important thing to note would be that the OV2640 is widely used with the ESP32-CAM board to provide users with a simple and efficient way of taking videos or photos, processing them, and sending them to or hosting servers through Wi-Fi and Bluetooth. We plan to purchase the OV2640 along with the ESP32-CAM since the microcontroller we have chosen does not handle image processing well. This will take some of the computational load off the microcontroller and can possibly be used with other sensors. More research will need to be conducted to determine this.

Table 3.19: Camera Comparison

	OV2640	OV7670	OV5642
Price	~$1-5	~$5-10	~$30
Operating Voltage	1.2-3.3V	1.8-3.3V	1.8 – 3.3V
Image Sizes	UXGA, SXGA, SVGA, any size scaling down to 40x30	VGA, CIF, any size scaling down from CIF to 40x30	5 Megapixel, any arbitrary size scaling down from 5 MP
Operation Modes	Video and Photo	Photo	Video and Photo
Image Transfer Rates	60fps(CIF), 30fps(SVGA), 15fps(UXGA,SXGA)	30 FPS (VGA)	15fps(5MP), 30fps(1080p), 60fps(720p,VGA), 120fps(QVGA)

Table 3.19.5: Camera Comparison Continued

	OV2640	OV7670	OV5642
Image Quality Controls	Color Saturation, Gamma, Sharpness, Lens	Color Saturation, Hue, Gamma,	color saturation, hue, gamma, sharpness (edge

	Correction, White Pixel Cancelling, Noise Canceling, 50/60 Hz luminance detection	Sharpness, Anti-Blooming	enhancement), lens correction, defective pixel canceling, and noise canceling
Automatic Image Control Functions	AEC, AGC, AWB, ABF, ABLC	AEC, AGC, AWB, ABF, ABLC	AEC, AGC, AWB, ABF, ABLC
LED and Flash mode	Yes	Yes	Yes

3.3.3 Fingerprint Sensor

The Fingerprint Sensor will be used to allow access to the home. The owner will be able to add their own fingerprint as well as add guests/family members. The fingerprint sensor should have optimal sensing as to not misinterpret the data its receiving. The fingerprint sensor like the camera should also be as small as possible. The fingerprint sensor must be able to communicate with our microcontroller/single board computer.

3.3.3.1 AS608 Optical Fingerprint Sensor

The AS608 is an all-in-one optical fingerprint sensor allows for adding fingerprint detection and verification super simple. There’s a high powered DSP chip that does the image rendering, calculation, feature-finding and searching.

Features:

- Based off the AS608 Processor
- Supply Voltage of 3.8 – 7 V
- Power Supply Current/Operating Current is < 60mA
- Peak Current is usually < 60mA
- Image Input Time is usually < 1 second
- 500 dpi resolution
- UART communication
- Search Time < 220 ms
- Storage: ~240 fingerprints
- Window Size: 15mm x 17mm
- Price: ~$20

3.3.3.2 ID809 Capacitive Fingerprint Sensor

The ID809 has a high-performance processor and semiconductor fingerprint sensor as the core, which is capable of completing all fingerprint identification work independently. The sensor adopts built-in IDfinger6.0 algorithm to complete that feat.

Features:

- Based off the ID809 processor
- Operating Voltage: 3.3V
- Operating Current: <60mA
- UART communication
- 508 dpi resolution
- Search Time: ~300-400ms
- Storage: 80 fingerprints
- Diameter: 21mm
- Height: 5mm
- Price: $16.50

3.3.3.4 Fingerprint Selection

We have decided to go with the AS608 Optical fingerprint sensor. While the ID809 is cheaper and similar to the AS608, the AS608 has three times the storage, a faster search time, and the rectangular size will be able to make better use of space for component layout in our custom enclosure.

Table 3.20: Fingerprint Sensor Comparison

	AS608	ID809
Price	~$20	~$17
Operating Voltage	3.8 – 7 V	3.3 V
Operating Current	<60 mA	<60 mA
Communication Method	UART	UART
Storage Capacity	~240	~80
Size	15mmx17mm	Diameter:21mm
DPI Resolution	500	508
Search Time	<220 ms	300-400 ms

3.3.4 Speaker

The purpose of the speaker module will be used to communicate with the owner, or any other owner-level members, and the visitor. The speaker module must be able to communicate with the microcontroller. The speaker module must be as small as possible, however a powerful and good enough speaker to provide proper audio levels.

3.3.4.1 Degraw Speaker

The Degraw speaker is one of the speakers that we have taken a look at. We intend to use this to help instruct the visitor to position themselves differently so that the camera could get a clear view of the guest.

Features:

- Power: 3 W
- Impedance: 4 Ohm
- Resonance Frequency: 500 ± 20% Hz
- Impedance: 4 Ohm ± 15%
- Rated Input Power: 2 W
- Sensitivity: 82 ± 3dB
- Size: 70mm x 31mm x 16mm
- Distortion Factor: <5% max
- Rated Frequency Range: 0-15 KHz
- Price: ~ $12

This speaker also comes with a PAM8403 amplifier that operates on 5 volts and uses a super smooth potentiometer to adjust the volume.

3.3.4.2 EK1794 Gikfun 1.5" Speaker

The EK1794 Gikfun Speaker is almost half the size of the Degraw speaker however it is slightly lower in performance. This is intended to help instruct visitors how to position themselves in front of the camera.

Features:

- Power: 3 W
- Impedance: 4 Ohm
- Diameter: 40mm
- Height: 20mm
- Input Power Rating: 2 W
- Resonance Frequency: 320Hz±20%
- Rated Frequency Range: 0-20 KHz
- Distortion Factor: max 5%
- Sensitivity: 83 ± 3 dB
- Price:~ $13

3.3.4.3 Speaker Selection

We have decided to go with the Degraw speaker. It has a higher resonance frequency than the Gikfun, it's cheaper, and since it is a rectangle form factor, we can make better use of space for component placement in the custom enclosure.

Table 3.21: Speaker Comparison

	Degraw	Gikfun
Price	$12	$13
Rated Power	3 W	3 W
Impeadance	4 Ohm	4 Ohms

Size	70mm x 31mm x 16mm	40 mm diameter, 20 mm height
Sensitivity	82 ± 3db	83 ± 3db
Resonance Frequency	500 Hz ± 20%	320 Hz ± 20%
Distortion Factor	Max 5%	Max 5%
Frequency Range	0-15KHz	0-20KHz

3.3.5 Lock Mechanism

After researching the different types of lock mechanisms to use, we decided that an electric solenoid would make the best use of space and would be the simplest and most efficient way to demonstrate the SMOCK. The solenoid does raise the problem of not having a back-up key, but we plan to give alerts to homeowners through the app well in advance that the battery life is low, and the batteries will need to be replaced soon.

For the most part the locking mechanisms we will be looking at in this section are relatively the same, except for some size differences and input conditions for the lock to actually function. We intend to provide power to the lock when necessary to help unlock/lock the door.

Features:

- Input Voltage: 12V
- Input Current: 350mA
- Small Size
- Latch style solenoid
- Has a positive and negative power connection
- Latch opens when power is supplied
- Latch stays locked when no power is supplied
- Dimensions: 17mm(H) x 27mm(L) x 15mm(W)

3.3.5.4 TAKAHA DC 6V 12V Electric Solenoid Lock

The Takaha Electric solenoid lock is the second lock we are taking a look at, compared to the QWORK the input current is substantially larger, however the dimensions are also a bit larger, so with the more current needed to power we can see that the lock size grew.

Features:

- Input Voltage: 6V or 12V
- Input Current: 1.3 A or 2.7A
- 10 mm thickness on main body
- Uses a latch catch style solenoid
- When power is supplied, the lock will unlock
- When no power is supplied, the lock remains locked

- Dimensions 47mm(H) x 10mm(W) x 105mm(L)

3.3.5.5 ATOPLEE Electromagnetic Solenoid Lock

The ATOPLEE electromagnetic solenoid lock is the last lock that we will be looking at, priced slightly higher than the QWORK, the ATOPLEE provides the same thing, however this lock is also larger than the QWORK which may cause some problems due to our size constraints.

Features:

- Input Voltage: DC 12 V
- Input Current 0.8 A
- Conduction Time: 10s
- Uses a Cylinder style solenoid
- Small Size
- Has a positive and negative power connection
- Cylinder opens when power is supplied
- Cylinder stays locked when no power is supplied
- Dimensions: 55mm x 42mm x 27mm

3.3.5.6 Lock Mechanism Selection

We have decided to go with the QWORK lock for our lock mechanism. Due to the number of components in our system, we needed to choose a small form locking mechanism. This divided the decision between the QWORK and the ATOPLEE electric solenoids. We decided that the latch style solenoid would be best for our product as the latch will allow the door to close and push against whereas the cylinder would provide resistance.

Table 3.22: Lock Mechanism

	QWORK	TAKAHA	ATOPLEE
Price	$14.70	$35.00	$19.99
Input Voltage	DC 12V	DC 6V or DC 12V	DC 12V
Input Current	350 mA	1.3 A or 2.7A	0.8 A
Solenoid Style	Latch(Pull)	Latch (Catch)	Cylinder (Pull)
Dimensions (mm)	17x27x15	47x10x105	55x42x27
Number of Pieces	4	1	2

3.3.6 PIR Sensor

The purpose of the PIR sensor is to sense people approaching the door. The goal is to have all the other biometric features disabled unless the PIR sensor senses movement made by a person. This is to allow for a longer lifespan for the power source. The PIR Sensor must be able to send information to the microcontroller when it registers that movement.

3.3.6.1 DIYmall HC-SR501 PIR Motion IR Sensor

The DIYmall HC-SR501 PIR Motion IR Sensor is prices at just above $10.00. The range of the motion sensor is adjustable as well as having a high delay time compared to the other options we are looking at.

Features:

- Operating Voltage DC 4.5 – 20 V
- Based on HC-SR501
- Quiescent Current: <50uA
- Delay Time of 5 – 18 seconds
- Uses Potentiometer 105 to adjust delay time and sensitivity
- Block Time of 2.5 seconds

3.3.6.2 Stemedu HC-SR501 PIR Sensor

The Stemedu HC-SR501 PIR Sensor, is the second PIR sensor we are taking a look at priced just like the DIYmall, this PIR sensor also comes with an adjustable range.

Features:

- Based on HC-SR501
- Uses Potentiometer 105 to adjust delay time and sensitivity
- Operating Voltage DC 4.5-20V
- Quiescent Current < 50 uA
- Delay Time of 0.5-200 seconds
- Block Time of 2.5 seconds

3.3.6.3 DaFuRui AM312 PIR Sensor

The DaFuRui is our highest priced PIR Sensor, however it does not seem that the range is adjustable like our other to options. This is a very important feature because, we intend to register movement from the PIR Sensor to send a power signal for the rest of the lock.

Features:

- Working Voltage: DC 2.7-12V
- Based on AM312 Chip
- Delay Time: 2 seconds
- Block Time: 2 seconds
- Static Power Consumption: < 0.1 mA
- Range of 3-5 meter

Table 3.23: PIR Sensor Comparison Table

	DIYmall	Stemedu	DaFuRui
Price	$10.49	$10.49	$11.99
Operating Voltage	4.5V-20V	4.5V-20V	2.7V - 12V
Quiescent Current	<50uA	<50uA	Not Stated
Interface Type	Uses triggers and digital pins	Uses triggers and digital pins	Uses triggers and digitial pins
Delay Time	5-18 seconds	0.5-200 seconds	2 seconds
Range	Adjustable	Adjustable	3-5 meters
Block Time	2.5 seconds	2.5 seconds	2 seconds
Number of Pieces	5	5	5

3.3.6.4 PIR Sensor Selection

We have decided to go with the DIYmall PIR sensor. This sensor has an adjustable range and delay through the use of potentiometers. It has an operating voltage of 4.5-20V which should be fine through the 5V the Arduino board provides but if 5V is not sufficient, we can make use of 12V provided by the Step-Up boost. This product is very similar to the PIR sensor provided by Stemendu but the DIYmall sensor has more reviews and documentation.

3.3.7 RFID

The purpose of the RFID Sensor is to serve as a key if necessary. Depending on our choice of lock an RFID sensor may be used. The sensor must be able to communicate with the microcontroller/single board computer, which will then unlock the door.

3.3.7.1 Mihappy RFID Sensor Module Kits

The Mihappy RFID Sensor Module Kit has a slightly larger read range than the SunFounder RFID kit, other than that the specifications of both parts are nearly identical which should make selecting a part easier.

Features:

- Based on the Phillips MFRC522 Chip
- Power Voltage of 3.3V
- Current of 13-26 mA
- Operating frequency 13.56 MHz
- Uses a SPI interface
- Has a max read range around 60mm

3.3.7.2 SunFounder RFID Kit

The SunFounder, like its Mihappy counter part has mostly the same specs except with a slight difference in the read range, coming just short of the Mihappy 60mm, with a read range of 35mm.

Features:

- Based on the Phillips MFRC522 Chip
- Uses a SPI interface
- Power Voltage of 3.3V
- Operating Frequency of 13.56 MHz
- Read Range: 0 ~ 35mm
- Operating current of 13-26mA

3.3.7.3 RFID Selection

We have decided to go with the Mihappy RFID Sensor Module. After comparing the two, we found that the Mihappy is quite similar to the SunFounder RFID module, but the Mihappy has a max read range of 60mm where the SunFounder has a max read range of 35mm. This module is priced at $10.80.

Table 3.24: RFID Comparison Table

	MiHappy	SunFounder
Price	$10.80	$6.99
Input Voltage	3.3V	3.3V
Operating Current	13-26mA	13-26mA
Interface Type	SPI	SPI
Read Range	0~60 mm	0~35 mm
Operating Frequency	13.56 MHz	13.56 MHz
Number of Pieces	1	1

3.3.8 Display

The display will be used to provide visual assistance to anyone unfamiliar with some of the features such as the camera. The display must be compatible with the microcontroller/single board computer.

3.3.8.1 16x2 LCD

This 16x2 LCD, is a 16-character x 2 line LCD, this should allow us to print all the necessary instructions however they will be limited to just 16 characters per line which is a restriction that we would like to avoid.

Features:

- 16 characters x 2 lines

- MPU Interface: 4-bit or 8-bit
- Size: 80mm x 36mm x 13.5mm
- Backlight: LED
- LCD Type: FSTN Negative
- Response Time: ~1ms
- Price: ~ $7

3.3.8.2 OLED

Our second option for the display is an OLED display, which has 128x32 resolution and is able to scroll through the text offering high resolution display, which will allow the reader to easily absorb the instructions that are being displayed.

Features:

- Every pixel can be illuminated
- Resolution: 128x32
- Backlight: N/A (Self-illuminated)
- Response Time: ~ .01ms
- Lower power consumption as there is no need to power a backlight
- Size: .91 inch
- Price: ~ $6

3.3.8.3 20x4 LCD

This 20x4 LCD offers more characters and lines compared to the 16x2 LCD, priced at around $8.00 it is the second most expensive Display.

Features:

- 20 characters x 4 lines
- MPU Interface: 8-bit
- Size: 97mm x 59mm x 12mm
- Backlight: LED
- LCD Type: FSTN Negative
- Response Time: ~1ms
- Price: ~ $8

3.3.8.4 Display Selection

We have decided to go with an OLED display. Since the response time is much faster than a traditional LCD, and since it is self-illuminated, the power consumption will be much lower than a traditional LCD. We believe this difference in power consumption will make up the price difference of $1. We are also trying purchase small components which this small but effective Display Selection will help us achieve.

Table 3.25: Display Comparison

	16x2 LCD	OLED	20x4 LCD
Price	$7	$9	$8
MPU	4-bit, 8-bit	4-bit, 8-bit	8-bit
Backlight	LED	Self-illuminated	LED
Response Time	~1ms	~.01 ms	~1ms
Size	80x36x13.5(mm)	38x12 (mm)	97x59x12 (mm)

3.3.9 Wi-Fi Module

The Wi-Fi Module will be used for any of the microcontrollers that come unequipped with one. It will be used so that the microcontroller can communicate with the database/server over the homeowners Wi-Fi.

3.3.9.1 ESP8266

This product is made by Espressif and makes use of the ESP8266EX. It delivers highly integrated Wi-Fi SoC solution to meet a user's demands with efficient power usage, and a compact design. It has complete and self-contained Wi-Fi networking capabilities and is capable of performing as either a standalone application or as the slave to a host MCU.

Features:

- CPU: Tensilica L106 32-bit processor
- 17 GPIO
- RAM size < 50 kB
- External Flash supports up to 16MB memory capacity.
- No ROM
- Protocols: 802.11 b/g/n (HT20)
- Frequency Range 2.4GHz ~ 2.5GHz
- UART/SDIO/SPI/I^{2}C/I^{2}S/IR Remote Control
- Operating Voltage: 2.5V ~ 3.6V
- Operating Current: Average value of 80 mA
- Package Size: QFN32-pin (5 mm x 5 mm)
- Wi-Fi Mode: Station/SoftAP/SoftAP+Station (Soft Access Point)
- Security Protocol: WPA/WPA2
- Encryption: WEP/TKIP/AES
- Network Protocols: IPv4, TCP/UDP/HTTP
- User Configuration: AT Instruction Set, Cloud Server, Android/iOS App

3.3.9.2 ESP32

The ESP32 is made by Espressif. ESP32 is a single 2.4 GHz Wi-Fi-and-Bluetooth combo chip. It's designed with the TSMC ultra-low-power 40nm technology. It is designed to achieve the best power and RF performance. Its versatile, robust, and reliable in a wide variety of applications and power scenarios.

Features:

- CPU: Xtensa® single-/dual-core 32-bit LX6 microprocessor(s)
- 34 programmable GPIOs
- 448 KB ROM
- 520 KB SRAM
- 8 KB of SRAM in RTC
- Up to 16 MB of external flash can be mapped into CPU instruction memory space and read-only memory space simultaneously
- 802.11 b/g/n
- 802.11 n (2.4 GHz), up to 150 Mbps
- Simultaneous support for Infrastructure Station, SoftAP, and Promiscuous modes
- Compliant with Bluetooth v4.2 BR/EDR and Bluetooth LE specifications
- 12-bit SAR ADC up to 18 channels
- 2 8-bit DAC
- 10 touch sensors
- 4 SPI
- 2 I^2S
- 2 I^2C
- 3 UART
- 1 host (SD/eMMC/SDIO)
- 1 slave (SDIO/SPI)
- Security: AES, Hash (SHA-2), RSA, ECC
- CCMP (CBC-MAC, counter mode), TKIP (MIC, RC4), WAPI (SMS4), WEP (RC4) and CRC
- Operating Voltage: 2.3 V to 3.6 V
- Recommended Output Current is 500 mA or more.
- Package: 6 mm x 6 mm

3.3.9.3 CC3120

The CC3120R device is part of the SimpleLink microcontroller (MCU) platform. It consists of Wi-Fi, Bluetooth low energy, Sub-1 GHz and host MCUs. A one-time integration of the SimpleLink platform enables anyone to add any combination of the devices from the portfolio into their design. This allows for code reuse whenever design requirements change.

Features:

- Processor: on-chip Arm network processor.
- Featuring a Dedicated Wi-Fi Internet-on-a chip™ Wi-Fi NWP that Completely Offloads Wi-Fi and Internet Protocols from the Application Microcontroller Unit (MCU)
- 802.11b/g/n Station

- The maximum supported serial flash size is 32MB
- WEP/WPA/WPA2/WPA3
- IPv4 and IPv6 TCP/IP Stack
- VBAT Wide-Voltage Mode: 2.1 V to 3.6 V
- Current Range: 420 mA to 700 mA
- 64 pins
- 9-mm × 9-mm Very Thin Quad Flat Nonleaded (VQFN) Package
- 1 SPI
- 1 UART

3.3.9.4 Wi-Fi Module Selection

We have decided to go with the ESP8266. After our research we chose the ESP8266 because of its low power consumption. It also uses WPA/WPA2 which are the two most popular forms of Wi-Fi protocols. It’s also the smallest chip out of the three we researched.

Table 3.26: Wi-Fi Module Comparison

	ESP8266	ESP32	CC3120
Price	$1.60	$2.00	$3.00
CPU	Tensilica L106 32-bit processor	Xtensa® single-/dual-core 32-bit LX6 microprocessor(s)	on-chip Arm network processor
RAM	RAM size < 50 kB	520 KB SRAM	N/A
Other Memory	External Flash supports up to 16MB	448 KB ROM, Up to 16 MB of external flash	maximum supported serial flash size is 32MB
Operating Voltage	2.5V ~ 3.6V	2.3 V to 3.6 V	2.1 V to 3.6 V
Current	Average 80 mA	500 mA	420 mA to 700 mA
SPI	2	4	1
UART	2	3	1
Wi-Fi Protocol	WPA/WPA2	N/A	WEP/WPA/WPA2/WPA3
Pins	17	34	64
Bluetooth	No	Yes	No
I²C	1	2	N/A
I²S	1	2	N/A
Package Size	5mm x 5mm QFN	6mm x 6mm QFN	9 mm x 9mm VQFN

3.3.10 Relay

To control when the lock opens and closes through the microcontroller, we need a component that can control when power is supplied to the lock since the lock is always locked when no power is supplied and unlocks when power is supplied. This can be done through a relay module.

3.3.10.1 Relay Selection

We have decided to go with a 5V 1-Channel SRD relay. Since we can supply a voltage of 5V from the board, a 5V relay would be the best voltage option. Since the lock mechanism only has a positive and negative wire, we will only need 1 channel on relay. We can then connect a digital pin from the microcontroller to the signal pin on the relay to control when the lock locks and unlocks.

3.3.11 Step-Up Boost Converter

If we decide to use a solenoid latch locking mechanism, most on the market require 12 V to operate. Since the board only supplies 5V maximum, we can make use of a step-up boost converter to get the 12V we need for the lock without the need of a separate battery. The step-up converter can be seen as a class of switch-mode power supply that contains at least two semiconductors, mainly a diode and transistor, and some type of energy storage element, usually a capacitor, a inductor, or a mix of the two.

3.3.11.1 XL6019

The XL6019, is a Step-Up Boost Converter, that has an input range of 5V-40V, this will allow us to send any signal we desire, given that our power supply is able to provide a sufficient amount of power. This will then Step-Up the Voltage from 5V to 12V.
Features:

- Input Range: 5V-40V
- Maximum Output: 60V
- Switching Frequency: 180 KHz
- Switching Current: 5 A
- Efficiency of 94%
- Built in Frequency Compensation
- Built in Thermal Shutdown Function
- Built in Current Limit Function
- EN PIN TTL shutdown capability
- Price: ~$0.85

3.3.11.2 XL6009

The XL6009 is the second step-up booster we are taking a look at with a slightly higher price point for a slightly better performing step-up booster, However, it does limit our Input Range, when comparing to the XL6019.

Features:

- Input Range: 5V-32V
- Maximum Output: 60V
- Switching Frequency: 400 kHz
- Efficiency of 94%
- Built in Frequency Compensation
- Built in Thermal Shutdown Function
- Built in Current Limit Function
- Switching Current: 4 A
- EN PIN TTL shutdown capability
- Price: ~$1.60

3.3.11.3 MT3608

The MT3608, is the least expensive step-up booster we are looking at, however, with that being said it does offer the highest efficiency rating which is something that we value a lot more than the price of the part we are purchasing. This may put the MT3608 on top, for more please view our comparison table below.

Features:

- Input Range: 2V-24V
- Switching Frequency: 1.2MHz
- Efficiency 97%
- Switch Current: 4A
- Built in Frequency Compensation
- Built in Thermal Shutdown Function
- Built in Current Limit Function
- EN PIN TTL shutdown capability
- Up to 28V Output
- Price: ~$0.60

3.3.11.4 Step-Up Boost Selection

We have decided to go with the MT3608 Step-Up converter due to its low price, higher switching frequency and higher efficiency. We only need to have an output of 12V so there is no need to go with a step-up boost with a higher output range. This component will provide more than enough power for our lock mechanism.

Table 3.27: Step-Up Boost Comparison

	XL6009	XL6019	MT3608
Price	$1.60	$0.85	$0.60
Input Range	5V-32V	5V-40V	2V-24V

Table 3.27.5: Step-Up Boost Comparison Continued

	XL6009	XL6019	MT3608
Output Range	Up to 60V	Up to 60V	Up to 28V
Efficiency	94%	94%	97%
Switching Frequency	180 KHz	400 KHz	1.2MHz
Switch Current	4A	5A	4A

3.4 Part Selection Summary

In this section, we are summarizing the parts that we have selected to use for the SMOCK Lock design.

Table 3.28: Final Parts List

Part	Selected Part	Part Description
Microcontroller	Atmega328p	Single chip microcontroller with 8-bit RISC processor core
Wi-Fi Module	ESP 8266	Low-cost Wi-Fi microchip
Camera	OV2640	2MP low power camera module. ESP32-CAM will support the cameras functions
Fingerprint Sensor	AS608	Optical fingerprint sensor with a storage of 240 fingerprints
Lock Mechanism	QWORK Electric Solenoid	Latch style electromagnetic solenoid.
PIR Sensor	DIYmall	Motion detection sensor
RFID	Mihappy	Passive RFID Sensor Module
Speaker	Degraw	3W 4Ohm Rectangular Speaker
Display	OLED	128x32 OLED Screen Display
Relay	5V 1 Channel	5V 1 channel relay to open and close lock with power
Step-Up Boost	MT3608	Highly efficient 2-24V input dc to dc converter with a max output voltage of 28V

4.0 Related Standards and Design Constraints

The standards written in this section will include all the standards necessary for our SMOCK LOCK. Which will speak about standards like Electrical and PCB Standards, Coding Language Standards, Security Standards, Testing Standards, Lock Standards, Recognition Standards, and General Standards.

4.1 General Standards

An engineering standard is essentially a technical document drafted by a group of engineers that acts as a guideline for all manufactures and designers. These guidelines act as a way to promote safe and cohesive integration of new technology into the public. Without these standards much of the technology we use today could not be possible. For instance, the standard American plug is a standard adopted nationally to allow the public to freely use all electronics developed using this standard. All standards are optional and are created and maintained by many companies, the most recognizable of these being The Institute of Electrical and Electronics Engineers Standards Association, The American National Standards Institute, and The International Organization for Standardization.

The International Organization for Standardization is a company, based in Geneva, Switzerland, that allows for technology to be standardized internationally by recruiting national standardization bodies to become members of this body. Almost all the countries in the world are member countries with voting rights, with the rest of the countries being correspondent members due to not having a national standard body. The Institute of Electrical and Electronics Engineers Standards Association and The American National Standards Institute are both members of the International Organization for Standardization.
The Institute of Electrical and Electronics Engineers Standards Association and The American National Standards Institute are national body of standards based in the United States that has many ties to international bodies allowing for the standards enforced to be compatible with the international market. Many of the standards we will be adhering too while designing the SMOCK lock will be from these two bodies.

The SMOCK lock also must comply with building standards and codes as it is going to be placed on a door of egress. The standards that the lock will follow are from the International Building Code. The International Building Code is a set of building codes and standards developed by the International Code Council, which is the most widely accepted set of building standards in the United States.

4.2 Electrical and PCB Standards

In this section we will research the different kinds of Electrical and PCB Standards. All of which will be necessary for the SMOCK Lock to fulfill those standards. We will dive into the IEEE Standard for Design and Verification of Low-Power Integrated Circuits and the ANSI/IPC-2221

4.2.1 IEEE Standard for Design and Verification of Low-Power Integrated Circuits (IEEE Std 1801-2013)

The standard above specifies a way for which a designer can safely and efficiently create a Low-Power Integrated Circuit. This is done through the use of continuous power refinement specifications which are from the following aspects of the circuit, supply, switches, isolation and retention. The standard also combines the power requirements and the design specification and creates a working relationship between them.

This standard would allow for an ease into the development of the SMOCK lock's electrical systems by allowing power consumption calculation to be made gradually allowing for some room to improve the design later.

4.2.2 ANSI/IPC-2221 Standards in Circuit Board Design

This standard is a generic method for the development of PCB and other components for electrical applications. As a PCB is being designed for the SMOCK lock's informational and power systems the standards above will ensure a PCB will be developed in the safest and efficient way possible. For specifics the main purpose is to create a general rule for the features of the PCB, these are shown below.

Table 4.0 - Circuit board design Standards

Feature	Specifics
Leads/Pins	.13mm
Probe Sites	3mm (2mm plus or minus depending on project)
Mounting	Cannot be farther then 6.4mm from the board
Creepage (space between traces)	Double the width of the trace itself

The standard also includes the format which to calculate the trace thickness based on the current given by $W = \frac{A^2}{T*1.378}$, where A is the area, T is the thickness and 1.378 is a constant based on the standard. The rest of the standard delves into high voltage circuits, greater than 50V, this will not be required for the SMOCK lock's PCB.

4.2.3 IEC 62368-1 An Introduction to the New Safety Standard

The main point of the above standard is to classify energy sources and how dangerous they are to human safety below is the provided levels of the dangerousness

Table 4.1 – Safety Standards

Class	Effect on Body	Effect on Materials
Class 1	Not painful	Ignition will probably not happen
Class 2	Painful, minor injury	Ignition possible but is greatly limited in the growth and spread.
Class 3	Injury	Ignition almost guaranteed, with rapid growth.

4.3 Coding and Language Standards

The different coding and language standards that are discussed in this are Information Technology -- Programming language – C, Systems and Software Engineering standard, and Other Coding Guidelines.

4.3.1 ISO/IEC 9899:2018 Information technology — Programming languages — C

The standard above states more the layout of a C program rather than any functional requirement and is only to be interpreted as a way to code legibly so other programmers can interpret the code being developed. As such the standard delves into the syntax, semantics, and representation of data in which the program is computing in C. The standard also goes into the limits of the language and a way to determine whether C is an effective language for the task.
The SMOCK lock will be using the C language as a high-level assembly language to program the microcontrollers or make simulations server side for recognition purposes.

4.3.2 Other Coding Guidelines

The SMOCK lock will utilize many languages from C++, SQL (for databases), React Native, MIPS, Java Script, and possibly others. All languages have a general suggested guideline for how to format programs, use syntax, and semantics. Below will be links to each of the guidelines we could possibly use, please reference Table 4.2: Coding Guidelines.

Table 4.2: Coding Guidelines

Language	Link to guideline
C++	https://users.ece.cmu.edu/~eno/coding/CppCodingStandard.html
Python	https://www.python.org/dev/peps/pep-0008/
MIPS	http://cs.brown.edu/courses/cs031/content/docs/asmguide.pdf
React Native	https://www.reactnative.guide/6-conventions-and-code-style/6.0-intro.html
SQL	https://www.sqlstyle.guide/
Java Script	https://google.github.io/styleguide/jsguide.html
Swift	https://google.github.io/swift/

4.3.3 ISO/IEC 12207:2008 Systems and software engineering — Software life cycle processes

This standard shows a flowchart of the development of software including development, maintenance, and operation. Also, a portion of the standard deals with the purchase and implementation of external software, this will not be required for the development of SMOCK lock. The processes of the standard are mainly used to define methods and execution of the program to allow for the easiest way to develop the program to the requirements that are specified.

4.4 Security Standards

In this section we will discuss the different security standards that we must abide by during the development of the SMOCK Lock.

4.4.1 ISO/IEC 15408 Standard

Also known as “Common Criteria” this allows for a secure way to test and implement requirements that a consumer provides without compromising the integrity of an existing system. Once the environment is ensured the standard then goes into the testing of the software to ensure two things. The first being whether it checks all the Security Assurance Requirements. The second being a score between EAL 1 and EAL 7 called the Evaluation Assurance Level, with 7 being the most stringent on security.

4.4.2 ISO/IEC 27001/27002 Standard

The main point of the ISO/IEC 27001 standard is to implement a management system that specifically brings any user information into it and allows any admins to the system to have direct control of the ability to wipe any sensitive data. This standard provides the framework for the management system.

The ISO/IEC 27002 standard is a guide to transfer an older system to adhere to this standard and allows for systems to be backwards compatible. This standard award a certification that lasts three years and must be renewed to keep good standing in the standard.

4.4.3 ETSI EN 303 645 Standard

The standard above provides a set of requirements when working with consumer technologies that is working with the Internet of Things. The following are the requirements provided in the standard.

- No default passwords
- Must have auto updating software
- Ensure a secure place to store any secure information including system parameters
- Have a secure line of communication
- Minimize attackable surfaces
- Have a method of ensuring software integrity
- Make the system impervious to outage damage
- Ensure the ability for the deletion of secure data
- Ensure easy installation and upkeep

4.4.4 IEEE 802.11 Standards- Wireless LAN technology

The IEEE 802.11 standard specifies the set of MAC and PHY protocols for implementing Wireless Local Area Networks or WLAN computer communication. The standard provides the basis for wireless network products using the Wi-Fi brand and is the most widely used standard in relation to wireless computer networking in the world.

4.5 Testing Standards

In this section we will be discussing the different testing standards that we must follow during testing the components and software of our SMOCK Lock design.

4.5.1 ISO/IEC/IEEE 29119-1:2013(en) Software and systems engineering — Software testing

The Standard above defines the terms and concepts used while testing programs to allow for codes to be compared and tested in a similar way internationally. The standard mostly is used to allow tests that are ran on software to be comparable to other similar software, thus allowing for benchmarks to be established. The tests range from capacity, data, run time, data retention, test cases, stress tests, security, portability, and load testing.

For the purposes of SMOCK Lock the software is to be tested at all stages of the code, which are broken down into the database, sever, microcontroller program, and recognition programs. All of which will be tested by using the methods described in the standard.

4.5.2 PCB / Lock Testing

In reference for the testing of the PCB the standard, *ANSI/IPC-2221 Standards in Circuit Board Design,* has a section for testing the PCB, this will be the method of testing for the PCB for the SMCOK Lock.

In reference for the testing of the lock itself the 3 codes in the section, Lock and Building Standards, the testing will be enacted by ensuring that the SMOCK Lock itself performs up to code.

4.6 Lock Standards

In this section we will discuss the different lock standards, they are Locks and Latches Standards, Door Hardware Release of electrically Egress doors Standard, and Sensor release of electronically locked egress doors.

4.6.1 IBC 1010.2.4 Locks and latches

This standard in the 2021 International Building Code (IBC) details in which cases locks or latches are permitted. Section 1010.2.4.5 states that doors of egress from individual dwelling units may have installed a “night latch, deadbolt or security chain” so long as it is operatable from the inside of the unit without a key or any kind of tool.

4.6.2 IBC 1010.2.11 Door hardware release of electrically locked egress doors

Residential properties are permitted the use of electronically locking and unlocking egress doors so long as the lock meets certain requirements. Electrically operated locks and latches must have obvious mechanical operation that must also have the ability to be performed singlehandedly. Operation of the handle must interrupt power to said lock and unlock it immediately. Outages or any form of power loss must also automatically unlock or unlatch said hardware.

4.6.3 IBC 1010.2.12 Sensor release of electrically locked egress doors

Residential properties may have sensor release electric locking mechanisms so long as they meet certain requirements. Sensors must be positioned on the egress (outside) to detect an approaching occupant, and hardware must have obvious mechanical operation. Loss of power or function to either the sensor or the lock must both result in automatic unlocking or unlatching. Use of mechanical locking hardware must interrupt power to electric operating mechanisms. Activation or use of any emergency system such as fire alarms or fire sprinkler release must also result in automatic unlocking or unlatching. Egress side (outside) of door must also have emergency lighting.

4.7 Recognition Standards

The recognition standards discussed about in this section are Standard for Performance Evaluation of Biometric Information: Facial Recognition, Standard for Performance Evaluation of Biometric Information: Fingerprint Recognition, and Ethical Standards.

4.7.1 P2884 - Standard for Performance Evaluation of Biometric Information: Facial Recognition

The standard above allows for the definition and testing of facial recognition against other systems to allow for a comparison, which determines whether or not the system created is up to standard. This allows for developing facial recognition systems to have a benchmark to hit by creating uniform tests. The testing includes mainly the calculation and comparison of two values the false accept rate and the false reject rate. Using these two values the standard allows for a benchmark.

4.7.2 P2891 - Standard for Performance Evaluation of Biometric Information: Fingerprint Recognition

The standard above is created by the same working group and essentially uses the same testing as the facial recognition standard, *P2884 - Standard for Performance Evaluation of Biometric Information: Facial Recognition.* The main difference will be the actual method of gaining the data, i.e. using a fingerprint scanner.

4.8 Ethical Standards

The Institute of Electronics and Electronics Engineers has a code of ethics that serves as a standard. The code of ethics is as follows:

I. To uphold the highest standards of integrity, responsible behavior, and ethical conduct in professional activities.

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment
2. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems
3. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist
4. to avoid unlawful conduct in professional activities, and to reject bribery in all its forms
5. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, to be honest and realistic in stating claims or estimates based on available data, and to credit properly the contributions of others
6. to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations

II. To treat all persons fairly and with respect, to not engage in harassment or discrimination, and to avoid injuring others.

7. to treat all persons fairly and with respect, and to not engage in discrimination based on characteristics such as race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression
8. to not engage in harassment of any kind, including sexual harassment or bullying behavior
9. to avoid injuring others, their property, reputation, or employment by false or malicious actions, rumors or any other verbal or physical abuses

III. To strive to ensure this code is upheld by colleagues and co-workers.

10. to support colleagues and co-workers in following this code of ethics, to strive to ensure the code is upheld, and to not retaliate against individuals reporting a violation.

4.9 Internet Protocol Standards

In this section we will go over all the Internet Protocol Standards that are relevant with respect to the parts that we have compared and selected. Those Internet Protocol Standards being Wired Equivalent Privacy (WEP), Wi-Fi Protected

Access (WPA), Wi-Fi Protected Access Pre-Shared Key (WPA-PSK), WPA2, and WPA2-PSK.

4.9.1 WEP

A WEP protected network contains a secret key called the root key which originally had a key length of 40 bits but can have a length of up to 232 bits which is shared between all stations on the network. WEP offers two modes of authentication for stations attempting to join the network. Open System authentication simply allows a client to request to join the network and the network responds with success. Shared key authentication uses a challenge response handshake. When a client attempts to join, the access point responds with a random number in plain text. The client needs to correctly send a frame containing the random number encrypted with the secret key. If the access point is able to decrypt the frame with the secret key and it contains the random number, the client will be allowed to join the network. Data frames that are sent over the network are encrypted and have checks for integrity. This is completed through a multistep process. First, the station will pick a 24-bit initialization vector that is prepended to the root key to form a per packet key. Next, a CRC32 checksum of the current payload called the integrity check value is produced. The perpacket key is fed into a RC4 stream cipher to produce a key stream of the length of the payload. Finally, the payload with checksum is XORed with the keystream to produce the cipher text. This text along with the initialization vector are used to build a packet to send to the receiver. The packet produced will contain multiple headers that are not encrypted, such as the initialization vector which could allow hackers to conduct partial key recovery attacks, which will help recover the full key in later attacks.

There are many flaws with WEP to name a few, WEP uses master keys directly allowing people to grab it from accessing one stolen packet. The secret keys were often only 40 bits, which is relatively small and easy to hack through brute force. These keys are rarely managed correctly and can often be long lived allowing repeated access to hackers who have already captured the secret key. WEP's implementation of RC4 can result in weak keys being created which are easy to sniff out.

The protocol also has vulnerabilities relating to reusing small sized initialization vectors and using a weak cryptographic hash in CRC-32 to create the integrity check value. Authorization vulnerabilities were also present. A hacker could sniff out a user's physical MAC address to imitate that user on the network. There have been many attacks on WEP developed over the years. One of the most advanced attacks on WEP is the PTW attack, which focuses on attacking the RC4 stream cipher to fully recover a secret key with nearly a 100 percent success rate and negligible computational power required. With the secret key, packages can be intercepted, decrypted, and encrypted with ease. This can allow for the hacker to gain the ability to read and edit any information a user is sending over the internet.

4.9.2 WPA

Due to the glaring deficiencies of the WEP protocol in protecting networks. A new protocol was developed to protect against all the vulnerabilities discovered from WEP, while still being compatible with networks that currently use the WEP protocol. The Wi-Fi Protected Access (WPA) protocol was introduced as a subsection in the 802.11i standard. This protocol shores up a lot of the breaches that were discovered in WEP.

With the introduction of WPA, a new Temporal Key Integrity Protocol (TKIP) is used for encryption and per packet key generation. There are also new checks for integrity of the data packet with the new “Michael” algorithm.

The WPA encryption process has a few key changes that prevent attacks similar to the ones used on WEP protected networks. To start, TKIP is used to generate a 128-bit temporal key that is unique for each packet. The initialization vector (IV) is now 48-bits and is part of the temporal key. The IV is used as a sequencing number to prove the freshness of the packet being sent. The sequencing number along with the introduction of the Medium Access Control Service Data Unit (MSDU) and Medium Access Control Protocol Data Unit (MPDU) prevents replay attacks that the WEP protocol was susceptible to. The “Michael” algorithm is used to create a 64-bit Message Integrity Code (MIC). The MIC is responsible for detecting errors in data content such as transfer errors, or purposeful manipulation of the data. The MIC is appended to the end of the plaintext in the MSDU, this is then used to create a CRC checksum which is now the Integrity check value. Thus, the encryption of the integrity check value is not reliant solely on the CRC checksum. The introduction of the “Michael” algorithm and MIC prevents the attacks that were possible on the ICV in WEP. The encryption process of WPA still uses the RC4 cipher stream, however, the base key and IV are hashed together before being fed into the RC4 cipher stream. The resulting stream will be XORed with the plaintext MPDU to create the ciphertext.

There are also two new modes in which WPA can function. These modes are pre-shared keys (PSK), and enterprise mode. Enterprise mode is much more secure, although it is much more difficult to set up.

4.9.3 WPA-PSK

WPA-PSK is generally used for small networks such as home or small office networks. In this mode, a key that is known by both the access point and the client attempting to connect is required to connect to the network. Once a connection is established, the client will have access to the MIC and encryption key to send and receive data packets from the network. The use of WPA-PSK is susceptible to a brute force attack on the plain text password used to connect. This will be discussed in depth later in the paper.

4.9.4 WPA2

Just like how the WPA was developed in order to overcome the WEP security flaws, the WPA2 was developed to do the same with the flaws that were uncovered with WPA. It's considered to be the one of the most if not the most secured protocol. WPA2 replaced its predecessors' TKIP and Michael algorithm with Pairwise Transient Key (PTK), which is 384 bits, and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) respectively. The WPA2 security protocol also added a block cipher algorithm named Advanced Encryption Standard (AES), which is a 128-bit authentication and encryption process.

The Packet Number (PN) is incremented every time an encryption needs to take place. The KeyID and PN are then used to Construct the CCMP Header, also the PN and the transmitter ad address (A2), Priority are being used to Construct Nonce, which is needed for the CCM Encryption. The MAC header is used to construct the AAD. The Nonce, Additional Authentication Data (AAD), alongside the data from the Plaintext MPDU, and the Temporal Key (TK), are all being used for the CCM Encryption.

For WPA2 there are two different versions of this security protocol, that being WPA2-PSK and WPA2-Enterprise. They use two different authentication processes.

4.9.5 WPA2-PSK

The Personal or Pre-shared Key (PSK) authentication process, although less secure than the Enterprise process, is still an efficient and secure security protocol for small business and residential WLAN. This process uses a plaintext passphrase, that along with the CCMP uses the password and network SSID to generate unique encryption keys.

The passphrase length can be 8-63 characters long. Which is used in the Password-Based Key Derivation Function 2 (PBKDF2), and then the process of using the plain text passphrase and the network SSID begins. The passphrase, network SSID, and the length of the SSID, are grabbed in order to produce the PMK; however before finishing, the components are then hashed 4096 times which results in a PMK which is 256-bits. The Pairwise Transient Key is generated using the PMK, Pairwise key expansion, the Access Point (AP) Mac address, the user's MAC address, a randomly generated number labeled Nonce from the Access Point and one from the user. As seen from the figure below this is where the Temporal Key is generated which is used in the Encryption Process for WPA2.

4.9.6 Vulnerabilities of WEP

WEP has many vulnerabilities that pose a major security risk for anyone who uses a WEP protected network. Things such as packet reinjection, fake authentication, and key recovery attacks are a few of the attacks WEP is susceptible to. A few of the most famous attacks on WEP include KoreK's chop attack, The KoreK key recovery attack, and the PTW attack. Hackers have dissected and discovered many flaws in WEP, allowing for a WEP protected network to be infiltrated within a minute on high traffic networks. These discoveries have been researched and published allowing for the improvements to be made with WPA/WPA2.

4.9.7 Vulnerabilities of WPA/WPA2

The vulnerabilities for WPA/WPA2 are quite similar. In WEP, statistical methods can be used to speed up the process of cracking. However in WPA/WPA2 usually the only attack strategy available is to attempt to determine the passphrase through plain brute force dictionary techniques. Since the keys are dynamic, unlike the static keys WEP uses, collecting IVs does not speed up the attack.One thing that can lead to an attack that also gives the information needed, is the handshake between the user and the Access Point (AP). Handshaking occurs when the user wishes to connect to the network. While the handshake is happening the AP and each station needs a Pairwise Transient Key (PTK), which is derived from the Pairwise Master Key (PMK) using the 4-Way Handshake and all the information that the PMK uses is transmitted in plain text. This plain text can be captured, and the attacker would have all the data required to subject the passphrase into a dictionary attack.

4.10 Design Constraints

In this section we will discuss the design constraints that will impact the development of the SMOCK LOCK, they are safety, economic, time, and power constraints.

4.10.1 Safety Constraints

As the SMOCK lock's electrical systems will be working with around 9V and 1 – 3A there is the issue of electrocution, this will be avoided as much as possible with safety precautions such as wearing a grounding bracelet and being careful in general while working with the system. As the lock is powered by batteries there is always a possibility for battery acid build up which can be toxic, the recommendation for remedying this will be for the user to regularly check or change the batteries. The lock chassis itself is going to be manufactured via 3D printing, the mounting of these components and the creation of the testing door however will be done with power tools so in the creation of these only experienced users will handle the power tools.

4.10.2 Economic Constraints

The most pressing economic constraint will be the acquisition of parts that are not only cost effective but also designed for longevity. Another constraint will be how much the team can put forward for the initial cost of the project, as all of the project is self-financed. Another would be with the general shortage of circuit boards in the United States which drastically lowers the number of boards that can be realistically used.

4.10.3 Time Constraints

There are only two major time constraints the first being the deadline of the project as the nature of the SMOCK Lock is a student project. The other time constraint would be the time all the group members have to spend doing other things whether its personal or on other projects. This constraint has a huge impact on the outcome of the SMOCK Lock development. Team members are taking other classes and working part-time job, so scheduling meetings throughout the semester will be difficult.

4.10.4 Power Constraints

The biggest power constraint is the use of batteries as building up a bank of batteries that matches the desired voltage proves to be difficult. Many different aspects go into this array of batteries to gain a specific bank needed for a product. The first aspect would be should the bank batteries be laid out in parallel or in series. If the battery in the bank is in series the battery bank will have a higher overall voltage if it’s in parallel the voltage will remain the same at around the same voltage but will have an increased amperage. Most common batteries have an amperage of around 500mA and a voltage of around 1.5V for AAA, AA and other common household batteries. For the purposes of SMOCK lock the battery of choice will most likely be a 9V battery arranged in a parallel configuration to allow for a higher amperage for the lock.

4.10.5 Electrical Material Constraints

Insulation is a crucial part in the electrical system in any technology as electrically all components need to be insulated from internal and external interference.

4.10 Quality Assurance

To gain the high quality we are aiming for with the SMOCK lock we heavily emphasized the research and testing of the individual components which allowed for the best selection of components. Also, In the following sections it goes over the hardware and software design details all of which has been looked over by all the team and our professors when the paper has been through its multiple checks. During and after the building and programming of the SMOCK lock tests will be run that will ensure the upmost quality. These tests will be ran consistently and especially if changes are made to the project midway, all of these tests are detailed in the hardware and software design details.

Table 4.3: Electrical Material Constraints Descriptions

Class	Description
Class A	cotton, silk, and paper when suitably impregnated or coated or when immersed in a dielectric liquid such as oil
Class B	mica, glass fibre, asbestos, etc., with suitable bonding, impregnating, or coating substances
Class C	mica, porcelain, glass, quartz with or without an inorganic binder
Class E	consists of materials or combinations of materials that can withstand temperatures of at least 15 C
Class F	mica, glass fibre, asbestos, etc., with suitable bonding, impregnating, or coating substances that can withstand at least temperatures of 25 C
Class H	silicone elastomer and combinations of materials such as mica, glass fibre, asbestos etc., with suitable bonding, impregnating, or coating substances such as appropriate silicone resins

5.0 Prototyping

In this section we will discuss what products contain the chips we intend to use that will provide the features that are required for the functionality of the SMOCK Lock. Our prototype will implement those products which will help us test our design, which will ultimately become our final product.

5.1 ATmega328P (Microcontroller)

In this section we will discuss the Microcontroller we intend to implement into our final product.

5.1.1 Miuzei R3

The Miuzei R3 is an Arduino based development board that's uses the ATmega328P microcontroller. This board does not include Bluetooth or Wi-Fi support which would require us to purchase extra parts to make sure the micro-controller can communicate with our database. Arduino is an open-source hardware, software, and content platform.

Features:

- Microcontroller: ATmega328P 8-bit @ 20 MHZ
- Processor: AVR CPU
- Input Voltage: 7-12V
- Operating Voltage: 5V
- Digital I/O Pins: 14
- PWM Digital I/O Pins: 6
- Analog Input Pins: 6
- Flash Memory: 32KB
- SRAM: 2 KB
- Length: 68.6 mm
- Width: 53.4 mm
- Weight: 25 g
- USB and AC power
- Pcs:1
- Price: $12

5.2 OV2640 with ESP32-CAM (Camera Module)

In this section we will discuss what camera module we intend to implement into our final design.

5.2.1 OV2640 Camera + MELIFE ESP32-CAM Board

The ESP32-CAM is a “tiny module based on a ESP32 chip and uses the OV2640 camera module. It consists of several GPIOs to connect peripherals and a microSD card slot for storing images taken with the camera.

Features:

- The smallest 802.11b/g/n Wi-Fi BT SoC module
- 2 MP
- Low power 32-bit CPU, it can also serve the application processor
- Up to 160MHz clock speed, summary computing power up to 600 DMIPS
- Built-in 520 KB SRAM, external 4MPSRAM
- Supports UART/SPI/I2C/PWM/ADC/DAC
- Support OV2640 and OV7670 cameras, built-in flash lamp
- Support image Wi-Fi upload
- Support TF card
- Supports multiple sleep modes
- Embedded Lwip and FreeRTOS
- Supports STA/AP/STA+AP operation mode
- Support Smart Config/AirKiss technology
- Support for serial port local and remote firmware upgrades (FOTA)
- Pcs: 1
- Price: $10.82

5.3 ESP8622 (Wi-Fi Module)

In this section we will discuss what Wi-Fi Module we intend to implement into our final design.

5.3.1 UPUNER ESP8266 Development Board

The UPUNER ESP8266 Development Board is an easy to program Wi-Fi development board with a built in Micro-USB. It also has a flash and reset switch for easy programming controls.

Features:

- Based on the ESP8266EX Wi-Fi chip
- 2.4 GHz
- Supports 802.11b/g/n
- Input Voltage of 5V via USB
- Operating Voltage: 3.3V
- 11 I/O Pins
- 1 Analog Input Pin

- 4 MB Flash memory
- WPA/WPA2 Security
- TCP/IP Integrated Protocol
- Pcs:3
- Price: $13.90

5.4 MT3608 (Step-Up Boost)

In this section we will discuss what Step-Up Boost we intend to implement into our final design.

5.4.1 Teyleten Robot Step Up Boost Converter

The Teyleten Robot step up boost converter is a 2A adjustable voltage regulator board that has an input range of 2-24V and an output range of 5-28V.

Features:

- Based off the MT3608 chip
- Input Voltage: 2-24V
- Output Voltage: 5-28V
- Max Output Current: 2A
- Efficiency Rating of 93%
- Adjust Voltage with a potentiometer
- Pcs: 5
- Price: $6.88

5.5 Relay

In this section we will discuss what Relay we intend to implement into our final design.

5.5.1 Tolako 5V 1 Channel Relay Module

The Tolako 5V 1 Channel relay is a simple and easy to use module that can control DC or AC signals and has a normally open and open normally closed contact connectors. The relay can be controlled using a digital output signal.

Features:

- 1 Channel Relay
- Control DC or AC signals
- Can control the 250 VAC -10A
- Can control the 125 VAC -10A
- Can control the 30 VDC -10A
- Can control the 28 VDC-10A

- 5V-12V control of the TTL
- Pcs: 1
- Price: $5.50

5.6 AS608 (Fingerprint Sensor)

In this section we will discuss what Fingerprint Sensor we intend to implement into our final design.

5.6.1 DIYmall Optical Fingerprint Reader

The DIYmall optical fingerprint sensor is an easy to use fingerprint reader that can store up to 240 prints and is based of the AS608 microchip.

Features:

- Based off the AS608 processor
- Communicates through UART
- Supply Voltage of DC 3.8-7.0V
- Image Input Time: < 0.5 seconds
- Operating Current <60 mA
- Peak Current < 85mA
- Search Time < 220ms
- Comparison Method (1:1)
- Search Method (1:N)
- Storage: 240 fingerprints
- Pcs: 1
- Price: $23.99

5.7 OLED Display

In this section we will discuss what OLED we intend to implement into our final design.

5.7.1 Frienda OLED Display Module

The Frienda OLED module is a self-illuminated power saving display. The display module makes use of the I2C interface for simpler connections than a traditional LCD module.

Features:

- Input Voltage: 3.3V-5V
- Size: 0.91 inch
- Resolution: 128 x 32
- Size: 38 x 12 mm

- Interface type: IIC interface
- Pin description:
- GND: power ground
- VCC: Power + (DC 3.3 - 5V)
- Operating temperature: -40 - 85 degree Celsius
- SCL: clock line
- SDA: data line
- PCS: 2
- Price: $9.49

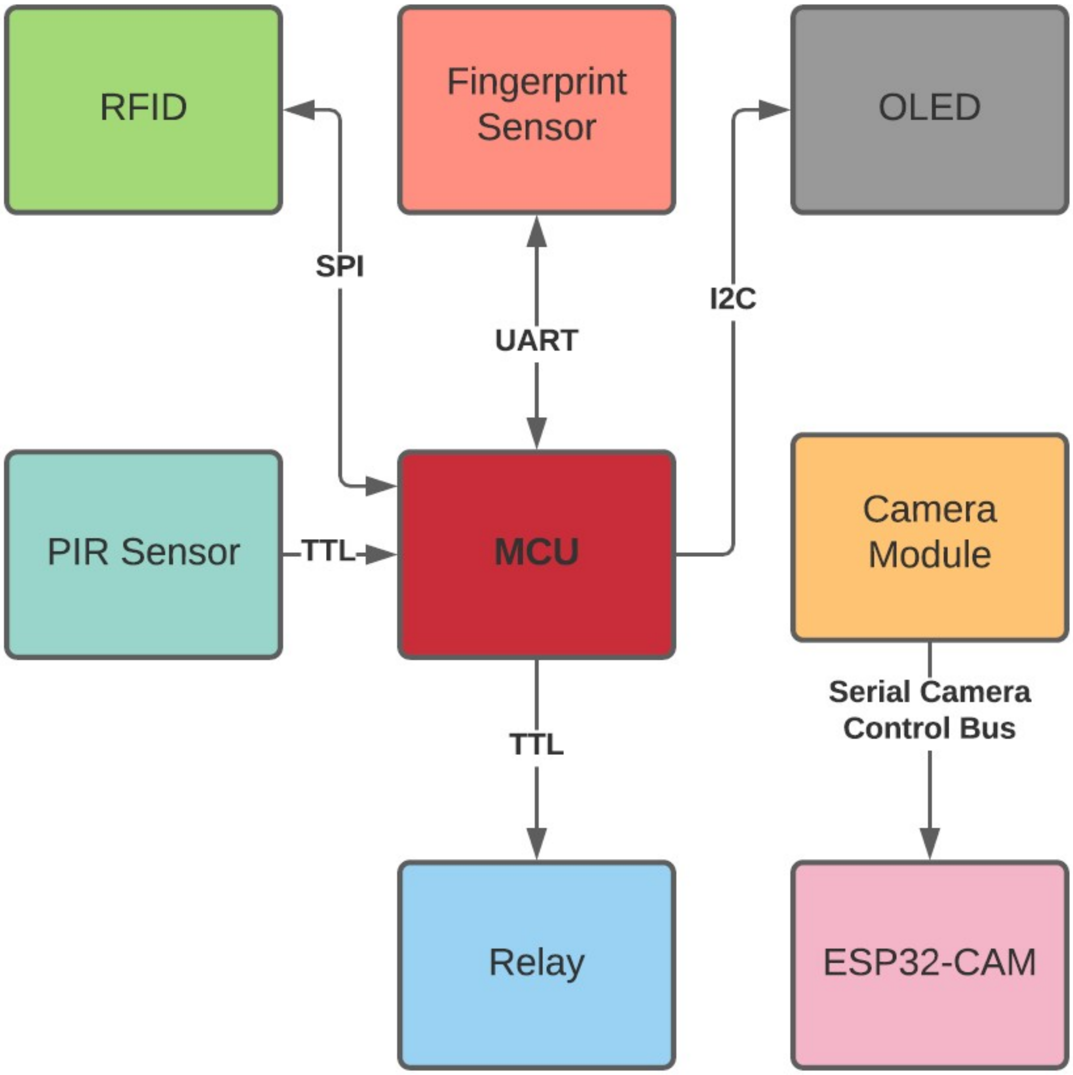
Table 5.0: Prototype Part Selection

Part	Part Selection	Part Description
Microcontroller	Mizuei R3 Development Board	The Miuzei R3 is a Arduino based development board that's uses the ATmega328P microcontroller.
Camera	OV2640+ESP32-CAM Development Board	Tiny module based on a ESP32 chip and makes use of the OV2640 camera
Fingerprint Sensor	DIYmall AS608 Optical Sensor	Optical fingerprint sensor based on the AS608 chip
Wi-Fi Module	UPUNER ESP8266 Development Board	Easy to program Wi-Fi development board based on the ESP8266EX chip
Relay	Tolako 1 Channel 5V Relay	Easy to use relay module that can control DC or AC signals
Step Up Boost Converter	Teyleten Robot MT3608 DC-DC Boost Converter	2A adjustable voltage regulator board with potentiometer to adjust voltage
Display	Frienda OLED Display Module	Self-illuminated power saving OLED display

5.8 Communication Design

In this section we will be explaining how we intend our hardware components to communicate, and what they are using to communicate such as SPI, UART, I^{2}C, TTL, and Serial Camera Buses.

Table 5.1: Hardware Communication Design



6.0 Hardware Design Details

In this section we will summarize what we plan to do with the hardware components that we have decided to use. The first step to for the lock to fully turn on, the lock should constantly be in low power mode unless the PIR sensor detect motion nearby. Once the PIR Sensor detects motion the camera will receive information to turn on and begin capturing images, the microcontroller will then receive information from the owner on whether or not to unlock the door. Essentially the microcontroller will serve as a switch that will decide on whether or not to provide components to other components based on instructions received from our server.

In this chapter we will discuss how the hardware will communicate with each other in detail as well as any relevant testing and potential hardware issues that we may run into when developing the SMOCK Lock.

6.1 Hardware Communication Diagram

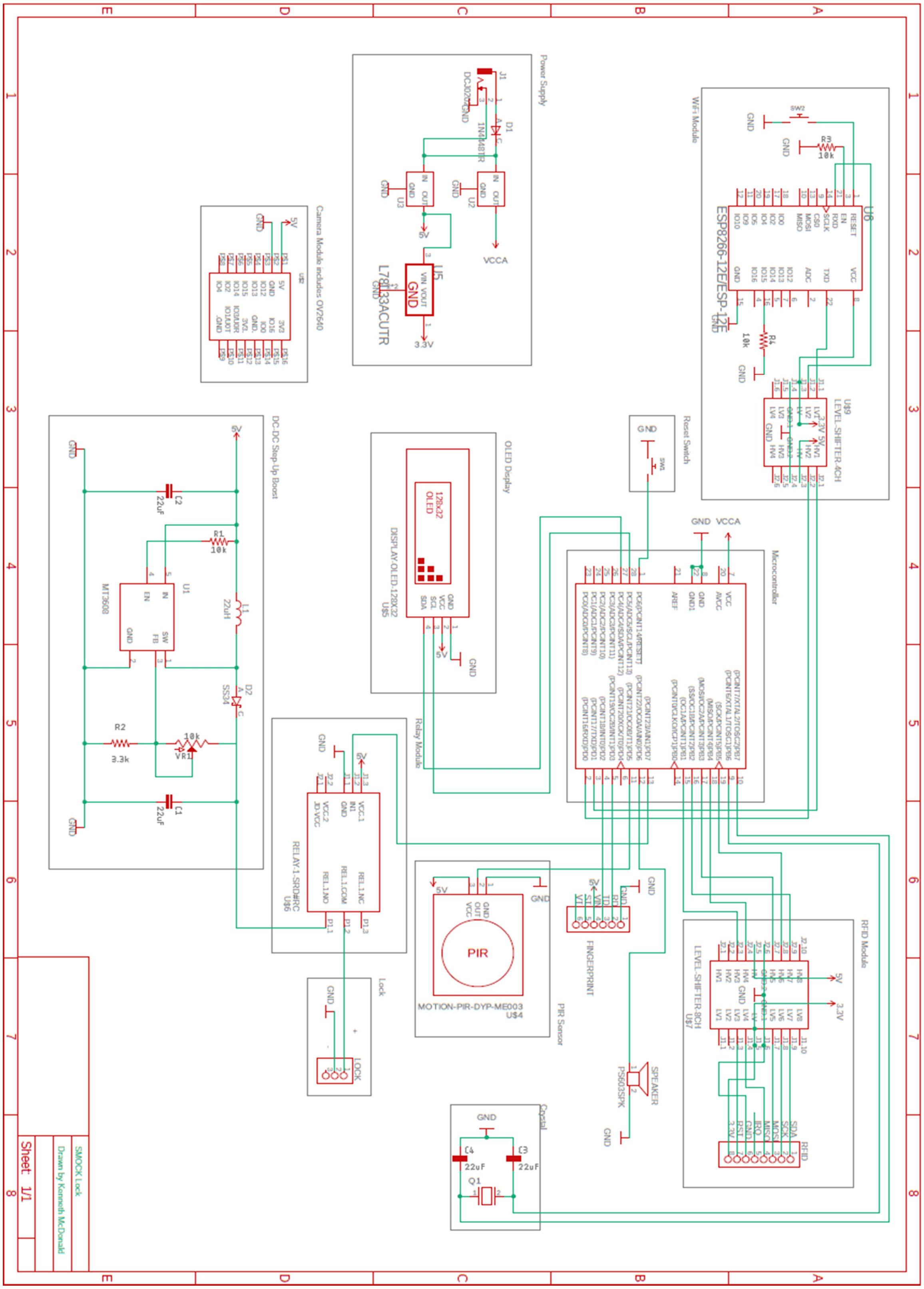
The schematic starts at the power supply section. In here we have designed a barrel jack power connector that will be supplied by a configuration of 2 9V batteries. The barrel jack is to a diode that is then connected to a separate 5V voltage regulator to power the microcontroller unit. The other end of the barrel jack is also connected to another 5V voltage regulator to supply 5V to components. The output of this regulator is branched off and provides input to the 3.3V voltage regular. This regulator will help supply components that require 3.3V. VCCA is used to label the power for the microcontroller. A 5V arrow is used to label the 5V supply for components and a 3.3V arrow is used to label the 3.3V supply for components. GND is used to label GND.

The Camera Module Section contains the ESP32-CAM standalone board. Since this board will be processing and uploading the images to the server, there will be no need to connect it to the main microcontroller. With that being said, the only connections needed for the ESP32-CAM is a 5V supply and a GND supply.

The OLED Display section contains the OLED display module. This module has 4 simple connections, 2 for supply and ground, and 2 for I2C communications. We connect a 5V supply to the VCC pin on the display and GND to the GND pin. The SDA pin on the display is connected to Analog (ADC) Pin 4 on the microcontroller and the SCL pin is connected to Analog (ADC) Pin 5 on the microcontroller.

The DC-DC Step-Up Boost section contains the MT3608 converter chip and its circuit. A 5V source is supplied to the circuit which is first connected to a 22uF capacitor which is connected to ground. It is then connected to the IN pin of the MT3608.The 5V source is then connected to a 10k Ohm resistor which is then connected to the E*N pin. After this, the 5V source is then connected to a 22uH inductor. The output of the inductor is connected to the SW pin on the MT3608.

Figure 3.0: SMOCK Lock Schematic



The output of the inductor is then passed through a Zener diode to maintain voltage regulation. The FB pin on the MT3608 is connected to a potentiometer represented by the 10kOhm resistor. The output of the Zener diode is connected to the potentiometer which is then connected to a 3.3kOhm resistor which is then connected to GND. The output of the diode is also connected in parallel with the 22uF capacitor and GND and is then finally passed as the positive output voltage which is then connected to the relay.

The relay module section contains the 5V 1-Channel SRD relay. The normally open (NO) pin on the relay is connected to the output of the step-up boost converter which would be 12V. The COM pin of the relay is connected to the positive terminal of the lock mechanism. The normally closed pin remains not connected. The VCC.1 pin on the relay is supplied by the 5V source. The IN1 pin on the relay is connected to the digital pin 7 on the microcontroller. The GND pin on the relay is connected to GND.

The PIR sensor section contains the PIR sensor. The GND pin is connected to GND. The OUT pin on the PIR sensor is connected to digital pin 5 on the microcontroller. The VCC pin is supplied by a 5V source.

The fingerprint sensor contains 6 pins. The GND pin is connected to GND. The RD pin on the sensor is connected to digital pin 3 on the microcontroller. The TD pin on the sensor is connected to digital pin 2 on the microcontroller. The VIN pin is supplied by the 5V source. The ST and VT pins remain unconnected as they are not needed.

The crystal section contains the 32MHz crystal. The XTAL1 pin on the microcontroller is connected to a the crystal in parallel and is connected in series with a 22uF capacitor. The XTAL2 pin on the microcontroller is connected to the crystal in parallel and is connected in series with a 22uF capacitor.

The RFID Module section contains the RFID and a 8 channel logic level shifter. The logic level shifter is used as a precaution since we will be converting 3.3V signals to 5V signals back and forth with the microcontroller. The RFID sensor uses a 3.3V input, so the 3.3V pin on the sensor is connected to the LV pin on the logic shifter which is supplied by the 3.3V source. The SDA pin of the sensor is connected to the LV7 pin on the logic level shifter. The HV7 pin on the logic level shifter is then connected to digital pin 10 on the microcontroller. The SCK pin on the sensor is connected to LV6 on the logic level shifter. The HV6 pin is connected to digital pin 13 on the microcontroller. The MOSI pin on the sensor is connected to LV5 on the logic level shifter. HV5 is then connected to digital pin 11 on the microcontroller. GND is connected to GND. The MISO pin is connected to LV4 on the logic level shifter. The HV4 pin is then connected to digital pin 12 on the microcontroller. The RST pin on the sensor is connected to the LV3 pin on the logic level shifter. The HV3 pin is connected to digital pin 9 on the microcontroller. The RFID sensor uses the SPI interface to communicate with the microcontroller.

The Wi-Fi module section contains the ESP8266 chip. The RESET pin on the ESP is connected to a button which is then connected to GND. The EN pin on the ESP is connected to a 10kOhm resistor which is then connected to GND. The RXD pin on the ESP is connected to LV2 on the 4 channel logic level shifter. The HV2 pin is then connected to digital pin 0 on the microcontroller. The TXD pin on the ESP is connected to the LV1 pin on the logic level shifter. The HV1 pin is then connected to digital pin 1 on the microcontroller. The VCC pin on the ESP is connected to LV on the logic level shifter which is then supplied by the 3.3V source. The HV pin on the logic level shifter is supplied by the 5V source. The GND pin is connected to GND. The IO15 pin is connected to a 10kOhm resistor which is then connected to GND.

6.2 Enclosure Development

There are a few things we must account for when design the enclosure of the SMOCK Lock, we have to make sure that all our products are enclosed for safety standards, however, certain parts like the Camera, Speaker, RFID, Fingerprint need to be exposed somewhat. The enclosure will hide all of our components and make sure to not leave any exposed wires out that can be affected by any environment factors. The Enclosure must also be securely fastened to the door, as to not damage the enclosure or the door itself. Inside the enclosure will be the locking mechanism as well. The locking mechanism should not be able to be seen from anyone's point-of-view unless the enclosure has been opened/tampered with.

A figure representing our enclosure is listed below please reference Figure 5.0: Enclosure Preliminary Design, for a better understanding of how we intend to enclose our lock and how it would be viewed by a person standing in front of the lock.

6.3 Sensor Testing

In this section we will discuss the testing that the different Sensors in our SMOCK LOCK require. Those sensors being the RFID, Fingerprint, Camera, PIR,OLED, Relay, Step-up Boost Converter. These are all necessary components for the functionality of the SMOCK Lock and will be pivotal for the development of the lock.

6.3.1 RFID

In this section we will discuss the necessary testing of the RFID Sensor which may be necessary to unlock the door. Each test was performed 10 times to get a accuracy score.

Table 6.0: RFID Tests

Test #	Description	Testing Accuracy
1	Initialize the module	10/10
2	Performing the automatic self-test using AutoTestReg	10/10
3	Reading tag data from the reciever	10/10
4	Writing data from the reciever to tag	10/10

The first test would be to ensure that RFID module can be initialized. If the module can be initialized, we move onto performing a self-test that is given in the MFRC522 library.

The self-test function starts by performing a soft reset. Upon successful reset, the internal buffer is cleared by writing 25 bytes of 00h. Then the self-test is enables by writing to the AutoTestReg. 00h is then written to the FIFO buffer and the self-test begins by issuing the CalcCRC command. After the self-test is complete, the resulting 64 bits from the FIFO buffer are read out. We compare these bits to the expected values provided in the datasheet. If the bits match, then we can conclude that chip is functional. If the bits do not match, then the test failed and will need to be reran to determine if chip is faulty.

Given that the self-test passes, we move onto setting the RFID into receiver mode. When a tag comes into proximity of the sensor, an interrupt should be triggered. If the interrupt is raised, we know the sensor is set up correctly. We move onto then storing the data in the FIFO buffer from the sensor and comparing the received data to the correct UID codes. If the data matches, then the sensor can read properly.

The next test would be to see if the sensor can write to a tag properly. This is done by changing register settings so data can be transmitted to the tag from the receiver. The data we want to write is passed to the FIFO buffer. When a tag comes into proximity of the sensor, the data from the FIFO buffer is written to the tag. To verify the write operation, we perform another read test with the newly written tag. If the read test is passed, then we can say that the RFID can read from and write to a tag.

6.3.2 Fingerprint

The fingerprint sensor will be tested using the Adafruit Fingerprint library. This library provides specific functions for detecting, enrolling, and saving fingerprint data. Each test was performed 10 times to get an accuracy score.

Table 6.1: Fingerprint Sensor Tests

Test #	Description	Testing Accuracy
1	Detecting the fingerprint scanner	10/10
2	Enrolling a fingerprint	10/10
3	Matching a fingerprint	10/10

Test 1 will be used to detect the fingerprint sensor. To do this, we need to upload the “enroll” sketch from the Adafruit library examples. The codes states that a fingerprint object is created and initialized. Using the specific pins stated for the input and output of the scanner, the code searches for the fingerprint sensor on those pins. If the sensor is detected, a message will be displayed in the serial monitor saying fingerprint scanner detected. If no message is displayed, then retry to determine whether the scanner is faulty or not.

Test 2 involves enrolling a fingerprint or adding a fingerprint. To test this, we repeat the procedure of test 1 since it uses the same code for enrolling. Once we get to the detection message, the serial monitor will prompt the user to enter a fingerprint id number. Once this number is entered the fingerprint sensor will then take in a fingerprint where you will need to lay your finger on the sensor. Once the print has been taken, the sensor will need to verify the print and will ask you to place the same finger back on the sensor. After this the fingerprint will be enrolled and is ready to be used to compare to another input.

The last test will involve matching the fingerprint. Since we have tested enrolling a fingerprint and have a print currently enrolled, we can now move on to checking for a match. We will now need to make use of Adafruit’s example called “fingerprint”. Once this sketch has been uploaded to the board, we can open the serial monitor and place the finger on the scanner. Upon a successful scan, the fingerprint ID will be displayed in the serial monitor. If the ID matches the ID used to enroll the fingerprint then the test was a success and you can assume the fingerprint sensor is fully functional.

6.3.3 Camera

We first needed to upload a sketch to the ESP32-CAM to test the functionality. Using an Arduino board we were able to upload a sketch successfully to the ESP32-CAM. From here we tested the camera through the following tests to ensure that it will work for our needs and that it functions as directed. Each test was performed 10 times to get an accuracy score.

Figure 4.0: Breadboard Testing

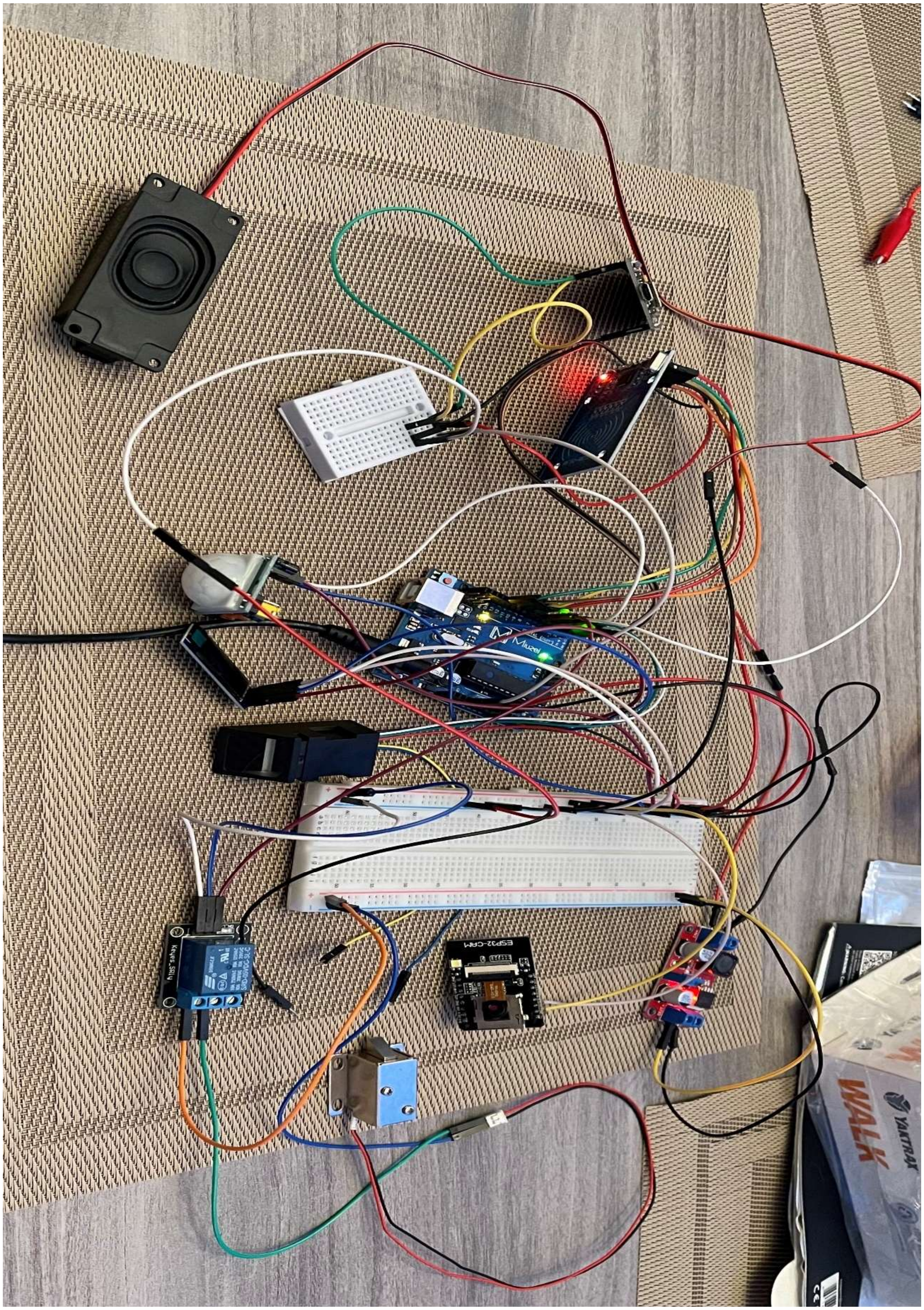


Figure 5.0: Enclosure Preliminary Design

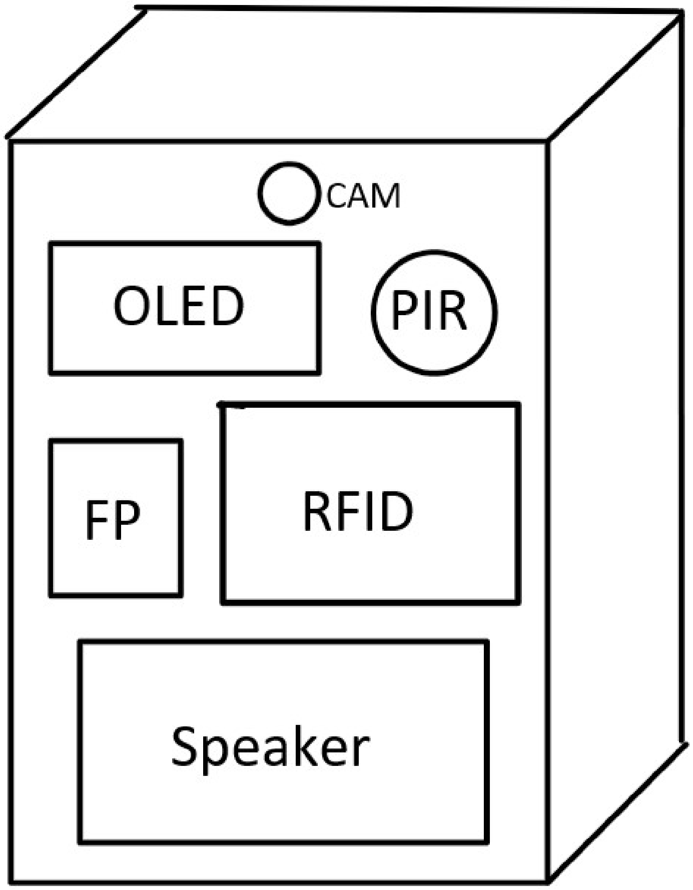


Table 6.2: Camera Tests

Test #	Description	Testing Accuracy
1	Have the camera either take a picture or produce a live feed and upload to local server over Wi-Fi	10/10
2	Use python code to call the live feed	10/10
3	Have the module detect eyes and faces from live feed	10/10
4	Test that the voltage stays constant at 5v	10/10

The first test involves taking a picture or producing a live feed with the camera module. We can make use of this with the ESP32-CAM library in the Arduino IDE. Once the library is added, we can use the ESP32-CAM example called Camera Web Server. You will need to uncomment the specific model of the ESP32-CAM, and you will need to input your wireless networks SSID and password so the ESP32-CAM can connect over Wi-Fi. Once these changes have been made, you can upload the sketch to the ESP32-CAM. Upon successful upload, the serial monitor will display the webserver address. Plug the address into an internet browser. If the ESP32-CAM page shows up, click start stream at the bottom. If the stream appears, then we can say that the camera has successfully produced a picture or live stream video and that it has been uploaded over Wi-Fi to a local server.

The second test we would like to perform is making calls to the ESP32-CAM live stream or picture from a python script. We plan to implement facial recognition in Python on the server so it is very important that we can access the data provided by the camera in Python. To test this we use a very simple code that opens a url link that is provided by the ESP32-CAM. We use the urllib python library to do this. Upon successful implementation, using a urllib request will open a window that should contain the livestream provided by the camera. If the livestream opens upon running the python script, then this test was successful.

The third test we want to run is that the camera produces a well enough image to perform facial recognition. To test this, we employ simple facial detection features such as drawing rectangles around detected faces and eyes using cascade classifiers provided by the openCV library. We employ these functions into the code used from the second test and run the script. Once the livestream windows open, if a face is in the cameras view, there will be rectangles drawn around the face and eyes of the person. If this is seen, then we can say that this test performed successfully.

The fourth test we would like to perform is to test the voltage when the ESP32-CAM is in use. We want to perform this test since a drop in voltage can lead to the ESP restarting unexpectedly and can cause server-side issues. To test this, we plug the ESP32-CAM into a breadboard where we can access the input voltage pins. We then have the ESP run the Webserver to simulate it running. We make motion and other kind of movements in front of the camera to mimic normal input. If the camera does not restart and the voltage from the multimeter stays constant then the camera is not experiencing voltage drops and can be considered fully functional and that the test was a success. If there is a restart, this issue may be fixed by adding a voltage regulator.

6.3.4 PIR

The PIR sensor is a simple module that can be connected standalone or through the Arduino board. The main purpose of the PIR sensor is to detect motion in a limited range. It includes potentiometers on the back to adjust the sensitivity and delay time. Each test was performed 10 times to get an accuracy score.

Table 6.3: PIR Tests

Test #	Description	Testing Accuracy
1	Detect Motion	10/10
2	Adjusting Sensitivity	10/10
3	Adjusting Delay Time	10/10

The first step is to connect the sensor to the breadboard along with a resistor, a LED and a 5V power supply. The positive and negative terminals of the sensor are connected to the power supply. The out pin of the sensor is connected to a resistor which is then connected to the LED and then connected to GND. Once the circuit is powered, wait 60 seconds for the PIR sensor to stabilize.

The first test can be conducted by simply moving in front of the sensor. If the sensor picks up the motion, the LED will turn on. If the LED turns on, we can say that the sensor can correctly detect motion.

The second test involves repeating the first test while adjusting the sensitivity potentiometer on the module. Increasing this potentiometer will allow for a farther range while decreasing will constrict the range. To test the sensitivity simply find the max point before adjusting the sensitivity and mark it. Next, increase the sensitivity potentiometer and return the max point you marked. If the LED shines, then the test was successful. If not, then repeat to determine if module is faulty.

The third test involves repeating the second test but instead adjusting the delay time instead of sensitivity. Increasing the delay time potentiometer will allow the LED to stay on longer after the sensor has detected motion. Decreasing will shorten the length the LED stays on. To test this, simply increase the delay potentiometer and move in front of the sensor. If the light stays on longer than before adjusting, then the test is successful.

6.3.5 OLED Testing

In this section we will be discussing the necessary testing of the OLED display. The OLED will display any instructions clearly to anyone that approaches the door. Such as, please get closer, to ensure that we capture a clear image of the guest at the door. It can also be used to tell the guest to show their QR Code. In order to begin testing of the display, we must connect the VIN pin of the display to the 5V pin of the Miuzei R3 board, connect the GND pin to GND, connect the SDA pin on the display to the Analog 4 pin on the R3 board, and the SCL pin of the display to the Analog 5 pin on the R3 board. Each test was performed 10 times to get an accuracy score.

Table 6.4: OLED Tests

Test	Description	Testing Accuracy
1	Testing different animations through Adafruits library example	10/10
2	Writing static text to the display	10/10
3	Writing scrolling text to the display	10/10

The purpose of test 1 is to run a general use test to check the pixels of the display. This test, when performed correctly will show different pixel animations on the display. We will first need to install the adafruit_SSD1306.h and adafruit_GFX.h libraries from adafruit. After the libraries have been installed, In the Arduino IDE, we will go to File > Examples > Adafruit SSD1306 > ssd1306_ 128x32_i2c. The code should load. Since our display doesn't have a reset pin, we need to set the OLED_RESET variable to -1. Then upload the code to the Miuzei board. The OLED should display a series of different animations. If the animations do not show, check the display is wired correctly and if it is, the display may be faulty.

The purpose of test 2 is to write static text to our display and have it show the text. We will make a new code in order to do this. We can use the beginning of the code in test 1 and the void setup function in this new code. After the setup function, we will want to add a delay with a value of 2000. Then we will need to clear the display by calling "display.clearDisplay()". We then will set the textSize to 1, the textColor to white and the cursor to be placed at (0,10). Then we will write the text we want to display through the display.println() function. This function takes a string as a parameter. After the println command, we will call the display() command to send the text to the screen. Once this is completed, upload the code to the R3 board. The string you entered in the println() function should appear on the display. If the text appears, the test was successful. If it does not display, check the wiring connections to make sure they are correct. If they are then the display may be faulty.

The purpose of test 3 is to write scrolling text to the display. This test will build off the code that we explained in test 2. We will add onto this code by making use of the loop function in the code. The Adafruit library provides methods to scroll text. These functions are startscrollright(), startscrollleft(), startscrolldiagright(), and startscrolldiagleft(). In the loop function, we can call a start scroll function, while passing the addresses of two corners or edges, along with a delay to slow the scroll, and then call the stopscroll() function to complete the scrolling effect. Once this has been added, we upload the new code to the R3 board. The display should now display your string as scrolling text. If it is not, check the connections and code, and if those are right as well then you may have a faulty display.

6.4 Relay Testing

In this section we discuss the relevant Relay testing. After looking through different articles and documents online, we can conclude that the 5V relay is healthy and functional through the following tests. Each test was performed 10 times to get a accuracy score.

Table 6.5: Relay Tests

Test #	Description	Testing Accuracy
1	Check if there is continuity between the N/C contacts and poles	10/10
2	Check for discontinuity between N/O contacts and poles	10/10
3	Listen for the clicking sound and red led when the relay is energized	10/10
4	While the relay is energized, check if there is continuity between the N/C contacts and poles	10/10
5	While the relay is energized, check if there is discontinuity between the N/O contacts and poles	10/10

The purpose of test 1 is to check for continuity between the N/C contacts and poles. We first start by setting the multimeter to continuity check mode. We will then place the positive probe on the N/C port on the relay and the negative probe on the COM port of the relay. If there is no change on the multimeter and no sound was made, then we can assume there is continuity and the test passes. If a sound is made or this is a change in the multimeter, then the test fails, and it may be a faulty relay.

Continuing from test 1, test 2 checks for discontinuity between the N/O contacts and poles. To perform this test simply place the positive probe on the N/O port of the relay and continue to keep the negative probe on the COM port. If there is a change on the multimeter and a buzzing sound is made, then we can say that there is a discontinuity between the ports and the test is a success. If this is not the case, then the test fails and may be due to a faulty relay.

Now for test 3, we want to make sure the relay engages when we energize it. To perform this simply connect a 5V source to the Vin pin, GND to GND and a digital pin on the Arduino to the Signal pin on the relay. Send a high signal to the relay. If the red led shines, then this test was a success and can confirm that the relay engages when it is energized.

The purpose of test 4 is to test for continuity while the relay is energized. To perform this simply energize the relay and perform test 1 again. The outcomes of this test have the same meaning of the outcomes of test 1 so if there is no change then the test is a success.

The purpose of test 4 is to test for continuity while the relay is energized. To perform this simply energize the relay and perform test 2 again. The outcomes of this test have the same meaning of the outcomes of test 2 so if there a change and a buzzing sound can be heard, then the test is a success. If all the tests pass, then we can say that the relay is functional.

6.5 Step-Up Boost Converter Testing

In this section we discuss the relevant tests we ran on the Step-Up Boost Converter. We can conclude that the step-up boost converter is healthy and function from the following Step-Up Boost Converter Tests Table. Each test was performed 10 times to get an accuracy score.

Table 6.6: Step-Up Boost Converter Tests

Test #	Description	Testing Accuracy
1	Check that the voltage supplied to boost converter is staying constant when the converter is idle	10/10
2	Check that the voltage leaving the boost converter is staying constant when the converter is idle	10/10
3	Adjusting the output voltage with the potentiometer	10/10

The purpose of test 1 is to check that there are no voltage fluctuations for the input of the Step-Up boost while the boost is idle. If there are fluctuations, this can lead to damaging other components that rely on the output of the step-up boost. To perform this test, simply connect a 5V source to the Vin pin on the step-up boost and GND to GND. Use the positive and negative probes of the multimeter to test the voltage. If the voltage stays between 5V ± .3V then the test passes, and we can say that there are no fluctuation’s that can damage the components from the input.

The purpose of test 2 is to ensure that there are no voltage fluctuations in the output of the step-up boost while the boost is idle. If there are fluctuations, this can lead to damaging other components and can lead to the assumption that the boost is faulty. To perform this test, simply place the positive and negative probes of the step-up boost on the out terminals of the boost. If the voltage stays constant between ± .3V then the test passes.

The purpose of test 3 is to ensure that we can adjust the output voltage using the potentiometer. To perform this test, simply connect the 5V source to the input voltage pin and GND to GND. With a screwdriver, rotate the potentiometer and measure the output voltage using a multimeter. If you see an increase or decrease in the output voltage, then this test was a success, and we can assume that the step-up boost is fully functional.

6.6 Potential Hardware Issues

The following table describes issues that may occur when installing or testing the hardware components involved in the development of the SMOCK Lock. These are all issues we hope we don't run into or otherwise overcome.

Table 6.7: Hardware Issues

Issue	Description
GPIO pins	GPIO pins on the microcontroller can be faulty and bridged to each other, which can cause false information to be relayed.
ADC converter	The analog to digital converter can be malfunctioning based on bad materials from the PCB or other current based problems
Shorting	With the development of PCB's, the probability of shorting out any of the components are inevitable, this can be avoided by taking precautions and having the correct documentation to ensure the correct current and voltage going to each piece.
WIFI or network loss	According to our standards and paper the lock should stay locked until a signal is given to open it, with specific contingency plans in place for cases such as this.
Electrical Surge	Many events can cause a surge but to ensure our components don't suffer the negative effects of a surge protectors will be placed on certain points of the PCB

Table 6.7.5: Hardware Issues Continued

Issue	Description
Extreme Temperature	The temperature can exceed a certain amount and cause permanent damage to any number of components. Only persistent monitoring and fail safes in order to protect components as best as possible.
Power Irregularities	This can come from many places but most likely a component taking too much power. This can be solved using voltage regulators on high power demand components

7.0 Software Design Details

The design details spoke about in the following sections is a thorough and complete explanation of the software design process and how we effectively came to our conclusion. In this section you will be reading a brief summary of the way the SMOCK LOCK works. You will receive a more detailed understanding by reading the sections in this chapter.

The main factor in the choosing of our database would be its compatibility with images. We chose the database based on familiarity and simplicity as long as it was able to get the job done, and we know that it will. Our database must also be accessible whenever necessary, and compatible with our server type. The server would ideally be running constantly 24/7 regardless of inactivity. However, some servers idle after inactivity and will need to be restarted to use again.

Our API will need to be able to communicate with both server and database, it will also be required to write API for the camera so that the camera can upload images to the database so the server can process that data. API will be written so that the server can communicate with the database whether we need the API to read/write onto the database.

The SMOCK Lock will have a PIR Sensor that will have our Microcontroller send an API to our server that will send the camera a signal that it should start running. It will then continue to capture images at a certain time interval until the PIR Sensor stops detecting motion. We will be setting a limit to how many images will be saved in one encounter. Those images will be able to be seen by the homeowner or resident and may be granted or denied access. The camera also capable of scanning for a QR code or any other Electronic Key that if given permission will allow access to the home. The fingerprint sensor will also turn on after the PIR Sensor registers movement and will be able to grab the read fingerprint and send it to the server to be compared to our database of fingerprints. If the fingerprint is a match above a certain threshold, we will unlock the door. However, if it matches a fingerprint stored but you are not given access to use the fingerprint, you will not be let in. Every user will have certain security privileges set on the backend of the application that may be altered by the owner, these security privileges will allow the homeowner to decide who has access to the home through biometric features and who does not.

The frontend of our app will take care of everything the user will experience while using the app. This is essentially the way the application looks and runs from the eyes of the user. Our app would be compatible with both Android and iOS, which means the software development kit of our choosing, or the language of our choosing must be compatible with both operating systems. For testing purposes there may also be a website created to check the API's we have written. With the API's we are able to retrieve data and display it with some frontend code.

7.1 Virtual Machine

For our Linux based Virtual Machine (Ubuntu) we will be using Oracle VM VirtualBox. This will be necessary to deploy certain servers, It's easier to work with when it comes to downloading from the command terminal. Downloading packages and libraries that are necessary to run our app will be many times less problematic with Ubuntu.

7.2 Database

In this section we will discuss the database we chose to go with and the structure of that database. The database we chose is MongoDB, which is an object-oriented, dynamic, and scalable NoSQL database. It is based on the NoSQL document store model, which is very easy and simple to use. The data objects are stored as separate documents inside a collection. Instead of creating tables we create collections. MongoDB is also capable of storing BSON documents, which is what will allow us to save images and also process them. BSON documents have a limit of 16MB. In the case that we need to store an object larger than this limit. MongoDB offers the gridFS feature, which breaks up the object into 256KB chunks and stores them. When it is time to retrieve them it will grab these chunks and put them back together to return.

Our Users collection will be able to communicate with our Authorized User collection through the use of the userId which is the ID every user is given upon account creation, and the extra ID they are given when granted access. That said every owner will be given userId, and authorized/extra ID upon linkage of lock and app. The authUserId will be an array of authorized users which tracks Ids and if they have been given a true value for our QR Code key or biometric features. The email, first name, last name, phone number will be saved to a user upon creation of account. The password will also be saved however it will be encrypted. Every user is given a Facial Recognition Encoding Array and Fingerprint Encoding Array, which will be an array of encodings associated with the user. The next time some user approaches the door with a facial encoding on the database, the lock will need confirmation that the facial recognition has been authorized for that user. The user also has the opportunity to add friends to quickly communicate or give features to. Each User is also given a security tier that helps determine if Facial, FingerPrint, and or QR Codes are to be accepted.

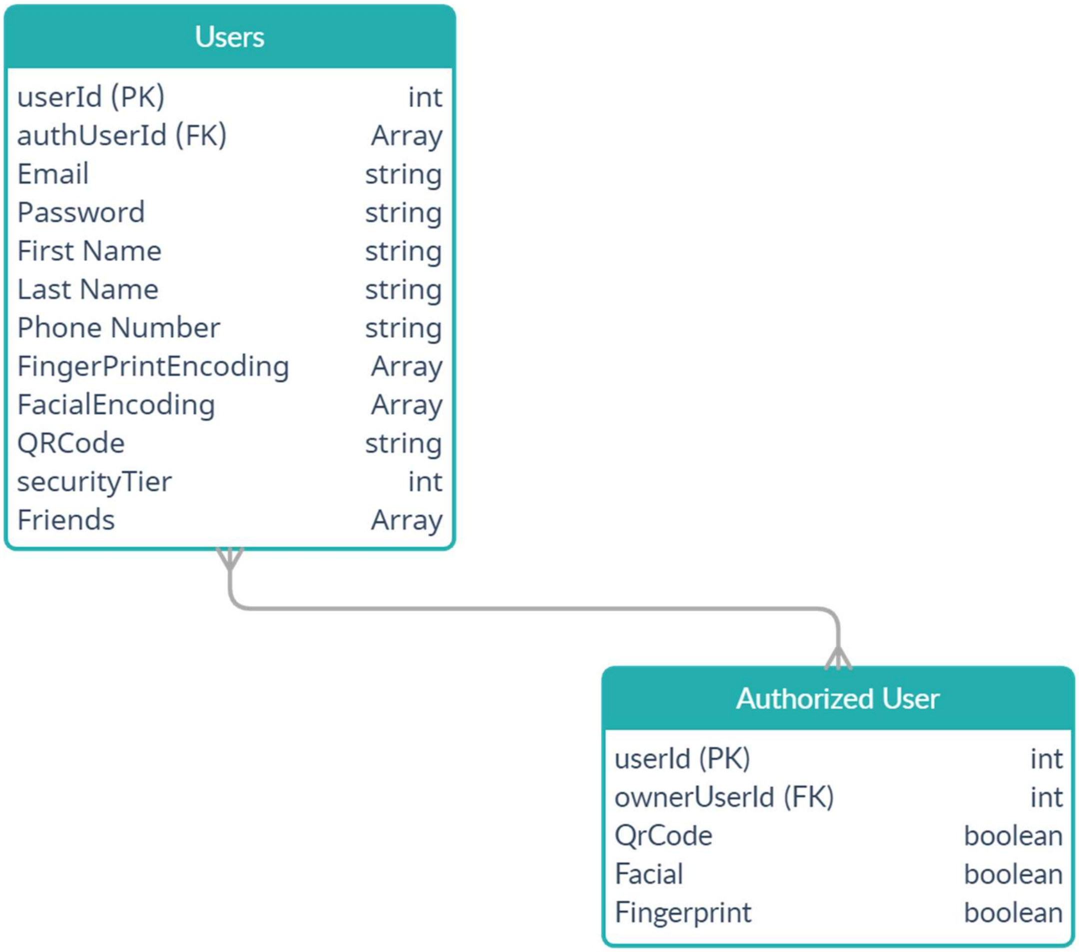
The purpose of the QR Code is for the Owner to give people QR Codes instead of having to go through the hassle of buying a lockbox for keys or giving them an actual key. If you have people coming into the home for construction or to watch the house while the owner is gone, the homeowner can rest assured that the guests are not able to make a copy of the key for the home.

Please visit the ERD Diagram figure below for a visual.

7.3 Server

In this section we will discuss the server host we chose to run the SMOCK LOCK application, which will mention the Server Framework and Server Host.

Figure 6.0: ERD



Users	
userId (PK)	int
authUserId (FK)	Array
Email	string
Password	string
First Name	string
Last Name	string
Phone Number	string
FingerPrintEncoding	Array
FacialEncoding	Array
QRCode	string
securityTier	int
Friends	Array

Authorized User	
userId (PK)	int
ownerUserId (FK)	int
QrCode	boolean
Facial	boolean
Fingerprint	boolean

7.3.1 Using Express.js as Server framework

We decided that we would like to use one of the most popular server frameworks for Node.js, Express.js. Express is a minimal and flexible Node.js web application framework that provides a complex yet easy to use set of features for web and mobile applications. Using Express won’t hinder the Node.js features that we are capable of implementing.

7.3.2 Heroku as Server Host

The server host we chose is Heroku. Heroku is a cloud-based hosting platform. It offers a platform as a service (PaaS), which can be utilized to build, deliver, and deploy our app. We had to decide between the free tier and the hobby tier of Heroku's dyno containers. We ultimately decided that the hobby tier at 7 dollars per month would be the best option for our lock as it does not idle, unlike the free tier. If the server was to go idle, it would require a restart and ultimately could cause our lock to fail. With the hobby tier, we will be able to use a lightweight, isolated Linux container to operate our application. Heroku officially supports Ruby, Node.js, Java, PHP, Python, Go, Scala, and Clojure. We plan on using Java, Node.js, and Python to create our application.

7.4 API

In this section we will discuss how API’s work and the way we will implement the API’s into the development of the SMOCK Lock.

The API will be written using Visual Studio Code, in Node.js.

7.4.1 Node.js

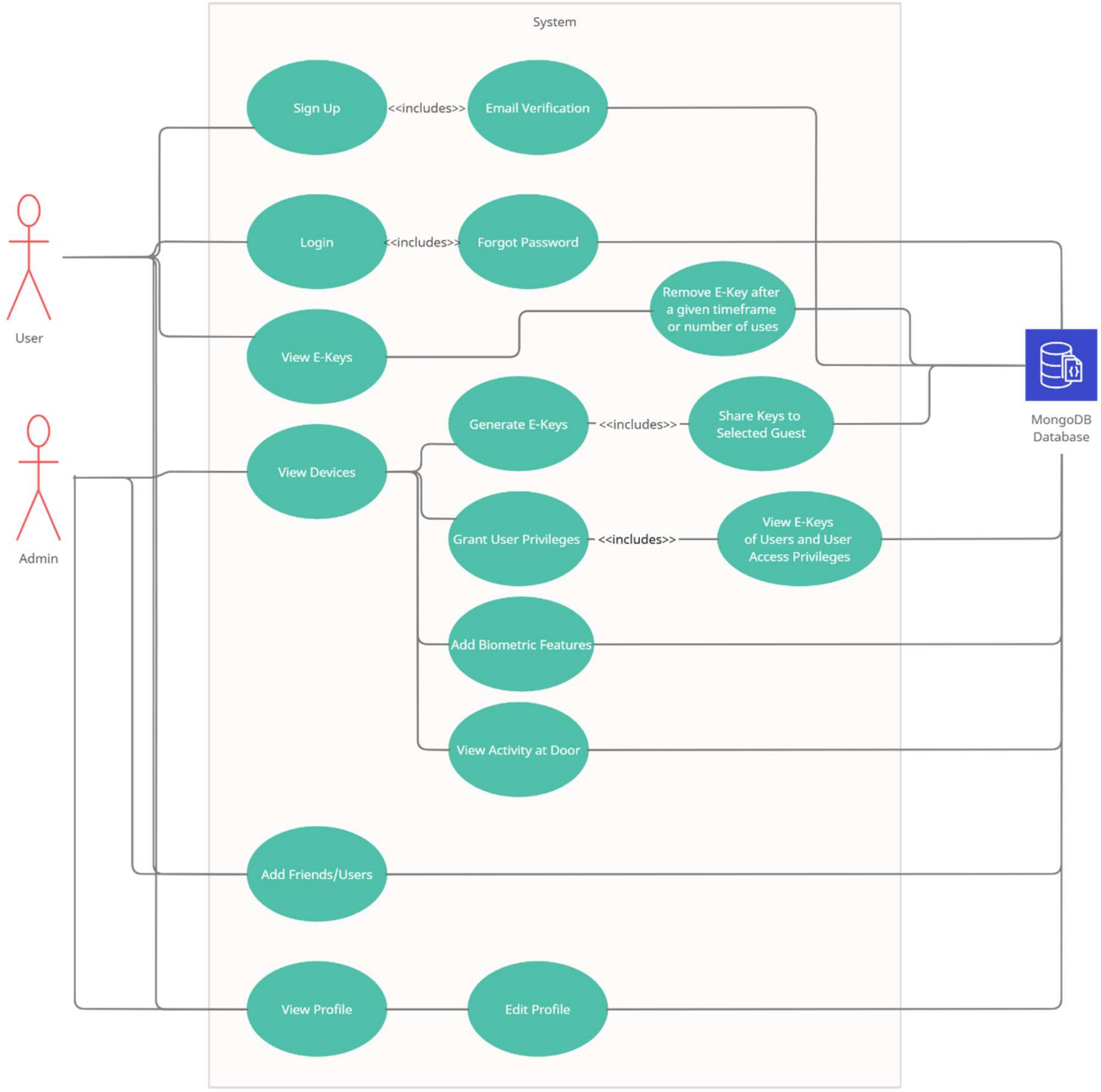
Since our we are using Express.js as our server framework, we can write our API to communicate with the server in Node.js. With Node.js we can create REST APIs that will communicate with the server and run essential operations for our SMOCK Lock. There are 4 main HTTP methods that we will implement with our REST APIs, GET, POST, DELETE, and PUT. With these tools, we will be able to read, create, update, and delete resources inside our database. For our application, we must be able to create accounts, login, update, and delete, as well as all the other essential operations required for operation of our lock detailed in the use case diagram figure below. In order to run, operations such as facial recognition we need to be able to run a python script that compares a live stream that is being sent from the ESP32 camera to the server. To do this we are able to create an API that is able to read the images from the livestream and read the images stored in the database and call a python script that will run the facial recognition and compare the two. The API will be able to run operations similar to this in order to implement the required functions.

7.4.2 API Testing with Advanced REST Client (ARC)

For the testing of API’s, we will be using ARC. ARC is a web developers helper program to create and test custom HTTP requests. This will allow us to make sure that we have functioning API. It will also help us with frontend testing. If we are getting incorrect results from the frontend code, we can test to see if the API is the issue with ARC, which will then allow us to find the mistake and fix it.

Testing is a huge component when developing an app, it allows us to make sure that all of our implementation is working properly, and ARC is one of the simplest and straightforward API testing programs out there. There are also other tools and programs out there, but ARC can be installed as a google chrome web store extension which is very quick and easy to set up. We will also be able to force information onto the database with this program which be nice to test with since we won't need any frontend development to get information onto the database.

Figure 7.0: Use Case Diagram



7.5 Frontend

In this section we will discuss what the frontend will be coded with and what different types of application development tools we will be using to develop our app. We will also go over some application prototypes.

The web development that will be used solely for testing will be developed using React. React is an open-source front-end JavaScript library for building user interfaces based on UI components. Which can easily be used to create the application features and to run API tests.

The app development will use Flutter which uses the dart coding language. Flutter is somewhat incomplete in the web development feature so it may be necessary to use React to complete the web application. We will create widgets to take us from page to page. If you were to click on the camera widget it will bring you to a new page that shows images or a live feed of the camera on the SMOCK Lock.

7.6 Application Design

In this section we will discuss the design of the mobile application. We will go into detail on how account setup is done, how the user can configure their profile, Facial Recognition, Fingerprint Scanning, Temporary E-Keys, and more.

7.6.1 Initial Account Setup

When a user first installs that application, they will be offered the option to either login in with an existing account or sign up with a new account. This can be done by completing a normal account setup using an email, using a google account, apple account, android account, etc. Once a user is logged in a JWT token will be created for that session. These are credentials that will grant secure access to resources. These tokens expire requiring a user to login after the expiration date is reached. The token is attached to all API communications between the app and the server ensuring that only those with the proper token can access their respective resources. After generating a JWT token, the user will be brought to the main page of the application. Here the user will be offered a variety of features including a status indicator of if the lock is currently locked or unlocked, the ability to view users with access to the lock, view a live feed of the camera on the lock, virtually unlock the lock, and talk to people at the door through the lock. This is just some of the main features that will be apparent to the user on the main page of the application.

7.6.2 User Configuration

A user can access their user profile, which will have a variety of settings to configure their user profile, such as name, password, etc. The User Configuration will also allow the user, if registered as the owner, to configure the settings of the lock.

7.6.2.1 Facial Recognition Configuration

Facial recognition is one of the modes of authentication that will be used for the lock. To set up facial recognition, the user will be required to use the app to scan their face using their phone. The database will securely store the facial images of the users and allow the user the ability to unlock the lock via facial recognition.

7.6.2.2 Fingerprint Scanning Configuration

Fingerprint scanning can also be set up through the app. The user will be required to interact with the fingerprint scanner on the lock to store their fingerprints in the database for future use.

7.6.2.3 Security Tier Level

A tier system can be used to determine the required actions that need to be taken to unlock the lock. For example, a security level 2 can be declared, which will require a person to provide 2 means of authentication to the lock in order for it to unlock, such as facial recognition and an RFID key. There will be multiple tiers of security available, and these can be configured in the application according to the owner’s preference.

7.6.3 Granting Access to Other Users

The owner will have the option of granting different means of access to others. This can be done by either sending an E-Key or inviting another person to setup an account to use the full features of the lock.

7.6.3.1 Temporary E-Keys

The app will include the feature of being able to send E-keys to friends, family, or guest. These are temporary keys in the form of a QR-code that can be emailed or sent via text to others. The owner has the right of revoking access of E-keys at any time.

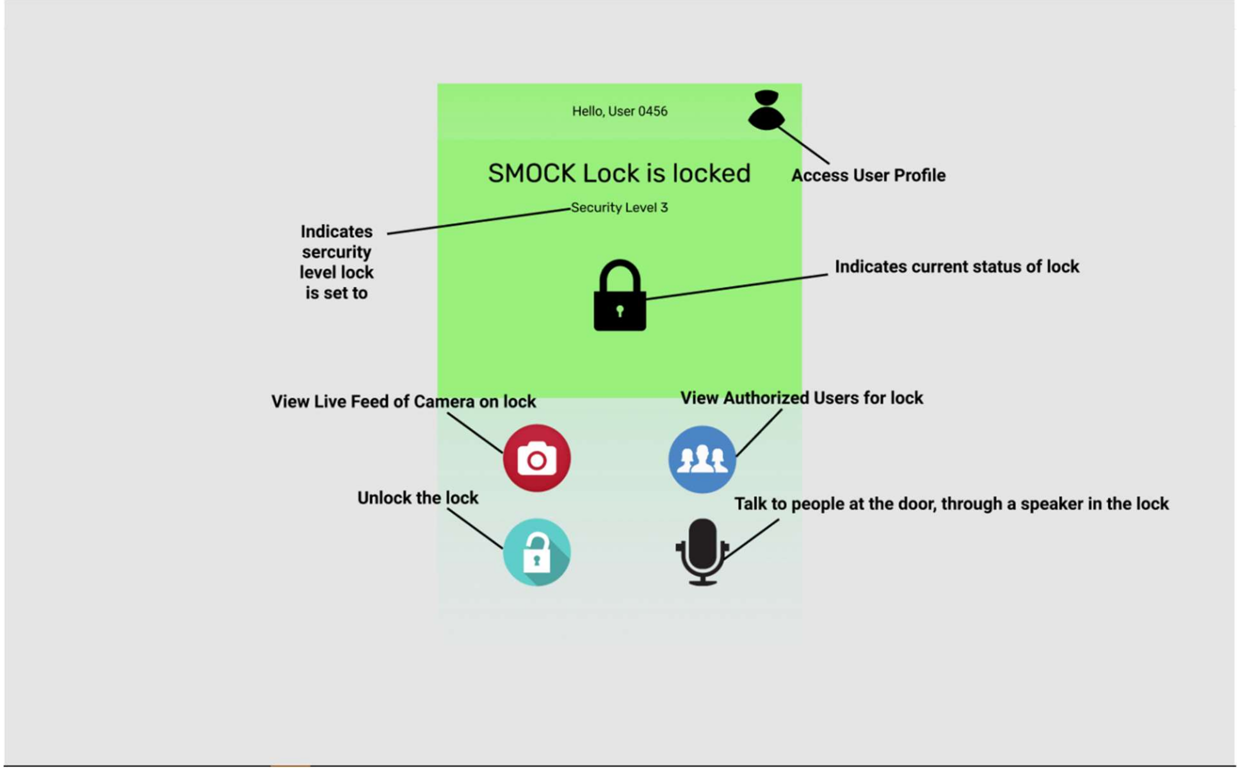
7.6.3.2 Granting Admin Level Privileges

If an owner wishes to grant a more permanent form of access to others. They can send an invite to download the app through email or text message. From here, they can setup their own account and the owner can add this user to their list of admin users. Admin users can use all the features such as facial recognition, fingerprint scanning, unlocking the door via the app, as well as send their own E-Keys if granted permission.

7.6.4 Removing Access from Other Users

The owner will also have the option to remove different access features, such as the Temporary E-Keys and Admin Level Privileges. They will also have the ability to remove the facial recognition and fingerprint readings for a specific user. The Owner will have total control of other users privileges who are given admin/guest access to the lock.

Figure 8.0: Application Prototype


Hello, User 0456
SMOCK Lock is locked
Security Level 3
Access User Profile
Indicates sercurity level lock is set to
Indicates current status of lock
View Live Feed of Camera on lock
View Authorized Users for lock
Unlock the lock
Talk to people at the door, through a speaker in the lock

7.7 Summary of Software Details

In this section we will summarize the software details that were included in this chapter into a table.

Everything discussed about in this chapter is software that everyone in our group currently has on their devices, these are all the necessary software required to develop the SMOCK Lock App.

We have also made sure to share our personal experiences with the different software applications so that every group member feels comfortable with each application. In the case of web-service applications, such as MongoDB where you don’t necessarily need to install an application to create the database, everyone has received an explanation on how to use the website correctly.

Table 7.0: Software Details Summary

Detail:	Description:
MongoDB	An object-oriented, dynamic, and scalable NoSQL database, based on the NoSQL document store model, which is very easy and simple to use.
Heroku	A cloud-based hosting platform. It offers a platform as a service (PaaS), which can be utilized to build, deliver, and deploy our app.
Node.js	Allows us to write our API to communicate with the server in Node.js. With Node.js we can create REST APIs that will communicate with the server and run essential operations
Express.js	Express is a minimal and flexible Node.js web application framework that provides features for web and mobile applications.
Advanced REST Client	A web developers helper program to create and test custom HTTP requests.
Flutter	An open-source UI software development kit used to develop cross platform applications for Android, iOS, Linux and more.
Android Studio	Used in conjunction with Flutter, the official integrated development environment for Google's Android operating system.
Visual Studio Code	An open source-code editor for Windows, Linux, and macOS.
React	Free and open-source front-end JavaScript library for building user interfaces based on UI components.
Ubuntu Virtual Machine (Oracle VM VirtualBox)	A free and open-source hosted hypervisor for x86 virtualization. It is capable of running an Ubuntu (Linux based OS) Virtual Machine which is necessary to deploy certain aspects of our project.

8.0 PCB Design

Printed Circuit Boards are the foundation for almost all the electronics we use today. These boards allow for the support of the mechanical parts of the board along with the electronic components which are listed below.

Table 8.0: PCB Component Descriptions

Component	Description
Resistors	A two terminal electrical component that allows for resistance to be applied into a circuit. This is done for many reasons like dividing voltages, controlling current flow, dissipation of power and many other applications. The measured resistance of the resistor is depicted using a numerical range and depicted using the symbol Ω.
Capacitor	Also, a two terminal electrical component that stores electrical energy and allows for a certain amount of capacitance to build up in a circuit. Essentially this capacitance allows for an electrical field to develop in the capacitor as a net positive charge develops on one side and a net negative charge develops on the other. This allows for the control or total cease of current through a circuit. The measured capacitance of the capacitor is depicted using a numerical range and depicted using the symbol *C*.
Inductor	Also, a two terminal electrical component that stores electrical energy that forms an electric field that can change when current runs through the inductor. The main application for this is in Alternating current to allow for DC to pass while blocking AC. Also this filter action is the basis for most of the uses for the inductor. The measured inductance of the inductor is depicted using a numerical range and depicted using the symbol *H.*
Conductive Pathways	Normally made of copper or gold these pathways allow for the electrical current to pass through the components of the Printed Circuit Board. These pathways are then covered in a material that insulates the pathways and allows for limited loss of power

Table 8.0.5: PCB Component Descriptions Continued

Component	Description
Conductive Pathways Continued	and to protect against accidental contact with the pathways
Active Components	This is a general term in calling all already built electrical components, many of them resting on printed circuit boards themselves. These include microcontrollers and other components that allow for the inclusion of other components.
Electronic Oscillators	Is the component responsible for ensuring the printed circuit board runs at its specified clock rate and allows for everything to occur exactly when its intended. This is done by allowing a board to ensure, through the oscillator, the creation of an electrical signal of constant frequency. The main version seen is the crystal oscillator and is the most recognizable piece of the board.
Transformers	Also, a two terminal electrical component that acts as a current regulator from a power supply that allows the reduction or increase of alternating currents. There are two types, surface or through-hole mounted. The first being the most common as it is much more compact and not penetrating the board which greatly limits the use of it.
Diode	Also, a two terminal electrical component that is a semiconductor device that acts as a stop gate for the current and only allows for it to flow one way. Diodes can also change the current from alternating to direct or vias versa, therefore they are also called rectifiers.
Voltage Regulator	Also, a two terminal electrical component that ensures that a specific voltage flows through and that the voltage stays constant. This ensures for more complex systems that the power needed for a specific piece is guaranteed and constant. The regulator can work on both alternating and direct currents and some can work with multiple flows or have multiple existing lines.

8.1 PCB Layer Types

Many types of layered PCBs can be created but are generally allowed to be categorized in the following categories.

8.1.1 Single Sided PCB

The most basic form of a printed circuit board and only allows for a single layer of conductive pathways which greatly limits the sophistication of the printed circuit board. The actual components are mounted on one side of the printed circuit board and on the reverse side the conductive pathways are etched into the board. However, the simplicity of the printed circuit board allows for the cheap, efficient, and high volume of manufacturing. Also, the simplicity allows for the PCB to easily interface into more complicated printed circuit boards. Some examples of simple printed circuit boards are calculators, simple electrical signal alternators and power supplies.

8.1.2 Double Sided PCB

A slightly more complex version of the single sided printed circuit board that has two layers of conductive pathways that are connected by vias. This allows for the number of traces to be much greater and allows for a much more sophisticated printed circuit board and is the most common type of printed circuit board. The main benefits of the double-sided printed circuit board are the decreased board size as the increased amount of conductive pathway space greatly increases the manufacturers' ability to hide the traces better. The applications unlike the single sided printed circuit board are practically limitless, the only real limitation would be the type of materials used in the construction of the board.

8.1.3 Multi-Layered PCB

The most complex version of the printed circuit board which allows for as many layers of conductive pathways as needed but not less than three. This limitless amount of conductive pathway layers is achieved by wrapping a core with the conductive pathway layer and then alternating a conductive pathway layer with a material called preneg to act as an insulator between the layers. These layers are laminated together using high temperatures to ensure no air or other foreign materials are trapped in the layers, as it would cause the printed circuit board to be defective. The benefits of the multi layered printed circuit board would be extremely high board density leading to smaller board size for the complexity of the board, flexible architecture that allows for a wide range of applications and easier implementation of standard electrical standards such as ground and power locations and durability of the printed circuit board itself. The applications of the multi layered printed circuit board would be any technology that needs extremely sophisticated printed circuit boards or needs a board that can communicate within itself through many layers.

8.2 PCB Material Types

Many types of material PCBs can be created but are generally allowed to be categorized in the following categories.

8.2.1 Rigid PCB

This printed circuit board can be any of the different type of layered printed circuit boards, however the rigidness of this board is due to the layering of many materials to create the board. For example, many of the boards are comprised of the following layers, copper, mask, silk screen and preneg. This combination is made for every conduction pathway layer and is compressed onto each other to make the board very rigid and unable to be twisted. This board type is cheap and easy to repair but at the cost of flexibility and hard to adhere to existing technologies. Some types of rigid printed circuit boards are computer motherboards, graphics cards, cameras, and solar panels.

8.2.2 Flex PCB

This printed circuit board can be any of the different type of layered printed circuit boards, however the board is developed on a kind of flexible material. This material is most commonly Polyether ether ketone or a transparent version of the material. As such the board is more complicated to produce as the layers all need to be flexible so most of the time the board is layered in a copper then mask layer. This allows the printed circuit board to keep is flexibleness while also decreasing the complexity. This board type takes away the usage of connectors, i.e. wires as the board can directly interface with the desired printed circuit board. Also, the board type is much better on space as it can literally flex into any position is needed, this also speaks on its ability to seamlessly adhere into other technologies. Some common uses of these are for OLED or for small scale technology such as laptops.

8.2.3 Flex-Rigid PCB

This printed circuit board can be any of the different type of layered printed circuit boards, however the board is developed on a rigid material using the same method as a rigid board. However, the use of flexible materials for the connectors allows the board to interface in ways that a normal rigid board cannot. The development of this board type is the most complicated of the three but brings all of the benefits of the other two with little downfall. This makes the Flex-Rigid printed circuit board the best for extremely complicated technology and is most likely the future of printed circuit boards.

8.3 PCB Construction

In this section we will discuss the process of PCB Construction, which consists of Traces for the PCB, Substrate for the PCB, and Solder Masks.

8.3.1 Traces for the PCB

A trace is the connection in the conductive pathways that interfaces two points in the printed circuit boards. These traces are around 4 – 12 mil in width with many considerations made to find the correct width. These include the board cost, density, layers of the board, what kinds of material are present, what insulator is used, what kind of layer board is it, space optimization and whether it’s a high voltage or current boards. Below are generally the guidelines for the traces

Table 8.1: Trace Descriptions

Type	Description	Values
Trace Width	The actual width of the trace on the conductive layer, this width mainly is affected on whether the board is dealing with high currents and voltages	Between 4 – 12 mils
Trace Spacing	The spacing of the traces are also mainly affected on whether the board is dealing with high currents and voltages. Also, the material of the trace and insulator is a big factor in the spacing	Between 1 – 5 mils
Vias Holes	This only is affected on boards that are not single layer printed circuit boards. The diameter of these holes is what the traces will go through when reaching other layers in the printed circuit board. The main attribute that effects this is the materials that the layers are comprised of.	Between 1 – 8 mils
Trace Thickness	The thickness of the traces are mainly for the current flowing through the trace.	.1 mils – .3 mils

8.3.2 Substrate for the PCB

The material used in the substrate of a printed circuit board can greatly affect all the aspects of your printed circuit board. Aspects such as price, longevity, and performance. Below are the generally accepted substrate materials that are allowed to be used.

Table 8.2: Substrate Descriptions

Name	Temperature Limit	Description
Polyimide	110 C	Extremely flame retardant and is the most used in simple electronic parts, as it is the cheapest of the selected. The rigidity of the material makes its use in only rigid printed circuit boards. It is commonly praised as the best all around material for its tensile strength and its ability to work perfectly in both dry and humid environment.
CEM1	122 C	CEM stands for composite epoxy material. Flame retardant, extremely low cost in comparison to the other CEM's and only uses one layer of a glass mask making it the worst of the three but also the cheapest
CEM2	125 C	Has a cellulose core that makes it susceptible to fires but allows for the most efficient substrate of the three.
CEM3	125 C	Flame retardant and has the same capabilities as the other three by using multiple layers of the glass mask. Making this the most popular of the three by far and making it extremely like FR-4
RF-35	130 C	Uses an organic ceramic mask, with a woven glass material that is high cost. This is mainly for wave applications and shouldn't be used for any other applications
FR-4	135 C	The most common used substrate that is comprised of a woven fiberglass and an epoxy mask. It is flame retardant and extremely cheap making the ideal substrate type.
PFTE	220 C	A synthetic polymer that is being tested as a new replacement for FR-4 that is also flame retardant. However, the cost is cheap with a high temperature limit thus allowing high stress printed circuit boards to be developed with a cheaper alternative. With more research this material is projected to pass FR-4 in popularity.

8.3.3 Solder Masks

A solder mask is a thin layer of polymer placed on the finished printed circuit board to allow for the soldering of pins on the board and to stop the oxidation of any connectors not concealed by the mask of the board. Also, this layer prevents

“Solder Bridges” from forming, these are connections made from a solder connection that is unintentional between two close pins. The most common form of a solder mask is a silkscreened epoxy that is applied to the face of the board and is then vacuum sealed on.

9.0 Administrative Content

In this section we will discuss Financing, and Initial Project Timeline. There are many things that our group must account for when developing and designing the SMOCK Lock. Such as Scheduling/Timeline, this will allow us to keep up to date with due dates and make sure we are allocating our time effectively and efficiently. Effective planning is a huge role and arguably is the most contributing factor in the success of a group project.

The Financing will also be discussed in this section, as this group does not have a sponsor, we will be purchasing all the items needed for the development and production of the SMOCK Lock to be out of pocket. We need to make sure that, all the items we are purchasing, will be purchased in advance, this will allow us to deal with any defective parts without having to stress about a nearing due date/submission.

We will soon be implementing everything into our PCB and begin testing next semester, with that in mind the below sections give a timeline and table of financing.

9.1 Financing:

We have set the initial estimated budget to be around $125 with a maximum budget of $200. The project will not be funded and will be paid for out of pocket. We plan to group the money into one account and only purchase supplies and materials from that account. This way each group member can have an even split.

Below is an estimated cost for supplies and materials to build the smart lock. These estimates were made by basing the price of specific and unique materials that will fit for our specifications and taking the mean average price of each item compared.

9.1.1 Financing Estimation

From this rough estimate, we can say that each group member will pay between $25.25 and $43.75 for a 4-way split of $101.00 - $175.00. This $101.00 - $175.00 estimate is a great price for other common products on the market that are priced in the range of $150-300 for a smart lock. The smart locks in this range also do not contain all the features that our smart lock will contain.

9.1.2 Final Financing

Below will be a table that shows the actual price of materials and the quantity of which we intend to purchase. Please note that the total price in the table is the price of each component purchased once.

Table 9.0: Estimated Price of Materials

Item	Price (Estimated)	Quantity
Power Supply 9V (8 pack)	$11.87	1
Wi-Fi Module	$3.49	2
Camera	$10.82	2
Solenoid Lock	$14.70	2
Speaker	$12.00	2
Casing	$30.00	2
Fingerprint Scanner	$23.99	2
PCB	$130.00	2
Prototype Parts	$48.00	2
Display	$9.49	2
RFID	$10.80	2
PIR	$10.49	2
Total	$363.65	23

Halfway through the development and research of the SMOCK Lock we anticipated spending somewhere between $186 and $279. After researching and looking for all the necessary parts to allow the SMOCK Lock to function, we now find that the total would be $363.65. Which if split up by 4, would mean that each person will have to pay around $90.91.

However, the total price in the table does not disclose how much it would cost considering we plan on buying multiple parts, in case of a faulty part. Which would mean we would pay twice as much, so every person would have to pay around $131.82. After all the research we've done we have concluded that these are the parts that are necessary and that must be purchased in order to ensure that the SMOCK Lock will be able to provide the safety we have talked about throughout this paper.

9.2 Project Timeline:

In this section we will discuss our Project Timeline and what we expect to have completed during our time in Senior Design.

The table below discusses our Initial Project Timeline and what we hope to complete during each month until the end of Senior Design 2. This is a rough estimate and is subject to change.

Table 9.1: Initial Project Timeline

Time	Tasks
August	Create Group and discuss potential project Ideas
September	Finish the divide and conquer, meet with Dr. Wei to discuss the idea, and begin designing key systems
October	Begin working on the SD1 paper and continue working on the key systems for the project
November	Continue working on the SD1 paper and on key systems while beginning the design on the hardware component of the system
December	Finalize the SD1 paper and the design of the project in preparation for the construction of the project
January	Begin Construction of the test environment and lock, start developing the server side of the project and establishing the database and implementing the fingerprint scanner
February	Begin training and testing the facial recognition systems, continue developing the server side of the system, begin working on the microcontroller systems
March	Continue working on the microcontroller portion of the project ensuring all components of the physical lock are

Table 9.1.5: Initial Project Timeline Continued

Time	Tasks
March Continued	working and creating the app to interface with the system.
April	Final testing of all components and aspects of the project. Any implementation that has not been completed should be completed by the end of the month.
May	Presentation of our SMOCK lock Senior Design Project.

10.0 Conclusion

In conclusion, the SMOCK Lock be a safe and secure lock that will be capable of saving and comparing faces, fingerprints, and QR Codes, all which can be used to gain access given that the Owner has given you permission to do so. The app will consist of biometric features that are accurate, and an easy-to-use app so that even those that are not completely proficient in using technology can still feel safe at home. The SMOCK Lock will abide by all relevant standards and constraints. It will be comparable and hopefully cheaper to produce than most smart locks that have the same features that we provide.

Appendix

References

[1] [Online] https://usa.kaspersky.com/blog/sas2020-fingerprint-cloning/21522/

[2] [Online] https://lowrysolutions.com/blog/how-rfid-and-rfid-readers-actually-work/

[3] [Online] https://www.iso.org/home.html

[4] [Online] https://standards.ieee.org/

[5] [Online] https://www.fictiv.com/teardowns/special-edition-teardown-lockitron-bolt-with-paul-gerhardt

[6] [Online] https://searchapparchitecture.techtarget.com/tip/What-are-the-types-of-APIs-and-their-differences

[7] [Online] https://www.ieee.org/about/corporate/governance/p7-8.html

[8] [Online] https://www.geeksforgeeks.org/python-vs-php/

[9] [Online] https://reactnative.dev/

[10] [Online] https://blog.matric.com/pcb-substrate-types

[11] [Online] https://www.sfcircuits.com/pcb-school/pcb-trace-widths

[12] [Online] https://www.javascript.com/resources

[13] [Online] https://www.fictiv.com/teardowns/special-edition-teardown-lockitron-bolt-with-paul-gerhardt

[14] [Online] https://www.ideamotive.co/blog/swift-vs-objective-c-which-should-you-pick-for-your-next-ios-mobile-app

[15] [Online] https://www.arducam.com/product/arducam-ov5647-standard-raspberry-pi-camera-b0033/

[16] [Online] https://security.iri.isu.edu/ViewPage.aspx?id=355

[17] [Online] https://www.ieee.org/about/corporate/governance/p7-8.html

[18] [Online] https://www.amazon.com/CQRobot-Speaker-Interface-Electronic-Projects/dp/B0822XCPT8

[19] [Online] https://wiki.seeedstudio.com/Grove-Fingerprint_Sensor/

[20] [Online] https://thepihut.com/products/sparkfun-analog-mems-microphone-breakout-ics-40180

[21] [Online] https://www.electronics-lab.com/project/video-streaming-server-esp32-cam/

[22] [Online] https://support.envistiamall.com/kb/ky-037-microphone-audio-sound-detection-sensor-module/

[23] [Online] https://worldsway.com/different-types-of-pcbs/

[24] [Online] https://www.xenonstack.com/blog/kotlin-andriod

[25] [Online] https://www.manchesterdigital.com/post/foresight-mobile/is-xamarin-dead

[26] [Online] https://dart.dev/

[27] [Online] https://nodejs.org/en/

[28] [Online] https://aws.amazon.com/

[29] [Online] https://piratelearner.com/en/bookmarks/how-to-check-whether-16x2-lcd-working-or-not/16/

[30] [Online] https://cloud.google.com/

[31] [Online] https://azure.microsoft.com/en-us/

[32] [Online] https://www.heroku.com/

[33] [Online] https://www.digitalocean.com/

[34] [Online] https://en.wikipedia.org/wiki/Android_Studio

[35] [Online] https://en.wikipedia.org/wiki/Flutter_(software)

[36] [Online] https://expressjs.com/

[37] [Online] https://www.uctronics.com/download/OV2640_DS.pdf

[38] [Online] http://www.datasheet-pdf.com/PDF/OV5642-Datasheet-Ommivision-685174

[39] [Online] http://web.mit.edu/6.111/www/f2016/tools/OV7670_2006.pdf

[40] [Online] https://www.amazon.com/Degraw-DIY-Speaker-Kit-Amplifier/dp/B07CRVRG83

[41] [Online] https://www.newegg.com/p/1B4-04F9-000H7

[42] [Online] https://wiki.dfrobot.com/Capacitive_Fingerprint_Sensor_SKU_SEN0348#target_3

[43] [Online] http://www.diymalls.com/Optical-Fingerprint-Reader-Sensor

[44] [Online] https://cdn-shop.adafruit.com/datasheets/TC1602A-01T.pdf

[45] [Online] http://www.xlsemi.com/datasheet/XL6019%20datasheet-English.pdf

[46] [Online] https://www.olimex.com/Products/Breadboarding/BB-PWR-3608/resources/MT3608.pdf

[47] [Online] http://www.haoyuelectronics.com/Attachment/XL6009/XL6009-DC-DC-Converter-Datasheet.pdf

[48] [Online] https://www.ti.com/lit/ds/symlink/cc3120.pdf?ts=1638666877060&ref_url=https%253A%252F%252Fwww.ti.com%252Fproduct%252FCC3120%253Futm_source%253Dgoogle%2526utm_medium%253Dcpc%2526utm_campaign%253Depd-con-null-prodfolderdynamic-cpc-pf-google-wwe%2526utm_content%253Dprodfolddynamic%2526ds_k%253DDYNAMIC%2BSEARCH%2BADS%2526DCM%253Dyes%2526gclid%253DCjwKCAiAwKyNBhBfEiwA_mrUMuTDGeFtzUrHARrjrLYJC_rXTe5Qqon2en1YITYiwPS1TcyMJbB4bhoCeO8QAvD_BwE%2526gclsrc%253Daw.ds

[49] [Online] https://www.espressif.com/sites/default/files/documentation/esp32_datasheet_en.pdf

[50] [Online] https://www.espressif.com/sites/default/files/documentation/0a-esp8266ex_datasheet_en.pdf

[51] [Online] https://eprint.iacr.org/2007/471.pdf

[52] [Online] https://en.wikipedia.org/wiki/IEEE_802.11

[53] [Online] https://www.securew2.com/blog/complete-guide-wi-fi-security

[54] [Online] https://hackercombat.com/serious-vulnerabilities-detected-in-the-wpa3-protocol/

[55] [Online] https://cs.gmu.edu/~yhwang1/INFS612/Sample_Projects/Fall_06_GPN_6_Final_Report.pdf.

[56] [Online] https://www.researchgate.net/publication/228721467_Wireless_network_security_Comparison_of_WEP_wired_equivalent_privacy_mechanism_WPA_wi-fi_protected_access_and_RSN_robust_security_network_security

[57] [Online] https://www.researchgate.net/publication/262282304_Exposing_WPA2_security_protocol_vulnerabilities

[58] [Online] https://www.researchgate.net/publication/290743584_A_Survey_on_Wi-Fi_Protocols_WPA_and_WPA2

[59] [Online] http://jin.ece.ufl.edu/papers/MILCOM15.pdf.

[60] [Online] https://ieeexplore.ieee.org/document/9152782/

[61] [Online] https://dl.irstu.com/wp-content/uploads/Download/Education/Book/Network/Network%20Security/WEP-WPA-Article/Vulnerabilities%20of%20Wireless%20Security%20protocols.pdf

[62] [Online] https://www.wwt.com/article/how-secure-is-wifi-really/

[63] [Online] https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/

[64] [Online] https://ww1.microchip.com/downloads/en/DeviceDoc/Atmel-7810-Automotive-Microcontrollers-ATmega328P_Datasheet.pdf

[65][Online] https://ww1.microchip.com/downloads/en/DeviceDoc/30010135E.pdf

[66] [Online] https://itchronicles.com/artificial-intelligence/where-is-ai-used-today/

[67] [Online] https://connectedremag.com/newsletter/is-facial-recognition-technology-a-no-go/

[68] [Online] https://recfaces.com/articles/what-is-voice-recognition

[69] [Online] https://www.marylandfingerprint.com/single-post/2020/10/26/3-types-of-fingerprints-latent-patent-and-plastic