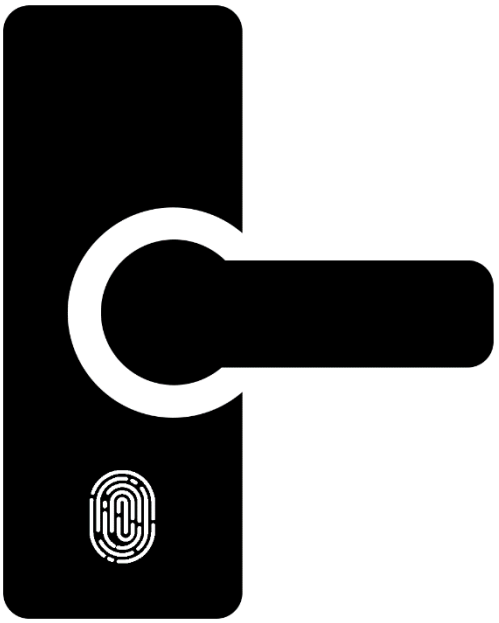
Senior Design 1
Summer 2019
Project: Smart Locking System

Department of Electrical Engineering and Computer Science
University of Central Florida
Dr. Samuel Richie



SMART LOCK

Group 6

Ali Al-Hajri - Electrical Engineering - alhajri@knights.ucf.edu
Mark Rodriguez - Electrical Engineering - mark.rodriguez@knights.edu
Noor Pirzada - Computer Engineering - noor.pirzada@knights.ucf.edu
Idoko Abuh - Electrical Engineering - idoko.abuh@knights.ucf.edu

Table of Contents

1 Executive Summary

Today, most households are left unattended for the majority of the day while everyone leaves for school or work. This poses security risks from potential home burglars who with the help of readily available door lock picks, can gain entrance into a home. With no one home to realize the danger, burglars are able to break into homes and take what they may without anyone being notified about it. Currently, the solution has been to install security cameras throughout the home as well as sensors in each of the entry ways such as, doors and windows. These are used to detect when an unknown presence has gained entry without authorization. While these systems work, they often require expensive upfront installation costs as well as costly equipment fees for sophisticated cameras and sensing equipment. In addition, there is usually a monthly service fee to cover the cost of monitoring the unattended home. In all, this is a costly system that is not always an option for most families. As a result, a great majority of unattended homes are left vulnerable to exploitation.

To better protect our homes while at a reasonable rate, we are proposing a solution by means of a smart lock system. This smart lock system installs easily in place of any deadbolt lock. With simple household tools, anyone will be capable of mounting the door lock without having to pay costly install fees. This system can be installed on all main entrances to the home such as the garage, front, and rear doors of the home. Our revolutionary locking system features a backlit LCD display that allows users to key in an access code to gain entry. The backlit display will provide enough lighting so that the user can easily read the digits on the display during night time. This method of authentication is excellent for guests and postal delivery personnel. For example, an access code can be generated and given to a guest so that they can easily access the home while they visit. This is also a great way to give access to a trusted postal worker so that they can place packages safely inside the garage when no one is home to receive them. In both cases, access can be limited to a specific time and turned off when it is not necessary. This way, whenever guests leave or if you are not expecting a package, access can be turned off to prevent anyone from entering the home without authorization. In addition to the LCD display, the smart lock system will also count on an RFID reader and fingerprint reader. Both options will allow someone to enter their home quickly by simply swiping the RFID key near the sensor or by pressing their thumb print against the finger print reader. We feel that by adding various authentication methods our smart lock system will separate itself from other competing options by having an additional convenience factor. Even still, we feel that more can be done to separate our product from other

competitors. If time allows, we would like to implement an additional feature to our product that will further separate it from its competitors by using cutting edge technology. We hope to incorporate a camera to perform facial recognition. This camera will allow a user to access their home by simply looking at the camera for a moment. In combining all of the aforementioned features, our smart lock system will be the smartest system available that will ensure safety of one's home at a relatively low cost.

2.0 Project Description

In the proceeding sections we will discuss the project and its properties. We will begin with an explanation for the motivation behind our project and the goals we hope to accomplish. We will also discuss our project requirements for both the hardware and software components of our project which encompass both industry standards and design constraints. These constraints will define our project as we will need to consider these throughout the process of designing and building our project to ensure we adhere to these set requirements. To further demonstrate the linkage between our project engineering specifications along with the functionality constraints we will discuss our project house of quality. To give perspective to our project, we will provide block diagrams and flowcharts to illustrate the process by which our project came to be. These flowcharts and diagrams also allow our team to keep track of our progress and ensure that all components are completed so that we adhere to our constrains and requirements. To show the process of our decision making, we will look at our decision matrix which shows the analysis and criteria comparisons made for the components that make up our project. We will conclude with our project measurables, a list of must have features, and extended goals we wish to incorporate in our project should we have time to implement them.

2.1 Project Motivation and Goals

Our motivation for this project is to improve the way people access their home by incorporating innovative technologies into a door locking system. This system is to replace the standard dead bolt lock found in most homes. This new technology would be beneficial for home, business, and recreational applications that have a door that requires a lock. With our new smart lock system, the need for keys to access a building will no longer be necessary as a new way of authentication would be in use. This is convenient for everyone as it means that we would no longer need to keep a key chain full of keys in our pockets to access the various buildings we frequent. It would also solve the problem of locking one's self out of their home after forgetting their keys inside. We recognize that our world is becoming increasingly digital and with this product, our customers would be able to simplify their lives further by switching their old locks for new innovative ones. We also realize that several smart door lock systems currently exist in the market. In fact, there are several that contain most of the features we plan on incorporating into our design. What separates us from the rest is that we combine the features found in several models into one package and offer room for improvements. In addition, we feel that

we can provide our product at a better price by sourcing our parts from the most affordable retailers. Providing a cost-effective solution for our customers is one of our goals as we would like everyone to be able to afford a smart lock system that will better their lives by simplifying the way they access their homes.

The three main goals we have for our project is to offer three modes of access via our smart lock system. They are RFID, LCD keypad, and Finger print sensor. These three key features would ensure we meet our design constraint of removing keys as the standard way of accessing one's residence. While all features perform essentially the same task, we feel that by providing all three, we give our customers the choice to select the mode of access that they find most convenient. This way, they do not have to decide on one single feature when purchasing a smart lock system. This is also beneficial to the customer as it allows them to create temporary accounts using the keypad feature while leaving the RFID and finger print sensor options available only for members of the home. Should we complete all of the three key features and still have time to work on our project before the deadline, our extended goal is to incorporate a camera into our design so that we could implement a facial recognition feature. This facial recognition feature would be highly reliant on our software design as we would be coding the capability ourselves in order to offer our customers greater affordability. This feature is not readily available on the market and if found, the cost is astronomical. We feel that if we can add it to our project, we will be able to offer a smart lock system that would blow away the competition by a large margin.

2.2 Agile

To maximize efficiency during the developmental stage and to ensure that that project requirements are met, agile development was used.

Agile is a model for sustainable development cycles. Agile advocates for the use of 'sprints' which serves as chunks of time devoted to specific developmental tasks. These chunks are made after the customer and the project manager negotiate requirements; the developers plan out a series of sprint. Each of the sprint will focus on one section of application and no other requirement can be added to the development once a sprint had begun. Each sprint should last no more than one month. After a sprint has ended, the development team should have an extended meeting. This meeting to make sure that the members discuss the last sprint progress; what went wrong, and what can be fixed.

2.3 Objectives

Our main objective for the project is to design the most innovative smart lock system that combines the features of most of the already available smart lock systems into one consolidated package. To have our project stand out from the others, we plan to offer the most features for the best price while ensuring optimal quality, functionality, and overall aesthetics which would complement our customers home and style. By combing our team's knowledge and capabilities, we will ensure thorough testing is

completed to ensure we deliver a fully functioning, well tested product that our customers will love. In addition, we will make sure that our product is easy to install and will provide easy to read instructions so that everyone is able to install our product in their homes without any frustration.

2.4 Requirement Specifications

This section exists to codify the exact engineering requirements the project must measure up to. What follows are the design specifications for the Smart Lock project. The specifications are broken down by which module they relate most closely too, but there is some overlap between the systems. These specifications will be used to select parts that best fit requirements and will heavily influence the design of the project. All engineering requirements and specifications are derived directly from the original marketing goals, or the features the design team set out to achieve from the outset of the project.

User Objectives and Design Constraints

- Low Price
- Durability
- Battery life
- Ease of Use

Market Requirements

- Device will be able to stay powered on for a minimum of one month without charging.
- LCD Backlight will provide an ambient light source to allow ease of use
- The cost of the device will not exceed $600 to stay under competitor pricing

2.4.1 Power Specifications

The primary source of energy that will power our smart lock system will come from an AC adapter that will provide 5 volts via the 120-volt, 60 hertz wall power connection provided in all North American homes. Our PCB will include a voltage transformer circuit in order to step down the 120-volt power source to our needed 9 volts to power the microcontroller along with the various components that make up our project. We decided to use a direct power source instead of a battery because we plan to incorporate a camera that will allow for facial recognition. This feature is heavy in power consumption and while a battery source would be able to power the unit, it would be inconvenient for the user to have to replace the battery packs routinely. Should time allow, we will consider adding a backup battery source so that the unit remains powered on when power is lost. Because our design will be installed on the wall near the door, running a power cord to the unit should not be a problem and will not make installation any more difficult as we will demonstrate in our product model in which we will have a working prototype of our product.

As one of our design constraints is to have a low power consumption, we will be utilizing software to set each of the authentication methods to low power mode so

that they will not drain as much power until a user triggers it This way, rather than having the fingerprint sensor, facial recognition camera, RFID sensor, and LCD display running all the time we will set the camera to simply detect the presence of an object and only then, will the smart lock turn on all capabilities to detect if the person present is authorized to unlock the door. We believe that by using software to conserve energy we are ensuring that our product is helping the environment by not consuming energy that is not necessary.

2.4.2 Safety Specification

The smart lock system will be free of any exposed wire connections to prevent injury to the user. The components will be securely mounted to the panel where we will be placing all the components so that they can be used safely and conveniently. Our smart lock system will be a flat panel that can be mounted on an adjacent wall near the door. The smart lock will be clearly lit so that the user is able to see it during night conditions so that they are able to safely operate the unit. We will be enclosing the PCB along with all the wiring inside of an enclosed housing which we will design using 3D printing. The idea behind our design is simple, approachable, and aesthetically pleasing. Because our locking system will not involve a door knob, we will not need to run additional wiring to trigger the dead bolt to lock and unlock. Instead, we will be using a magnetic lock which attaches to the wall and door. The door remains locked until the user authenticates their access by using the smart lock. At that point, the magnetic lock disengages and allows the user to open the door. By using a magnetic lock, we reduce the number of components that are needed as we will not have to develop a rotary system to rotate the knob and move the dead lock. This makes our design sleeker and, in the process, saves money by requiring less materials.

2.4.3 Bluetooth System Specification

The lock microcontroller uses Bluetooth module to communicate. HC-05 module is used along with Arduino. A mobile application will then be used to communicate with the Bluetooth allowing the user the view the statuses of lock or unlock the door as long as they are in the Bluetooth range. Upon the Bluetooth receiving the change of status command from the mobile application, it will create a new table for the event (to keep a log). This instruction will be passed along to the lock microcontroller. At this point, the team is only creating one lock, but the application will give leverage to the user to add/connect more locks through the application, which means that there can be many functional locks in one application. Moreover, one lock can have many users that can be added to the application as many people live in the same house/apartment.

2.4.4 Mobile application feature Specification

The initial design for the mobile application is to be available on Android devices because as more research was done, creating an iOS application is much more expensive and challenging therefore it was decided not to include it. With that being

said, the mobile application will be used to control the Smart Lock will have both android versions. It will send and receive JSON payloads to the server in order to interact with the system. From the mobile application, the user will be able to create an account, create an association between the user and a lock, and to view and change the status of locks associated with their user account. The home screen of the application will display each lock associated with the user account along with a toggle switch to interact with it. A settings menu will also be available to the user where they can toggle “lock after a certain amount of time” and “give push notifications” on or off. Instead of having push notifications, the final product will display the current status of the lock on the main screen as well as a pop up that shows the action and when that action was executed whenever the lock/unlock button was pushed.

2.4.5 Facial Recognition Camera Specification

There will be an additional security feature integrated in the Smart Lock; a Facial Recognition Camera. This feature is only activated when unlocking of the door fails through the application, passcode, RFID or finger print. The user has to face the camera attached to the system. This camera will take less than a minute to detect the face of the person. As the camera finds the face of the person, it will extract features of the face. The extracted features are then compared with those of the image of faces stored in the database. If the image matches to that of what is stored in the database, the door unlocks. However, if the unlocking through the application fails, or if the face is not recognized by the camera, it takes a picture of the person and sends it to the Android application using the Bluetooth connectivity. Upon receiving the picture, the user can decide if they want to let the door stay locked or unlock it through the application.

2.5 Hardware Constraints

In practically all engineering projects, there exists hardware and structural components which have their own sets of limitations and constraints. Our project has many different components that connect to the microcontroller and require their own set of power and data connections. In fact, an electrical anomaly in one component such as the finger print sensor, can cause catastrophic failure to the other components by means of causing a short to the microcontroller. One way an electrical short can happen is when the PCB or electrical components come into contact with water. Because our smart lock system is installed on the outside of the home, it is very likely that the smart lock will be exposed to elements on many occasions. To combat this problem, our design is an enclosed box that is thin enough to house the wiring and PCB board. The internal components will be securely enclosed by a front panel that will have the authentication components mounted onto it. In this way, while the sensors and camera are exposed to the elements, the wiring and PCB are protected from rust, corrosion, and liquid damage. This will ensure that our smart lock system adheres to our design constraint of being durable. To ensure that the fitment of the closure is precise, we will be using a 3D printer to create the enclosure is sized perfectly so that water and moisture is unable to enter which can

greatly affect the electrical components. In addition to ensuring protection from the elements, this enclosure will securely hold the PCB in place so that none of the soldered components are accidentally dislodged during transportation. This design also makes our product look and feel more professional as it will show that thought was placed in the design such that even the case was built around the design of PCB circuit.

Because wires can be cut to size, we are not extremely concerned with the wiring of our circuit. However, we do find it important that wires are neatly tucked in the enclosure so that if the unit needs to be opened for repair, damage is not caused to the electrical components. For this, we will be running the wiring neatly along the borders of the unit and provide a sufficient amount of flex in the cabling so that when the unit is opened, enough room is provided so that it can be worked on. We will also be using U.S. wiring color conventions to distinguish the wires from one another. While the PCB will have labeling to describe what each wire connection is for, we feel it is important to incorporate the wiring color convention into our design so that we prevent accidental damage to the unit when being repaired. In the U.S., a 120 V power source should be enclosed by a red insulator and conversely, the ground wire should be either green or green with yellow as can be seen in Figure 1.

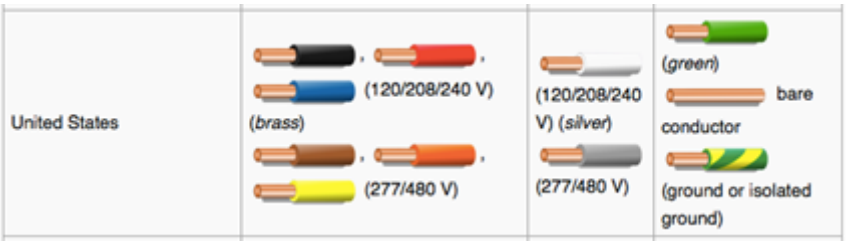


Figure 1 U.S. Wiring Color Convention [32] Creative Commons license, image allowed for non-commercial use

For our project, we will use red and blue for all positive “hot” signals and green or white for all negative “cold” signals. By utilizing this standard, we are creating a clean and professional design that complies with our regional standards.

2.6 Hardware Specifications

Prior to building our project, our team discussed the hardware specifications for each of the features we desired to implement on our build. The first and most important specification is that we maintain the electronic components safe from the elements. To achieve this, we designed a mockup of the enclosure which will house all of the components securing them neatly so that the wiring does not become loose when jostled or moved. In addition, the enclosure will have mounting holes to be used when installing the device. The enclosure will be a box with dimensions of 4 inches long, by 4 inches wide, by 1 inch thick.

Our device will have an array of various sensors which need to communicate with the microcontroller. The finger print sensor and RFID sensor must be able to monitor the environment so that it is enabled when a user comes into contact with it. It must conserve energy when not in use by switching to lower power mode. Once a user

comes into contact with either of the sensors, they must switch to full power and function as normal. We will be controlling both sensors by using the microcontroller to program the sensors to switch power modes. In a similar way, the facial recognition camera will remain on low power mode until a user comes into the viewing area of the camera, at which point the microcontroller will begin to process the image captured in order to verify if the person at the door is authorized to unlock. To indicate whether the system is active, we will have an LED indicator on the unit such that if the light is green then the system is in active mode. Conversely, if the LED indicator is red, then the system is in low power mode or in an inactive mode.

All the components that make up the smart lock system will be controlled by the microcontroller. The microcontroller will be responsible for controlling the power mode of all the components as well as obtaining and processing the sensory detail received. Once the data is processed, the microcontroller will determine if the user request to unlock should be granted.

2.7 System Architecture Specification

The system architecture of the Bluetooth Connection consists of different parts which are shown in figure 2. The microcontroller is connected to the decoder, memory, buzzer, LCD Display, Relay and Motor Driver. The Bluetooth receiver is attached to the motor driver.

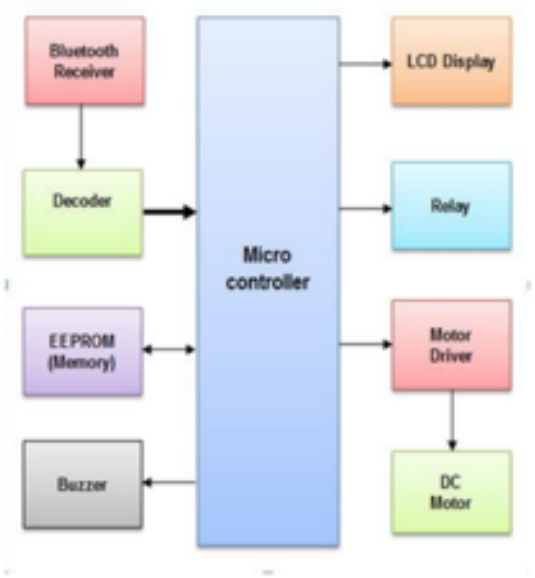


Figure 2 System architecture design for smart lock

2.8 House of Quality Analysis

The house of quality for the smart lock system is best described by the data in table 1. To ensure the highest possible quality, our product must achieve a balance between our engineering requirements and marketing requirements. The following house of quality diagram allows us to allocate a level of importance and devise a strategy on how to achieve our requirements.

To begin, we list the marketing and engineering design requirements as specified earlier in our project. Then, we align each of the categories with one another and compare how each of the requirements effects the other. In this house of quality analysis, we want to see how our engineering design requirements will affect our marketing requirements. When we assess how the weight of our smart lock system will impact our marketing requirements, we list either an up or down arrow, positive and negative polarity respectively, for how it will affect the durability, low cost, ease of install, power consumption, ease of customizing and ease of use. We see that by having a sturdy yet light weight design we increase durability and ease of install as it will not require special hardware to mount. Because we want a high-quality durable design, the cost will increase slightly and so it negatively effects the low-cost aspect to our design. The rest of the marketing requirements are unaffected by this design requirement. In a similar way, we assess the impacts the dimensions of our project. We would like our smart lock to be easily visible for our users and so we have decided on a 4”x4”x1” enclosure. This design will lower cost by not requiring a lot of materials to build and will be easy to install as it will not require additional help to mount on a wall. However, it will negatively impact our ability to customize our design in the future as little room will be available to add on more components. Next, we look at the power input. Our microcontroller requires 5 volts of power, so we will be stepping down the input voltage received from the power source to supply this amount of voltage. By using the homes’ power source, it lowers the cost by not having to replace batteries repeatedly. Because our project will be designed to consume the least amount of power possible, we will ensure power consumption is as least as possible. Setup time for our device affects our ease of install as this product will take nearly 2 hours to install due to running wires and installing the device on the wall. Also, users will need to take time to setup their lock codes and program their face with the facial recognition component. Fortunately, once the product is installed, users will save a lot of time when unlocking their home. Lastly, we see how cost will affect each of our marketing requirements. By providing durability we drive the cost up because we must use more expensive materials that last longer. In addition, to simplify the user experience, a lot of time must go into programming the features to ensure ease of use which drives the cost up as well. This chart helps us determine which requirements are most important while ensuring that we consider all aspects of our requirements when deciding which capabilities, we want to implement on our design.

Table 1 Engineering Design Requirements

			Engineering Design Requirements				
			Weight	Dimensions	Power Input	Setup Time	Cost
			-	-	-	-	-
Marketing Requirements	Durability	+	↑				↓
	Low Cost	+	↓	↑	↑		
	Ease of Install	+	↑	↑	↑	↓	
	Power Consumption	+			↑		↑
	Ease of Customizing	+		↓		↓	↓
	Ease of Use	+		↑	↑	↓	↓

	Targets for Engineering Requirements		< 1 lbs	4 in x4 in x 1 in	5V	< 2 hrs	< $600

Legend

- \+ Positive Polarity
- \- Negative Polarity
- ↑ Positive Polarity
- ↓ Negative Polarity

2.9 Block Diagram

The block diagram describes the architecture of our smart lock. We list all of the components and show where they connect to. Our controller will manage all connections by processing data and providing power. Once all of the features were identified, we assign each of the components to an engineer on the team. Our goal was to split the work evenly amongst all members of the team so that everyone is able to complete their tasks by the deadline. When determining who is assigned what, we asked each of the group members for their preferences and strengths. After discussing our options, we came up with the project assignments for each of the group members. Ali Al-Hajri will be responsible for the LCD Touchscreen, and RFID sensor. He will ensure that both of these capabilities have been tested and will design the layout of the touchscreen so that we are able to implement it as a passcode entry system. Idoko Abuh will be working on the finger print sensor and the LED indicator. He will ensure that these have been tested and are in working order. Noor Pirzada will be working on the Bluetooth and Facial recognition camera. Noor will also help as our team's main software developer as she will use her software programming skills to assist with debugging and coding to ensure that all features work seamlessly together. In addition, she will be working on developing a mobile application that works with Bluetooth to allow for mobile unlocking. Lastly, Mark Rodriguez will be working on power distribution for the smart lock. He will ensure that all components receive power. He will also work with the rest of the team to develop a low power mode to conserve energy. At this phase in our project, we are all currently researching the technology behind each of our assigned tasks in order to determine the best options for our smart lock. As can be seen in our block diagram, some of the components have been determined and purchased for our project. For these items, we have begun to test them using an Arduino UNO board which has the same microcontroller we intend to use.

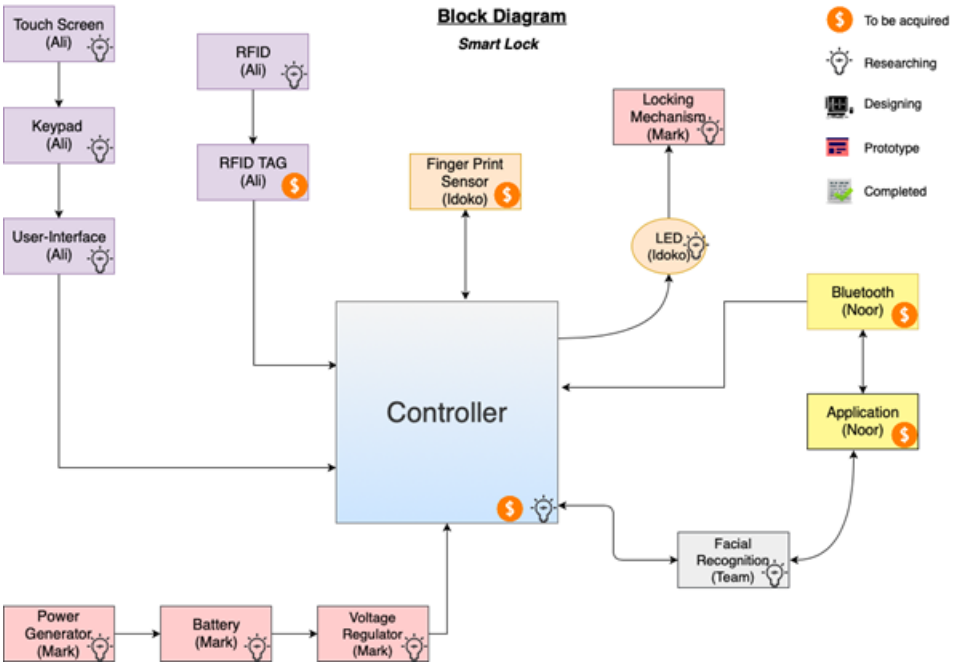


Figure 3 Block Diagram for smart lock

2.10 Electrical Engineering Design Flowchart

Our smart lock is composed of many electrical components. In the flowchart shown in figure 4, we discuss the electrical layout of our project. We begin by showing our input power source which is from a standard wall plug supplying 120 Volts AC. Because we do not need this much voltage, we will need to drop the voltage so that we will not damage the electrical components. For this we will use a voltage drop circuit to convert the 120 V input voltage to 5 volts. This will be a sufficient amount of power for our low powered microcontroller and components. Next, we use a relay switch to protect our components from damage due to power surges, noise, or inductive kickbacks which cause arcing. The relay acts as a safety measure to prevent any damage to the electrical components or end users. In the event of a power failure which triggers a damaging effect to the smart lock, the relay switch becomes damaged but protects the rest of the components. Should this happen, the user would only need to replace the relay switch in order to have the system back in working order. The microcontroller will be responsible for receiving and processing all of the sensory data to verify authentication. To show that the smart lock is working, we will have an LED indicator which will switch colors between red and green. This will show the user that the system is on and operating. In addition, the LCD panel will be lit at all times so that the user is able to see the digits on the screen. To control the smart lock using the mobile application, we will use a Bluetooth module to connect to the microcontroller. Using the mobile app, the user will be able to send a command to unlock the door. When the command is sent via the Bluetooth signal, the microcontroller will receive the command and unlock the door at the users' request. When the microcontroller authenticates the users input via any of the provided door unlocking methods, the microcontroller will send a signal to the LED Indicator to switch from red, to green color to indicate that the door has

been unlocked. Also, the microcontroller will send a signal to the magnetic door lock to release so that the door can be opened.

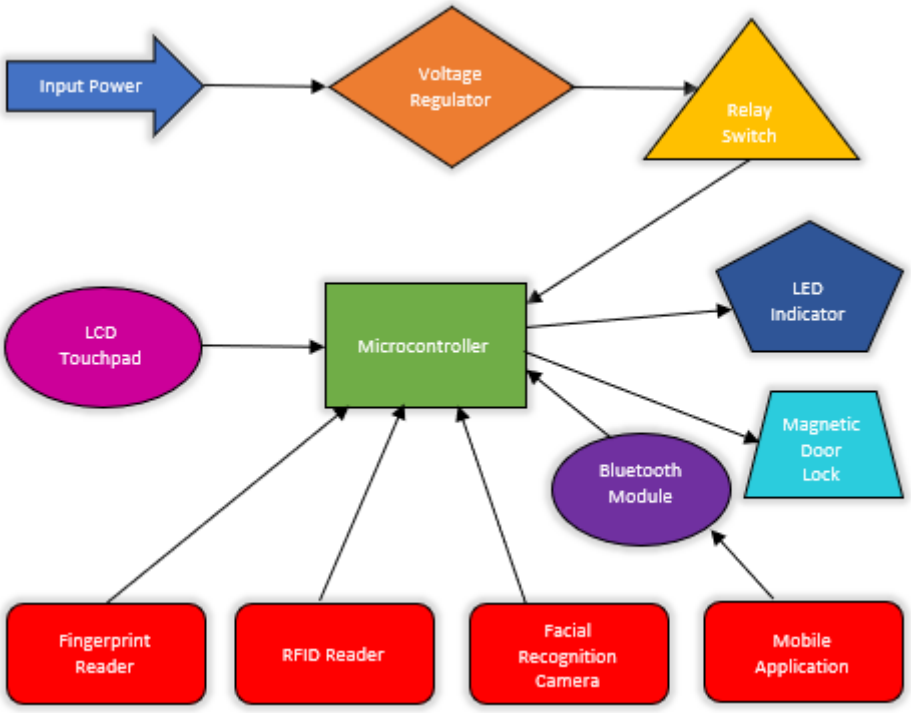


Figure 4 Electrical engineering flow chart

2.11 Decision Matrix

The decision matrix lists the features we provide in our project and then we rate how well we compare to other similar cost, ease of use, durability, convenience, support, power usage, and installation time. We will analyze each of these independently and then gauge a score for each of the categories and compare it to a few options currently available on the market. The models we decided to compare our smart lock to are the closest in design to what we are offering in our product. This goes to say that there are not many options with the exact features we intend to implement in our project. The only two that were by far the closest in design to our model come from a company called ZKTECO which is not widely known but has some state-of-the-art smart lock options. We also include a model from August Smartlock as they are one of the leading makers of smart lock technology and are widely known in the market for having some of the best smart lock products. We also wanted to include an economy option which had a good amount of capabilities but was at a relatively lower cost in comparison to the other smart lock options. Ultraloq's UL3 is a very good-looking option with its brushed aluminum body and easy to read digit display.

A decision matrix is useful because it allows us to determine which decision factors will give our product a leading edge over its competitors. We can then use this advantage as part of our product marketing scheme to further emphasize the components that not only set us apart, but also make us the better option all around. The way that a decision matrix works is that each category is assigned a max value depending on its level of importance. For us cost, ease of use durability,

convenience and support have the highest degree of importance for our design and so we assign a three, or extremely important, to each of these categories. For power usage and installation time we set to two, or very important, as these are also important characteristics that can set apart a smart lock from all others.

After determining the factors of decision, we analyze each product and assign a value for all of the categories judging each option based on how it compares to the rest of the available smart lock options. Once we have analyzed all of the products, we tally up the results and determine which of the products is best all around. This tool is also great because we can visually show our customers the comparison of similar products to further illustrate how our model is the best option.

Table 2 Decision Matrix

Decision Matrix

Attribute	Level of Importance	Student Smart Lock	August Smartlock Pro	Ultraloq UL3	ZKTECO ZM100	ZKTECO FL1000
Cost	Extremely Important (3	0	1	1	0	1
Ease of Use	Extremely Important (3	1	1	-1	-1	-1
Durability	Extremely Important (3	0	0	0	0	0
Convenience	Extremely Important (3	1	-1	0	1	1
Support	Extremely Important (3	1	1	0	-1	-1
Power Usage	Very Important (2)	1	-1	1	0	0
Install Time	Very Important (2)	-1	1	1	-1	-1
	Total:	9	6	4	-5	-2

Notes:

The options available for each of the categories Is 0 (average), 1 (better than average), and -1 (worse than average).

From the results of the decision matrix, we see that the student designed smart lock is by far the best option when compared to existing models. What sets us apart is that our model is easy to use and offers a great variety of options for unlocking which increases the level of convenience. Another characteristic that sets us apart is the fact that our product will have the best customer support available such as that given by the products of August. The reason why we find customer support so important is that we understand that not all our customers are tech savvy and we understand the frustration that can be caused when trying to setup a new technology in one's home. By having exceptional customer service, we will ensure our customers are familiarized with their new product and are able to safely install it in their homes without any frustrations or worries. One characteristic of our product that we identified as being inferior to other models is the fact that our model will take a significant amount of time to setup. The reason for this is that drilling, and wiring will be necessary to install the unit in one's home. While it won't be necessary to have an electrician or home repair person to install the unit, basic tools will be needed to ensure proper installation. A how to guide will provided with our product to illustrate the process for installing the unit in one's home. We realize that while the time it takes to install our product is much greater in comparison to other models, we feel

that the time spent will be a good investment. The reason for this is that once the unit is installed a great level of convenience will be at the customers disposal. This level of convenience would not be available by models that would require less amount of time to install such as the August smart lock pro and Ultraloq UL3. When comparing our model to the models from ZKTECO which have the facial recognition feature, installation time is comparable for these models. The reason why installation takes longer is because facial recognition requires a frontal view of the users face and so the unit needs to be installed at either an angle, or at eye level so that the camera used for facial recognition has a clear view of the person trying to unlock the door.

After summing the results from the decision matrix, we saw how our unit will be far superior to its competitors. Combining the ease of use, relatively fair cost, and increase in convenience and support makes our unit a user-friendly option for those seeking to make their homes *smarter.* We feel that while the installation time is greater than some of the models currently available, the newly integrated features out way this pitfall as the amount of time saved once the unit is installed will compensate the users for many years to come.

2.12 Project Measurables

The purpose of our project is to create a state-of-the-art smart lock system to improve the lives of people by making the way they access their homes easier and more convenient. Combing RFID, Touchscreen LCD, Fingerprint sensor, magnetic lock, and facial recognition our lock will be a fun new way of entering our homes. Our smart lock will provide the following project measurable specifications to our customers:

A. Cost

   a. We understand that many consumers want to innovate their homes by implementing smart technology into their homes to automate the mundane tasks. While home automation has included temperature control, ambient lighting, a push for automated door locks has recently hit the market. To alleviate the costs of a smart lock will providing the latest technologies we plan on purchasing all of the sensory components in bulk and develop our own components and software were possible. Our projected price for our smart lock is $600 dollars. At this price range, you will find most high-end smart lock systems although the available units have poor support and lack ease of use.

   b. Our smart lock will be made in the USA which will bring a cost savings in not having to increase our sales price in the form of a tariff tax. Our closest competitor ZKTeco manufactures their products in china which means that their prices may soon go up in cost while ours will remain the same.

B. Ease of Use

a. The purpose of automating one's home is to do away with a mundane task. In this case, that task involves having to fidget with your keys to find the correct one to unlock your home. With our smart lock system, we will simplify this process by removing the need for a key and replacing it with various options for unlocking the home. This system also fixes the need for a locksmith as it will not be necessary to call for help when one has locked themselves out.

b. All of the features we will implement on our system will be easy to use and self-explanatory. The LCD screen will have a clear digit display where one can key in their access code to unlock. Similarly, the fingerprint and RFID reader will offer an ease of access to a person's home. To make our customer's lives even easier, the facial recognition feature will allow the user to unlock their home by simply looking at the facial recognition camera to unlock. This will make the process of opening their home much more efficient.

C. Durability

a. We will be using high quality materials to construct the enclosure. This will provide the user a long-lasting product that will survive harsh weather conditions and usage. We have decided on building the housing out of high-quality plastic as it does not heat up as much as stainless steel. As we are in very warm climates, we would prefer a surface that will not cause harm to the users.

b. We will also use components that have been tested and tried to ensure that they will be able to withstand common use so that they will not fail in a short lifetime. In the event that one of the components fails, we will offer our customers a warranty of replacement for any damaged units.

D. Convenience

a. The main reason for someone wanting to buy a smart lock is to improve the convenience of unlocking one's home. Our smart lock will be the ultimate in convenience as it will have many features available for our customers. For this reason, convenience has the tallest order of must haves for our project as we hope to improve the lives of our customers by increasing the conveniences available to them by purchasing our smart lock.

b. Our success in this project will be measured based on the level of convenience that is achieved by switching a standard smart lock with our new smart lock system.

E. Support

a. As mentioned under convenience, our major goal is to improve the lives of our customers by simplifying their lives further. Sometimes technical issues happen, and in those cases, we plan to have customer support available for our customers so that they can receive assistance with setting up their smart lock.

b. Also, we plan on having documentation for dealing with common problems as well as steps for installation and setup.

F. Power Usage

a. Power usage must be kept to a minimum. To achieve this we will write software that controls all modules of the smart lock and turns them on low power mode whenever they are not in use.

b. We take consideration of power usage because we want to conserve electricity as much as possible as it is unnecessary and wasteful to do the contrary.

G. Installation Time

a. Our product will take approximately 1-2 hours to install. To listen the burden of installation, we will be providing a how to guide which will give instructions on how to properly install the smart lock.

b. Our goal will be to try to package the smart lock in a way were everything needed is included minus the tools. This way the customer will not need to invent parts for the smart lock to work for their housing application.

3 Research and Investigation

Extensive research is done for the development of the Smart Lock. With one other senior design team also building an electric lock system, Group 6 must implement

features that make the Smart Lock stand out, so much time is spent researching features from similar products in the market and the technologies relevant to successfully creating a working prototype.

3.1 Existing Similar Projects and Products in the Market

The FL1000 from ZKTECO, is a smart lock with embedded face recognition technology. The entire unit is built into the door handle and features a 3-inch capacitive touch screen display. It features 4 independent unlocking protocols; face, password, card, mechanical key. There is a built-in smart alarm system that will notify the user when the battery becomes low or when an illegal operation occurs. The standard European mortise lock features an automated deadbolt as the locking mechanism. The FL1000 can recognize up to 100 faces, store 100 passwords, 100 RFID cards, and has a log capacity of 30000. Communication with this device is done via USB flash disk. Power is supplied to the unit from the building but there are additional external terminals that draw back-up power from a 9 volt battery source.

ZKTECO also produces the ZM100 which is a robust smart lock with embedded face recognition technology. The ZM uses AK Face Algorithm version 7.0 with verifications speeds less than one second. The SilkID fingerprint sensor uses a PIV certificate and is capable of live fingerprint detection whether dry, wet, or rough. This lock sports a lithium ion battery back that can last for a year on a full charge. Data is uploaded and downloaded to and from the unit via USB and a smart alarm system is also used to warn of low battery or illegal operation. The ZM100 supports English, Spanish, and Portuguese. It also utilizes a Mifare Card which implements an advanced encryption technology for additional security.

Nuki is a smart lock security system that implements measures designed to simplify ones experience when interacting with the device. As the user approaches the door, the smartphone is detected and Nuki automatically unlocks the door. Nuki then automatically locks the door when the user leaves. Nuki has a simple design that mounts on the inside of an existing door lock and actuates the deadbolt. Nuki is accessed from an app on the smartphone. The app can allocate access to chosen individuals like friends and loved ones and temporary access can be given to chosen individuals for work orders. Up to 200 access permissions can be allocated with the Nuki app. The Nuki app can keep track of who locked your door, when they locked your door and whether the door is securely locked. The app integrates with apple home kit, Amazon Alexa, and Google Home.

The Ultraloq UL3 BT smart lever lock is an intuitive smart lock that allows its users to use fingerprint, code, key or smartphone to unlock the door. The UL3 BT uses Bluetooth 4.0 Low Energy Connectivity to unlock the door using the smartphone Ultraloq app. It is capable of storing up to 95 fingerprints and can identify a fingerprint in less than .5 second. The UL3 detects fingerprints seamlessly regardless of the age of the user. The UL3 BT has an anti-peep touchscreen that serves to protect the user's password when entering it onto the keypad. If the user is near the door and the IOS smartphone is in their pocket, the user can simply knock on the smartphone four times to unlock the door. For Android users, a simple

shaking of the smartphone after waking up the smartphone screen will unlock the door. The Ultraloq app keeps a log record so that the user can see who has entered and exactly when. The power is supplied by 3 AA batteries that last up to a year.

The August Smart Lock Pro is a Bluetooth enabled smart lock that provides two-factor authentication to enable its users to lock and unlock their doors from anywhere, grant access for friends and family, and tack who is coming and going from the August App. The auto unlock feature allows August to automatically lock and unlock the door when it detects the smartphone in close proximity. August is works with Siri, Amazon Alexa, and the Google Assistant. August Smart Locks also integrate directly with the HomeAway and Airbnb hosting platform and completely automates the check-in and check-out process. The August Smart Lock Pro easily attaches to the user's existing deadbolt and installs in minutes, giving users an upgraded keyless entry experience. When a phone is lost, Access to August can easily be disabled on the August app at any time so a lost phone doesn't compromise security. The August Smart Lock Pro is powered by 4 AA batteries. A warning on the website states that "This product can expose you to chemicals including Ethylbenzene, Acrylonitrile, Carbon Black Formaldehyde and Cumene, which are known to the State of California to cause cancer", so that would be a cause for concern while installing and handling the product.

3.2 Relevant Technologies

The relevant technologies needed to execute the Smart Lock's functionality is introduced in this section. Technology necessary for sensing, actuating, storing data, and performing calculations are researched and discussed in later chapters.

For code implementation, there are several languages that can be used. Assembly is a low-level programming language that converts instructions into machine code via an assembler. Assembly language is fast, but the code can be cumbersome since all code needed to run the program is written in the main program and no headers are used. This is an efficient language for a seasoned programmer with organized code but can quickly be overwhelming for a programmer that is just beginning. C is a higher-level programming language than Assembly and provides the programmer with a syntax that is closer to human language and logic. C programming language allows for the use of libraries and header files which helps to organize the programmers code. Single board computers with operating systems can use high level languages like Python and C++. These high-level languages have the advantage of implementing object-oriented programming which is useful when working with objects and their attributes.

For the biometric features of the Smart Lock, facial recognition and fingerprint sensing technology will be implemented. Computer vision is a cutting-edge field that gives computers the ability to understand the contents in an image. With facial recognition, machine learning algorithms are able to take a digital image of a face and, using features on the face, create a complex signature. This signature is then compared to the signatures in the computer database to see if there is another

signature with a high percentage of matching features. These algorithms need large amounts of data sets and image processing power.

Fingerprint authentication technology can be conducted in a number of ways. Optical scanners use LEDs and a camera to capture high contrast images of the fingerprint and use feature matching algorithms to enroll and verify it. Because of the LED's, optical scanners are bulky and do not provide a high level of security since they only record a 2-dimensional image and a high quality image of a fingerprint could actually fool the sensor into verifying an entry. Capacitive scanners use an array of capacitors to collect the fingerprint data as an array of electric charge. This type of fingerprint sensor cannot be fooled by a high quality 2-dimensional image because it senses data in 3-dimensions so it provides a higher level of security. It also allows for a thin design. Ultrasonic fingerprint sensors work by using an ultrasonic transceiver to transmit an ultrasonic pulse, then listen and map out the 3-dimensional information from the echo that is returned from the finger. This method also allows for a thin design and high level of security

Radio Frequency Identification allows for any object to be scanned via radio frequency. RFID systems consist of a reader, antenna, and a tag. The reader uses the radio frequency antenna to transmit a signal. In a passive RFID tag, the signal from the antenna powers the tags in proximity which sends a signal back to the reader. Passive RFID tags are small and thin and can be used to identify small assets like consumer goods. They can also be implemented into an ID card which is great for quickly identifying people. In an active RFID tag, the tag has a built in power source and can also transmit environmental information like light intensity, humidity and temperature back to the reader. Active tags are more expensive and better for large assets like vehicles.

Bluetooth technology is relevant to the Smart Lock because it would give the ability to interact with a smart phone application so that when a user is within a certain proximity to the Smart Lock, the system can intuitively grant the user access. Bluetooth can also allow multiple Smart Lock systems to communicate with each other which can be very useful in the enrolling process because the database for one lock can update all the other locks within the system. This would mean that a user can be enrolled on any Smart Lock device and automatically update the rest of the devices.

WIFI technology can greatly increase the functionality and ability to update the Smart Lock system because WIFI will extend the Smart Locks connectivity to local and online networks. This brings it into the realm of the Internet Of Things, integrating the Smart Lock into a system of interlinked smart devices. WIFI technology will also give the ability to enroll and update user information via a software or webpage. This allows for enrolling large databases to the system quickly without having to enroll each user in series. This also helps in the event that a system reset is needed. The databases of each Smart Lock can be erased then loaded with the updated list of user data. WIFI technology can also give the user more versatility by allowing them to give and revoke access to the Smart Lock system from any location by accessing

it online. This will free the user from having to be at a certain location in order to give or revoke access.

The Smart System will need the ability to store a data for 100 users, therefor non-volatile data storage will be needed. The use of an SD card reader/writer will enable the system to read and write data from the card memory. This data will be accessed through an application. SD cards can communicate through SD and SPI protocol. The Smart Lock system will communicate with the SD card using the SPI protocol.

3D Printing technology gives the ability to print 2 dimensional layers on top of each other to create a 3 dimensional object. This technology can create objects beyond the capability of other fabrication methods. It allows for very low startup costs and a lot of customizability. Printing resolutions vary from +-.5mm to +-.01mm depending on the method used. This is excellent for the prototyping process. 3D printing technology is one of the methods that is considered for the manufacturing of the hardware enclosure.

Laser Cutting is another method that is considered for the manufacturing of the hardware enclosure of the Smart Lock System. With Laser cutting, materials like stainless steel, aluminum and titanium can be cut to a high precision, leaving the product with a quality finish. A metallic finish will better ensure that the device is secure and will not be breached and tampered with. Laser cutting machines are also capable of cutting up to 6.4 mm of plywood. The advantages of working with metal are the added security and high quality output. The disadvantage is that the material cost exceeds that of 3D printing.

3.2.1 Computational Device

When it comes to the computational aspect of the Smart Lock, different approaches can be taken. Implementing the code needed to operate the hardware can be done with a Micro Controller Unit, Field Programming Gate Arrays, or using a single board computer. Comparing these methods with the requirements of the Smart Lock functionality provides an aid in the selection of the optimal architecture for hardware computation.

3.2.2 FPGA

Field Programmable Gate Arrays are semiconductor devices with a matrix of logic blocks that can be configured. These logic blocks are connected with programmable interconnects so after fabrication, they can be programmed to the necessary application.

One of the major advantages of FPGA is its hardware structure is not fixed but is defined by the user with HDL code. This allows the FPGA to perform calculations in parallel which serves an appropriate solution for processing large amounts of data quickly, so applications such as video and image processing can be executed using

FPGA's. Another advantage with having a hardware structure that is not fixed is that the hardware structure can evolve with the application. The hardware Updates can be made to t2edxhe hardware structure or entirely new functions can be added, modified, or removed from the system without the need to upgrade hardware.

Some drawbacks presented with FPGA are they generally have higher cost and power consumption than sequential processors. Verilog Language is also more complicated that c-programming and knowledge of digital systems required for programming hardware schematics.

3.2.3 Micro-controller Unit

Micro-Controller Units or MCUs are computers embedded on a single integrated circuit. The architecture consists of a CPU, program memory, data memory, a clock and, general purpose input and output ports

An advantage of using a MCU is the size and cost of the processor chips are very small and easy to integrate into larger systems. They serve as a cost effective solution for implementing a simple task or tasks repetitively with low amounts of power. The MCU architectures allows for programming in low level language with assembly and C and in higher level languages like JavaScript. This gives the programmer the option to code closer to the machine or software. The main drawback is that micro-controller units' process information sequentially, making them slower than systems that process information in parallel, a big disadvantage if speed is imperative for the desired application.

3.2.4 Single Board Computers

Single board computers are complete computer systems built on a single circuit board. A single board computer consists of microprocessors, memory, general purpose input/outputs, and more. A single board computer is capable of implementing code to operate the hardware devices of the Smart Lock. Single board computers can support a range of operating systems like Embedded LINUX/Windows, Desktop LINUX/Windows, RTOS, UNIX, Sun Solaris and more. Programmers can also program their embedded application in C and use the single board computer without an operating system.

The advantage of using a single board computer is that a number devices are built into the system such. The raspberry pi comes with Bluetooth, WIFI, HDMI, Ethernet, and an audio adapter. This makes interfacing with an external monitor, Bluetooth/WIFI device, and connecting to the internet a breeze. The communication protocols such as USART, I^2C, and SPI, can be accessed using the intuitive Linux based operating system. This provides a simple interface for navigating, organizing, and executing programs. The Raspberry Pi can implement code using python language which is intuitive due to its extensive support libraries and open source community. Python allows the programmer to code in fewer steps as compared to C. The Raspberry Pi can be controlled remotely via the terminal window. This helps

when the Raspberry Pi is integrated into a design that may not allow for it to be connected to an external monitor or keyboard and mouse.

Another popular single board computer, Beaglebone also has a variety of on board features. It allows for USB connectivity and also has an on board barometer, accelerometer, gyroscope, and temperature sensor. These features give the single board computer complex capabilities right out of the package without the need for external components.

When speed is an important factor in the application, the single board computer is at a disadvantage. The simplicity provided by using high level language also translate to a slower execution of commands. The time it takes to boot up the operating system is considerably long so in the event of a momentary power failure, single board computers would need a few seconds to reboot. This also is a disadvantage for systems that cannot afford a temporary failure.

3.3 Computational Device Selection

After comparing the different approaches for fulfilling the computational requirements of the Smart Lock, the method of using a Microcontroller Computing Unit is selected as the appropriate solution for controlling the hardware. The decision to use a microcontroller is mainly due to the low cost of micro-controllers that meet the requirements. In addition to the micro controller unit, a Field Programmable Gate Array will also be used for image and video processing and to implement the algorithms for facial recognition. The parallel processing capabilities of FPGA make it the ideal choice for processing video data from a camera and implementing almost real time facial recognition.

3.3.1 Microcontroller Research

Another layer of research is done to determine which MCU should be selected for execution. The MCUs in consideration are MSP430F149IPM, Atmega2560, STM32F407VGT6, and PIC32MX250F128D.

3.3.1.1 Texas Instruments MSP430F149IPM

The MSP430F149 is a low powered MCU from Texas Instruments with an 8 MHz clock speed. It features SPI communication and one USART. The chip is programmed using Code Composer. Online support for Code Composer and the msp430 outside of TI is minimal. Programming this chip is done by connecting through USB to an onboard emulator circuit or by using the MSP430 Flash Emulation Tool which cost $115. This is a high cost considering the budget to get the chip up and running. The MSP430F149 also lacks multiple UARTs and the procedure of implementing software UART on other pins will complicate the code.

3.3.1.2 STMicroelectronics STM32F407VGT6

The STM32F407VGT6 is a high performance 32 bit MCU with an ARM Cortex RISC core. It operates at 160 MHz and features 1 Mb of flash memory. The STM32f407VGT6 also features lots of connectivity options like 2 CAN bus, 3 I^2C interfaces, 4 USARTs/2 UARTs, 3 SPIs, an SDIO and a USB interface. It can also support an 8-14-bit parallel camera interface which is very useful for image and video processing. Code can be written in any word processor then uploaded to the chip from the STM32 ST-LINK Utility software using a SWD or J-tag interface.

3.3.1.3 Microchip PIC32MX250F128D

The PIC32MX250F128D is also a low powered MCU that boast a 32-bit data but width and has a 40 MHz clock speed. It has a Parallel Master Port which is great for an LCD connection and external memory devices. It also features an audio interface and USB support. This is ideal for any sound implementation. The PIC32 is capable of 4 methods of device programming including In-Circuit Serial Programming, Enhanced In-Circuit Serial Programming, EJTAG programming, and Enhanced EJTAG programming. Debugging is done with ICSP and EJTAG Debugging. The PIC32MX250F128D only features 2 USARTs but it also has 2 SPI interfaces and 2 I^2C interfaces.

3.3.1.4 ATMEL ATMEGA2560AU

The Atmega2560 from Microchip is a low powered RISC- based MCU with a 16 MHz clock speed. It has an 8-bit data bus width, 256 KB of flash memory, and 4 USARTs. The Atmega2560 can also communicate over Two-Wire and SPI. With 86 general purpose IO pins, the Atmega2560 can seamlessly interface many modules. Code can be written and compiled in Atmel Studio and there is plenty of online support. It can be programmed using an AVR Dragon programmer which cost $60.

3.3.2 Microcontroller Comparisons

Table 3 Microcontroller Comparison Chart

	Micro-Controller Unit			
Features	MSP430F149IPM	Atmega25608AU	STM32F407VGT6	PIC32MX250F128D
MCU Price	$ 10.96	$ 12.20	$ 12.74	$ 4.09
Debugger Price	$ 115.00	$ 60.00	$ 10.00	$ 10.00
Clock Speed	8 MHz	16 MHz	160 MHz	40 MHz
Data Bus Width	16 bit	8 bit	32 bit	32 bit
Memory size	60 kB	256 kB	1024 kB	128 kB
IO pins	48	86	82	33
Interface	SPI,UART	2-Wire, SPI, 4USART	2 CAN, 3 I^2C, I^2S, 3 SPI, SDIO 4 USART, USB	I^2C, I^2S, IrDA, LINbus, PMP, SPI, USART, USB

Operating Voltage	1.8-3.6 V	4.5-5.5 V	1.8-3.6 V	2.3-3.6 V

3.3.3 Microcontroller Selection

The Smart Lock requires a few features from the MCU in order to operate. First, the MCU must have a data bus width that is at least 8-bit, this is to be able to efficiently pass a byte long instruction to a module. The MCU must have at least 3 UART ports to accommodate the facial recognition camera module, the fingerprint scanner module, and the Bluetooth connectivity module which must each connect via USART. The MCU must also be able to communicate over SPI and I^2C for the SD card reader/writer, RFID scanner, and LCD controller module. Finally, the MCU chip and debugger cost must be below $100.

After careful consideration to the MCU needs for Smart Lock functionality, the Atmega2560 is selected. This is because the Atmega2560 has the connectivity to accommodate all the modules, there is plenty of online support, and the price falls within the budget for the project.

3.4 Environment Measurement Metrics

When designing our project, great thought must be placed on the effects it will have on the environment. We must consider all impacts in order to try to minimize the effects we place in our surroundings. Some of the impacts may be radiation exposure from the sensors, integrity of the biometric data captured during usage which includes proper storage of such information, and electronic disposal hazards. In all cases we must ensure that proper research is done to try to lessen the effects we place on the environment. One way we have placed consideration in this aspect, is by deploying the use of low power modes when the unit is not in use. This will ensure that we utilize the least amount of electricity and therefore lessoning the burden on the environment.

Other ways we can consider the effects of the environment in our project is by giving disposal instructions within the user manual for our product so that our customers are informed on how to properly dispose of all electronics should they decide to remove the unit from the home. This is important because a great deal of natural resources are used to develop electronic components, and these should never be disposed of in the landfill as they can be recycled and reused for other purposes.

3.5 Sensors

Sensors are devices that detects, collects, or measures data. A sensor often detects a predetermined condition which triggers it to collect information regarding its environment. The sensor then sends this information to a data repository where it can be collected and examined. There are various types of sensors available and have multiple forms of applications in which they can be used. In the preceding sections, we will discuss the sensors we will be using in our project in greater detail.

3.5.1 RFID Sensor

The radio-frequency identification sensor (RFID) uses electromagnetic fields to detect a signal from a preprogrammed chip. This chip is often embedded in either a card or dongle and is to be held by the user who wishes to gain access. On the other hand, the RFID reader is usually mounted onto a device where the user is to swipe or wave the RFID chip to engage a connection. The chip contains tracking information which the reader detects and then uses it to grant the user access. There are two types of tags in RFID. They are the passive and active tags. The passive tag gains energy from the RFID reader via radio waves. The active tag contains a power source such as a battery. The benefits of having an active tag is that the RFID reader is capable of reading the active tag from much further away in comparison to the passive tag. The benefits of a passive tag is that you will never have to replace batteries and therefore will always work granted, the tag is in close proximity to the reader. RFID is far superior in comparison to barcode systems because it is capable of storing much more information. Also, the RFID tag does not need to be scanned in a particular way such as with a bar code.

RFID uses low frequency, high frequency, and ultra-high frequency to communicate with the tag. When determining which band to use, you must take into consideration the distance at which you will need the reader and tag to be in order to operate. When using low frequency, the read rate when communicating will be much slower in comparison to the other two options. This may be a problem because the tag will need to remain within the acceptable distance to the reader while the data transfer is taking place. The benefits of using low frequency is that interferences from metal, walls, and fluid surfaces will be very minimal. High frequency signals work in the opposite way. They are susceptible to interferences much more easily, but communication can travel at a much faster rate. In a similar way, ultra-high frequency bands allow for much faster data transmission rates but are also susceptible to interference from metals and other objects that may be in the way.

Low frequency band works within the frequency ranges of 30 KHz to 300 KHz. In order to communicate between the reader and tag, the distance between the two must be within 10 cm or just under 4 inches away. When considering if low frequency band is the correct option for your project, one must consider the short distance as this characteristic limit the ability of the feature. In most cases, low frequency is used for access control applications since people trying to access a door are typically standing very near the RFID reader and are able to scan their tag within the required distance.

High frequency band operates within the frequency ranges of 3 MHz to 30 MHz This band has a much faster transfer rate in comparison to low frequency and can transfer data between distances of up to one meter. High frequency band seems to be an appropriate option for quick transfers between two neighboring students who wish to transfer a file between themselves. This option is good for tags stored on cars to be used with readers that detect when a person with access is able to open a gate. Because the distance must be less than a meter, we must consider that while

the tag doesn't have to be very close to the reader, it still has to be relatively close to the reader and also must avoid any interferences caused by metals or barriers such as walls.

Ultra-high frequency band covers the frequency range of 300 MHz to 3 GHz. This band can transfer data at distance of up to 12 meters away. One downside to this, is that the transfer rate is much slower than the other two options which may cause impedances. It is also important that there are no obstructions in the way of the tag and reader as this too may cause delays in transfer. Usually, the tag is connected to an antenna in order to ensure that the reader has a clear signal to the tag.

Passive and active tags are what make communication via RFID possible. These two technologies are great because while passive is the most convenient, active gives users a way to expand their applications by allowing for greater distances of data transfer. While active tags user a power source to work, passive tags receive a small amount of energy wirelessly via interrogating radio waves. The passive tag system is limited by the amount of power it receives which usually permit it to transfer data no more than 10 meters away. Also, passive tags are much cheaper since an antenna and power source are not necessary.

Active tags are great options because they allow for applications that are hundreds of meters away from the RFID reader. This is possible because of an antenna that is connected to the RFID chip. When combining active tags with an ultra-high frequency system, the distances are greatly increased.

Table 4 RFID Comparison

Property	LF	HF	UHF
Tag Expense	High	High, Medium	Medium
Reader cost	Low	Medium	High, Medium
Working Range	~ 30 cm	~ 1 m	~ 30 m (active)
Data Transfer	Low	Medium	High
Interfaces	Low	Low	Medium
Advantages	Low environmental absobtion	Available worldwide	Good for medium range applications
Common Application	Animal ID tags, security, engine immobilizers	Security, item tracking, ticketing	Container, Truck tracking

3.5.2 Fingerprint Sensor

A fingerprint is created by the ridges on a person's finger when pressed against a surface. As we know, fingerprints are unique to each person, which is why they make

an excellent way of tracking people. In the past, fingerprints have been used to identify people in criminal offenses. Today, they can be used for far more than just that. Because fingerprints can be used to identify people, they make an excellent way to replace keys and wallets. With a single fingerprint scan, a person can be identified, and their virtual profile can be accessed which would grant a person access to a location or their personal belongings. This is the way of the future. Fingerprints will be replacing so many of the physical aspects of our life. This can be both good and band. The good is that we will no longer need to carry additional items to access our property. It is also much more secure because it is impossible to lose one's fingerprint, yet it is incredibly easy to lose physical property especially when they are small in size such as keys. The bad side of this technology is that if the biometric information falls in the wrong hands, people are liable to lose a lot of their personal belongings. Hackers who are able to acquire this information can easily wipe out a person's bank accounts and access their homes without anyone knowing about it. This means that if we hope to use this technology, great caution must be taken to ensure that any biometric data used is properly encrypted and secured to prevent it from falling in the wrong hands. We have decided to include a fingerprint reader to our smart lock as a way to gain access to one's home. Our goal is to ensure that our customers are able to take advantage of the huge convenience offered by the fingerprint scanner to simplify their lives. At the same time, we will ensure their data is protected by encrypting all biometric data obtained from our customers. This way, if the data happens to fall in the wrong hands, it will be very difficult for hackers to obtain the data without having the encryption key to access our customer's information. Through careful consideration, our team selected the GT11C1R fingerprint scanner. This scanner is low in cost while having a high esthetic quality. This scanner allows for a large storage capacity so that many users can store their biometric data to access their home.

3.5.3 Camera Sensor

One of our project's extended goals is to include facial recognition as a way to unlock a person's home. This technology has recently become increasingly popular in the area of home security systems. In the past cameras were used to secure a property by identifying unknown persons who have tried who access a building. Today, we can use it a way of obtaining biometric information and then using it to grant someone access to a building. This technology is great because a user does not have to have an RFID card or memorize a code to access their home. Instead, all they have to do is stare a camera and wait for the system to recognize them. This process happens very quickly allowing for a person to access their home quickly and efficiently. Like fingerprint technology, facial recognition modules are highly controversial because of the threat of someone's' privacy. Our camera is not intended to be connected to the internet which means that any observances detected by the camera will not be viewable by any outside sources. This way we prevent any attack towards someone's privacy while utilizing this great technology to simplify our customer's lives. In the current state of our project we are looking at different camera options although we hope to design our own facial recognition software by utilizing open sources libraries such as OpenCV while developing our machine learning program that will detect our customer's faces quickly and

efficiently. By designing our own in-house software, we will drive cost down by not having to subcontract work or pay an extra fee for premade facial recognition systems.

3.6 Weather Proofing and Enclosure Design

Our project contains many components that are sensitive to water. Because our smart lock is installed on the outside of the home, this means that our product will be exposed to the elements at all times. To protect the electrical equipment, we will be creating and 3D printing our component housing. We intend to use a slick plastic design as it absorbs heat well making it safe to touch even when the heat is extremely high such as it is here in Florida. Also, plastic is a great material because it does not corrode when it left outside. Our housing will have all mounting holes predrilled so that it is easy to install on the wall. In addition, we will be designing screw holes on our enclosure so that we can securely mount the PCB and electrical components in place. This will make our product look and feel much more professional as careful consideration was placed in the design. At the same time, this will ensure that minimal moisture will enter the inside of the enclosure. To further protect the components inside, a foam edging will be installed around the border of the encloser to seal the back of the enclose against the wall where it will be mounted on. Figure 5 shows a schematic of what we anticipate our enclosure to look like.

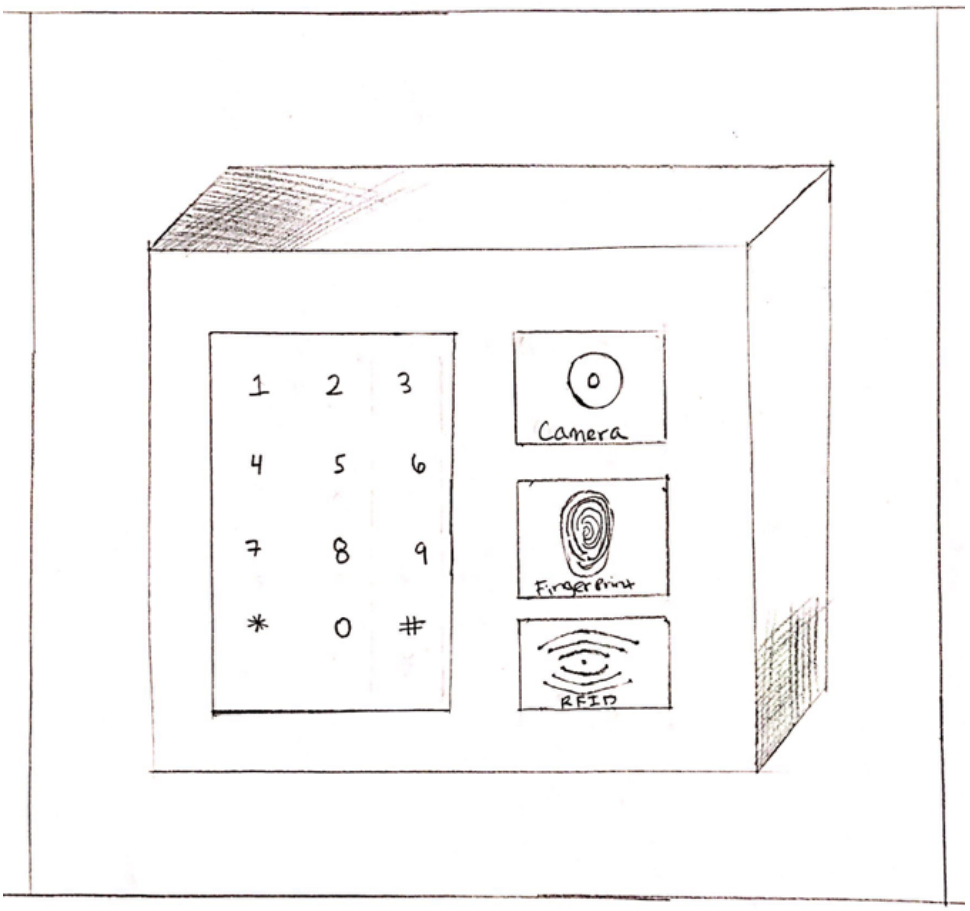


Figure 5 Weatherproofing encloser for smart lock

3.7 Part Decision

For each part required for the smart lock project, careful consideration was made when determining the best part for the design. The proceeding sections will detail the research completed for determining the part decision.

3.7.1 Microcontroller

After reviewing several options such as the MSP430F149IPM, Atmega25608AU, STM32F407VGT6, and PIC32MX250F128D we have concluded that the MCU that best suits our needs for the smart lock functionality is the Atmega2560. The Atmega2560 MCU is the best option for us because it will allow us to connect all of the modules we have in mind, has plenty of online support, and most importantly the price falls within the amount we plan to spend for our microcontroller unit.

3.7.2 Fingerprint sensor

For the optical fingerprint scanner we reviewed several different models including the FPM10A and GT11C1R. After careful consideration in the areas of price, storage capacity, scan time, and ease of use we have decided to select the GT11CIR fingerprint sensor. This sensor allows for simple upgrades to allow for a higher storage capacity and has a great amount of user support available online making it easy to implement and troubleshoot. This unit is priced lower than its competitor which will mean that we will be able to pass along greater savings to our customers.

3.7.3 Facial Recognition Camera

The facial recognition camera selected for the smart lock was decided after careful comparison of camera models that were inexpensive and that have been tested and used in the past for other similar projects found online. The models we considered were the Pixy2 and the ESP32-CAM. The ESP32-CAM is an inexpensive camera with onboard chip, which has an LED flash and is recommended for simple video streaming and security camera applications. The ESP32-CAM has an average cost of $7- $15 per unit. On the other hand, the Pixy2 camera is very versatile in that it has several interfaces (SPI, I2C, UART, and USB) making it easier to configure with the Arduino MCU. In fact, the Pixy2 comes with a USB cable that can be connected directly into the Arduino for easy install which will make testing and configuring the facial recognition software with the camera a lot more convenient as we will have plug-and-play compatibility. Also, the Pixy2 has its own predefined software library called pixy.ccc and it is compatible with both Arduino and Raspberry Pi. The Pixy2 has a price range of $60 - $80 per unit. Both cameras have decent amount of support available online and both have been used for facial recognition applications. The Pixy2 is a lot easier to code because of its own prebuilt library, which is most likely why it has the higher price range. Given that the ESP32-CAM is nearly 10x cheaper and is known to work for the purpose of facial recognition, the smart lock will utilize this camera for its facial recognition capability.

3.7.4 Bluetooth Module

When comparing the various Bluetooth modules available on the market we assessed the price differences, operational range, and compatibility. Two of the commonly used models are the ESP 8266 and ESP 32. The ESP 8266 has a channel width of 20 MHz while the ESP 32 has twice that at 40 MHz While a greater bandwidth may seem better, occasionally a very wide signal may cause packets to be lost during transmission. Also, ESP 32 is not compatible with many client radios that operate in the 2.4 GHz band which is quite unfortunate because this band is commonly used in most electronic applications. The ESP 32 is also more expensive with an average price range of $6 - $12 while the ESP 8266 costs a mere $3 - $6 per unit. After careful consideration, it has been decided that the smart lock will be outfitted with an ESP 8266 Bluetooth module.

3.7.5 RFID Sensor

There are two main types of RFID sensors. They are active RFID and passive RFID. Active RFID is mainly used for long-range applications because it uses a battery to give off a greater signal so that the RFID reader can communicate with the transponder. This version of RFID is great for vehicle tolls and community gate applications. For the smart lock, users will be in close proximity it it when trying to unlock their home and so passive RFID is a great choice for this type of application. There a lot of options for passive RFID transponders and so we have selected a commonly used model that is compatible with Arduino MCUs and is quite easy to work with. The model selected for the smart lock is an RC 522 RFID reader. This model is great because it is very affordable with a price range of $2 - $5 per unit and it includes 2 – 3 RFID cards per reader. This is great because the RFID cards can be given to several members of the home.

3.7.6 LCD Display

We have selected to use a TFT touchscreen display for our smart lock. This display will all the user to punch in their pass code to unlock their home. We decided to use this version of display because it offers good quality while using very little power. Also, there are easy to follow guides online that show us how to create a display with digits so that we can implement the passcode option for our smart lock. Due to its low cost, great quality, low power consumption, and ease of use, we decided that this model will be a perfect fit for our product.

3.8 Inter Integrated Circuit (I2C)

I2C also known as I2C is an acronym of Inter-Integrated Circuit. It is a serial communication protocol developed by the Philip Semiconductor. On one PCB, more than one chips can be integrated like in simple in simple integrated schematics. Communication between these chips is required in developing a system. Here, the

concept of inter Integrated circuit or I2C came into existence. It is developed with the intention of communication between these chips.

Generally, interfacing of ICs (having slow speed) to the processors or microcontroller is done. Master-slave protocol is used in Inter integrated circuits. Casually, Microcontroller or some other processor is treated as the master while other chips like Temperature sensors, EPROM, EEPROM, RTC are used as the slave device. No restriction is applied in using the number of master and slave. Usage of multiple master and multiple slaves is common in complex design. Hence, it is justified to declare that this protocol is a multi-master and multi-slave protocol.

It is usually used to interface slow speed ICs to processor or microcontroller. It is a master slave protocol, usually, a processor or microcontroller is the master and other chips like RTC, Temperature Sensor, EEPROM will be the slave. We can have multiple masters and multiple slaves in the same I2C bus. Hence it is a multi-master, multi-slave protocol (htt28).

A wired medium used for the bidirectional data transfer is known as a bus. In I2C the bidirectional bus helps to communicate between master and slave. A single line, called SDA line, is there to transfer the data bit by bit. Like many other communication protocols, synchronization is the foundation of the I2C protocol. A clock signal is shared between the master and slave for this purpose. Figure 1 (htt43)OBJ (htt29).

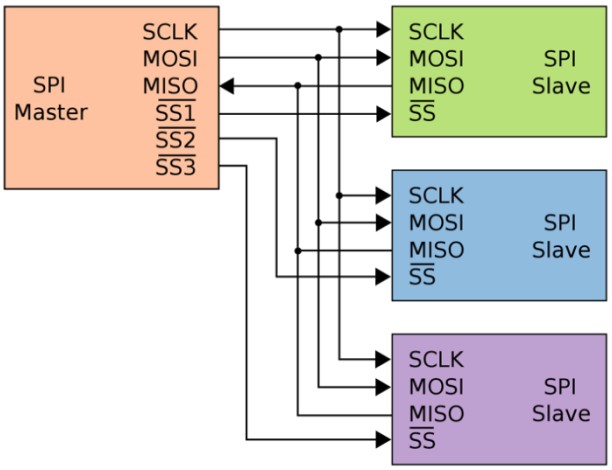


Figure 6 I2C communication protocol

3.8.1 Design

The following section explains the hardware implementation details of I2C. Explanation below depicts the versatility and reliability of serial communication in terms of I2C.

Each device on the I2C bus is supposed to be connected to both the SCL (the clock signal) and SDA (the acronym of data signal). The connection between them is

made via open-collector or open drain output drivers. To understand the topology, the inverting stage of the CMOS needs to be explained (htt30).

It is known that the PMOS will be turned on when the input is low and it will remain off when the input is high. While the behavior of NMOS is completely converse; it will remain off when the input is low and conducts when the high voltage is applied at the input. An inverter is designed using both NMOS and PMOS, combined together known as CMOS (Complementary Metal Oxide Semiconductor). The output is connected at the junction of both PMOS and NMOS. It can be seen that the CMOS converter will convert the low input to high output by turning the PMOS on and connecting the output to VDD. High input makes the output low by making the NMOS short and output connected to ground. Static power dissipation is avoided in the design by evading the direct path between VDD and ground at any instance of time.

Now open drain output configuration is discussed. The PMOS transistor in the previous inverter implementation has been replaced by an external resistor. The basic functionality of the circuit remains same. When the low voltage level is applied at the input, NMOS is turned off; behaving as a high impedance and connects the output to VDD making it a logic one via a resistor. Similarly, when the input is logic high, NMOS turns on and acts as a low impedance, making output pulled down to the ground. The Figure 3 shows the design.

Two main difference can be seen in two topologies. First, When the output is at a low logic level, there is a direct connection between the supply voltage and ground through external resistor and NMOS. This introduces the non-trivial power consumption in the circuit. This is avoided in the previous case (CMOS inverter)
Second difference comes when the output is at a high logic level. In this case, the output is connected to the supply voltage via a resistor which is relatively much higher in its value. This characteristic makes it possible for this topology to connect more than two open drain drivers. When one of them is logic low then the other will be at a logic high and free current from supply voltage to ground is avoided by the pull-up resistor.
Open drain configuration has three basic implications related to the I2C which are listed below.

1. The default value of the signal is set to logic high. For instance, when a master in I2C attempts to communicate with a slave device which has become non-functional then the data signal will work properly and never enters in the undefined state. Another case in which the slave is not driving a signal then a logic high value will be read. Similarly, for some reason, if the salve losses the power during transmission the SCL and SDA will be made logic high. In this way, other devices can communicate setting their own values of SDA and SCL.
2. In I2C on the bus if some other device is attempting to drive the signals high, even then the bus can safely make it signals at a low level. This is the foundation of clock synchronization. Serial clock is generated by the master which can be used by a slave device depending upon the condition it is facing, giving the flexibility of decreasing the clock frequency.

3. On the same bus, supply voltages of different kinds can exist, but it is required to make sure that the device with the lower voltage will not be damaged by the high voltage value. For instance, communication between two devices possessing different voltages, 3.3V and 5V, can happen but SDA and SCL should be pulled up to 5V. The value of 5V will be assigned to the logic high voltage as per the open drain configuration. However, it is not possible for the 3.3V device to drive 5V from the push-pull output stage.

3.8.2 Reference Design

The reference design in I2C is a bus with two signal line, a data (SDA) having 7-bit addressing and a clock (SCL). Nodes can be either master or slave. Many numbers of nodes can be present because of the multi-master bus, described in the later section. After the Stop notification, the role of master and slave can be varied between messages.

Generally, four modes of operation for a given bus is defined but many of the devices just stick to an only single role.

1. The master node sends the data to the slave known as the **master transmit**.
2. The master node receives the data sent by the slave called the **master receive**.
3. Slave node sends data to the master known as the **slave transmit**.
4. Slave node receives data from the master known as the **slave receive**.

In addition to this, the stop and start bits allow the synchronization in communication. Along with this it also acts as message delimiters and is distinguishable from the data bits. This is in contrast to the other communication protocols in which the start and the stop bits are distinguished from data on the basis of their arrival time (htt32).

3.8.3 Physical Layer

At the physical layer in I2C protocol, both SCL and SDA lines are designed on the basis of open drain design, described previously. Pull up resistors can be considered as one of the basic building blocks of the design. A low logic level is obtained at the output when the line is pulled to the ground. Similarly, the logic level 1 is achieved by permitting the line float so that the pull-up resistor can pull the output high. A line is never allowed to actively driven high. Multiple nodes are permitted to connect to the bus because of this type of wiring. Along with this short circuit is also avoided from signal contention. The current source can be used at the place of a resistor to pull up the SCL or both SCL and SDA in many high-speed systems. Along with accommodation of high bus capacitance, faster rise times can also be enabled using this current source.

Many consequences occur due to this. One of the most important consequence is that the line is driven by multiple nodes at the same time. If a low line is driven by any of the nodes, then it will be low. Some other node may try to transmit the high

logic level, this node can detect the transmission of the previous node and concludes that some other node is active at the same time.

This is called clock stretching when used on SCL and when it is used on SDA, this is known as arbitration making sure that only one node transmits at one time.

When used on SCL, this is called clock stretching and used as a flow-control mechanism for slaves. When used on SDA, this is called arbitration and ensures that there is only one transmitter at a time.

3.8.4 Slave Addressing and Packet Format

In I2C multi-masters and multi slaves can be there which needs to communicate with each other. Speed of these devices may vary but the designer ensures that the slower devices communicate with the system without making the faster devices slow. For this purpose, a serial bus is required.

The formats, connections, protocol, addresses and procedures defining the rules on the bus is specified by the means of bus. Any device in the system can transmit, receive or both. The bus clock is generated by the master device to initiate the communication on the bus. While the slave devices just respond to the command by the master on the bus. For communication, a unique address is assigned to each of the slave devices. Master devices normally do not need an address because no command is being sent to it by the slave.

At the beginning of communication, the start condition is checked which is then followed by the 7-bit slave address. Data direction bit decides the type of operation; either it is a read or write operation. 0 value of this bit indicates that the master will write on the slave device. Contrary to this, if the direction bit has value 1 then the master will perform the read operation and reads data from the slave device. After sending the particularities, reading or writing operation can be continued by the master. End of communication is indicated by the stop signal which informs that the I2C bus is free for communication. If one master needs to communicate with more than one slave, a repeated start is produced with another slave address without generating the Stop condition. MSB is shifted first followed by the LSB. The Figure 4 describes the format of the address (htt34).

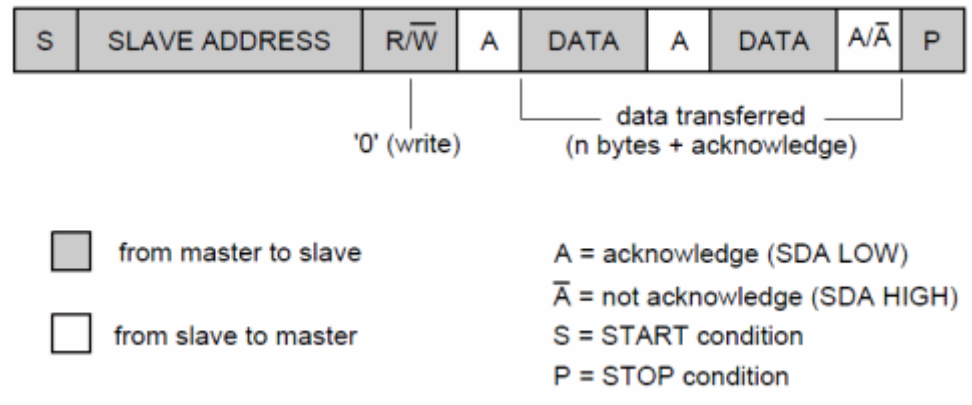


Figure 7 Address format of the packet

3.8.5 Clock Stretching using SCL

During the generating of the clock signal by the master in I2C, it is compulsory to meet the required specification that may include the minimum period for the high and low phases of the clock signal. Hence, it is concluded that the actual clock signal can be at the speed lower compared to the nominal clock signal. For instance, in I2C due to high capacitance rise time may increase.

Communication in I2C can be slow down through stretching the SCL. During the low phase of the SCL, any device on the bus has the choice to prevent the SCL signal from rising by holding it down. This enables the system to slow down the rate of SCL signal or it can also stop the communication for some moments. Sometimes this is also mentioned as clock synchronization.

One important flexibility provided is that I2C does not apply any restriction on the amount of time or does not specify any time out which implies that SCL signal can be held down by any I2C device as long as it requires (htt35).

3.9 Types of Electronic Door's Lock

An electric or electronic lock is the device which can lock and unlock the doors electronically. These are even more reliable, robust and highly secure electronic devices. This is the technological advancement which turned the conventional methods to entirely new, convenient and modern techniques. These are in fact the assembly of electronics mounted directly to the locks. These kinds of locks are best and modern to replace the tumbler-and-key ones, and can be installed at various different places such as homes, buildings, vaults, secret and sensitive places.
The locks can be accessed through key-pad locks, Iris scanning, finger scanning locks, voice recognition and through many others means. There is always access control system which can be advantageous in adding and removing keys without even re-keying the lock. For time and place sensitive areas, fine access controls are available. These locks can be remotely controlled and monitored, can be lock and unlock easily.

3.10 Electric Deadbolt Lock

Electronic locks have become popular security locks which are used at buildings, households and other places. These locks do not need to have key instead these are operated electronically. These are even more accurate and reliable than the manual ones. And these locks do not allow easy break in into the buildings. These are widely used in corporate offices, buildings, hospitals and defense centers.
Electric deadbolt lock contains the electric circuit. Old or conventional locks are locked or unlocked manually however, this lock with its circuitry allow lock to control in different way such as key-pad locks, voice locks and voice locks etc. The lock uses the solenoid or electronic motor to get the bolt mechanism.

- Unlike simple conventional locks, this electronic deadbolt lock comes with the digital technologies with modern techniques applied for locking and unlocking
- These are equipped with both electronic keying and locking system.
- Its demerit is that the solenoid or motor required high power
- It can cause awkward situation if its password or code is known by any other

3.10.1 Electromagnetic Lock

An Electromagnetic lock comprises of a coil assembly and an armature. When an electric current pass through it, the coil becomes magnetized. This produced magnetic field electronically controls when doors are locked and unlocked and also secures the lock. By design, these locks are fail safe.
These locks work such that entire locking mechanism is controlled by electromagnetism. The energized magnet makes bond with the armature and thus locks the door. Magnet is de-energized by a switch, which allows the access. The bolt locks the door when electric power is applied, and it is unlocked on removing the power.

3.10.2 Fail Safe and Fail Secure

Fail secure locks
Fail secure is the type of locks, which on losing the power automatically locks. However, in order to open or unlock, these locks require power. This is the standard kind of lock which is used for many access control systems. In fail secure locks, doors remain unlock unless power is interrupted.

Fail-safe locks
Fail safe locks open when there is no power. In order to secure or lock the door power is required. These kinds of locks are suitable for emergency exists or when power outrage occurs.

Summary of Basic understanding:

- When power is removed, the Fail-safe products are unlocked. Power is supplied to lock the door.
- When power is removed, fail secure products are locked. Power is supplied to unlock the door.

- Fail safe/fail secure refers to the status of the secure side (key side, outside) of the door.

3.10.2.1 Fail Safe and Fail Secure Usages

- **Fail- Safe locks**
  - This kind of lock is widely used in emergency situations such as for quick exit of building occupants, doors to stairwells and fire exists etc.
  - Power failure situations also require these kind of locks.
  - Point to remember: When a fail-safe product is used, the door will be unlocked. whenever there is a fire alarm, power failure or similar situation, which is an obvious security risk.

- **Fail-secure locks**
  - These locks ensure that tools, equipment or any inventory remain protected from any intruder during power failure.
  - Suitable for sensitive or expensive items' places.
  - It prevents unauthorized entry and locks automatically.

3.11 Display Research

Research on the display has gain much importance in the world of technology. From a researcher to the scientist, a developer to a gamer or a layman to an expert, everyone is keeping an eye on the advancement in the better display. Some of the common technologies is elaborated in following sections.

3.11.1 LCD

LCD (Liquid Crystal Displays) is a flat panel display technology which is mainly used in consumer electronics such as televisions, desktop monitor, small electronic displays on various appliances such as weight machines, thermometers, etc.

An LCD consists of a backlight which provides a consistent and even light from behind the display. The light coming from the backlight is then polarized as it passes through a liquid crystal layer. This liquid crystal layer is made of a substance which is part solid and part liquid, with the help of applying voltage this substance can be twisted. The layer blocks the lights when off but reflects red, blue and green light when operational. Each LCD contains a matrix of pixels which is like a rectangular grid. When this technology originated passive-matrix screens were used, through which the pixels were controlled by sending a charge to their row and column. The number of charges that were possible to send through the grid was limited; the image displayed appeared blurry when a fast-moving object moved through the screen. So, manufacturers started using active-matrix technology which consisted of TFTs (thin film transistors), these transistors had capacitors which enabled the pixels to retain their charge "actively" as a result of which the active-matrix technology appeared more responsive and efficient than its predecessor passive-matrix displays. The number of pixels in a grid depends on the resolution of the display for example in a 1920 x 1080 display will be 1920 pixels in width and 1080 pixels in

height. Every single pixel has 3 sub pixels, red, green and blue which can be toggled either fully on and off or they could be turned on to some extent like 50%. When the pixel is fully turned off that is red0%, blue0%, and green 0% then the pixel shows black and vice-versa, by fine-tuning all the sub pixels a single pixel can possess more than 16 million unique colors. The pixel only creates a filter in front of the backlight, so when the backlight turned on, we see the pixels allocated color. The inner structure of the LCD is further elaborated with the help of the Figure 5.

And LCD display has a few advantages over the traditional plasma TV as its resolution is higher and has better color contrast but when we compare it to the more modern technology such as LED and OLED it becomes very clear that LCD is becoming very obsolete. LCD displayed are less power efficient, have poor viewing angles that is if you move away from the center of the screen the colons start messing up and it lacks in the compartment of the deep blacks as it never shuts off completely (htt36).

3.11.2 Active and Passive Matrix Displays

Technology based on the active and passive displays is mainly developed to use them in LCDs. The basic difference between the two technologies is clear from the names assigned to them. In passive display, all passive components are used. On the other hand, active displays use all the active components like the transistors and capacitors. Both technologies have their own pit and falls. Decision among them can be made based on the application. Each of them is described below in detail.

3.11.3 **Passive M**atrix Displays

In a passive matrix display, the charge is supplied to a particular pixel through a simple grid. The main process in making the display is the development of the grid. Two layers of the glass are used as a substrate. One of the layers is used to decide the row and the second layer is used to determine the column of the display which is made from a transparent conductive material. Normally, the material used is indium-tin-oxide. To show an image on the display some particular rows and column values needs to lighten up. This is controlled by the charge supply. On the integrated circuit board, the rows and columns are attached making it possible to charge a particular entry on the matrix. Between the two-substrate layer, there is a liquid crystal material sandwiched. On the outer sides of these layers, a polarizing film is attached.

A particular pixel will be turned on when the charge is sent down to the correct column through the integrated circuit and ground is provided by activating the corresponding row on the other substrate layer. The intersection of the selected row and the column is the desired pixel point and the charge is delivered which untwist the liquid crystal between the substrate layer at that pixel point. Slow response time and imprecise voltage control are the two major draw backs of this (htt37).

3.11.4 Active Matrix Displays

Active matrix display mainly depends upon the TFT (An acronym of Thin Film Transistor). Contrary to the passive matrix display, an arrangement of TFTs in the form of the matrix is used in this technology. TFTs are basically a special kind of FETs (Field Effect Transistor) which acts as a switch. The glass substrate is used as a base material on which the pixels are arranged. A particular pixel is approached by turning on the correct row. Afterwards, the charge is applied to the proper column. Just like the passive displays, the intersection of the row and column will determine the addressed pixel. All other pixels of that row intersecting the column will remain turned off. The capacitor at the required pixel will charge up by receiving the charge. Until the next refresh cycle, the charge will remain on the capacitor. The Liquid crystal can be untwisted just enough to pass through some light by controlling the voltage level. On each pixel, multiple levels of brightness (up to 256) can be obtained by incrementing the voltage in a very small amount. A grey scale used in modern LCDs can be made through this.
The Figure 6 displays both the active and passive matrix display.

3.11.5 LED

An LED display is just like an LCD but it uses LEDs (light emitting diodes) as the backlight in different formats. The use of LEDs over the traditional backlight enables the manufacturers to construct much thinner displays and also it increases the power efficiency of the display. LED displays are mainly used in products such as TVs, smartphones, laptops, computer tablets, desktop monitors, etc. There are three formats in which the LEDs are arranged behind the display.

At first, full array format is required, in which the LEDs are space out evenly behind the entire screen as a result of which we get a more evenly lit backlight and this also allows for a much more effective implementation of local dimming where specific parts of the screen can be displayed darker by decreasing the luminosity of the LEDs behind that part of the screen. The layout of the full array format is further elaborated in Figure 7.

Secondly, we have the more mainstream format used by the majority of the manufacturers which is called edge lighting. In this format, an array of LEDs is arranged vertically on the left and right side of the display in some displays its lining the all the edges of the screen this allows the screen to be a very thin and also much more power efficient. However, this can also result in the sides of the display to be much brighter than the center. Such issues are most noticeable when a dark scene is playing on the television screen. This is called clouding.

Lastly, we have the format which is mainly used in the lower end products as it is cheaper to achieve, and it’s called direct-lit. This format is very much like the full array format but the spacing between the lights is a much greater as a result of which the number of LEDs behind the screen is lesser compared to the full array. But in this format, the individual sections of the screen cannot be toggled on and off to

achieve deeper blacks and much accurate representation of the picture. These displays are not thin because the space required to accommodate the LEDs and to diffuse light is rather large. This format is explained in Figure 9.

On a whole an LED has a lot of advantages as it is much thinner than an LCD, it has a better power consumption, better color contrast, quality and sharper images and also flicker-free images. However, these displays are much more expensive than LCDs and the LEDs can shift their color due to age, hence losing their quality.

3.11.6 OLED

The OLED display technology is the evolved version of its little brother LED. Like an LED, OLED is also mainly used in modern displays for devices such as TVs, Monitors and smartphones. The main difference between an LED display and an OLED display is that in an OLED display a backlight is not present, each and every individual LED emits its own light which allows the luminosity of each pixel to be dialed down to zero independently. An OLED is considered a solid-state device. It composes of a thin sheet of organic molecules that emits light when an electric current is provided to it.

As we turn on the power, electrons from the power supply are sent to the cathode (the negative terminal) and the electrons which were originally possessed by the anode (the positive terminal) are lost because of which the layer adjacent to the cathode known as the emissive layer starts getting negatively charged (as a result of increased supply of electrons) and the conductive layer is now positively charged. The structure of the OLED.

As the agility and the mobility of positively charged particles(holes) is much more superior to that of the electrons, to make their way to the emissive layer. Whenever a positively charged particle collides with electrons, rapid bursts of energy are emitted in the form of photons (fundamental particles of light) and due to this light is generated. Positively charged particles keep bumping into electrons, and as long as there is a constant supply of power, constant production of light will keep happening via this process. As soon as the plug for the power supply is pulled out, the energy transfer stops instantaneously, and the screen goes black.

Due to such advancement and the replacement of the traditional backlight with OLEDs, many doses of opportunities have opened. This allowed inventors to create transparent displays. Now a transparent display would make lives really easy for them, for example, it can be used in heads up displays for cars due to which the concentration of the driver will never be taken off the road and all the necessary information can be right in front of rather than down in the dashboard. Another implementation is that it can be used to create foldable displays which can allow for mobile devices to be even more compact and this technology is foldable, as the name depicts, which allows people to fold away after use. The ways that it has helped inventors till now is that it has decreased the power consumptions of the displays even more than LEDs. It is also much thinner. LED adds to the contrast, sharpness, color accuracy and overall quality of the image displayed on the screen.

On the other hand, it has a few other problems such as it is much more expensive and if a still image is displayed on the screen for too long it can cause a burn-in which is when the effect of the color is imprinted on the pixel for some time and it is visible when the color of the pixel is changed. Like LED displays, OLED displays also lose their quality over time due to ageing pixel.

3.11.7 Capacitive Touch Screen

A capacitive touch screen is best described as a control display that uses either the conductive touch of your finger or either a specially designed input device such as a stylus.

This technology works quite a bit differently, the surface wave panel and resistive, as it cannot sense the input of either finger or basic styluses. A capacitive touch requires input from either a finer or a special capacitive pen or either a glove. The panel has a coating of a material which is capable of storing electrical charges along with the location of where the capacitance of the screen is changed due to a touch input was registered. When a finger interacts with a capacitive touch panel a charge of a small amount is drawn to the point of contact which in return becomes a functional capacitor. The discrepancy within the electrostatic field is measured to determine the location of the input. In a few designs, each corner of the panel circuits is located whose function is to measure the charge and then send the information regarding that corresponding charge towards the controller for further processing. In case of a multi-touch screen the presence of sensors arranged in grid-like patterns allow for the display to accept complicated inputs.

However, a resistive touch screen works in a different way, it uses the pressure relating two conductive layers applied by a press. In comparison, outside elements do not affect the working of a capacitive touch screen, and these screens have high clarity and allow the functions to be executed with much ease as they can register lighter contact with greater accuracy.

The main implementation of touch displays is in mobile devices precisely smartphones, the introduction of the touch displays was revolutionary, and it changed the world and potential that was seen in mobile phone. Touch displays allow for the much bigger screen as the front of the devices did not require any buttons so more of the body could be used for the screen. This allowed more content to be displayed, navigation took the most advantage of this, secondly, it made a world of difference in the area of user interaction and ease of navigation. In the modern world, touch screens are being implemented in laptops which allow for an increase in productivity. However, a few major drawbacks are that these displays are more prone damage such as scratches or cracks plus it also adds to the price of the products possessing this technology.

3.11.8 Resistive Touch Screen

The main components found in a resistive touch screen are two layers of glass or plastic, both of the layers are covered in a coat of indium tin oxide (ITO). The faces

of these layers which is conductive are in front of each other and are set apart by the help of an air gap.

When the user exerts a pressure on the display, the topmost layer bends and touches the bottom layer as a result of which a small amount of current is generated which flows at the point where they connected. With the help of the sensors, the location of the touch can be calculated. These displays can be manufactured in three major ways.

The first one is called analogue 4 wire resistive. In this variant, if the sheet on the top possesses electrode in the direction of Y-axis, the sheet on the bottom possesses the electrodes in the direction of X-axis. The sheets on both, the bottom and top, calculate each other's voltage and the sensors help to determine the location where the touch was registered.

Secondly, we have analogue 5 resistive. In this version of the resistive display, the voltage possessed by the bottom sheet is measured by the sheet on the top with the help of electrodes in each corner of the sheet at the bottom. The highest sheet does not possess any electrodes.

Finally, we have analogue 8 wire resistive, this format is very similar to that of analogue 4 wire screens. The key difference between the both is that analogue 8 has an extra set of electrodes, which deals with the alignment and also the issues regarding the recalibration that crop up in the screen containing 4 wires which occur, when used over a long period of time. One advantage is this that they are really suitable for commercial use in devices such as ATM machines, but the image quality of these displays is not the best.

3.11.9 Display Selection

Display selection depends basically on your work requirement and also your budget. For example, when designing a phone which is targeted towards high quality and thin form factor, a touch OLED panel is the best choice. If you are making an industrial machine that needs a display to require one or two quantities you the manufacturer should go for an LCD display as it would be the cheapest and is more than enough for this purpose and would also shave the manufacturing cost of the machine. Another scenario may be that you are a content video editor and have color sensitive work then ideal choice would be an OLED monitor.

In our design, we are going to use TFT touch screen which is thin film technology. It would allow multiple touches on screen, and it would allow us to create custom drawings that fit our needs. I believe this would improve the quality of our lock to a different league. This will improve our design and compete with current in market designs. It is described briefly below in its specified section.

3.11.10 2.8” TFT Resistive Touch Screen (TF028)

TFTs are a type of an active matrix LCD which is also called TFT screen, with the ability to display millions of high contrasts, bright and clear color pixels. They are mainly used in HDTV sets, desktop monitors, laptop monitors, tablets etc. The first implementation of a TFT screen was seen in the IBM ThinkPad's 1992 model. The TFT technology operates by changing the brightness of the green, blue and red subpixels with the help of transistors for each pixel +on the screen. the pixels are not self-lit instead there is a backlight present in the back of this display to illuminate the pixels. The TFT family include LEDs, which is a hybrid of LCD screen, but it uses LEDs in place of a backlight (htt38). Both images of the actual 2.8” TFT Screen and LCD pinout is going to be provided Figure 3 and Figure 4 below, respectively.

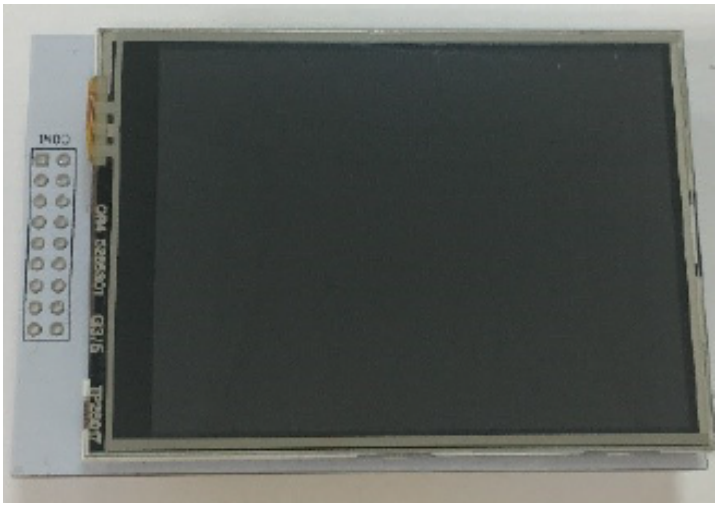


Figure 8 2.8” TFT Screen

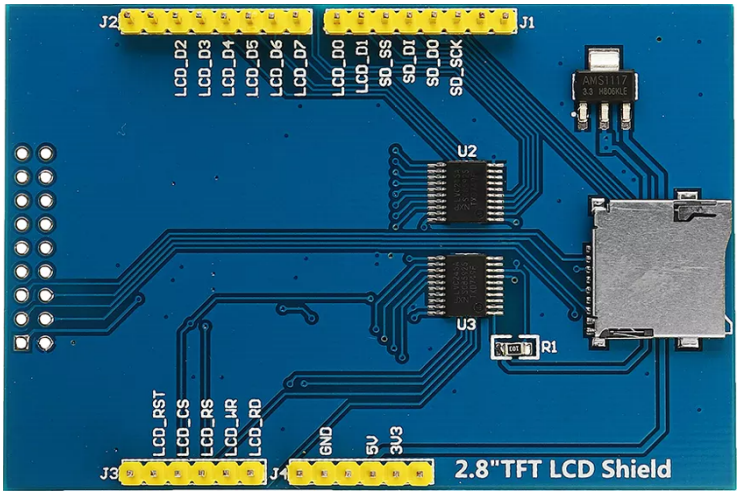


Figure 9 LCD Pinout

3.12 On-Device Storage

Storage of data on the device is the hour of the need. All processed data needs to be stored to save time. The already stored data should be easily accessible for later use. Storage on a device is mainly divided into three categories.

1. Optical
2. Magnetic

3. Semiconductor

The eldest among the mentioned storage technique is the magnetic device. The most common device, computer systems, started with this storage technique in the form of tapes which are then evolved into the hard disk drive and later to a floppy disk.

Using different expertise data will be stored in devices like hard drive, CD-ROM, DVD-ROM, flash media, "thumb" drive and many other. Normally a device has two areas for storage. One is "internal storage" and the other is "external storage". Permanent and temporary storage has been separated in almost every device using the partition. These spaces will always be there no matter the device is attached to some external storage medium. The internal storage is considered as the non-volatile memory. Small external storage device exists in the form of some SD card or a USB.

3.13 Electrical Relay

Relay is an electronic or electromechanical switch that can connect or break the circuit. More than one circuit is interlinked using relays. A circuit having a relay can control the other circuit, physically detached, just by opening or closing it. Two of the option exists in relay structure. Either a relay can be normally open (NO) or normally closed (NC). In the normally open relay, there will be no connection as long as it is energized. However, in normally closed relay there exists a short circuit but as energy is applied circuit will be broken. The basic concept remains similar in both cases. The state will be changed as the energy is applied to it. This configuration shows the normally open and normally close relay to further elaborate the concept.

Commonly, it is used in relatively simpler control circuits to switch smaller currents. Ordinarily, they are not employed in power consuming devices other than those which draw fewer amps like solenoids or small motor. Moreover, it has various applications like pilot lights, switches starting coils, pilot lights or heating elements.

Although large voltages and amperes can be controlled by the relays using the amplifying effect. This is because of the fact that a large voltage can be produced by applying the small voltage to the coil of the relay.
To prevent the damage, protective layers are introduced. They are capable of detecting the electrical abnormalities which involve overload conditions, excessive current, undercurrent or reverse currents (htt39).

3.13.1 Relevant Electrical Relay Technologies

There exist various kinds of relays including the electromagnetic relays or solid-state relays. Some of them are listed below.

1. Electromechanical Relays
2. Reed Relays
3. Solid State Relays (SSRs)

4. FET Switches

Each of them is explained briefly here. In the electromagnetic relay, the name itself depicts that magnetic force is used to open or close the contacts. While the solid-state relay is completely electronic. Switching is done through the electronic circuit and there does not exist any contacts. The electromagnetic relay and solid-state relay are shown in the Figure 13 and Figure 14 respectively.

Reed relay is just like the electromagnetic relays. A circuit path is opened or closed mechanically via physical contacts. However, the size of the contacts is relatively small and the lower in mass as compared to the electromagnetic relays.

Dry reed relays are constructed using the reed switches and coils and a couple of ferromagnetic blades overlapped with each other are used in the manufacturing of the reed switch. A glass capsule, filled with inert gas, seals these blades. At the overlapping ends, contacts are placed.

As soon as the coil is energized, two reeds will come towards each other to complete the circuit path. Contacts will be moved apart through the spring force as the coil is de-energized.

3.13.2 Electrical Relay Selection

The type of relay being used in any application utterly depends upon the electrical requirements, limitation of cost and life of it. Popularity and usage of both the relays are comparable, each of them having their own pit and falls. Electromagnetic relays are used to implement the switching functions of heavy-duty devices. In solid state relay, non-moving electronic equipment is used to switch the current. The common example of such a device is silicon-controlled rectifiers.

Solid state relay has the advantage that in this coil does not need to be energized or contacts do not need to open. In fact, a small voltage can change the state (on or off) of the relay. Likewise, this can work on a high frequency as there is no physical part that is required to move. Along with these advantages, a trade-off needs to be made in the sense that arcing cannot happen due to the absence of contacts. Similarly, it is not possible to replace this relay while the other, electromagnetic relay can be replaced in case of any fault.

Residual electrical resistance can exist while constructing the solid-state relay due to which leakage current will be there no matter what the state of the switch is (either open or close).

The small voltage drop may not harm the circuit in solid state relay, but the electromagnetic relay produces the efficient and noise free version of ON or OFF. This is because of the considerable large distance between the contacts. This air acts as insulation and gives better results. In Figure 5, it shows the actual Relay that is going to be used to amplify the voltage in order to make it work with our locking mechanism

With this relay, it would only need a small signal to be sent to it and it would amplify it and send it to the locking mechanism.

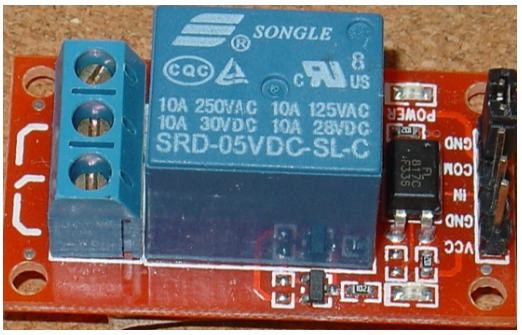


Figure 10 5v Relay module

3.14 RFID Research

The RC522 RFID module is developed using MFRC522 IC and some other basic electronic components. It is one of the most radially available, inexpensive RFID options. An RFID tag is also provided along with the module on which data can be written and stored. The RFID reader module is quite straightforward to use and can be employed in various applications like an automatic door. It provides good compatibility with some other third-party libraries like Raspberry Pi and Arduino. The module is shown in the Figure 13.

Figure 11 RFID RC522 module

3.15 Facial Recognition Camera Research

The initial plan was to use a USB HD camera with good megapixel, that needs to be properly connected with the system for execution. Following research and plan was made for the USB camera for facial recognition.

3.15.1 Algorithm

Open source Computer Vision Library (OpenCV) is an open source BSD licensed library that includes several hundred of computer vision algorithms. The available algorithms

- Eigenfaces
- Fisherfaces
- Local Binary Patterns Histograms

The desired algorithm was Histogram Face Recognizer Algorithm as it has efficient ways to detect faces rather than the rest of the algorithm.

3.15.2 Local Binary Pattern Histogram (LBPH) Recognizer Algorithm

This algorithm analyzes each face in the training set separately and independently. Each image is analyzed independently, while Eigenfaces looks at the dataset as a whole. In LBPH each image in the dataset is characterized locally. Once a new image is taken, the same analysis is performed by comparing the results to each of the images in the dataset. This how an image is analyzed by characterizing the local pattern in each location in the image. Face recognition using LBPH works better in different environment and light conditions. However, it also depends on the training and testing the data set. To do this analysis, ten different pictures of a person are needed for the camera to recognize them. The LBP operator can be described as:

Equation 1 Local Binary Pattern Histogram Recognizer Algorithm

$$\mathrm{LBP}(x_c, y_c) = \sum_{p=0}^{P-1} 2\mathrm{ps}\ (i_p - i_c).$$

In this formula:

- (x_c, y_c) is the central pixel with intensity
- I_p and i_c are the intensity of the neighbor pixel
- S is the sign function that can be defined as:

Equation 2 The Sign function

$$s(x) = \begin{cases} 1 & if\ x \geq 0 \\ 0 & else \end{cases}$$

This description allows to capture fine grained details in images. To capture the following neighborhoods, the idea is to align an arbitrary number of neighbors on a circle with a variable radius.

3.15.3 Facial Recognition Module

The face detection is a major part of the system as this completes the entire process of opening the door if other criteria of opening the door are not met. This section has a few methods that require a a properly implementation.

- First is to make a data base of faces with several images for each individual person.

- The next step is to detect the faces that are stored in the data base images and use them to train the face recognizer.
- In the end, face recognizer will be tested so that it is trained enough to recognize faces.

3.15.4 Database of Images

The user must have a database of images, of themselves, stored in the system. There are at least ten pictures taken from different angles and stored in the system. This helps to extract features and helps the recognizer to have most of the expression a human can come up in front of the camera. Therefore, features of 10 arrays are stored.

3.15.5 Connecting the Camera

The camera can be any USB HD camera, which needs to be properly connected with the system for execution. It should be kept in mind that the megapixel of the camera is good enough to detect a face properly.

3.15.6 Inputting Modules

In this step modules are imported: CV2, OS, Image and NumPy

- CV2 is used for face detection and recognition. The OpenCV module contains the functions.
- OS, first extracts the image names in the database directory. From these names, individual number, which will be used as a label for the face in that image is extracted. This module will be used to maneuver with image and directory names.
- Image uses Image modules from Python Imaging Library (PIL) to read the image in grayscale format. Since the datasheet images are in gif format.
- NumPy stores the images in NumPy arrays.

3.15.7 Training Recognizer for Face Detection

First in the database an image is created, which contains faces of the user with whom the face on the camera can be matched. In each image, the individual has a different facial expression. For example, there will be several images of each individual to train the recognizer. The algorithm used in this process is Local Binary Pattern Histogram (LBPH). In LBPH each image is analyzed independently. The LBPH method is simpler as it characterizer each image in the dataset locally. When a new image is provided through a camera that the camera does not recognize, same analysis is performed on it and compares the result to each of the images stored in the dataset. Therefore, characterizing the local pattern in each location in the image, and thus analyzing the image.

3.15.8 Applying Local Binary Pattern Histogram

Functions like FaceRecognizer.train, trains the recognizer. FaceRecognizer.predict recognizes a face. This is where the Local Binary Pattern Histogram Face Recognizer algorithm is used.

The function that prepares the training set has a function called get_images_labels, which takes the absolute path to the image database as input argument and return tuple is 2 lists, one containing the detected faces and the other containing the corresponding label for the faces. After preparing the training set, the get_images_labels function with the path of the database directory is passed. This has to be an absolute path. This function reutrns the feature of the images and labels or caption of the images, which will be used to train the face recognizer afterwards. FaceRecognizer.train is used to perform the training. It requires two arguments.

- The features as images of faces.
- Corresponding the labels assigned to the images, which in this case are the individual number that are extracted from the image names.

3.15.9 Extracting Features from the Images

The first step is to detect the face in each image. As it starts to get the region of interest (ROI) containing the face in the image, it will use it for training the recognizer. For the purpose of face detection, the Haar Cascase provided by OpenCv installation. For detecting the facem haarcascase_frontalface_default.xml is used. The cascade is loaded using module called CV2. Then the function called CascadeClassifier takes the path to the cascase xml file where it is copied in the current working directory, to use the relative path.

3.15.10 Displaying Result as Confidence

As the detection of faces is done, the result of detection is played accordingly in Python in a way where the confidence of detection is mentioned. The confidence tells how much accurate the face is detected of that human being. The less the confidence found, the more the accuracy.

3.16 Fingerprint Research

The US Department of Homeland Security defines biometrics as unique physical characteristics that can be used for automated recognition. Biometric identification provides a quick and accurate means of identifying a person or biological entity. The most common methods of biometric identification is fingerprint scanning, iris scanning, voice recognition, and facial recognition. For the Smart Lock, the biometric identification will be implemented using the fingerprint scanning method and facial recognition.

Analyzing fingerprints is one of the oldest forms of biometric identification. Fingerprint impressions were used on clay seals as early as the Quin Dynasty 221 BC. In 1788 a German Anatomist Dr. J.C.A Mayer declared that the friction ridge on skin is unique and never duplicated in two persons. Even identical twins have differences in fingerprint structures. This became the basis that the idea that fingerprints could be used to accurately identify a person was built on. In courts, fingerprints are recognized as forensic evidence and today there are many fingerprint verification technology systems. Fingerprint verification systems are generally comprised of a scanner which inputs the fingerprint data, and a processor to store and compare the acquired fingerprint data against a pre-populated database. Three popular methods that are researched and compared are optical, capacitive, and ultrasonic.

The optical scanner uses a charged coupled device which is an array of photosensitive diodes called photosites. When photosites are exposed to photons, they generate an electric signal. When a finger is pressed on the scanner, LEDs are used to illuminate the surface of the finger and photons are then reflected back to the photosites. The signal intensity generated by each photosite is used as information for a single pixel so the array provides a quantized two dimensional representation of the surface of the object scanned. Areas with high photon reflection represent the ridges of the fingers because the light interacts with the ridges first and is then reflected back the photosites. Areas with low photon reflection represent the valleys of the finger. After acquiring the image, the image is inverted so that the ridges appear dark and the valleys appear light. This is because the data used for identifying fingerprint features is the ridges. By checking the average pixel intensity, image is then analyzed and rejected if it is too bright or too dark. Another test is performed to check if the image is sharp and properly exposed. When these tests are passed, the image data is then finally compared with its database for possible matches.

Like optical scanners, capacitive scanners also take an image of ridges and valleys of the finger, not by measuring light intensity but by measuring changes in capacitance. Capacitive scanners use an array of electrodes and operational amplifiers to measure capacitance. When a finger is pressed upon the scanner, the ridges of the finger decrease the distance of the parallel plate capacitor that is formed which increases the capacitance, while the valleys of the finger increase the distance of the parallel plate capacitor formed and decrease the capacitance. Equation 1 shows how the distance of parallel conducting plates change the capacitance. Measuring the capacitance is done by first shorting all of the capacitors to reset them, then applying a fixed charge to the circuit. The capacitance is related to the charge and voltage using equation 2. As the capacitors charge, areas under ridges will have a greater capacity than areas under valleys. This will result in different voltage values so by measuring the operational amplifier voltage outputs in every cell in the sensor array, the ridges can be discerned from the valley and a high-quality image is produced. The system finally compares the features within the image to the features from the fingerprints in the database.

Ultrasonic fingerprint scanners use an ultrasonic impulse to acquire the fingerprint data. First an array of ultrasonic transmitters sends out a short acoustic pulse. The

pulse interacts with the surface of the finger and is reflected back. Next, an array of receivers listens for the reflected pulse and the processor acquires the depth information from the ridges and valleys of the finger. Ultrasonic fingerprint scanning produces the highest quality fingerprint image but due to cost, size, and speed, it is not widely used compared to other sensors.

3.16.1 Fingerprint Module Comparisons

For the Smart Lock system, the optical scanning method is selected for fingerprint verification because its low cost and descent image quality. Two different optical scanners, the FPM10A and the GT511C1R, are researched and compared in order to select the appropriate scanner module.

The FPM10A Optical Fingerprint Scanner features a high-speed digital signal processor with a built in identification algorithm that can search through one thousand fingerprints in one second. It operates at 3.6-6V dc with a current of 120 mA and communicates over UART at baud rates speeds ranging from 9600 to 57600. It captures images using a CMOS image sensor and can hold 160 fingerprints in its database. This module is widely used in open source projects and there is a large amount of online support available.

The GT11C1R Optical Fingerprint Scanner features an ARM Cortex M3 Core that implements the SmackFiner 3.0 algorithm for feature recognition. It operates at 3.3 to 6v with 130 mA and also communicates over UART but only at a baud rate of 9600. Up to 20 fingerprints can be enrolled which is ideal for small home systems but would need an upgrade to the heftier GT11C3R unit if a higher enrollment count in needed. The GT11C1R uses an esthetically pleasing blue LED for illumination and also features a thin, sleek design that would complement a wall mounted system.

Table 5 Fingerprint Module Comparison

	Operating Current	Protocol	Storage	Scan time	LED Color	Price
FPM10A	120 mA	UART	162	1.0 seconds	Red	$ 20.99
GT11C1R	130 mA	UART	20 Fingerprints	1.5 seconds	Blue	$ 18.00

3.16.2 Fingerprint Module Selection

After comparing the optical fingerprint scanners, the GT11C1R as shown in Figure 3 is chosen for its low cost and esthetic quality. They both operate at nearly the same voltage and currents and speeds, so those factors are negligible. Although the FPM10A is capable of storing a larger database, a simple upgrade to the GT11C3R module can be implemented when a higher enrollment count is necessary.

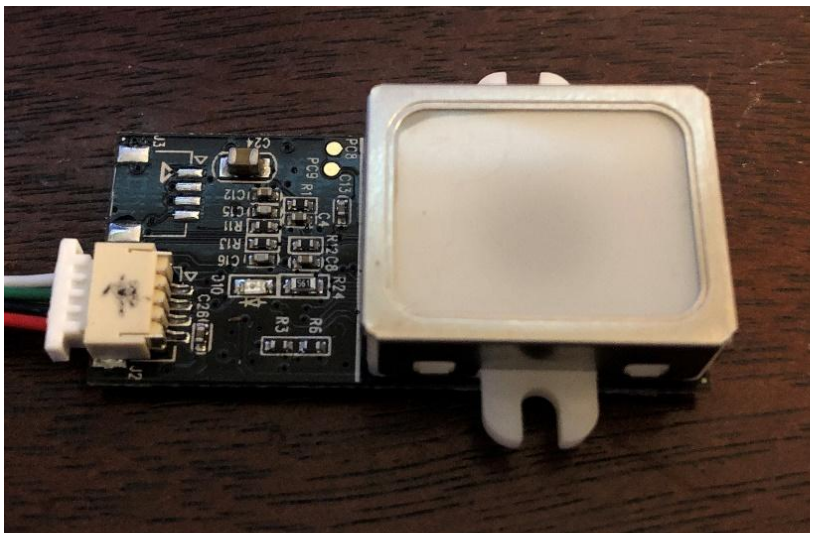


Figure 12 Finger print scanner

3.17 Wi-Fi and Bluetooth Research

A research was done to come to conclusion if Wi-Fi was a better choice over Bluetooth. A Wi-Fi module was to be connected with a server using LAMP stack, the design of which the team itself was to host. A mobile application would then communicate with the server through the internet. It was later decided that the connectivity of the system with that of the device will be done using Bluetooth Module. This decision was made due to the major con of Wi-Fi requiring an internet connection. Most of the times Bluetooth acts better than Wi-Fi in terms of connection. The connection speed although is much greater in Wi-Fi, but there can be loss of connection due to absence of internet, which can cause Smart Lock to not function properly. Therefore, Bluetooth was chosen over Wi-Fi.

Connection of software to hardware can be complex and convoluted, in the case of mobile devices sending and receiving data has abundant methods and among many ways to connection, Bluetooth is a manageable option, Mobile devices support Bluetooth to allow wireless connection of exchange of data between the hardware and software and provides a connection between API and framework between mobile and Bluetooth.

Bluetooth can support multiple platform; the Android platform can support the network stack to allow the communication between devices. The wireless exchange of data uses the framework to access and connect from Bluetooth with Android API, to enable point to point features. Android has a built-in fuction to allow multiple Blutooth devices connectivity all at once by using API in the Android system application for scanning, query local adapter, establishing channels, and transferring sata while all with the capabilities.

- Scan Bluetooth device
- Query local Bluetooth Device
- Establish RFCOMM channels
- Connectivity to another device discover

- Transfer data to another device
- Manage multiple connection

3.17.1 Bluetooth Development

Bluetooth pairing requires data to be transmitted between devices in order to enable the communication process. Security levels can be set to place precaution of connectivity between devices by pairing and bonding, doing so requires permission to request, accept, connect and transfer data. Setting up applications to take Bluetooth connectivity requires permission of the location of devices to be scanned and can also be used to gather information for the process to transfer data. To set permission between connectivity application and device, declarations must be made for an access point to initiate the device to be enable for discovery by declaring ACCESS_COARSE_LOCATION or ACCESS_FINE_LOCATION.

Application allows profile for any device connected via Bluetooth, giving it an identity to distinguish from other device wirelessly since Android 3.0 with full support of API. Profiles comes with interfaces such as Hands-Free, that supports mobile devices to connect the Smart Lock the application and Facial recognition camera, etc. Proxy is setup to connect objects of the profile data to establish transmission.

3.17.2 Bluetooth Pairing

It is important to know which device can be compatible for communication to ensure that connectivity can be supported. Device that can be supported will send discovery. Point for the scanning in the local area for any enabled Bluetooth devices to request transmission and information exchange. The process of pairing Bluetooth will enable devices is often called discovering, inquiring or scanning. Device that are within range of discovery will respond by requesting and accepting information to exchange name, class and unique address. After pairing is made between connection for the first time, request can be sent automatically as the device will be remembered for the information already paired which is then saved. There are distinguished differences between being paired and being connected.

- **Paired**
  Being aware of existing devices that share an already established link for authentication and encrypted connection.

- **Connected**
  Sharing an RFCOMM channel that are capable of transmitting data between Bluetooth devices
  Pairing will be established once initiation occurs to encrypt the connection with API

To pair devices in order to make it discoverable, the devices must be querying to return objects to bond and connect, that way it can be recognized, and the data will bring up the profile for specific devices. The querying process will then acquire the

name and MAC (Media Access Control) address to initiate connection begins as an asynchronous to return Boolean value in the scanning inquiry.

3.17.3 Bluetooth Low Energy

Running Bluetooth on devices can drain battery life faster than normal while being active, by keeping connectivity and communication between other devices. To save power for the user in order to make usage of mobile device for longer period of time thanks to latest Android API connection. The new Android 4.3 latest update for API (level 18) platform, provides support built into the device for Bluetooth Low Energy (BLE) for connectivity of the API. Since BLE has a stricter usage power consumption in comparison to classic Bluetooth, it operates on key term and concept from GATT, ATT, characteristics, descriptor and service that can be more explored below:

- GATT (Generic Attribute Profile) - Specification profile that links BLE to send an receive data in short pieces called attributes that every BLE uses.
- ATT (Attribute Protocol) – Optimization of running BLE devices that was built on GATT that is identified as Universally Unique Identifier (UUID) from standardized 128-bit format.
- Characteristic – A way to contain single value that can either be analogous to a class
- Descriptor – Defining attributes of characteristic value that could be reusable description from within range of the characteristic value, that could be readable description from within range of the characteristic value, or even units of measurement
- Service – Collection made from characteristic that can list GATT profiles.

Bluetooth come in different generations from 2.0 to the newer 4.0 which are BLE for low power consumption to perform the same functionality and better. This is possible because BLE stays in sleep mode unless a connection is being initiated. The latency it takes for the BLE to be connection would be in the few milliseconds while Bluetooth 2.0 takes about 100ms to establish connection. This makes BLE for more towards an industry and technological advancement purposes such as:

- Connecting smart apps to the devices
- Monitoring sensors
- Geographical beacon
- Public transportation app

While both 2.0 and BLE have different purposes, the 2.0 version is widely used for exchanging large data transfer and BLE have different purposes than the 2.0. The Bluetooth research that was done on Bluetooth 2.0 and Bluetooth 4.0, which is also known as Bluetooth low energy (BLE) MLT-BT05. For proper comparison, HC-05 boards were used. To use it, pins were connected using voltage divider on the breadboard along with Arduino. This way, 4.5V was converted down to 3.0V, which is compatible with HC-05 3.3V. After uploading the code, using an application; Serial Bluetooth Terminal, which works for both blue tooth classic and Bluetooth terminals, ascii texts were sent. As such no real effect was noticed, but upon connecting the

multimeter in series with power connection of the board, it could be seen that 2.0 when it is not paired with a device, it was around 9.0 mA. During sending and receiving data it was around 9.13 mA, which is not much different from when it is not in use.

However, when Bluetooth Low Energy was connected, it drew about 20 mA unpaired, 19 mA while sending and receiving messages. Once the Bluetooth Low Energy is not in use, it drops down to 2 mA as soon as its in low power mode. This shows that Bluetooth Low Energy is in sleep mode constantly except for when a connection is initiated. This ensures that data exchange for applications that do not need a lot of data exchange, can run on battery power for years at a cheaper cost. Moreover, Bluetooth 4.0 pairs faster with the phone than 2.0. This upgrade from 2.0 to 4.0 is important as these aspects play a major role in the conservation of power is of significance, which affects the cost of overall product.

3.17.4 Bluetooth Vs Bluetooth Low Energy (BLE)

Bluetooth is used to exchange data over a short range. When it comes to using microcontrollers, Bluetooth is an easy to implement option. When talking about Bluetooth and Bluetooth low energy, it is important to talk about power consumption. As well as knowing the advantages and disadvantages that can prove to be beneficial in projects for wireless communication. Bluetooth technology was created with the purpose of not replying on wired connection to exchange data, which is proven useful for short-range and long-range connection that can be implemented in the devices. Built into the technology of Bluetooth is frequency 2400-2483 Mhz of band, that allows operations to send data by splitting into packages. While having the purpose of continuous streaming of data and in applications, a new version of the technology is Bluetooth Low Energy that has more efficient power consumption all the while being capable of sending more data at close range, making this more marketable for consumer products.

3.17.5 Bluetooth Low Energy 4.0 modules Comparison

Bluetooth Low energy can be beneficial for saving power and like the HC series, this also uses SMD module based on the Bluetooth SOC (System On Chip. The type of Bluetooth comes in 2 versions from the HM-10 series, the S version and C version that does not need pads from the bottom connector (USB connection). Both C and S versions have 26 pads instead of the usual 34 from the other modules, making this the cheaper option to produce the manufacture. BLE itself is not considered an upgrade from the Bluetooth Classic modules, but instead it uses different system and intention of usage.

3.17.6 HM-10

The basic component specification of this module give manufacture cheaper and easier to produce while having the same operations for C and S versions. Unlike the 2.0 modules, these BLE modules contain the standard UART seriel

connection that is more familiar to connect along with microcontroller. While being Bluetooth 4.0, it cannot connect to 2.0 modules such as HC-05 and HC-06, although being BLE it is simpler to use and allows no actual control towards BLE side of the module itself. The HM-10 module can be controlled through AT commands that transmit data through serial UART connection. The pin configuration of the specification is listed below:

- **Voltage:** +2.5 to +3.3V
- **Current:** 50mA
- **Active Status:** 9mA
- **Sleep Mode:** 50-200 μA
- **RF Power:** -23dbm, -6dbm, 0dbm, 6dbm
- **Version:** 4.0 BLE
- **Baud Rate Pre-Firmware:** 700V up to 9600
- **Baud Rate Firmware:** 700V up to 115200
- **Default Pin:** 000000
- **Default Name:** HMSoft
- **Based:** CC2540 or CC2541 chip

This module uses the standard UART serial communication which makes straight forward connection for microcontrollers with the same standard layer of UART. This connection from the serial UART controls the HM-10 through the AT commands. It can also be used for mounting on breakout boards that allows the power more exposed from the connection to the breadboards process more seamless to activate the module from 3.3V pin. Like the HC series, this module has similar pin configurations that includes, STATE, Vcc, GND, TXD, RXD, BRK. There is also a built in LED that blinks while waiting for connection but once connection is made then the LED stays solid and can also change to pairing which leaves LED to continue flashing to establish connection.

3.17.7 ESP32

Another type of Bluetooth 4.0 and BLE that is also developed by Espressif Systems based in Shanghai. It is similar to the ESP8266 that works as both Bluetooth and WIFI combo module. This would be beneficial for projects with higher performance and ultra-low power consumption. The ESP 32 is an integrated dual-core processor chipset with firmware updates along with an SDK that supports fast on-line programming that has available open source toolchains. This module can be used for many purposes ranging from video streaming, WIFI and Bluetooth enabling devices, home automation, mesh network app, hardware engineers, software engineers, that can provide solutions to develop with wireless implementation. It is designed to be the optimal module with a single chip capable of 2.4GHz from TSMC ultra low power 40nm technology to be compact with full functionality of both Bluetooth and WIFI that is well optimized.

Specification

- **Processor:** Tensilica Xtensa 32-bit LX6 microprocessor with a clock 2/1, which is dependent on variation. It has Clock frequency up to 240 MHz and performes up to 600 DIMPS.

- **Wireless Connectivity:** 802.11 @ 2.4GHz up to 150 Mbits/s and Bluetooth version 4.2 Br/EDR and Bluetooth Low Energy.

- **Memory:** The internal memory consists of 448 KiB, SRAM of 520 Kib, RTC slow RAM of 8 Kib, RTC fast RAM of 8 Kib, eFuse of 1 Kbit, embedded flash, IO17, SD_CMD, SD_CLK, SD_DATA_0 and SD_DATA_1. The external memory consists of flash and SRAM up to 4x16 MiB. 8MiB SRAM hardware encryption. However, the embedded flash does not support for mapping with peripherals.

- **Security:** It uses IEEE 802.11 standard security which inludes WFA, WPA/WPA2, WAPI, secure boot, flash encryption, 1024-bit OTP – up to 786 bit, as well as cryptographic hardware acceleration like AES, SHA-2, RSA, elliptic, curve cryptography.

3.17.8 Selected Bluetooth Module

The technology built-in Bluetooth can be embedded in any device, while the module that is communicating with the mobile devices, by building personal area network (PAN), the range can be reached from the band would be approximately 9 meters or 30 feet. Each pin on the Bluetooth module serves a purpose, with the Enable/Key, Vcc, Ground, TX, RX, State as pins to connect with features for functionality.

- **Enable Key:**
  - The enable pin serves as a switch for the Data Mode and AT Command Mode
  - The switch for Data Mode is setting low power for the module
  - The switch for AT Command Mode is setting high power for the module
  - Normally at default, the module is set to Data Mode for low power
- **Vcc**
  - The is the pin that powers-up the module and serves as the supply voltage
  - Connection for supply voltage can go up to 5V

- **Ground**
  - The ground pin of the module to regulate the voltage to zero potential

- **TX**
  - This pin is the Transmit Serial Data on the Bluetooth module so that it connects to the RX on the other device acts as the receiver
  - Serial data that gets transmitted is being achieved through the other end to give out data which goes to the pin to the receiver UART of the microcontroller

- **RX**
  - This pin is the Receiver Serial Data on the Bluetooth module so that it connects to the TX on the other device to acts as the transmitter
  - This acts to request serial data that is given to this pin and the other end of the connection transmit from the microcontroller
- **State**
  - Serves as the connection of the LED on the Bluetooth module
  - Checks if Bluetooth is functional and flash or blinks for feedback

Sending sensor data from Bluetooth to communicate requires few simple tools, which are Bluetooth Module, microcontroller, USB cable, breadboard, and sensor. The microcontroller used for this module is Arduino and the Bluetooth module will be HC-05. These will be connected to a computer to the code the project. The experiment will require multiple procedures like Bluetooth connectivity, the coding process, transmitting data and troubleshooting to have the electronic device function shown in the following steps.

- **Circuit Setup**
  - The Bluetooth module will be connected by having the voltage lines through a voltage divider, that way the module does not get burned and burn the circuit
  - The wire will be connected to a line, but because of the voltage divider, 5V may not be sustained in the line to pass through so it does not damage the module
  - The module can also be connected to 3.3V line, unless more power is required for other inputs

- **Bluetooth Connection**
  - The next step is pairing the Bluetooth module with any computer with built-in Bluetooth capabilities, otherwise an external dongle can be implemented
  - Connecting the Bluetooth can be done on the computer by going into settings, locating, detecting the module and pair with a pass code
  - Going to the main setting of the computer can be followed as such: Control Panel, Hardware and Sound, add a Sound, add a Device
  - Detecting the HC-05 and typing code of 0000 or 1234 to begin implementing to finish the pairing

- **Arduino Code**
  - From the sketch provided of the design to implement the experiment proper functionality
  - Finding the correct ports of the board to connect the Bluetooth module can be found in the setting of the IDE
  - Once the correct port and board is selected, the TX and RX pins can be disconnected the code

- Otherwise an error will occur when the COM port is busy if not disconnected after the code is uploaded
- When uploading the code is successfully completed, reconnecting the TX and the RX pins to the original port

- **Receiving Data**
  - After the code is uploaded to the board, the power source can be used to connect the board
  - After the code is uploaded and power source is used, then the USB cable can be disconnected from the board.
  - This step ensures that PC is no longer needed to power the device and the sensor functions remotely by gathering data to transfer to the PC through Bluetooth
  - Notification can also be set to see if Bluetooth and sensors are functional
  - Locating the COM port can be set to sending and requesting data

- **Troubleshoot**
  - A sign that shows data is fully functional, is when the serial can be monitored to show notification is set
  - In case the connection is delayed usually means that an error may occur
  - This happens due to signal interface, but can be avoided to ensure a firm signal
  - Rechecking the TX and RX pin connection to ensure functional communication
  - Changing voltage so power can distribute evenly, like connecting Vcc to 3.3V
  - Loose connection stops the module from working. A constant blinking LED light indicates this
  - Module out of range from the PC

3.17.9 Bluetooth Breadboarding Experiment

To begin testing, the Bluetooth module is connected and powered by the microcontroller, the module will continue to blink until it is properly setup to communicate with a mobile device. An LED will be used as an indicator, which can be used on a program to set other forms of notification by exchanging data. The proper wiring of the module and microcontroller can be set as follows

Table 6 Bluetooth Pin Connections

Vcc	5V/3.3 V
GND	GND
TX	RX
RX	TX

The wire connection process of the Bluetooth module to the microcontroller functions in a master and slave device connection. The master gives commands to external device to follow, in a transfer and receiving data process. Following the writing connection, to power up the device it must be connected to Vcc of the module to either 5V or 3.3V of the microcontroller pin and the ground pin. The next wire connects the other TX pin, where TX is the transmitter serial data that gets connected to the RX pin, which is the receiver data. The TX and RX functions by having one end, the master uses TX to transmit data to the Bluetooth module, and begins by sending back data to respond which goes to RX of the master where it receives data for communication. On the Bluetooth module side, it will blink continuously unless a connection is established, and as the slave device, commands can be given to this form the master to exchange data to operate with other external connection either wired or wireless.

Cathode (Short pin/ Negative)	GND
Anode (Long pin / Positive)	D2 (any digital pin is fine)

This connection of an LED will serve as an indicator to recognize the exchange in data from master to slave device and can be modified in many ways to be set as a notification module. The red LED on the breadboard will be used as an example experiment that can be controlled from a mobile device, which is done through digital communication. Unlike the analog pins, which requires external parts to be controlled physically, the digital pins allows more intricate process to light up an LED by creating mobile application that allowed data to send from that app to the Bluetooth module, then the microcontroller, and then finally giving commands to the LED to light up.

3.17.10 Bluetooth Communication to Android

Bluetooth modules and mobile devices such as Android can communicate with the use of microcontrollers to integrate between software and hardware. Using microcontrollers to implement the communication between software and hardware are main factors in electronics for creative prototypes of experiments like the Bluetooth to mobile device. Bluetooth is a useful tool for shirt-range wireless communication to other electronic devices in developing hardware connectivity along with mobile application for software implementation using microcontroller. While there are multiple microcontrollers exist for electronic experiment, the prime device used with the ATmega 2560 for the practice of the experiment.

Implementing Bluetooth connectivity with the mobile device is uncomplicated since writing the code does not use libraries but rather simple and only needs the serial transmission as well as setup methods. Locating the serial transmission is simply done by connecting the right wire to the pins of the microcontroller assigning to that specific command in the code along with the baud rate for transmission. The serial transmission should be set at the proper baud rate of 9600 as the default, any higher baud rate can cause the transmission to be more susceptible to noise that would disrupt the connectivity. Once the Bluetooth connects to the microcontroller, the next process would be sending and receiving data to devices that have paired with the Bluetooth.

3.17.11 Cross Platform Development Environment

Instead of writing an application an application can also be written to be an independent platform. Cross-platform are popular in the software development. This category of framework is not only cost effective but its time saving and is easy to maintain. Below are some of reliable platforms that are discussed in details.

Flutter

Flutter is a new development tool that was released by Google to develop web frontend and mobile application. Being a Software Development Kit (SDK) from Google, this also comes with complete framework, widgets, and tools to allow developers to create application that can be easy to build and deploy visually pleasing, quick and smooth mobile apps that can be used for Android.

One of the many benefits of using Flutter as compared to another SDK is that it can be cross platform, being able to run on both Android and iOS, instead of separately. Having to run on one codebase rather than multiple SDK, makes it more convenient and save time for developers. Having the utilities already built into the system provides very accessible told such as widgets as customized design for developers. These beneficial functionalities can be broken down as follow:

- Object-Oriented Language that is based on Dart, making it easy to learn
- Built-in Widgets that can be drawn from its own high-performance rendering engine
- Widgets that are fast, visually pleasing and customizable
- Ability to create own custom app design, with UI elements available
- Architecture based on React, simple and reactive programming

Pros

The advantages of using Flutter is not only to the developers but also to the user as well. Since it speeds up the developmental process of the mobile application, while also reducing the cost of production. Development teams would greatly benefit from building an application with aesthetically pleasing UI with smooth animation.

- **Code Writing**
  - Mobile Application Development will be faster and dynamic
  - Making changes are more seamless through the process known as Hot Reload
  - Hot Reload is the process of editing code by updating code into source file while the Dart Virtual Machine stays running
  - Speed of Hot Reload is in the millisecond to run and test for development and experimenting
  - Design application made simpler and more comfortable for development process to improve for both designer and tester.
  - Less time and building, unlike other native application development which requires rebuilding to reset and experiment the application which can take minutes

- **Multiplatform**
  - Codebase can run on Android and iOS on the same code development
  - Does not need to depend on platform, such as iOS requiring MAC to develop applications
  - Built in library and widgets to create designs for application

- **Testing**
  - Multi-Platform allows developers to save time from running on different system
  - One codebase for an application will work the same on different platform
  - Process Quality Assurance is faster to maintain the level of desired quality of product for close attention to detail on every stage in development

- **Speed**
  - Functions in smooth and fast working environment
  - Seamless transition of mobile application to hanging and cutting while scrolling
  - This section can be further explained in flutter Technical View

- **Design**
  - Creating widget is made easier with library and customizing existing ones

- **User Interface**
  - Flutter can work with older platform while maintaining functionality of newer supporting system

- **Minimum Viable Product**

- MVP is the conceptual process when new product development learns of consumer needs and what requires satisfaction through feedback or collective status

Cons

The disadvantages of Flutter, since it is new in developing environment, support is not very abundant for this software Development Kit. While many libraries are yet to be implemented to Flutter, features are not fully available like any other SDK to develop applications.

- **Libraries and Support**
  - Not every functionality has been featured to Flutter as compared to native development
  - Developers would need to mainly use Google support in order to fully utilize beneficial libraries
  - Even without having full support of libraries like native development, Google has full libraries necessary to develop applications

- **Lack of Continuous Integration Support**
  - Flutter is not widely known compared to other continuous integration platform due to being primarily Google SDK
  - Custom scripts will be necessary to create application using Flutter because of libraries that might not exist at the time for development

Development of mobile application connects many technologies together, with Flutter, the advantages outweighs the disadvantages since it can well support business and development teams rather than having risk of lacking support. Developing applications with that functions with high-performance while maintaining to be aesthetically pleasing proves to be beneficial while it also runs faster than other SDK to develop such Android iOS platform

Hot Reload

This feature allows experimenting on building UI, fix bugs, updating from the source code to automatically make changes thanks to the Dart Virtual Machine to make the process possible. By using an application made by Flutter, editor or from a terminal line, this can allow modification of Dart files to make projects so long as IDE or editor in use is capable of supporting Flutter. This is especially helpful on rebuilding widgets in order to save time and reloading the source code. Hot Reload shows visible changes made from automatic execution of the application. It also has a feature that preserves the state of which the application enables the design to be viewed with the most screen changes. This is known as Stateful Hot Reload.

Widgets

Creating designs for application can make appealing user interface that can also function in efficient interactive experience that communicate well with data

management. Widget can make application accessible, take inputs, design layout, responsive routing, scrolling, visual behavior and display and style text. Instead of giving information, on the user screen with listing long and strenuous text that can be daunting to read. Since the dawn of smart phones, the idea of using icons to hold the data and application in place, allows simpler and organized access on screen while also saving battery life in the process. Designing widgets can be creative and exciting that brings emersion for the user. Some features of basic widgets are:

- Row: This feature can help organize the display window of an application in horizontal view
- Column
- Text
- Icon
- Button
- Container
- Padding
- Center
- Align
- Aspect Ratio

Firebase

Firebase is an SDK (software development kit0 with numerous capabilities that can create multiplatform applications all the while giving the develop test lab and crash reporting to diagnose errors. Backend side of the application can be supported much faster due to the abilities of having Realtime database feedback while editing the software, keeping the file storage, and hosting solution without needing external sources under the same SDK. Authentication to log user in is a simple process with minimal resistance. While implementing notification allowing cloud messaging, and index of the application can be seamless development process under Firebase. Testing new configuration does not need to take any delay from the user, since implementing new structure can be done in real time with a feature unique to Firebase, the Analytics feature, allows the application to be observed and insights on how components are working for developers and users. The Analytics feature is useful for giving statistics of how the application can be used, so that developers can use this information to either fix bugs or improve upon features. This SDK is proved to be useful for developing Android, iOS, and Web applications.

Realtime Database

This feature of Firebase SDK is as seamless process of using Realtime functionality of connecting to the database all while working on the improvement of the application, without the delay testing and running implementation process. Having Realtime implementation helps developers with faster improvement since it can be tested and run concurrently. This can also be beneficial while the chance that the application is offline, since Firebase allows storing and synching data in Realtime through web, mobile, or simultaneously throughout every platform at the same time. While being offline, the data is stored at a local cache on the device to serve and

store changes, so whenever the user gets back online, data that was stored on the local device gets synchronized to the database.

- **Realtime**:
  - This method works by data synchronization of every changes that occurs to any connected devices upon updates are made.
  - This is different from HTTP (Hyper Transfer Protocol) request that works by communicating between the client and server to response to changes.

- **Offline**:
  - The responsive of Realtime can still function by storing data to local devices while waiting to be available online, that way it begins synchronizing when ready.
  - Changes from one platform will synchronize with the database and update changes across every platform the data serves.

- **Accessibility:**
  - For being a multiplatform system, Firebase can be accessed directly from either mobile device or web browser without needing a server for the application.
  - Having security and validation for the data is still available due to Realtime synchronizing, the rules allow data to be read and written when it is executed.

- **Multiple Database**
  - Having scale of how much data can be a problem, but Firebase scales by splitting the data by having it stored across multiple database instances.
  - Accessing database can be better controlled and managed by Realtime for each database instance when authentication is required.

3.17.12 Bluetooth API

Firebase Communication to Microcontroller

Connecting the database to microcontroller using Firebase requires set of libraries that can be use in the Arduino IDE, which is a problematic process to setup and obtain connectivity. The setup process needs the database authentication key and the database API URL from the software side through either the web or mobile application, while on the hardware side, it is more than simply typing code into Arduino IDE to implement connectivity. The code will then allow communication from the database and the Arduino with the API URL of the host, database secret that sets up the authentication in the settings, can complete the process to successfully connect to the database.

The biggest issue is establishing communication of microcontroller with software application when developing internet or wireless exchange of data between devices. Methods can be implemented such as Bluetooth or Near-Field communication (NFC) to remotely accessing devices and database mainframe, methods such as HTTP (Hyper Text Transfer Protocol). While the communication process for device and software can be complex even for simple task. Google Firebase serves as the intermediary medium to allow connection. The use of Realtime database (explained in Flutter section of Realtime Database) provides simple development for application with Firebase SDK along with libraries for the microcontroller.

Creating application with firebase would be simpler than traditional database creation like MySQL, Firebase Database has data sorted while in the format of JASON which is an easier access for storing application data. Implementing new elements in Firebase is simply clicking the (+) sign on the top right from the screenshot below, which is available and seen from the Graphic User Interface (GUI) to allow minimal effort in changing elements and accessing the database that can serve as a huge time saving method for developers. While a new element is stored in the database, it becomes hash (giving a generated ID) so that the data transmit and receives to other devices while being recognized only during the exchange communication of designated interface.

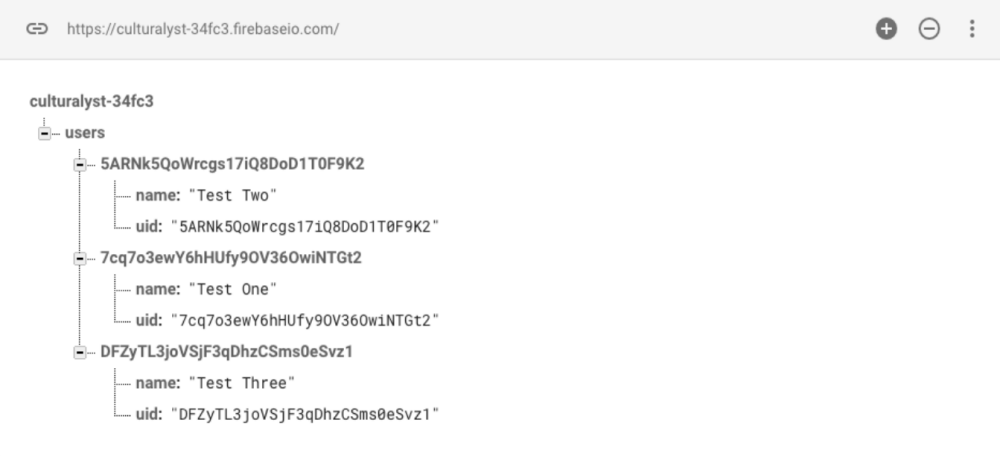
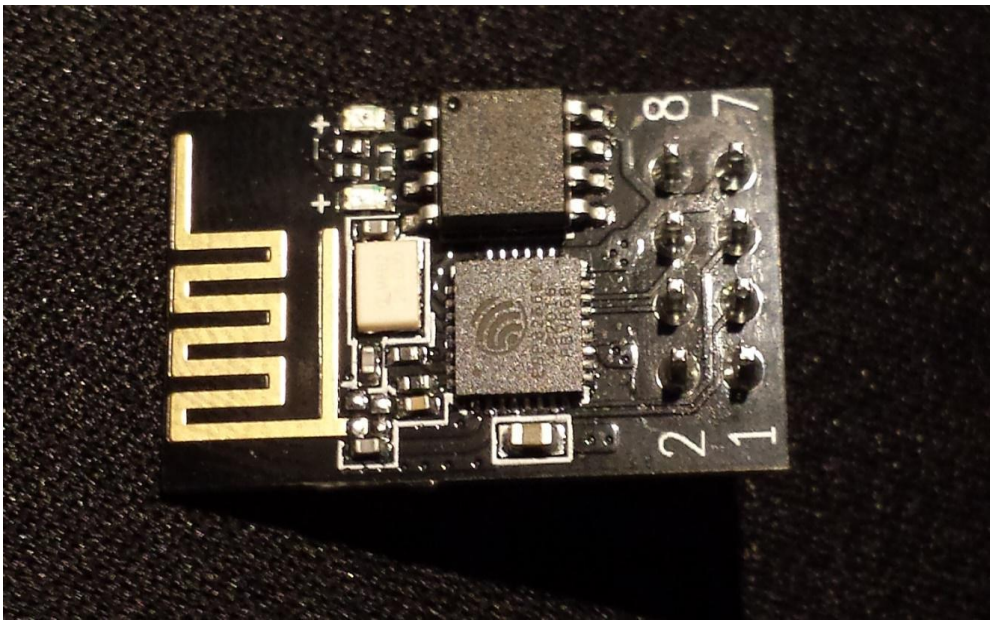


Figure 12: Implementing new elements

What makes this important in term of hardware is the implementation of the stored data that can be transmitted wirelessly, with the use of Firebase library and wireless device which is the Bluetooth module. Parsing data from the database can be done through C language along with sets of Firebase classes. Firebase Arduino serves as the main class to interact between the Microcontrollers and Firebase that can be complex through user cases and control but can be simple to design and implement

Establishing the communication with the Bluetooth to the mobile device requires both to be enabled for discoverability in order to have both be paired. On mobile devices such as Android, enabling the option to scan other device should display multiple devices and detect the Bluetooth module. Pairing request is send to the module from Android, and a pop-up option window will display on screen with password input.

This form of connection is based on models for client server that waits for connection request or send out the request to the server, meaning the Bluetooth device.



3.17.13 Wi-Fi Module Research

In order to send packets of data between the server and the door microcontroller, an 802.11 module is required. Designing one would carry a high cost in time, labor and funds. Therefore, the team looked into purchasing a self-contained Wi-Fi module. The ESP8266 has following pros.

- Extensive documentation
- Has small profile
- Contains a built-in-network stack
- Low Power Microcontroller to run it
- Built in voltage regulator
- Low unit cost

This Wi-Fi module is used in a lot of hobbyist microcontroller projects, which has let to a large amount of documentations and tutorials on its setup and operations as well as regular firmware updates for the network TCP/IP protocol stack included. The module itself is really small and will have no problems fitting inside the door lock microcontroller. The module that was given more preference has been discontinued in the favor of Wi-Fi modules with more powerful microcontrollers and the more GPIO pins, which drives the cost of this module down to under four dollars. The ESP8266 module is powered by 3.3V VCC. It has TX and TX pins to be used for serial UART communication with the main micro controller. The two-general purpose of input/output pins will not be used in the final design. The RST pin is used to reset the module and may be used for as a way to fix bugs related to the module that can be solved with a hard reset. The CH_PD pin is used for shutting off the module entirely to save power, but the Smart Lock design requires the ESP8266 to be in

sleep mode. While in sleep mode, an external interrupt can be used to trigger an interrupt and wake the module. The through- hole ESP 8266 module to be used during the initial prototyping can be seen in figure 13.

The manufacturer of ESP8266 provides firmware updates. These updates are available for download on their website. In order to update firmware, a USB to serial converter myst be utilized to serially communicate with a desktop computer. Using a terminal program such as Hyper Terminal or PuTTY, the commands to update firmware and network SSID and password can be programmed to the module. This is acceptable for the prototype version of the Smart Lock, but a more user-friendly way of connecting to a local area network must be developed for later versions.

Figure 14 Schematic ESP8266

The pinned ESP8266 may be ideal for early prototypes and troubleshooting. However, for a lower profile on the printed circuit board and for a cleaner final product, the surface mountable ESP8266 shown in figure 14 is more preferable. Like its pinned counterpart, the surface mountable ESP8266 has a full TCP/IP stack. It is it's own, self-contained, low powered micro controller that is capable of bringing the system our of sleep mode by receiving packets. This is perfect for a battery powered microcontroller where battery life is a chief concern. It is a Wi-Fi module designed for hobbyists, meaning that documentation is extensive. Also, the hobbyist target of this module has made the documentation exceedingly easy to read and comprehend. There are many tutorials available to help less experienced team integrate it into the final project.

While doing the research and in planning to develop the prototype of the Smart Lock system, the plan to implement Wi-Fi outlined above was found to be inadequate. The ESP8266 comes with built in firmware and an instruction set of AT commands that it can receive via a UART connection with the main MCU. These commands are at

times unreliable. This was discussed with other senior design groups that were considering Wi-Fi for their projects, one of the design team opted to abandon use of ESP8266 and switch to the development board powered by the ESP32.

This switch came with a couple distinct advantages. Firstly, the ESP32 development board has a built-in serial port. This allowed the programming to be done along with viewing its outputs on the terminal directly. Debugging a project involving communication with remote servers is much easier when outputs can be printed to a terminal and when the programming process is streamlined by built in features like a serial port. The second major advantage was power consumption. The ESP32 has an extremely low powered sleep mode consuming less powered sleep mode, consuming less than micro amps while asleep. This low powered mode was used in conjunction with a timer interrupt to wake up and poll the server after a certain increment of time.

Although, the ESP32 did come with some negative tradeoffs like cost, but the ESP32 development board cost roughly $12. This is four times more expensive than the ESP8266 that the group was planning on during the initial research. It is not a budget breaking expense, but still has a fair impact on the final per unit cost of the project. The second main tradeoff is size. The ESP8266 is relatively small piece of hardware, while the ESP32 development board would have increased the PCB size of the project by roughly 50%. Luckily, the ESP32 can function with the same pin connection allocated for the ESP8266. The PCB design at the moment is left unchanged and wires are soldered between the main PCB and ESP32 Wi-Fi module. This allowed to stash away Wi-Fi module wherever the size different would have less impact on the final look and the dimension of the project.

3.18 Mobile Application

To accommodate more mobile devices, the mobile application will be available in both IOS and Android devices. Both will be programmed in JAVA language and will have English as display language. The main user interface for both applications will be closely similar in a way that both mobile applications will have the same fonts, font size and placements of button and menus. Finally, both applications will be free to download from Google Play or Apple Store.

A further research is being done on developing the iOS. It costs around $99 to the total budget to make an iOS app. As for Android application, it is relatively easier to debug, cheaper to produce and it is open source, this makes problem solving much easier.

The integrated development environment (IDE) that will be used for the Android and iOS applications are Android Studio and XCode. Both IDE’s are available online and can be downloaded for free. In addition, numerous tutorials are found online that can provide information on how to start coding the application. With that being said, the cost of creating a mobile application will be almost free as it would still need to be determined if either of the application store require applications to be published and for the publisher to pay any fees.

After successfully installing the mobile application, user will be required to create an account which allows them to use their phone to access the door lock system. To Create an account, user must provide the following: a unique email address, user name and a password. If any of the three-information provided is not unique, another user has the same information, the user who is currently trying to make the new account will not be successful at creating it. After creating the account user must provide the information to their Smart Lock as it will be used as a connection between the two.

For both the mobile application be more user friendly, they would have to have the following standard designs such as fonts, font sizes, background colors and placement of button and menus. Despite the fact that the type of fonts, font sizes, and the placement of the menus are decided, The basic design of the main page of the mobile application on an iOS device as well as an android device. Additionally, both figures show a toggle switch for the unlock and lock button. It will be placed on the middle of the page for an easy access.

There will be total of three different types of fonts that will be used to allow clarity throughout the whole mobile application. The types of fonts that will be used are fonts that are simple and are certainly readable by the users. Combination of different front size will give priority to the information being presented for example the important that information, the bigger the font of it.

Regarding the color of the fonts and the background colors everything will be standard and are neutral. Text colors will definitely be in the dark shades like black while the background colors will be in neutral shares. They would give good contrast between the text and the background color resulting in higher resolution. Giving more clarity to the texts.

With regards to the placements of the buttons and menus, the main lock/unlock toggle switch will be placed on the center of the screen to allow easy access. Important information will also be on the same page as the toggle switch such as the status of the lock and the timer.

There will be two features included in the mobile application that will benefit the users when verifying what is the status of the door. First is the real time Lock Status feature, which will be placed right underneath the toggle switch, it will display whether the door is locked or unlocked. The last feature is the push notification feature, which needs the user’s confirmation to be able to use it. To turn it on, the user will have to click the three horizontal bars located on either top right or top left of the screen

After checking it, a drop-down menu will appear and an option that displays notification will be listed. User must click the notification menu to go to the notification page where they can turn on or turn off the push notification. Once that is set to on then the user will start receiving information whenever the Smart Lock has either locked or unlocked someone. As mentioned before, the notification is omitted

to the design, nevertheless, a popup message will appear every time the unlock/lock button is pushed. It will have the name of the user who did the action and when the action was sent to the server.

Both mobile applications will have to be connected to the internet to be able to have the application communicating to the Smart Lock. Failing to connect to the internet will prevent both Smart Lock and the mobile application from sending and receiving signals to one another. A poor internet connection may also result from the situation previously mentioned or can delay the Smart Lock and the mobile application from sending or receiving signals to one another.

One of the problems that was discussed when designing the push notification feature is that user can spam the Smart Lock and can lock or unlock or vice versa, the door in a short period of time, which would result to multiple notification being sent to the mobile application. In order to not have this problematic situation, Smart Lock would wait five seconds after the last activity to push the notification to the user. With that being said the last activity will be one that will be push instead of all the activity within that five second window

Server Design

One of the key features of the Smart Lock is it's 802.11 integration and the ser's ability to access the lock's status or interact with it from any distance over the internet. Such a feature requires a remote database be connected to a hosted server for both the door lock microcontroller and a mobile application to interact with Any door lock must be in constant communication with the server to be able to feed its status and receive instructions. As stated previously, the server will utilize a LAMP stack (Linux, Apache, MySQL, PHP) and will be self-hosted by the design team. A visual representation of the network stack**.** This stack was chosen because it is extremely prolific, with nine out of ten of the top websites using this stack. Such proliferation of a standard has led it to be extremely well documented, errors are patched in quickly, and debugging resources can be found with ease. In addition to the extensive documentation, members of the design team have previous experience setting up this stack, which makes it an obvious choice.

To briefly explain the functionality of a LAMP stack, all the server programs run inside a Linux kernel. The Apache web server acts as a network listener and the network stack. The database, in our case, will be MySQL for reasons outlined below. Server-side scripting is done using PHP. These scripts allow for the communication between the database and the web server.

The team will be self-hosting the server. This will both cut down on the final cost and ensure there is no dependency on an outside organization's services for a small upfront cost and low maintenance cost. The server hardware required for the prototype version of the Smart Lock is not process, storage or bandwidth intensive enough to justify outsourcing the server. The bandwidth overhead of the mobile application portion of the Smart Lock is expected to be extremely small, with only a

few JASON packages being sent with every operation of the lock, so residential internet speeds and latency should be acceptable.

As with other aspects of this project, when it is time to implement the server portion, better sending options presented themselves. The server API Smart Lock system was implemented using the Node.js with Express framework and a MongoDB database. The decision to switch framework was not based on any difficulty or roadblock the team had with implementing a LAMP stack, However, the decision to switch was based one team members skillset. Between beginning the project design and implementing any part of the design, one team member worked on a project writing Node.js back ends for mobile applications. After sending a large amount of time gaining proficiency in the Nodejs with Express framework. It seemed silly to develop the back end for the Smart Lock using a LAMP stack.

The decision to switch frameworks was based on more than just familiarity. Nide.js is an emerging framework that is quickly joining popularity. It is incredibly powerful and scalable. The node package manager contains many different useful packages that add features to the framework such as an error logging, unit testing, data validation, and much more. For API, Joi for data validation is used. Joi acts as a line of defense to stop bad data from querying the database. If a bad request is sent to an API endpoint Joi will allow us to catch the bad request and kick it back to the front end before anything is queried or posted. This is very useful for maintaining a stable server. However, no API is perfect, and something bugs or holes in programs are overlooked. We implemented Winston as our error logger for this reason. With a middleware function that catches all uncaught expectations and by using Winston to log those errors to a file, a robust API can be made. It is equivalent to having the whole API inside of one big try/catch block. If an uncaught exception can be logged to a file so the team can patch the code causing the exception in the future.

Server API

Sever side scripting will be done using PHP, which is short for Hypertext Preprocessor. It is one the most widely used server-side scripting languages and complements well with Linux, Apache and My SQL. Each of the following paragraphs represent a PHP file present on the server to be called to fulfill their described function. These PHP files present on the server to be called to fulfill their described function. These PHP files are to be called by one overall index.psp. As the Smart Lock is secure device, security from attacks is a large concern. JASON packages sent between the mobile application and the server must be encrypted. User password must be hashed in the User's table. The mobile application must be given a method of verifying if a user has permission to be viewing the information, he/she is requesting.

Create account: The user is able to create a new account using the mobile application. LoginID, user email and a hashed password are received by the server via JASON. A new table is created for that user account. If account creation is successful, a confirmation message is sent back to the application in a JASON. If

unsuccessful, the appropriate error message is sent instead i.e. LoginID already exists, internal server error etc.

Verifying login: Login verification is done by the user sending the LoginID and hashed password via a JASON payload to the server through the mobile application. Access to the rest of the application is contingent on a successful login. Once the login info is received, the script checks the database for accuracy and respond s appropriately. Either, access is allowed to the rest of the application that the user has permissions for, or the appropriate error message is returned via JASON package.

error messages for ‘LoginID does not exist’ and ‘incorrect password’ as well as any possible server errors.

Add lock to account: All manufactured locks will have a unique idLock. The database will be preloaded with a table for each lock. A section of the mobile application will allow the user to associate a lock with their user account using this unique idLock. As with the other sections, A JASON of the uderID and LockID will be received by the server, which will then create an associative table between the two in the database. If the lock was added to the account successfully, it should appear on the mobile application home screen for the user.

View status of the lock: In order to populate the user’s home screen with locks associated with their account, the PHP script will search the MYSQL database by LoginID for UserLockAssociation tables with that particular user’s identification. After all the locks associated with the user are identified, their status can be found in the table for each lock. These names and statuses are sent to the mobile application with JASON payload.

Change lock status: When a change lock status requests is received from the mobile application as a JASON, the server must complete three operations:

- Change the status of the lock in the Lock table.
- Send instructions to the lock.
- Send the confirmation to the mobile application.

All lock should have their own threads open with the server at all times. So, its simple a matter of sending a JASON to the lock microcontroller an acknowledgement that the operation was successful should be received back from the microcontroller or an error message if the operation failed. Failure could include the lock not being found or the door sensor not opening the door. After the acknowledgment, or error message is received by the server, it is sent to the mobile application.

Database

The database will be created using MySQL and it is open source and has extensive documentation, allowing for a shallow learning curve. It is extremely prolific. Major websites such as Facebook, twitter and Wikipedia rely on MYSQL. MySQL performs well at all scales, so if the prototype were to be put into production, the database would not suffer performance issues from having more users or locks added,

The database for the prototype will only have one lock, the back-end software is to be designed as if there were thousands of locks, allowing for expansion of the product.

The database will consist of four separate tables. The users table fields have a one to many relationships with the UserLockAssociation table and has different values unique to each user, a unique user ID, a unique LoginID, a user email and a user password. The lock table only contains its unique ID and the current status of the lock. Since one user can have many locks associated with their account, and one lock can be associated with many users, an associative table between the two is very necessary. The associative table's fields are simple its unique primary key and the two foreign keys of the User and Lock creating the relationship between them. It exists for the server-side scripting to compile a list of all the locks associated with a user account to verify which locks the user should have access to. When the user triggers an unlocking evet through the mobile application through the webserver an event table is created with fields for the time, date, and user that triggered the unlocking event. This event table is used to keep a log of all users interactions with the lock that occur through the mobile application.

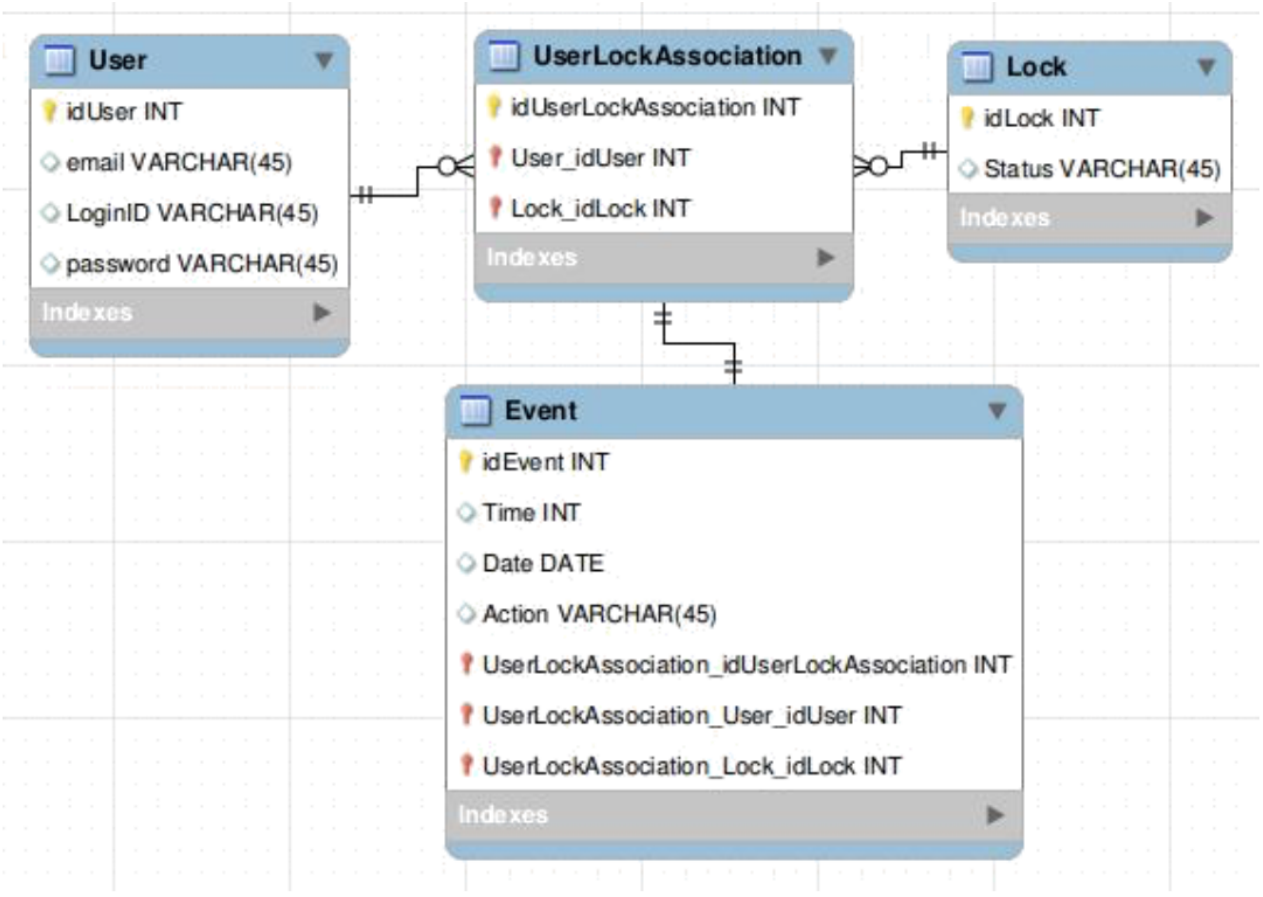


Figure 26: Entity Relationship diagram for MySQL database to be stored on the server

While building the back end for the Smart Lock project, MongoDB would be used in lieu of MySQL. Generally, with Node.js framework, noSql database are used. MySQL

is fully supported, but the standard is to use NoSql because there are no large dependencies on associations between database entities (there is just the user/lock association) it was very simple to use NoSql database and draw the associations manually by adding ObjectIds inside of the User and lock models.

4 Standards and Design Constraints

A crucial component of our project goal is to ensure that our product meets the industry standards and design constraints. Standards are important because they provide a set of guidelines that a project should meet to ensure safety and high quality. By recognizing and implementing features in accordance to the standards we can ensure that our smart lock is safe to use for our customers and will last a long time. Also, in knowing what our limitations are due to measures applied to meet our standards, we are able to inform our customers so that they help protect the equipment and prevent any harm to themselves.

4.1 Standards

Standards with respect to electronic devices such as PCBs are usually defined by professional engineers and scientists who have performed tests and research to create a set of guidelines that limit the use and application of the product in order to ensure safety of use. One notable commission that places standards on electronic devices is known as the International Electrotechnical Commission (IEC). The IEC creates and publishes various standards for electrical devices to help protect, synchronize, and set global policies for current and future electrical technologies.

4.1.1 Standards of Electricity

Electricity and water are two that cannot exist together. To ensure the safety of all electronic products, there exist safety standards to protect the end user. The outside of the smart lock is composed of plastic and houses all of the electronic components so that they are not exposed to water. Also, electrical wires are housed neatly inside

of the enclosure to prevent any exposed wires from being touched by the user or exposed to the elements. In the event that there is an electrical problem caused by either elements or user misuse, electrical relays are used to prevent power surges from occurring, which could potentially ruin the smart lock. A power surge occurs when a high quantity of voltage or current flows through the system which exceeds the operating standards for the electrical components receiving power. Relays are a blockage that prevents the system from overheating or short-circuiting during the event of a surge. Rather than replacing the entire circuit board after a power surge occurs the end user would only need to replace the blown relay. This makes repairing the system much more cost effective allowing us to supply a long-term warranty for our product.

Standards such as the ones we are deploying to ensure product safety are often created by organizations such as the IEC. They are known for devising standards to prevent safety hazards, equipment failure and misuse as well as worldwide compatibility. In the article, ANSI/IEC 60529-2004 published by the IEC, we obtain the classification of the degrees of protection provided by enclosures of electrical equipment for two conditions. These conditions are to protect persons against access to hazardous parts and protection of equipment against exposure to foreign objects and the second condition is to prevent exposure of water to electrical components. To determine the degree of safety for an enclosure, the IP code table may be used. This table lists the degrees of protection. Products rated based on this table obtain an IP code based on their rating. An example may be IP 20C, which signifies the product has a degree 2 – protected against penetration of solid objects having diameter greater or equal to 12.5 mm and protected against direct finger contact while offering no protection towards liquid damage and protection for persons using a 2.5 mm too during repairs.[80]

Furthermore, the 1st characteristic numeral corresponds to protection of the equipment against penetration of solid objects and protection of people against direct contact with charged parts. The 2nd characteristic numeral corresponds to protection of the electrical equipment against exposure to water with harmful effects. Finally, the additional letter corresponds to protection of people against direct contact with live parts.

Table 7 IP code 2 Characteristic Numerals

IP Code - 2 Characteristic Numerals		
1st Characteristic Numeral		
Degree	Protection of the Equipment	Protection of per

		sonnel
0	Not Protected	Not Protected
1	Protected against penetration of solid objects having diameter greater than or equal to 50 mm	Protected against direct contact with the back of the hand (accidental contact)
2	Protected against penetration of solid objects having diameter greater than or equal to 12.5 mm	Protected against direct finger contact

3	Protected against penetration of solid objects having diameter greater than or equal to 2.5 mm	Protected against direct contact with a 2.5 mm tool
4	Protected against penetration of solid objects having diameter greater than or equal to 1 mm	Protected against direct contact with a 1 mm wire
5	Dust protected (no harmful deposits)	Protected against direct contact wit

		h a 1 m m wir e
6	Dust tight	Pro tec ted ag ain st dir ect co nta ct wit h a 1 m m wir e

2nd Characteristic Numeral			
Degr ee	Protection of the Equipment		
0	Not Protected	A	With the back of the hand
1	Protected against vertical dripping water (condensation)	B	With the finger
2	Protected against dripping water at an angle of up to 15 degrees	C	with a 2.5 mm tool
3	Protected against dripping water at an angle of up to 60 degrees	D	with a 1 mm wire
4	Protected against splashing water in all directions		
5	Protected against water jets in all directions		

6	Protected against powerful jets of water and waves		
7	Protected against the effects of temporary immersion		
8	Protected against the effects of prolonged immersion under specified conditions		

Our enclosure has an IP code rating of **IP 44A.** This means that the smart lock is protected against penetration of solid objects having diameter greater or equal to 1 mm and protected against direct contact with a 1 mm wire. This means that no physical objects can enter the enclosure except for small dust particles. Our

enclosure is also protected against splashing water from all directions but will not be protected against water jets. The unit will also be safe to touch with the back of the hand, which is necessary to operate the smart lock even when conditions are wet outside.

4.2 PCB Standards

The Institute of Printed Circuits (IPC) is a trade association who standardizes the assembly and production requirements of printed circuit boards (PCB). It was first founded in the year 1957 and since then has been publishing global standards in the electronics industry. The IPC is responsible for creating standards in the areas of design, printed electronics, printed circuit boards, electronic enclosures, assembly, and embedded technologies.

All PCB made for commercial use are required to meet the IPC standard for circuit boards better known as **IPC-2221**. There are three different classes of standards in relation to PCB design. The first class deals with general electronic products including computer and computer peripherals such as the ones used in general military hardware applications. Class 2 is for dedicated service electronic products including communication equipment and high performance military equipment. The last class deals with high reliability electronic products. This class includes products that require a high degree of performance and reliability where equipment downtime cannot be tolerated such as with life support equipment and critical weapons systems.[79]

4.2.1 Class One

Most consumer bought electronic products fall under class one. Class one standard electronic items are those, which are mainly concerned with functionality rather than reliability and performance. Inclusively, some of the items used by the military such as personal computers are commonly class one products.

4.2.2 Class Two

Dedicated service electronic products fall under class two. These electronics not only focus on functionality but also must have high reliability and durability. While uninterruptible service is preferred occasional failures are acceptable. One important note is that the environment must not impose a failure on the functionality of the product should it be deemed a class 2 product.

4.2.3 Class Three

High performance electronic products are of the highest class. Class 3 products contain all the characteristics of class 2 and in addition, must work exceptionally well in harsh conditions such that equipment downtime are intolerable. These products

have the strictest conditions because they are used to save or protect lives and their failure would inherently cause human casualty. Class 3 products are generally found in military and medical applications.

4.3 Power Supply Standards

One of the major safety standards in the industry of electronics deals with power supply standards. The international Electro technical Commission (IEC) and the Associated International Organization for Standardization (ISO) are two of the principal agencies that deal with electrical safety standards. If a product meets an IEC standard as an example, IEC 62368-1, then it protects users from hazards such as electric shock, fire, dangerous temperatures, and mechanical instability. IEC 62368-1 deals with main or battery-powered information technology equipment and office machines with a rated voltage does not exceed 600 volts.[81]

4.3.1 Classes of Equipment

There are three classes of equipment that fall under the IEC 62368-1 standard. Class 1 equipment protects users from electric shock through basic insulation measures and protective earth grounding methods. To achieve this, all parts that can hold a hazardous amount voltage are connected to a protective earth conductor. This is so that in the event that the basic insulation protection fails and live wires are exposed, the end user will not be shocked. Class 2 equipment does not require earth grounding however the wire insulation used is twice as thick to further protect from accidental cable exposure. By doubling the insulation the odds of tearing through it are much less and therefore lessons the risks of electrocution. The highest standard is class 3, which is for equipment that operates at extra low voltage, which prevents hazards due to electric shock. By operating at very low voltages there are no dangers should someone become exposed to live wires.

Table 8 Classification of Energy Sources According to Potential for Injury

Classification of Energy Sources According to Potential for Injury		
Energy Source	Effect on the Body	Effect on Combustible Materials
Class 1	Not painful, but may be detectable	Ignition not likely
Class 2	Painful, but not an injury	Ignition possible, but limited growth and spread of fire
Class 3	Injury	Ignition likely, rapid growth and spread of fire

4.3.2 Hazardous and Extra-Low Voltage

For a voltage to be considered hazardous, it must exceed 42.2 Vac peak or 60 Vdc without a limited current circuit. Conversely, if a circuit is extra-low voltage (ELV),

then the voltage going through the circuit must not exceed 42.2 Vac peak or 60 Vdc and the circuit must be separated from hazardous voltages by at least basic insulation.

4.3.3 Limited Current Circuits

Limited current circuits are those that are considered safe for operator access given that they have very low output power. The current that can be drawn from the circuit must not be at hazardous quantities, which defined as follows:

- If frequencies are less that 1 KHz the steady state current must not exceed 0.7 mA peak ac or 2 mA dc. If the frequencies are greater than 1 KHz, the max current limit is 0.7 mA multiplied by the frequency in kHz but shall not surpass 70 mA.

- Any parts accessible to the end user with voltage not exceeding 450 Vac peak or 450 Vdc may have a circuit capacitance of no more than 0.1 uF.

- Accessible parts to the end user with voltage not exceeding 1500 Vac peak or 1500 Vdc may have a max stored charge of 45 uC and the total energy must not exceed 350 mJ.

- The circuit must also meet the same rules as Safety Extra-Low Voltage (SELV) circuits.

4.3.4 Limited Power Sources

Limited Power Sources **(**LPS) are limitations on output voltage, power, and short circuit current limits. This limitation also sets requirements for wiring and the loads supplied by LPS certified power supplies. These power supplies must have either internal power limiting features or external components that limit the current that is delivered to the load. There are several ways to limit the internal power, below is a list of the various ways possible:

- Limiting power during construction of the power supply such as by winding resistance of the transformer.

- Implementing a linear or non-linear impedance such as by using a PTC resistor.

- Using a regulating network such as implementing voltage regulator control chips.

For external devices limiting current to the load can be achieved by using circuit breakers and fuses such as those used in home electrical systems. If circuit breakers are used, they must be of a fixed rating that cannot be manually adjusted and cannot automatically reset themselves after being triggered.

4.3.5 Insulation and Isolation

There are five types of insulation to protect live wires that have hazardous amounts of voltage from having contact with other components and wires on the circuit. The use of each of these types varies depending on the needs of the classification of the equipment. The greater the classification of the equipment the higher the order of insulation and isolation that is required. These types are listed from least protection to the highest degree of protection.

1. Operational and Functional Insulation

   Meets no specific standard and is merely there for the correct functionality of the equipment.

2. Basic Insulation

It is the minimum standard for insulating live wires to provide minimal protection against electrocution.

3. Supplementary Insulation

This is an extra layer added on top of the basic insulation to provide additional protection against electric shock. This layer is great as it improves the longevity of the equipment.

4. Double Insulation

This type of insulation is used for class 2 equipment. It is substantially better than the basil insulation and ensures that the end user will be protected from shock while not requiring additional grounding.

5. Reinforced Insulation

Similar to double insulation, this type has the same thickness as double insulation but rather than having a tubing over another to have *double insulation* this type is one single layer but of greater thickness such that the thickness of reinforced insulation is the same as double insulation.

For most power supplies, the minimum requirement for insulation is as follows. For primary to secondary power supplies, reinforced insulation with a dielectric strength of no less than 3000 Vrms is required. For primary to ground power supplies, basic insulation may be used with a dielectric strength of 1500 Vrms or greater.

4.4 Legal Standards

For consumer products intended for use in the United States, there are several federal agencies that are responsible for setting regulations pertaining to electrical and electronic products. Each agency covers its own respective scope and together their purpose is to ensure that all electronic products sold to the public are deemed safe for use. Table # lists the agencies and the regulatory scope that they govern.

Table 9 Federal regulatory Authorities and Technical Regulations

Federal Regulatory Authorities and Technical Regulations	
Agency	Scope
Consumer Product Safety Commission (CPSC)	Products for use by children, hazardous substances, labeling of hazardous products, and consumer product safety
Customs and Border Protection (CBP)	Country of origin for most imported products
Environmental Protection Agency (EPA)	Energy ratings and toxic substances
Federal Communication Commission (FCC)	radio communication frequecies and digital electronics
Food and Drug Administration (FDA)	Food contact substances and medical equipment
Federal Trade Commission (FTC)	Labeling and environmental standards
Occupational Safety and Health Administration (OSHA)	workplace safety and testing

Together, these federal agencies make sure that all products sold in the United States comply with all of the legal standards. Failure to comply with any of the standards set in place by the above federal agencies may result in penalties, removal of products from the market, and possible criminal sanctions for those involved in cases that involve the death of human life.

4.5 Comparison of 802.11 Standard

The Smart Lock will allow the user to lock/unlock the lock or see its status using mobile application through the internet. For this, to be accomplished, the lock PCB will need a Wi-Fi module, which is capable of communicating with most home networks. There four main 802.11 standard in use home networks today.

All 802.11 standard releases are backward compatible with previous releases, meaning that any older standard used in our design will still be compatible with

wireless networks using the newer standards. However, if we were to select standard such as 802.11AC wireless networks older than 2013 would not be compatible with Smart Lock.

Every current standard has an acceptable range for the purpose of our design. The benefit of the double range 802.11N would be negligible for both the prototype or the marketed product. The majority of the population will have their wireless router within 125 feet of their door. Most 802.11 standards operate on 2.4Ghz, which is an unregulated frequency and very prone to interference from other home devices such as microwaves. Using these 2.4 Ghz frequencies in a design would mean possible packet losses that need to be compensated in software. For the purpose the design, any of the current standards have enough data rate. The Smart Lock will only need to send small Jason payloads, meaning network speed is almost irrelevant. Passive power consumption is one the largest concerns in our design and the higher 5Ghz frequencies of 802.11AC and 802.11N will mean a higher power consumption with little tangible benefit.

4.6 Mobile Application Standards

Mobile application had become widespread in global market for software and technology for consumer usage and innovative design and as part of core modeling to develop application now available on small devices, standard are set to create a universal understanding on how mobile devices function. Great potential can be achieved through mobile devices that allowed user access to web, app, planner, media and information that can support daily life, while developers can expand the capabilities and enhancing cross device design. Standards can be set in principles, interfaces, patterns and guidelines to developing mobile applications.

4.7 Principle Application Standards

The overall Principles can be numerous ways to create a platform that can document and function natively with individual operating system on each device. Mobile platform can greatly benefit consumer to allow a system that create an experience to unify others with an ecosystem to support. Other platforms can also support a unifying experience with its own ecosystem, with the day to day usage of devices enhancing user to fully utilize such feature, the mobility of a small platform that goes straight into pockets makes convenience the key leverage to the capabilities. While mobile devices can be identifying as a phone, application can exist in a cross platform to scale functionality among ecosystem created with similar experience. The overall principles can be broken down as following:

- **Platform**
  - An important factor is documenting the necessity such as the pattern and components that comes in the native operating systems in the application such as Android and iOS

- Designing platform that is native to the device should remain consistent with the operating system and guidelines to focus on optimal quality
- Native operating system to the platform can improve and evolve with new guidelines to enhance interface

- **Benefit**
  - Importance of consumer needs is to prioritize focus in developing mobile application that offers capabilities to support day to day needs
  - Designs should be able to bring together multiple user to unify an experience with an ecosystem across any device
- **Device**
  - Device should capabilities such as locking, unlocking, receive a picture from the camera etc
  - The design of the application should revolve around being able to be utilized on the device that can benefit not only the screen but beyond that
- **Scalability**
  - Mobile device can go beyond than just a phone that can talk and text. Modern phones can search through the web applications to plan and schedule, gaming platform, media for music, video and much more
  - Capabilities on the phone can also be scaled on tablets with the same features and if not more, and grow beyond simple screen usage
  - Although challenges can be met by scaling interface between web and tablet design of the patterns and guidelines
  - There can be similarity between mobile devices and full web applications on a computer that proves to be difficult to be used similarly

4.8 Interface platform Standard

Another challenge met by developers is the compact and small size of phones which are typically less than 7 inches, that can only display more limited amount of information and screen usage as compared to the web on a computer. To compromise with the smaller size display of mobile devices, the fundamental design must include primarily the necessary information for users to search and view so that the device does not overload. Since mobile devices are the most convenient platform to access information for users, it can also be useful device for business to quickly access and continue work that the user is not usually readily available at an office.

Other than phones, another mobile device would be a tablet, which are greater than seven inches of mobile display for the user interface that would allow more space for design and usability. While alignments do not have to be the same from tablets to phones, having larger interface display would greatly benefit by having more information for the fundamental design to include in the platform. While tablets have the designs that tend to have an experience similar to desktop to search the web plan and schedule, workspace and media, which is also available on phones, the main functionality of tablets can be considered as a hybrid device.

4.9 Pattern and Guidelines Standard

Mobile applications have design. Patterns that follows to fit on small platform to navigate through content while feeling quick and easy to use, simplicity should be the key factor in creating applications. Navigating content should have transition phase to display through applications to feel smooth and organize without feeling cluttered and disarrange.

4.10 Industry Implementation Standard

Establishing set of rules and guidelines for platform to follow becomes a universal practice for industries to develop mobile applications while also evolving on new and inventive ideas for technology of the software. There multiple set of standards the industry implements.

- **Visibility and Timing**
  - Notification is an important feature that allows user to view information is provided in application to be relevant for the framework.
  - Accessing data also collects and transmit important application features while prioritizing user accessibility with privacy
  - Sensitive information such as financial data will be held accountable on the company to provide and ensure secure utilization

- **Security and Data Retention**
  - Importance of security in transmitting data must be for legitimate purpose and should be access in the application only unless it is required to do so
  - Sensitive information should be given as an option that lets the user to allow their data to be collected to avoid risk
  - Developers must implement this option in order to avoid danger of data being leaked to give users security in experience
  - Rules and regulations must be met for developers to publish the application that follows the application store and platform terms and services
  - Sensitive data must be stored on a time frame where it has the chance of being deleted after user no longer needs data stored in server
  - Respecting the user privacy keeps their interest in the service of the application with procedures holding accountable of private information
  - De-Identification is another solution to ensure security of data by deleting previous data to reestablish identification by hashing and linked back to original source of ser or device.

- **Enabling security measures**

- Applications are susceptible to security risks of accessing or transferring data from individuals to another that requires careful attention
- Testing and solutions must be taken for security measure for implementing retention policies for safeguarding data

- **Data Encryption**
  - Encryption data allows authentications of the user personal data through transmission to provide protection
  - Proper utilization of server by avoiding SSL/TLS and other forms of communications of transmitting data
  - Sensitive information such as email, address, username, and password, must be encrypted to maintain authentication

- **De-Identification**
  - Like encryption, changing identification on multiple efforts makes it difficult for data to be at risk since it does not link to particular result
  - Numerous identification elements require scrambling encrypted data to have comparable link to that element
  - This method ensures higher security measures to terms of privacy to avoid possible risk while maintaining retention

- **User Authentication**
  - Logging in the out require authentication of the user by inputting either email, address, username, and password for session with validation.
  - Implementing mobile client to ensure validation of the user to access their data from the server database where it is stored with sensitive encryption protocol

- **Accountability**
  - Logging in and out requires authentication of the user by inputting either email address, username, and password for the session with validation
  - Implementing mobile client to ensure validation of the user to access their data from the server database where it is stored with sensitive encryption protocol

- **User feedback**
  - Maintaining good relations with user can be provided by having feedback for opportunities to improve flaws of bugs of the application
  - Companies gain positive note from questions, contacts, queries, or complains of application interface and usage
  - Fixes and patched can follow from feedback to highlight functionality to bring more efficient solution

4.11 Economic & Time Constraints

The economic constraints mainly consist of cost of parts and out of pocket expenses like food and gas. The time constraints come from family and other responsibilities, the time it takes to manufacture and deliver parts, and the deadline for the project completion.

4.12 Safety Constraints

Safety constraints are considered because the Smart Lock's power source will be able to deliver 2 amps of current, so redundancies are considered to contain high current anomalies. Electromagnetic energy will be emitted from the RFID reader/writer and according to the FDA, RFID devices can cause malfunctions in pacemakers [36], so the proper warning will be placed on the device to avoid exposure to anyone with a medical device that is susceptible to radio frequency devices. The smart lock will not contain any dangerous liquids or chemicals. Constructing the container for the Smart Lock may pose a few health risks. The use of power tools and laser cutters could be dangerous if not handled properly so precaution will be taken during the construction.

4.13 Presentation Constraints

Fort the presentation, the Smart Lock system will operate on a battery source so there is no constrain on the location of the presentation, however for the facial recognition system to work, adequate lighting must be available. This puts a constrain on the conditions of the presentation as it must be done in a well-lit area for proper facial recognition functionality.

4.14 Energy Constraints

The energy constraints are minimal due to the fact that the Lock mainly operates at logic level. The energy constraint comes in the form of power use. The Smart lock system will be programmed to put the sensors and display in low power or power down mode while the system is idle in order to reduce the energy demand of the system. Much effort will be used to ensure that the Smart Lock is energy efficient.

4.15 Ethical Standards

Having proper ethics is a very important aspect of being an engineer because ethics must be applied in the design of any technology and its application. The Institute of Electronic and Electronics Engineers has a code of ethics that serves as a standard for many engineers, which is,

1. to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, and to disclose promptly factors that might endanger the public or the environment;
2. to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
3. to be honest and realistic in stating claims or estimates based on available data;
4. to reject bribery in all its forms;
5. to improve the understanding by individuals and society of the capabilities and societal implications of conventional and emerging technologies, including intelligent systems;
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;
7. to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
8. to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;
9. to avoid injuring others, their property, reputation, or employment by false or malicious action;
10. to assist colleagues and co-workers in their professional development and to support them in following this code of ethics. [32]

The safety of the engineer, the consumer, and the environment should always be considered when designing or developing technology. In a world that is being transformed by technological infrastructure that is growing in complexity and connectivity, engineers hold enormous power. Engineers control the machines that operate the modern world, therefore are endowed with an enormous responsibility. An engineer that does not have a code of ethics could put themselves or others in danger.

In a world with increased and growing surveillance capability, many devices have the ability to record information about people. This information can be very intimate to an individual and could be used to harm, discriminate, extort, or persuade them. It can also be a form of illegal surveillance if this information is used for anything other than its intended uses. Ethics must be used when developing or operating technology that is capable of collecting information about its users. In the case of the Smart Lock, will have the ability to record the fingerprints and data from the facial features of an individual and store it in a data base. We have a responsibility to protect the data collected from its users from theft. We are also responsible for demonstrating proper ethics by only using the data for its intended purposes.

Ethics in school takes the form of academic honesty. Students are taught how important academic honesty is because it is the pillar that is built on well into one's professional career. The senior design project is one of the first major applications of ethics as a student transitions from an academic to a professional environment. In

the professional environment many issues regarding ethics exist such as plagiarism, theft, and not owning up to mistakes. It is essential than an engineer has a good code of ethics in order to navigate these issues.

4.16 Environmental Standards

The environmental impact of manufacturing the Smart Lock system is researched and applied to designing a product that has a minimal effect on the environment. The Smart Lock will operate on a rectified AC source and will only use a battery as a secondary source of power. This battery will rarely need to be replaced and will only serve as an indicator when the main power source has failed. Biodegradable materials will be selected, when available, when printing and machining the body of the Smart Lock system and no harmful chemicals will be used.

4.17 Quality Assurance

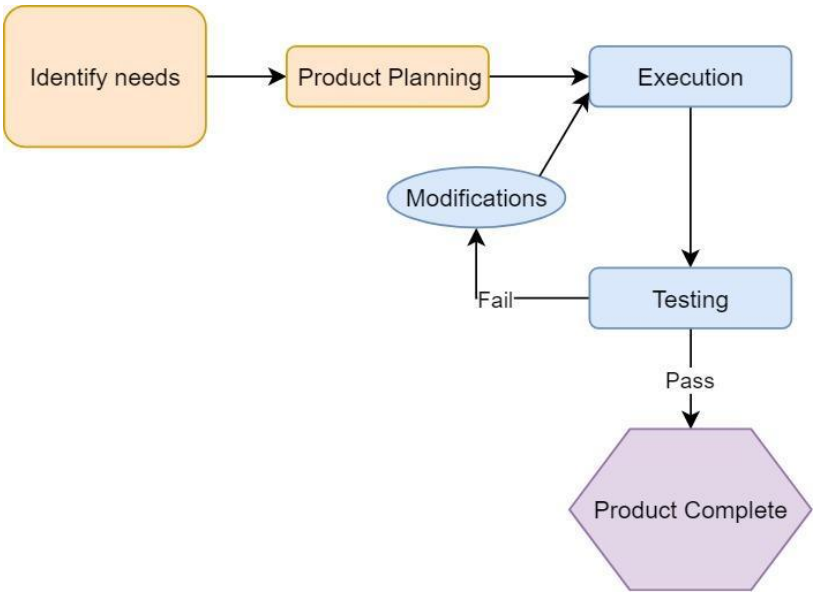


Figure 15 Quality Assurance Flowchart

To maintain the desired level of quality in the product, quality assurance will be implemented as shown in Figure 24. First the desired functionality of the Smart Lock is identified. A detailed hardware and software plan is deducted and implemented. Each section of the Smart Lock that is completed will be reviewed and vetted for errors by another engineer. After the construction and programming is complete, a series of hardware and software tests will be performed to ensure proper functionality. Errors during the test will be used to implement modifications to the hardware or software. Once the changes are implemented, the testing procedure is done again. The product will only be considered complete once it can pass the testing procedures without error.

5 Hardware and Software Design Details

The Hardware and Software design details show the Smart Lock's electrical connectivity and software flow. Each of the modules are connected to the smart lock using a communication protocol. The Smart Lock schematic as shown in Figure 4 details the electrical connections that will be realized on the printed circuit board.

5.1 Hardware Design Details

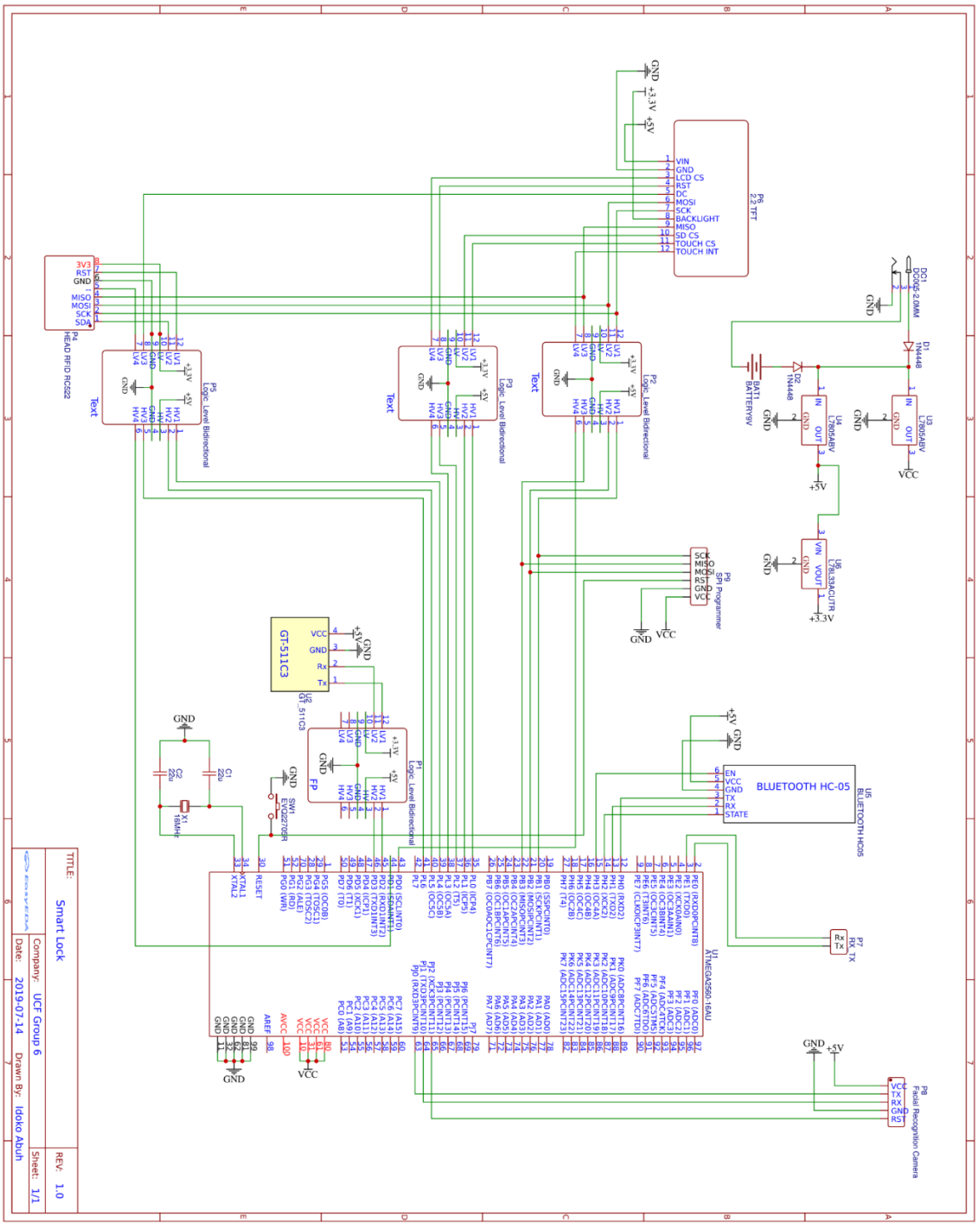


Figure 16 Smart Lock Hardware Schematic

The power circuit begins with a barrel jack connection that is supplied by a 9-volt 3 Amp external supply as its primary supply, and a 9-volt battery as the secondary supply. To separate the external supply voltage from the battery voltage, two diodes are used. One diode is place after the external voltage and the other diode is placed after the battery's positive terminal. Two voltage regulators are used to regulate the

9-volt supply to 5 volts. One regulator is used to solely for the MCU. During breadboard testing, it was discovered that the current fluctuations caused by the LCD and fingerprint module when they powered on caused the MCU to reset so to solve this issue, a voltage regulator is dedicated to the MCU to provide a clean current. The second voltage regulator is used to power the Fingerprint sensor, the Bluetooth module, and also is used as the voltage input for a third 3.3-volt regulator that provides power for the RFID sensor, the LCD and Facial Recognition Camera. To protect the circuit, one 5-volt zener diode is placed between ground and the MCU's 5-volt terminal and another 5 volt zener diode is placed between ground and the other 5 volt terminal. A 3.3-volt diode is also placed between ground and the 3.3-volt output terminal of the voltage regulator.

The first USART communication protocol channel is reserved for debugging purposes so a header is attached to the RXD0 and TXD0 pins. During the programming phase, this header will be connected to a serial TTL adapter enabling the program to read the data that is transmitted and received on the debug channel. The second USART channel is reserved for the Fingerprint Scanner module. It is connected to P1, a logic level converter that converts signals from 5 volts to 3.3 volts and from 3.3 volts to 5 volts. P1 is connected to the RXD1 and TXD1 pins. The third USART channel is reserved for the Bluetooth Module and is connected to the RXD2 and TXD2 pins. The Fourth USART channel is reserved for the Facial Recognition camera module and is connected to the RXD3 and TXD3 pins.

The TFT LCD screen is the first module that uses the SPI protocol. It is connected through the logic level converter P2 to the SCK, MISO, and MOSI pins. The chip select pin for the LCD screen is connected through P3 to PORT L pin 3. The SD card slot on the TFT screen is also connected through P2 to the SPI pins and the SD card chip select is connected though P3 to PORT L pin 1. The touch screen is also connected to the SPI port and the Touch screen chip select pin is connected though P3 to PORT L pin 0. The touch screen interrupt pin is connected through P3 to PORT D pin 0. The RFID reader is also connected to the SPI port through P2 and the RFID reader's chip select pin is connected through P5 to PORT L pin 5. The RFID reader's interrupt pin is connected through P3 to PORT D pin 1.

Pending further testing, an external oscillator crystal is needed for the TFT display to refresh at a rate that is seamless to the user. A 32 MHz crystal is initially chosen and is connected to XTAL1 and XTAL 2. Two 22uF capacitors are placed from ground to XTAL1 and from ground to XTAL2

5.1.1 Initial Design Architectures

The initial design architecture is to use an MCU to drive a TFT touch screen display, an SD card module, and an RFID scanner using the SPI bus and corresponding chip select lines. Utilizing the UART protocol are the fingerprint module, facial recognition scanner, Bluetooth module, and WIFI module. A pin setup as an output will be connected to a bipolar junction transistor will be used to trigger a relay circuit. The device will be fabricated and installed into a slim, weatherproof housing that allows easy access to the LCD screen as well as the fingerprint sensor.

5.2 Block Diagram

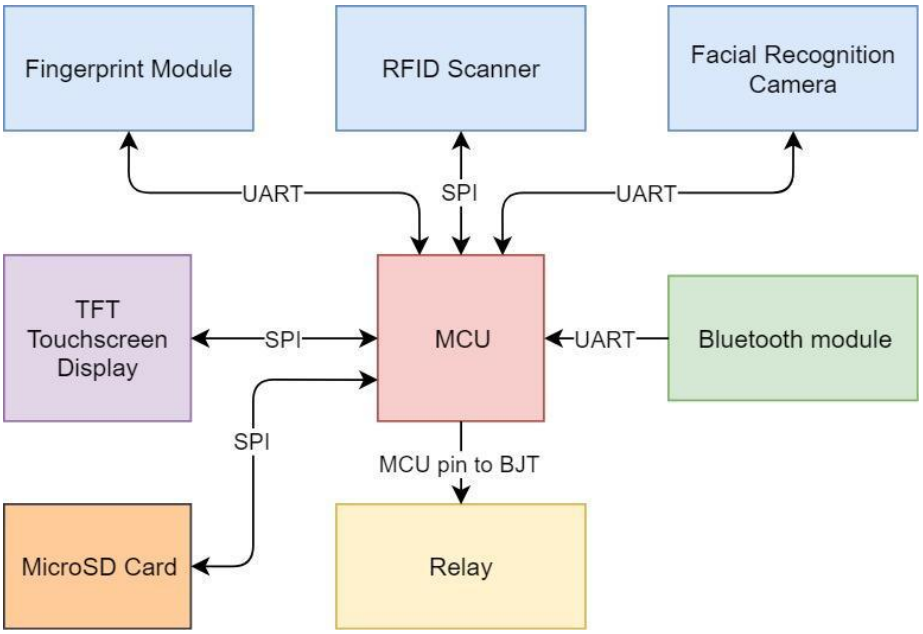


Figure 17 Hardware communication protocol

The hardware communication protocols between the MCU and the sensors as shown in Figure 25. The UART0 channel will be used for debugging purposes. UART1 will be assigned to the fingerprint module, UART2 will be assigned to the Facial Recognition Camera, and UART3 will be assigned to the Bluetooth Module. The first SPI chip select will be assigned to the TFT LCD screen, the second SPI chip select will be assigned to the TFT Touch Screen, and the third and fourth SPI chip selects will be assigned to the SD Card reader and the RFID reader. When the necessary input sequence to unlock the lock is initiated, the MCU sends a high signal using one of its pins. This pin will be connected to the base of an NPN BJT, used to deliver 80 mA from its collector. The relay's inductor circuit will be connected in series from the 5V terminal to the collector terminal of the BJT. This allows the pin to trigger the relay on and off without using much current from the microcontroller.

5.3 Bread Board Testing

Testing the breadboard is an important initial step to building the circuit because it helps to ensure device functionality. The breadboard as shown in figure 18 is tested for continuity using a multi-meter and jumper cables. Each of the power and ground rails are tested from opposite ends for continuity. After testing the power and ground rails, each of the numbered columns are tested for continuity. Once all of the columns have been tested and passed, the power circuit is constructed, and the external 9-volt supply is turned on. Using the multi-meter, the 5V, 3.3V, GND and VCC rails are tested to ensure that they are outputting the correct voltage. After this

ensuring that the voltages are correct, the MCU is then attached to the breadboard along with each of the sensors.

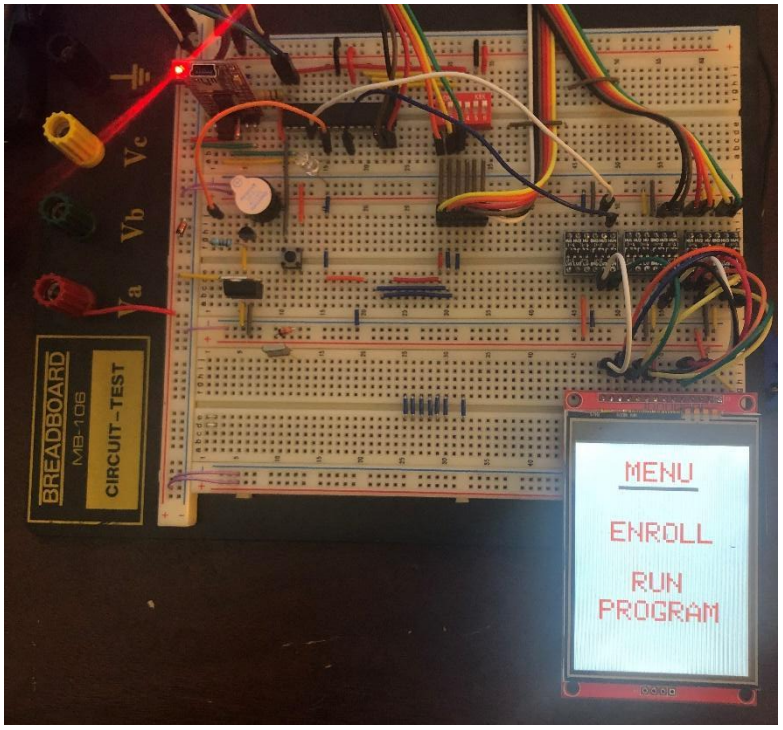


Figure 18 Breadboard Testing

5.4 Sensor Testing

Sensor testing will be carried out on each of the sensors to ensure that the hardware is functioning properly. First this is done by inserting the sensor pins into the breadboard then supplying power to the breadboard. Using a multi-meter, all the pins will be tested to ensure that they are at the correct voltage for operation as recommended by the datasheet. After the voltages are verified, research is done to find a c library for the module and if no library is found, a library is created from scratch to operate the module.

5.4.1 RFID Sensor

The first test for the RFID sensor is to initialize the module. A function the performs a soft reset, then powers on the radio antenna, and enables the radio transmitter and receiver so that it is ready to receive a signal. If this function is successfully completed, the module is initialized.

The RC522 is capable of performing and automatic self-test and this is done by using the AutoTestReg register. After a soft reset is performed the internal buffer is cleared by writing 0x00 to them and then 0x09 is written to the AutoTestReg register. Then 0x00 is written to the FIFO buffer and send the CalcCRC command. When the CalcCRC command is sent, it enables the digital self-test which transfers the FIFO buffer content to the CRC coprocessor then begins the calculation and a self-test result is written to the FIFO buffer. Examination of this buffer tells the state of the

chip. The datasheet shows what the 64-byte content of the FIFO buffer should contain after the execution of a self-test for each version of the RFID chip. If the test returns back the expected data, it is a functional chip and further testing can begin. If the test fails or returns garbage values, the breadboard is powered down and the module is unplugged and re inserted back into the breadboard and then the breadboard is powered up and the test is conducted 3 more times. Repeat failures indicate that the module is defective, and the module is replaced.

Next the receive command is sent to the RFID reader and the modem's state in Status Register 2 in the RFID reader changes from idle to RxWait. This makes the RFID reader chip wait until a radio frequency field is present then triggers an interrupt. If an interrupt is triggered when an RFID tag is held in close proximity to the radio antenna, then the device is setup correctly and now the FIFO buffer is tested by sending the command to read the FIFO register. 64 bytes of data will need to be analyzed from the FIFO buffer, so a loop is created to store the 64 bytes in an array. Once the bytes are stored, they are analyzed to see if they contain the correct UID code and data in the storage locations. If the information is correct, then the RFID chip is properly reading form an RFID tag.

After successfully reading data from the RFID tag, the ability to write to the tag is then tested. This is done by first changing the register settings to enable data transmission then loading the desired data to transmit into the FIFO buffer then sending the transmit command. When an RFID tag is in proximity the contents of the FIFO buffer will be written to the tag. When the write is successfully completed and verified by a subsequent read routine, the RFID module successfully passes the test and is ready for project integration.

5.4.2 Fingerprint Scanner

A search was performed to find a c library for the fingerprint sensor but was unsuccessful, so a library is created from scratch in order to test and to operate the fingerprint scanner. From the datasheet, the commands list and data structures for the command and response packets, as shown in Table 7-9, are obtained.

Table 10 GT 115 Commands Protocol [63]

Number (Hex)	Alias	Description
01	Open	Initialization
02	Close	Termination
03	UsbInternalCheck	Check if the connected USB device is valid
04	ChangeBaudrad	Change UART baud rate
05	SetIAPMode	Enter IAP Mode In this mode for FW Upgrade
12	CmosLed	Control CMOS LED
20	GetEnrollCount	Get enrolled fingerprint count
21	CheckEnrolled	Check whether the specified ID is already enrolled
22	EnrollStart	Start an enrollment
23	Enroll1	Make 1st template for an enrollment
24	Enroll2	Make 2nd template for an enrollment

25	Enroll3	Make 3rd template for an enrollment, merge three templates into one template, save merged template to the database
26	IsPressFinger	Check if a finger is placed on the sensor
30	Ack	Acknowledge
31	Nack	Non-Acknowledge
40	DeleteID	Delete the fingerprint with the specified ID
41	DeleteAll	Delete all fingerprints from the database
50	Verify	1:1 Verification of the capture fingerprint image with the specified ID
51	Identify	1:N Identification of the capture fingerprint image with the database
52	VerifyTemplate	1:1 Verification of a fingerprint template with the specified ID
53	IdentifyTemplate	1:N Identification of a fingerprint template with the database
60	CaptureFinger	Capture a fingerprint image(256x256) from the sensor
61	MakeTemplate	Make template for transmission
62	GetImage	Download the captured fingerprint image(256x256)
63	GetRawImage	Capture & Download raw fingerprint image(320x240)
70	GetTemplate	Download the template of the specified ID
71	SetTemplate	Upload the template of the specified ID
72	GetDatabaseStart	Start database download, obsolete
73	GetDatabaseEnd	End database download, obsolete
80	UpgradeFirmware	Firmware Upgrade
81	UpgradeISOCDImage	Not supported

Table 8: Data structure for a Command Packet

CMD code 1	CMD code 2	Device ID	Parameter	Command	Check Sum
BYTE	BYTE	WORD	DWORD	WORD	WORD
0x55	0xAA	0x0001	Input Parameter	Command code	Sum of each offset

Table 9: Data structure for a Response Packet

RSP code 1	RSP code 2	Device ID	Parameter	Command	Check Sum
BYTE	BYTE	WORD	DWORD	WORD	WORD
0x55	0xAA	0x0001	0x0030 = ACK 0x0031 = Non-ACK	0x0030 = ACK 0x0031 = Non-ACK	Sum of each offset

The library begins with by defining the command and corresponding values from the manual. Then the Open command is used to initialize the device using the command packet data structure as shown in Table 8. The CmosLed command is used to turn the internal LED on and off. After successfully toggling the LED on and off. The enroll command can be tested.

Enroll is initiated by first using the Command Packet structure to enter the commands as shown in Table 8. Send EnrollStart command, setting the parameter to an unused index from 0-100. Next the command to capture finger is sent. Capturing the fingerprint takes a bit of intuitive thinking timer wise. Because the MCU's clock runs much faster than the human perception, delays are required to give the human user enough time to perform certain actions that the program requires.

The IsPressFinger command is used to check weather a finger is placed on the sensor. When a finger is placed on the sensor, the finger needs some time to evenly apply pressure to the sensor, so a delay is used when a finger is sensed then the CaptureFinger command is sent. The same goes for when the finger is lifted from the sensor, a delay is needed so that the user feels that they are at a good pace with the interface. If the program's request for the user to lift their finger off of the sensor changes as soon as the user lifts their finger, the user may feel uneasy so a delay is used to give the user adequate time to remove their finger from the sensor before being instructed to take two additional readings. Once all the readings are successful, the fingerprint is successfully enrolled

After using the CaptureFinger command to scan a fingerprint, the Identify or Verify commands can then be used to identify, or scan the data base to for a match and display the match, or verify that the user in the selected index has provided fingerprint data that matches the fingerprint data on file. When a fingerprint is successfully enrolled and successfully verified and identified, the testing for the fingerprint sensor is complete.

5.4.3 Camera Sensor

Testing the camera sensor begins with properly connecting it to the UART protocol and testing that all pins are at their correct voltage. Next a header file needs to be created that defines all of the commands shown in Table 10

Table 11 Facial Recognition Camera Commands[64]

Command number	Command name	Command Description
00h	Get model and version	Gets the Device's model and version
01h	Set camera angle	Sets the camera angle.
02h	Get camera angle	Gets the camera angle set
04h	Execute detection	Executes the specified functions, e.g. Face Detection, Hand Detection, Face Detection and/or Face Recognition
05h	Set threshold value	Sets the threshold values for Human Body Detection, Hand Detection, Face Detection and/or Face Recognition
06h	Get threshold value	Gets the threshold value set for Human Body Detection, Hand Detection, Face Detection and/or Face Recognition
07h	Set detection size	Sets the detection size for Human Body Detection Hand Detection, and/or FaceDetection
08h	Get detection size	Gets the detection size set for Human Body Detection Hand Detection, and/or FaceDetection
09h	Set face angle	Sets the face angle, i.e. the yaw angle range and the roll angle range for Face Detection
0Ah	Get face angle	Gets the face angle set for Face Detection
0Eh	Set UART forwarding rate	Sets the UART forwarding rate.
10h	Register data	Registers data for Face Recognition and gets a normalized image
11h	Delete specified data	Deletes a specified registered data

12h	Delete specified user	Deletes specified registered user
13h	Delete all data	Deletes all the registered data
15h	Get user info	Gests the registration info of a specified user
20h	Save Album	Saves the Album on the Host side
21h	Load Album	Loads the Album from the Host side to the Device
22h	Save Album on Flash ROM	Saves the Album save area on the flash ROM
30h	Reformat Flash ROM	Reformats the Album save area on the flash ROM

Table 12 Data structure for command packet[64]

Synchronous code	Command number	Data Length	Data

Table 13 Data structure for response packet[64]

Synchronous code	Response code	Data Length	Data

After defining the commands, a loop is created that loads the correct information as the data structure for the command packet. This will be used to send the camera module commands. Another loop will be used to receive the response packet from the facial detection camera module. After a command is sent, analysis of the response packet indicates weather the command was properly received and executed or not.

The first command that will be sent is the Get Model and Version command. The response code that indicates that the module is functioning correctly is FEh for the Synchronous code, 00h for the Response code, 13h 00h 00h 00h for the Data length, and the data contains the Model information. If this is correct, the module is ready for detector testing.

The next command is Set Camera Angle. The B5T has the ability to operate in its original orientation and at 90 degrees. Both angles are investigated to decide which orientation is appropriate for the application.

Now the Execute detection command is sent. A data packet of 3 bytes is sent to the facial recognition camera module enabling or disabling a list of detectable features such as:

First Byte
- Human Body Detection
- Hand Detection
- Face Detection
- Face Direction Estimation
- Age Estimation
- Gender Estimation
- Gaze Estimation
- Blink Estimation

Second Byte
- Expression Estimation
- Face Recognition

The third byte give the option to output an image or not. 00h means no image, 01h means output a 320x240 pixel resolution (QVGA) image, and 02h means output a 160x120 resolution image. If a command is sent and the response packet containing the data is received and correct, testing can proceed to recognition.

In order to test the facial recognition feature, a face must first be enrolled into the database. Send the Set Face Angle command and set the data to 00h for a +-30h degree yaw angle and 00h for the second byte for a +-15-degree roll angle. This will detect a face that is facing the camera. The command Register Data can now be used to register the facial recognition data that is in front of the camera into the user ID slot that is selected.

The ability to recognize a face is performed by registering facial data of a subject in a well-lit area using the Register Data function. Then the recognition process can be tested by sending the Detection command to the module for the same subject. If the response packet does not return the user ID used to train the subject, there is an error. If the response data packed for the detection returns the user ID as the face that is detected with a high certainty, the module is properly set up and operational.

5.4.4 Touch Screen Sensor

The Touch Screen sensor testing only requires a simple approach. When the touch screen is powered on, all of the pins are tested to verify that they are the correct voltage. Then an LED is placed from the touch screen interrupt pin to ground. The LED should initially be lit then the touch screen is repeatedly pressed. If the LED turns off each time the touch screen is pressed, then the interrupt function is working on the LCD and testing for the position of the touch can be done.

The global interrupt bit needs to be set and the interrupt pin selected needs to trigger on the falling edge, so the interrupt registers are configured to allow the touch screen interrupt pin to trigger an interrupt in the MCU. When the interrupt is triggered, the interrupt service routine is now triggered. To test for the position information, some information must be first obtained from the data sheet.

Table 14 Input Configuration [66]

A2	A1	A0	YBAT	AUXIN	TEMP	YN	XP	YP	Y-POSITION	X-POSITION	Z1-POSITION	Z2-POSITION	X-DRIVERS	Y-DRIVERS
0	0	0			+IN (TEMPO)								Off	Off
0	0	1					+IN		M				Off	On
0	1	0	+IN										XN, on	YP, On
0	1	1					+IN				M		XN, On	YP, On
1	0	0				+IN						M	On	Off
1	0	1						+IN		M			Off	Off

1	1	0		+IN								Off	Off
1	1	1			+IN							Off	Off

Table 15 Data Structure for Command Packet[66]

BIT7(MSB)	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0(LSB)
S	A2	A1	A0	MODE	SER/DFR	PD1	PD0

Table 16 Data Structure for Response Packet[66]

BYTE 1								BYTE 2					
	BIT11	BIT10	BIT9	BIT8	BIT7	BIT6	BIT5	BIT4	BIT3	BIT2	BIT1	BIT0	

From the data sheet, the input configuration as shown in Table 13 for getting the x and y and z positions are shown. A loop is created that will modify the values in the command packet, shown in Table 14 in order to receive the position information. When this command is sent, 2 dummy bytes are sent and used to read the response of the module. The 12-bit response should contain the value of the coordinate requested by the command. To test this, output the value to the UART within the interrupt service routine and continue to press the screen. The value displayed on the USART should be relatively similar and should not change drastically. For the TFT LCD display, it is known to give false report the first or second time the value is read so after testing by touching the screen a few times, it is evident which values are valid and represent the area on the screen that is being touched and which values are garbage values. Each coordinate can be mapped out and this information now gives the location that the screen was touched and this information can then lead us to executing certain tasks when this region of the board is pressed. Successful mapping of the LCD screen can be tested by creating a button that when the LCD screen is touched within the area of the button, an action is triggered. The successful trigger of an action from a button press means that the TFT LCD module passes the test and is functioning properly.

5.5 Potential Hardware Issues

During the Installation and operation of the Smart Lock System, there exists a potential for hardware issues including:

- Improper installation
- Electrical Surges
- High current event
- Thermal event
- Sags and Dips in Power
- Improper software functionality
- Bluetooth & WIFI connection loss
- Module Reset required

During the installation of the Smart Lock System. Careful consideration to details is required to obtain optimal functionality so a trained engineer or technician is required for the installation process

Electrical surges can be caused by a number of factors. It could be caused by damaged power lines, lightning strikes, or faulty electrical wires or appliances. In the event that electrical surges occur, the Smart Lock System implements safely counter measures to protect the logic level circuitry. Zener Transient Suppression will be used to protect the 9v power source so when this terminal experiences a surge greater than 9 volts, the Zener diode will open and a leakage current will flow to ground allowing the voltage to be limited at 9 volts. Transient Suppression will also be used to protect each of the 5-volt regulators. Since power surges typically last for short periods of time this is an appropriate countermeasure.

A high current event could happen if a device on an electrical system short circuit. Sections of the circuit and components may experience currents much higher than their recommended operating currents and this can cause damage or incorrect functionality to the circuit. To protect against a high current event, a fuse is put into place at the main power source so that a high current event would not damage the device but would only damage the easily replicable fuse.

In the event that the circuit and or its components do experience a high current event, this could also be coupled with a thermal event. The temperature of a component may rise to a level where thermal runaway takes over and the circuit may no longer be able to operate within the recommended operating temperatures. This can be caused by internal factors like high current or external factors such as high external temperature or prolonged exposure to sunlight. Protective measures will be put into place to protect the circuit and its components from thermal events. Insulation will be used within the case to separate the logic board from the other components and heat sinks will be used on the voltage regulators

Sags and dips in the power supply can occur when appliances begin to draw large amounts of current from the grid. Dips in the supply could be problematic for the ability of the Smart Lock System to function properly. When the MCU experiences lags or dips in the voltage or current, it may reset itself, causing the previous running operation to be abandoned as the program runs its code again from the beginning. This is a serious problem that would set back the performance of the Smart Lock System and potentially make it dangerous during emergency situations. The ability of the smart lock to be able to function uninhibited by the current and voltage dips is essential to ensuring that the Smart Lock System takes safety into consideration. To solve the problem of sags and dips in the power supply, the voltage regulator for the MCU will be a buck boost converter configuration. To protect against a power outage, the Smart Lock System will be equipped with a backup battery supply. This supply will be rechargeable and able to supply the entire circuit with the power it needs should the power from the grid fall below the operating level.

Improper software functionality could occur for a number of reasons. Each of the events previously discussed has the potential to affect the software functionality of the Smart Lock System. Temperature and humidity can also be factors to improper software functionality. To deal with the risk of improper software functionality. The user will always have the option to perform a software reset on the device that will

reset the MCU and all of the Hardware on the circuit. After a software reset, the program should return to normal functionality. To protect against freezes as well as to protect user data, a timer will be implemented in the software to increment a counter that resets every time the touch screen is pressed on each scene. If the counter increments to a certain value, this indicates that the user is idle and the program executes a low power mode loop where it powers down all of the modules then the MCU goes into low power mode. The LCD touch panel is not powered down but the backlight is turned off. The next time the touch screen is pressed and triggers an interrupt, the MCU will come out of sleep mode, the touch screen LED will light up and the program will power up and initialize all of the devices. This process is done to make the Smart Lock System energy efficient.

A Bluetooth or WIFI connection loss can also be caused by a number or issues. Moving out of the range of the Bluetooth or WIFI connection could cause a severe degradation in the ability to transmit and receive signals or even cause a complete drop in the connection which would require that the connection be reestablished to continue correct App functionality. To avoid this problem a timer is used during the beginning of a Bluetooth or WIFI transmit or response data packet. Completion of the data packet transmission or reception will reset and turn off the timer. In the event that the transmission is interrupted and or incomplete, the program will power down the receiver then power it back up then initialize it. Then the program will attempt to reestablish a communication with the Bluetooth device or WIFI network. If unsuccessful, the program will wait for 5 seconds and attempt to reestablish a communication with the Bluetooth device or WIFI network 3 more times. If unsuccessful, the program prints “Connectivity Issue”. If the connection is successfully reestablished, the program will then reattempt the previously failed transmission or reception of data.

6 Printed Circuit Board Integrated Schematics

In electronics, integrated schematics is a pictorial representation of the circuit workflow in the form of a block diagram. As the name itself suggests “integrated” and “schematic”, making this clear that different or same type of modules is combined in one symbolic diagram.

Each module is a single block and different modules are connected through wires. A module can be the actual IC design given in the datasheet displaying the exact pin numbers of connection. It is not always compulsory to use all of the pins. Unused pins can remain unconnected, which are omitted in the schematic. Order of the pins needs not to be maintained as well. Same block can be used in a repetitive manner with some of the short circuit connections like if the system has a common power supply.

It is not to be overlooked that the purpose of the schematic diagrams is not to elaborate the circuit but just to show how the integrated circuits are represented. Many known modules (e.g. Timer 555 or 556) have built-in IC block in the software where some of the components like power supply can be provided to the circuits through plenty of ways like AC adapters or solar cells but the most common and the practical source is the battery. A sample integrated schematic is shown in Figure 20.

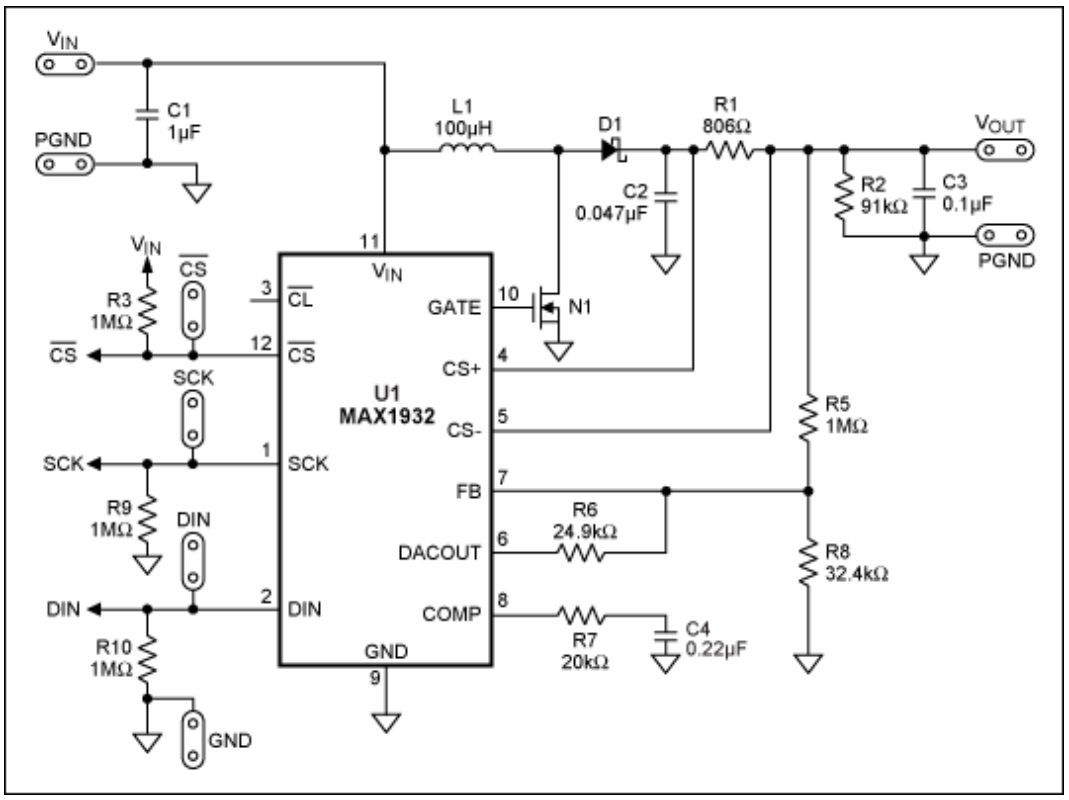


Figure SEQ Figure * ARABIC 20
Integrated Schematic Example

In this way, extensive flexibility is available to demonstrate the working of the circuit using integrated schematics.

6.1 Different Software

Many Software facilitates the design of PCB from schematic design till the manufacturing. Some of them are explained in the section below.

6.1.1 KiCad

Schematic capture is effective as it is equipped with all the tools you might expect for such a task. Many features are provided for the ease of the user like the built-in libraries of the components, PCB layout and 3D viewer. The main focus of the interface is productivity. Bounds on complexity are no existent because of the hierarchical design approach used in this. Numerous formats are available to export like PDF, SVG, HPGL or Postscript.

Along with the schematic diagrams, it provides the best environment to design a professional PCB layout of the circuit using 32 layers of copper. It has an auto route which is skilled enough to do routing keeping intact the integrity of the DRC. Tracks can be rerouted if there exist obstacles in the path.

The designed structure can be inspected in the 3D view. Rotate and pan around options are there to inspect the layout which is a bit more complex in 2D view [35].

6.1.2 Eagle

EAGLE is an acronym of Easily Applicable Graphical Layout Editor having various features including schematic capture, PCB layout, auto-router and computer-aided manufacturing.

For designing circuit diagrams, EAGLE contains the “schematic editor”. Different modules of the circuit are connected through ports which makes it possible to place them on more than one sheets. The extension used for the schematic files is “. SCH" whereas parts of the circuits can be found in “. LRB".

EAGLE also facilitates to import the schematic design on board by allowing the development of PCB layout and stores them in board files. Board files are stored in the editor with the extension “. BRD". It allows auto-routing of the layout corresponding to the schematic as well as back-annotation. This way connections defined in schematics are automatically tracked in the layout. The “. BRD" file is further used by the industry to fabricate the layout of the design. At the professional level, Gerber, PostScript layout files as well as Excellon and Sieb & Meyer drill files are also saved in this software which depicts the flexibility and professional environment of the software [36].

6.1.3 Custom Library

Normally PCB software demands three things to take an IC into the library. These are
Footprint, Symbol (schematic), and Complete device (to map everything together).
Each of them is explained below in detail. Each of them is fully customized to provide flexibility in the design.

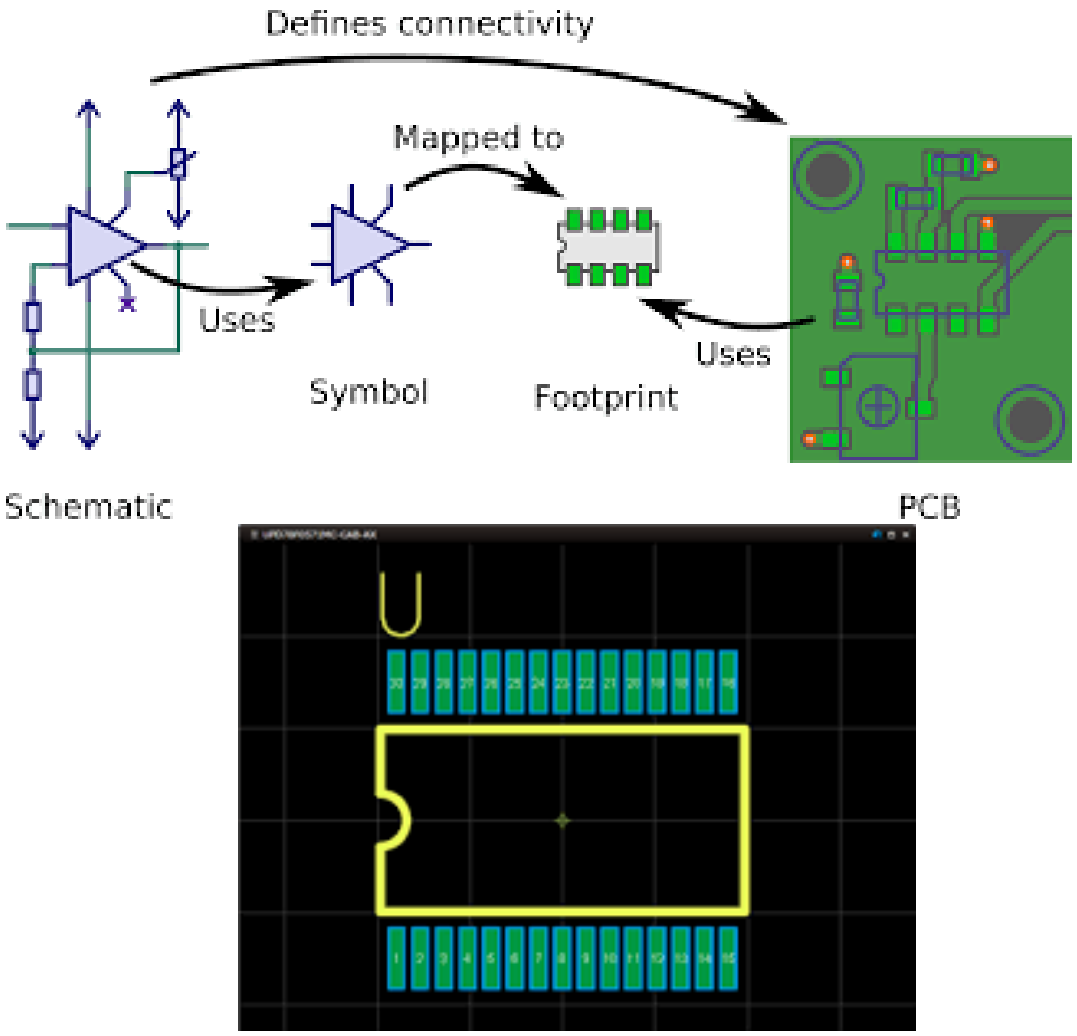
6.1.4 Foot Print

For the development of the PCB, the required components need to be soldered. The placement of these components is justified during the layout design. A footprint is used to describe the mechanical and physical spacing of the component on the board [37].

Depending on the tolerance of component, some standards can be used to create the footprint. For maximum optimization of power and space, designers prefer to develop the footprints of each component manually (htt12).

In a fully customized design, guidelines are provided about the size of elements like the copper, solder mask, and solder paste to assure secure and reliable production.

Otherwise, calculations are already known for standard. Applying these calculations to the mechanical dimensions gives us the footprint of that component. A fully customized footprint is made at the cost of increased complexity. A sample foot print can be seen in figure 21.



6.1.5 Symbol

Circuit with the customized footprint of the components requires a customized symbol as well. A custom symbol possesses its own unique identifier. This is connected to the PCB component using the make symbol window for the circuit symbol. Figure 22 illustrates this characteristic well.

6.2 PCB Terminology

PCB is a piece of plastic boards making our lives a million times efficient and easy by eliminating all the connecting wires and breadboards.

Printed Circuit Boards is a plastic board that is used as a base structure for manufacturing of schematic design on a hardware level. It connects the electronic components together through traces of wires. From a very basic digital watch to the supercomputer, PCBs are the most important part.

The board itself is certainly not a conductive material and frequently plastic or fiberglass is utilized as the base material. The essential use of PCBs is to control where the power is coordinated too.

6.2.1 PCB Terminology

Table 17 PCB Terminology

Terminology	Description
Via	In multi-layer PCB, different layers are connected through some holes called as via. Via helps to avoid the overlapping of traces. They are useful where there are different components connected through the wires between different layers. For the ease of the user in soldering, vias are kept uncovered.
V-Source	Sometimes it is required to snap the PCB board to make it of fitting size. In order to do so, a line is directed as reference and snapping are performed. This whole process is done using V-Source.
DRC	DRC is an acronym of Design Rule Check. This can commonly be seen in many software like EAGLE. This is used to make sure that the traces, either in the same layer or different layers, do not overlap. Along with this, it also makes sure that the size of the drill holes is neither too larger nor too small. Its size should be appropriate for the components to fit perfectly.
Pad	On the surface of a PCB, a small portion of metal is left exposed. Components are soldered to this part. This makes the electrical connection of the components with the PCB.
Thermal	For the proper working of PCB, previously explained pads and PCB planes needs to be connected. A small trace is placed to do so. The pad needs to be thermally relieved because during the soldering the temperature can rise as high as 95 degrees Celsius. If it not thermally flexible enough then either a good solder cannot be done or it will take an unacceptably long time.

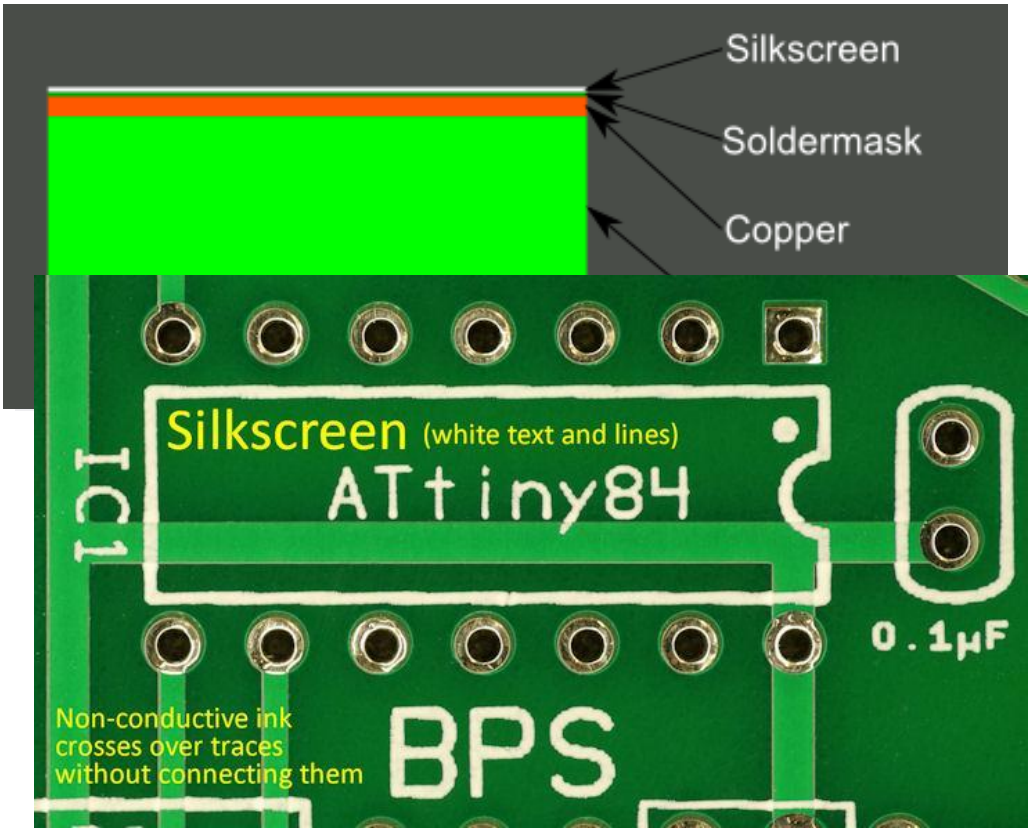
Plane	For a large and complex design of boards, a hierarchical approach is easy to adopt. Many small boards are designed and then combined together to form a larger one. These small PCBs are separated before use. Automated circuit board handling equipment face problem quite often while handling these small pieces.
Surface Mount	Surface Mount is the method used nowadays for proper and efficient soldering of components on the PCB boards. It is a modern and easy way to place the components for soldering. One main advantage it provides is the compact design as compared to the other technology.
Plated Through hole	A PCB has a number of holes on it. Many of them have an annular metal ring. They can go all the way through the board. Commonly, used to solder the components along with the long metal leads.
Trace	Traces are one of the most important parts of the PCB. They are developed using the path of copper metal. All electrical components are connected using these copper traces, acting as the wires.
Mouse Bites	There are plenty of drill hits on the board that are assembled together to create a weak spot. These are the points with the higher probability of the damage, even the board can break afterwards.
Drilling hit	These are the places on the PCB indicating that a hole can be drilled at this point. These can be used for numerous purposes.
Finger	Fingers are used to provide the flexibility to the component that can be placed at different dimensions with the same specifications.

6.3 Silkscreen

A layer of ink trace is applied onto the PCB board for the identification of components, testing points and parts of the board and many other. This layer is called a silk screen. Normally, it is applied to the PCB where the components are placed, however, sometimes it can be put on the solder side of the PCB too. Cost is

compromised to get the ease both for the manufacturer to develop and the engineer to design [40].

Silk screen used the ink that is a non-conductive epoxy in nature. On the basis of the sensitivity, it is highly formulated before its composition. Some basic standard colors include black, white and yellow. Similarly, standard font size is also used in silkscreen layers which is not a compulsion. Other fonts can also be selected depending upon the requirement. The traditional procedure demands some common equipment like an aluminum frame, polyester screen, laser photo plotter, curing ovens and spray developers. A PCB with the silk screen can be seen in figure 23



6.3.1 Solder mask

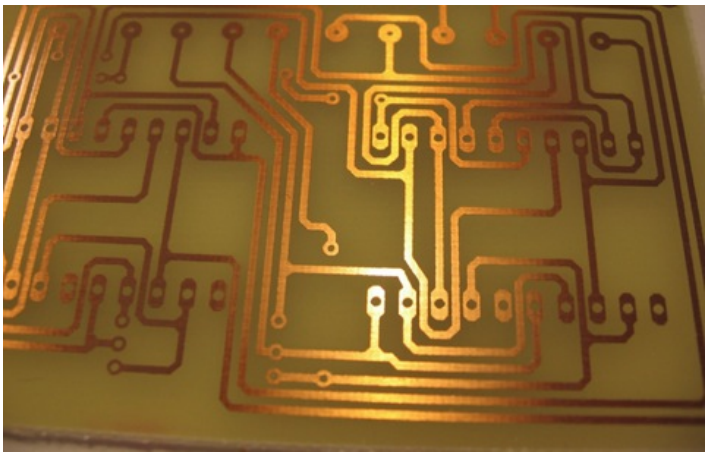
Generally, it is placed on both sides of the board along with the silkscreen. A coating is done on the PCB to protect the circuit from the corrosion and short circuit problem. This coating is known as the solder mask. Another advantage it provides is that it insulates circuit electrically, allowing the high voltage wires to be placed near to each other. This may help to compact the design.

The most important benefit provided by the solder mask is that it keeps the solder on the pads, not letting it flowing on other parts like traces, planes or any empty space left on the board. This is how efficiency is enhanced by reducing the probability of a short circuit on the board.

Otherwise, solder can act as a bridge between different elements resulting in unwanted connections. In the light of manufacturing, solder mask presents the hand soldering in a faster, easier, and more accurate way. Figure 24 shows the PCB

solder mask. It can be observed that the Solder mask is applied everywhere on the board except the pads. The significance behind lies in providing space for soldering.

6.3.2 Copper



One of the most common statements in the science world is that copper is a good conductor of heat and electricity. It is known that copper is a lattice of positive copper ions with free electrons moving between them. These conduction electrons help copper to be a good conductor of heat and electricity. For this reason, copper is used on the PCB to make the traces. It is a highly conductive metal, allowing the electrical signal to transmit from one point to another without losing any electricity along its way [43].

The amount of copper being used while developing the board is measured in ounces. PCB Copper Thickness needs to be defined before manufacturing. Some standard Copper PCBs, thickness level for internal layers is around 1.4 mm to 2.8 mm [44]. This way final weight would be between 2 oz and 3 oz including the external layers. This can be changed according to the specifications of your design. PCB after applying copper layer can be seen in figure 25.

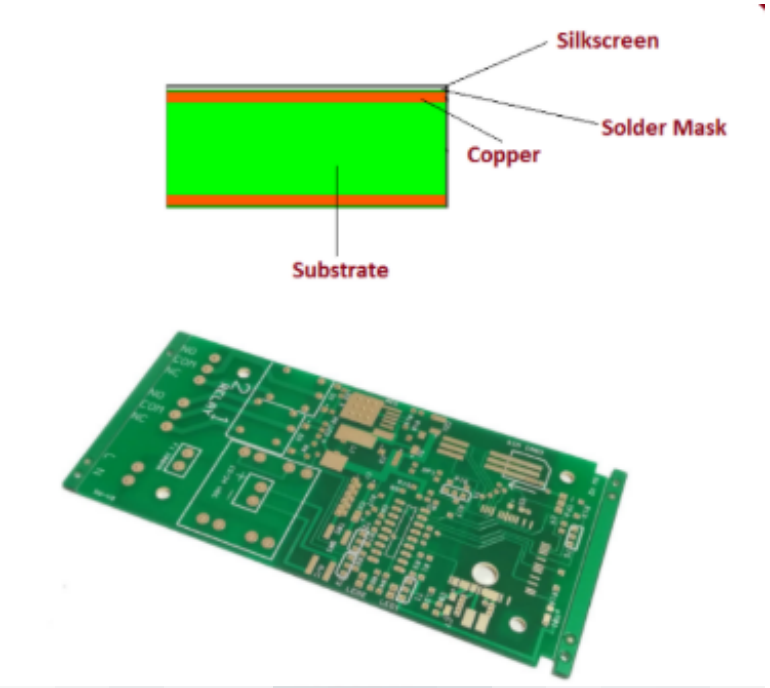
6.3.3 Substrate

Substrate identifies the attributes and performance of the PCB. For better performance of the board, the substrate needs to be optimized and better. Different types of material are used nowadays to meet the design requirements as well as the marketing trend.

PCBs base substrate mostly put together into the same brackets, hard/rigid or soft/flexible. The construction of a PCB is done with a solid substrate material which is used to avoid the board from bending. A computer motherboard, perhaps the most common application for a strong and robust PCB.

A motherboard is an example of a multilayer PCB. Such a design is used to allocate electricity from the power supply simultaneously enabling all computers parts to communicate with each other, such as RAM, GPU and CPU. When the PCB has to

retain one uniform shape then a hard and rigid material is used for its manufacturing. Arrangement of all the layers can clearly be seen in figure 26.



A designed circuit in the schematic is supposed to be fabricated by the industry. Where there is a fabrication, there are defined rules that need to be met. These rules are called the constraints which are decided by the industry. To meet these rules, constraint management and editing tools are used. Different design requirements are imposed on PCB tools.

While designing the PCB, from pre-schematic to PCB layout through routing and then manufacturing, it should be made sure that it is efficient, easy to use, accurate and consistent. Flexibility in the design should remain intact so to give the designer the ease of modification [47].

Efficiency will be enhanced as the design is more compact and productive. Accuracy of the design is validated by comparing the design file data with the DRC constraint file.

Numerous areas of constraint management are there that should be considered. Some of them are given as follows.

Classes are defined at the start of the design that should be followed in the entire files including schematic, layout and post-layout editing.

System specifications are defined by different specific constraint types such as topology, matched lengths, differential pairs and clearance rules.

Post layout editing can be minimized by sticking to aforementioned rules during placement and routing.

To ensure that all of your constraints are met, Post-layout validation and verification will be carried out.

Some common constraint issues are explained below.

6.4 Thermal Issues

PCB thermal design is one of the most significant areas of research. It is one of the constraints that is not applied by the industry but still ensured by the designer. Heat can somehow be dangerous such that it may entirely affect the working of the circuit. Design with accurate simulation can give disastrous results if thermal constraints are not considered while designing.

In the practical scenario, thermal constraints cannot be overlooked because of the fact that too much heat applied to the PCB board can possibly damage even the components or weaken or deform the whole PCB. It won't be unjustified to declare that heat dissipation is one of the most crucial factors of the PCB board. Engineers need to make sure that the board dissipate a tolerable amount of heat such that components can remain intact and functional [48].

These problems can be solved using cooling fans or heat sinks. The solution should be provided at the very basic, pre-schematic, stage of the design.

While manufacturing the PCB, two steps are considered the most important during assembly. During soldering, it is ensured that the surface mount devices (SMDs) are securely mounted on the PCB board. To solder the components properly and efficiently, they are placed on their exact locations on the board. After that solder paste is applied and the joints are heated. This makes sure the secure connection of the components with the PCB board by efficient filling the pads. This process is known as solder reflow. Throughout the heating process, the temperature may rise as high as 95°C across the PCB. So, this heat needs to be considered while designing the board to make sure the proper working of the component placed.

While soldering the components in the reflow there is a fair probability of originating many errors including misaligned components, some part of the component may remain unattached (tombstoning) or any other lose connections. These are the reason which increases the temperature to a significant level. The solution to this lies in the second step of soldering i.e. Rework. Issues may arise in these areas:

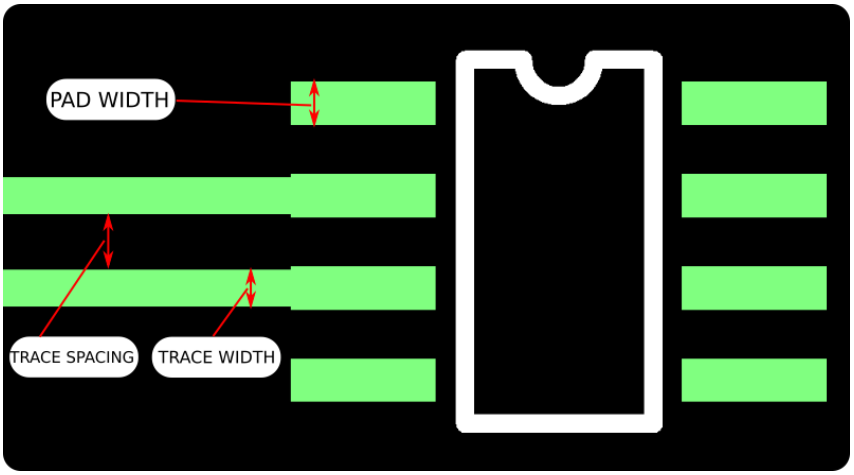
Thermal relief – The path for heat dissipation during PCB assembly.
Solder parts – Depending upon the type of solder used, the temperature at the solder joints of your components varies.
Thermal stress – Excessive heat or repeated heating of the board applies stress to the board.

The highlighted problems can be resolved by taking some simple measures according to the conditions and specifications in the design. Some of them are listed below.

For good employment, minimum safe space should be kept between the component.
Try to place components on only one side of the PCB board.
Consider the coefficient of temperature expansion (CTE) when selecting a Finish type should be considered while selecting the board, according to design specifications.
Copper weights can be increased to aid thermal relief.
For good heat distribution, the board size should be preferred according to the design specifications.

6.5 Traces Guidelines

While designing a PCB, many traces can be seen after routing. Each trace on the board (PCB) is the equivalent of a wire corresponding to schematic design. A single trace comprises of a flat, thin portion of the copper foil that will stay even after



etching.
Size of the trace can be made of any length and width as long as DRC (Design Rule Check) is not violated. Minimum feature size and spacing should also be cross-checked by the fabrication industry for the particular price point. It is to be noted that the large traces have to be narrow down before connecting to any of the pins of the IC. Whole layout can be made better using some of the simple guidelines like the one shown below.

Typical size, used by most of the fabrication industry, for the fast and inexpensive boards have a trace width of at least 5 or 6 mils, but it can be made larger a bit for the better routing [50]. This size can be made much smaller while designing military and other high-tech boards. Power traces should be made much wider and larger so that it would be easily accessible to all other ICs and make them work properly.

Different calculators are available to calculate the different trace length and width but this will give the ridiculously small trace widths for power trace that is not acceptable.

6.6 PCB Details

A printed circuit board (PCB) is supported both mechanically and electrically, connecting all electronic and electrical components through conductive tracks, pads and other etched features. Complex circuits can be extended from one or more sheet layers of copper. The substrate is used as a lamination between different copper layers. Soldering of components on PCB is performed to both electrically connect and mechanically fasten the board [50].

6.7 PCB Powered

On a PCB board, multiple layers of the copper can be used depending upon the complexity of the design. A two-layer board has copper on both sides.

However, a multilayer board sandwiches additional copper layers between layers of insulating material. Different copper layers are connected through vias, which are composed of copper-plated holes that function as electrical tunnels through the insulating substrate. In complex design after layers, four layers PCB is used. In which two copper layers are dedicated as power supply and ground planes; the other two layers are used for routing.

6.8 Voltage Regulator

A voltage regulator is an electrical component designed to regulate the voltage at a constant particular designed level. A voltage regulator can be made flexible enough to regulate one or more AC or DC voltages.

It produces a constant fixed voltage level at the output that persists for any fluctuation in the input voltage or load conditions. A voltage regulator basically acts as a buffer for protecting components from damages. The main advantage provided by this electrical component is that it makes the whole system somehow independent from the load resistance. Different methodologies can be used to develop a regulator. It may consist either of an electromechanical system or electrical components.

Any electrical system cannot work properly without a voltage regulator. They are located in almost every other electronic device such as computer power supplies. In this, a regulator stabilizes the DC voltages used by the sub-parts of the computer like the processor and other elements. Regulators can be placed both at the input and the output stage depending upon the design specifications. It keeps the output voltage within the prescribed limit which the electrical equipment, using that voltage, can tolerate.

One more defined voltage regulator is the Automatic Voltage regulator (AVR). The function of the AVR is same as the simple regulators, the difference comes at the point where it is required to maintain a constant voltage at load under an extensive variety of conditions, even when the input voltage, frequency or system load vary widely.

6.9 Electrical Switch

A switch is one of the fundamental components of any circuit design. A switch is an electrical component that provides the flexibility to "make" or "break" a circuit from the required point in real time. It allows the current to get interrupted or diverted from one point to another (Lowe, n.d.). A number of switches are available for use, selected on the basis of the design requirement. Some of them are listed below.

- Push Button Switch.
- Toggle Switch.
- Limit Switch.
- Float Switches.
- Single Pole Single Throw Switch (SPST)
- Single Pole Double Throw Switch (SPDT)
- Double Pole Single Throw Switch (DPST)
- Double Pole Double Throw Switch (DPDT)

Some common types are shown in figure 28.

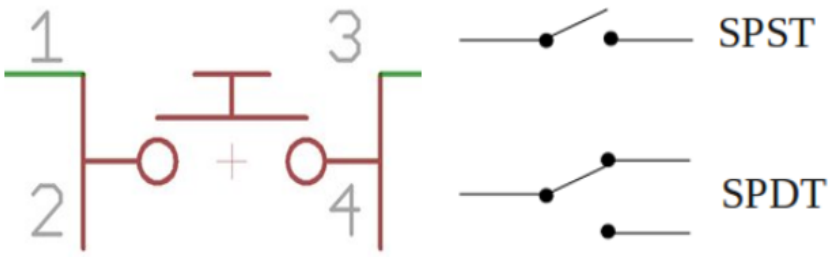


Figure 28 Types of Switches

6.10 PCB Parts Powered

All the component needs to be placed on the board requires the power supply to work properly. Every component transforms and maintains the current and voltages through them. The utmost prolonged aspect of PCB building is gathering the supplies, and there is no actual way to make it go quicker. Power supply is designed such that all the components get the proper supply without any voltage drop. This ensures the proper working of the circuit. To make that happen, different aspects in each of the stage needs to designed with precision like the traces of the power supply should be thickened enough so that proper current is supplied through every component. Some of the side effects need to be taken care of like the electromagnetic effect.

6.11 PCB Design

Designing a PCB is a challenge. It has so many things to know and understand. Going from different schematics and zones. So, it is better to know them before working on any PCB. More details to be covered in the specified sections below.

6.12 Layout

Schematic of the design can be printed on the board using the footprint of the components used, connected through the traces of wires. This results in the layout of the circuit design. A sample layout of the circuit is shown in figure 29.

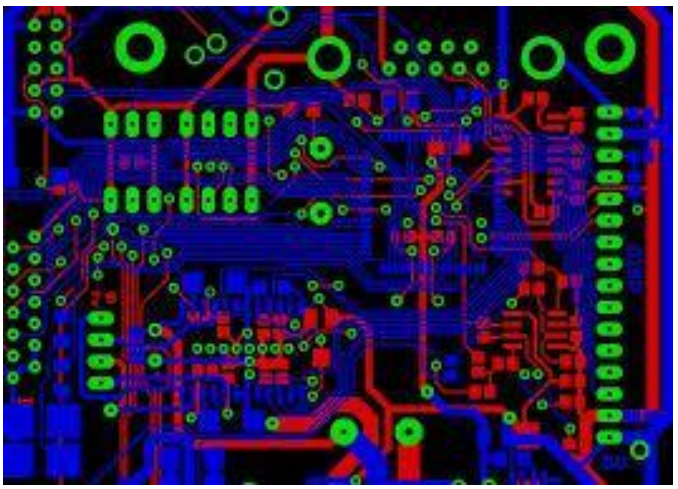


Figure 29 Sample layout of a circuit [14]

The footprint of an electrical component determines the physical dimensions and deployment of the copper pads. Then the time comes to select the type of component used.

Analyzing before designing is more valuable. To make an optimized design the circuit design should be identified and divided into parts according to their functionalities. Each section is grouped together and placed on the same area of the board. It will keep the conductive traces short. Long traces are avoided to eliminate noise and external interference that can be produced due to the electromagnetic radiation from other sources.

All sections are gathered such that the path of electric current remains as linear as possible. For better design, the current should flow in a direct path from one section to another. In layout, the power should be supplied to each section separately through the traces of equal length. This solidifies the working of the circuit by providing each section equal voltage level. Attention and precision are required to avoid the voltage drops which can affect the circuit functionalities. A board after the deployment of the layout design is shown in figure 30.

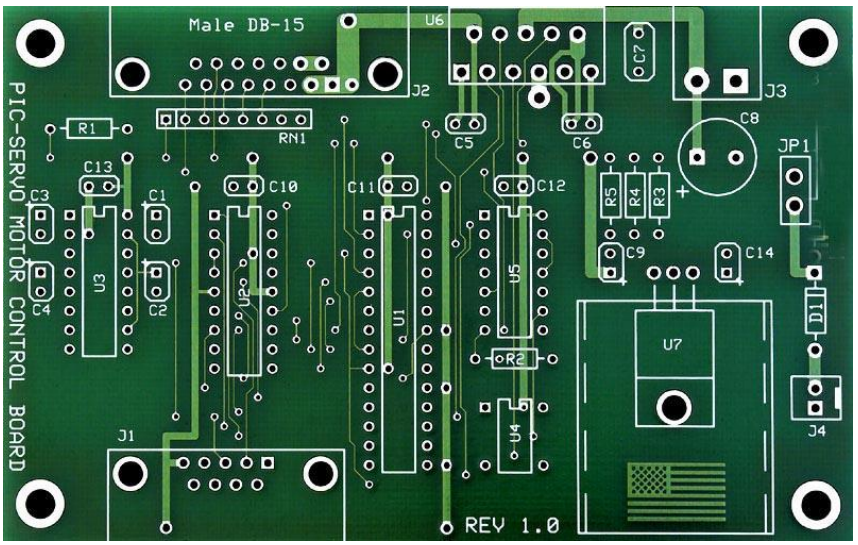


Figure 30 PCB after the layout [15]

6.13 Zones

Fillers is an important item required in designing of PCB. When a schematic of the circuit is exported to the layout, there is a lot of space left on the area that is required to be filled by some material. After the complete layout design of the PCB, it is comparatively simple to create a copper fill. Fillers is added after drawing the outline of the board. Before this, it is needed to be ensured that one of the copper layers is selected. Then filled zone option is selected in the software to fill all the empty spaces left behind, after the complete design.

Generally, Copper is filled on both sides, the top and bottom, of PCB. Other sides of the board are filled just by clicking a few simple steps in the software like Zone outline**.**

6.14 PCB Vendor and Assembly

Many vendors do their PCB different than others, but all of them uses the Gerber file to print. In the below sections it is going to be explained in-depth.

6.15 Circuit Board Types

The full form of the printed circuit board is PCB, it is a self-contained board explained in previous sections. Depending upon specifications of the application, different types of the boards can be selected. In complex designs, more than one layer might be required to develop the board. Similarly, other factors include precision, complexity, size, or sensitivity (htt6). Manufacturing of PCB necessitates special tools. A wide variety of PCB is available in the industry. Some common and main types are listed below.

- Single Sided PCBs
- Double Sided PCBs

- Multilayer PCBs
- Rigid PCBs
- Flex PCBs
- Rigid-Flex PCBs

The figure shows the single- and double-sided PCBs.

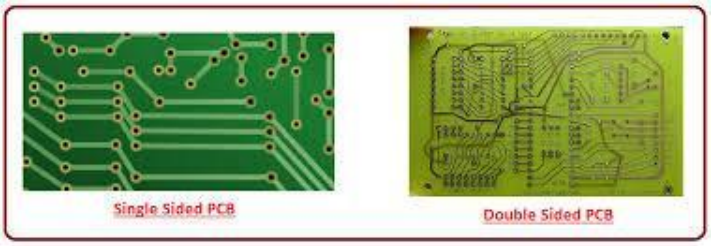


Figure 31 Types of PCBs [17]

Single sided PCB is the type of printed circuit board which has a single layer of the substrate, which is sort of base material. Along with this, it has components placed on only one side of the component. It is comparatively cheaper and best for small and less massive projects but not suitable for the complex and heavy system.

Compared to the single sided, double sided PCBs are much common. Substrate covers both sides of the board. As well as parts are also connected on both sides. One side of the board is connected to the other side through the holes in it.

In the multilayer PCBs, technology is expanded; double-sided boards are upgraded. Rather than two layers, it has multilayers of the substrate on the board. These layers are separated by the insulation material such that each layer can be distinguished. All the components on the different layers are connected through vias or holes.

One dependence factor describing the types of PCBs is the number of layers. Another factor can be rigidity. In rigid PCBs, the substrate material is solid and inflexible like fiberglass. It prevents the board from bending.

In flex PCB, the substrate is usually plastic. It provides flexibility and avoids rigidity. It prevents the board from damaging.

Rigid and flex PCBs is the merger of both technologies, rigid PCB and flex PCB.

6.16 Surface Mounted

SMT has opened a new era in the world of PCBs. The acronym of SMT is Surface-mount technology, the name itself explains the method in which the printed circuit boards (PCBs) contains all the electronic components mounted directly onto their surface. The device made using SMT is known as a surface-mount device (SMD). SMD led is displayed in figure 32. This shows the compact design presented by this technology.

Figure 32 SMD LED light showing the compact design [18]

In this epoch, all PCB boards are manufactured commercially using surface mount technology, SMT, because of the significant advantages it offers during and after the manufacturing process. The most notable benefit is the reduction in the size of the electronic component and overall PCB. It packed the whole circuit into a quite small size. A PCB manufactured with SMT is shown in figure 33.

Figure 33 PCB manufactured using SMT [19]

7 Embedded Software Design

The Embedded software design implements all of the code that runs the Smart Lock system. Research is done to decide which Integrated Development environment is the most appropriate for the Smart Lock System. The IDE's that are considered are Eclipse IDE, Microsoft Visual Studio, Arduino IDE, and Atmel Studio.

The Eclipse IDE is a professional level Java, C++, Pearl, Python and PHP integrated development environment. It was inspired by the visualAge family of integrated development environment. Eclipse comes with a set of powerful tools for each

language built into it's architecture and many tools can be added on. Eclipse uses Git for version control and can setup remote and local repositories. Eclipse is a free and open source software development kit released under the Eclipse Public License [64]. Eclipse provides support for AVR devices using the software add-ons and the project solution can be built and uploaded to microcontrollers using software for the hardware debugger.

Microsoft Visual Studio IDE is a powerful integrated development environment that runs on windows. It is capable of mobile development on Android and IOS and Windows. Add-ons can be included to expand its language capabilities. Projects can also be built for the cloud or IOT. With Microsoft Visual Studio, up to 10 web applications can be hosted for free projects can be open to collaboration using Github.
There is also a large online community that provides lots of support for Microsoft visual studio projects. There are over 5 thousand different extensions and products that plug into Microsoft visual studio making it a great choice for large web based or object oriented programming projects. Microsoft Visual Studio Provides AVR support with the use of the software plug-ins. C code solutions can also be built in Microsoft visual studio and the Hex files can be uploaded to the microcontroller by using software for the hardware debugger.

Arduino IDE is the integrated development environment used to write and upload code to the Arduino product line of development boards. Arduino IDE is written in Java and supports C and C++. Arduino is open source software that runs on Windows, Mac OSX, and Linux. Arduino provides a large library to support Arduino compatible devices and the libraries make interfacing with the hardware very easy. Although the ease of use is an advantage, Arduino functions run slower than C so in an application where timing is critical, this is a disadvantage. Arduino is not considered an engineering level integrated development environment because it lacks direct hardware access which is critical in embedded design. Despite this fact Arduino is used in many companies as a prototype step to developing products.

Atmel Studio is a professional integrated development platform that gives the AVR and SAM microcontroller programmer debugging capabilities for applications written in C/ C++ and Assembly. Atmel studio also has the ability to extend the development environment using plug-ins. It has support for over 500 AVR and SAM devices using a variety of hardware programmers like the Atmel Ice, the AVR dragon, and the STK500.

Table 18 Integrated Development Environment comparison

Integrated Development Environment comparison				
Name	View Registers	AVR support	Debug	Modify chip Fuses
Eclipse IDE	Yes	Hex	Yes	No
MS Visual Studio	Yes	Hex	Yes	No
Arduino IDE	No	No	No	No
Atmel Studio	Yes	Yes	Yes	Yes

Upon comparison as shown in Table 14 the appropriate IDE to use for the AVR Atmega 2560 is Atmel Studio. It provides the hardware and software support to the chosen MCU and allows for debugging which is critical for developing and testing embedded applications. Atmel studio also allows the programmer to change the chip fuses enabling functions like changing the clock from internal to an external crystal or resonator. Other options include changing the reset pin to an IO pin (Care must be taken when setting this fuse because once it is set, the chip can no longer be programmed by the hardware debugger and will need High Voltage programming in order to clear this fuse and return the reset pin back to its normal functionality).

The code for the program is written in C and the AVR dragon, as shown in Figure 27, is the hardware debugger that is used to upload code and debug the embedded program. The AVR dragon is also an emulator so the selected chip's behavior can be simulated allowing a programmer to program without the immediate need for an embedded chip. The AVR dragon will connect to the Atmega2650 using SPI and the Ground, VCC and Reset pins. It supports up to 32 breakpoints for software and 3 hardware breakpoints and uploads quickly. 265 Kb of code is uploaded in approximately 60 seconds using the JTAG interface.

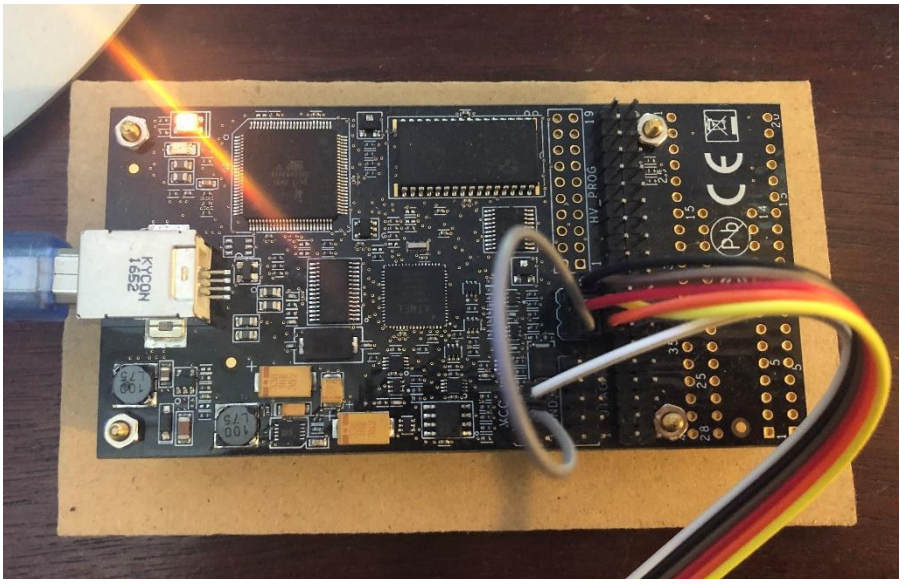


Figure 34 AVR Dragon Hardware debugging tool

In order to simplify the code, header and c files are used. This helps to organize the code as more modules are integrated into the main project. The use of the header file is basically everything that comes before the main function in. The header file defines all of the commands for the module, contains the communication protocol settings, defines the macro functions, and contains the implicit function declarations. The header file is used to share this information between several source files.

The c file shares the same name as the header file and contains everything that would come after the main functions. The c file contains all of the functions for the specific module. When a project is opened in Atmel Studio, the header and c file can be included in a few ways. One way is to put all of the header files into a folder then add that folder to the project directories then include the line #include "myHeaderName.h". Another way is to place both of the files into a source file within

the project directory then in Atmel studio right click on the project and select add existing and add the c file. Then include the line #include “myHeaderName.h”. This links the header file and the include file to the project and allows the compiler to access all of the files relevant to the code.

All the header files for each of the modules used in the project are included in the top of the embedded code. Then the clock frequency for the chip is defined and followed by the initialization of the USART protocol. The SPI bus is initialized and then each hardware module is initialized. Once the modules are initialized, functions from their corresponding libraries are used to control the modules. The global interrupt bit is then set along with the int0 enable bit and falling edge parameter bit so that the chip can trigger an interrupt service routine when the state of int0 goes from high to low. This interrupt is reserved for the interrupts that occur when the user touches the touch screen. Int1 is also enabled and intended for use whenever an interrupt is triggered because the user has scanned an RFID tag on the RFID reader. A switch case is used to select between a series of options during the interrupt service routine.

The main function of the code consists of a while loop that contains a Boolean value that is set to true and functions that change the TFT LCD screen scene. While this value is set to true, the program repeats this loop, doing nothing. The program is essentially just waiting for an input in the form of an RFID tag scan or a touch on the touch screen. Both events will trigger an interrupt service routine that will change the Boolean value to false if a scene change is necessary. When the Boolean is false, the program leaves the while loop and triggers the next scene for the TFT scene and also gives the parameters on how to handle the interrupt service routine that corresponds to that scene. The main function will initially lead the user to the main menu where the user has the ability to select whether to enroll a new user or whether to run the program. For security purposes, after choosing enroll the user will need to enter a password and biometric data that has a level 3 clearance. This way the level 3 Clearance would give the user the ability to modify the users that are enrolled within the smart lock.

A timer will be used whenever the program is idle and if the timer passes a certain predefined threshold, then the program will put the display into low power mode and power down the backlight. The program will also put all of the other devices that it can into low power mode in an effort to operate in an energy efficient.

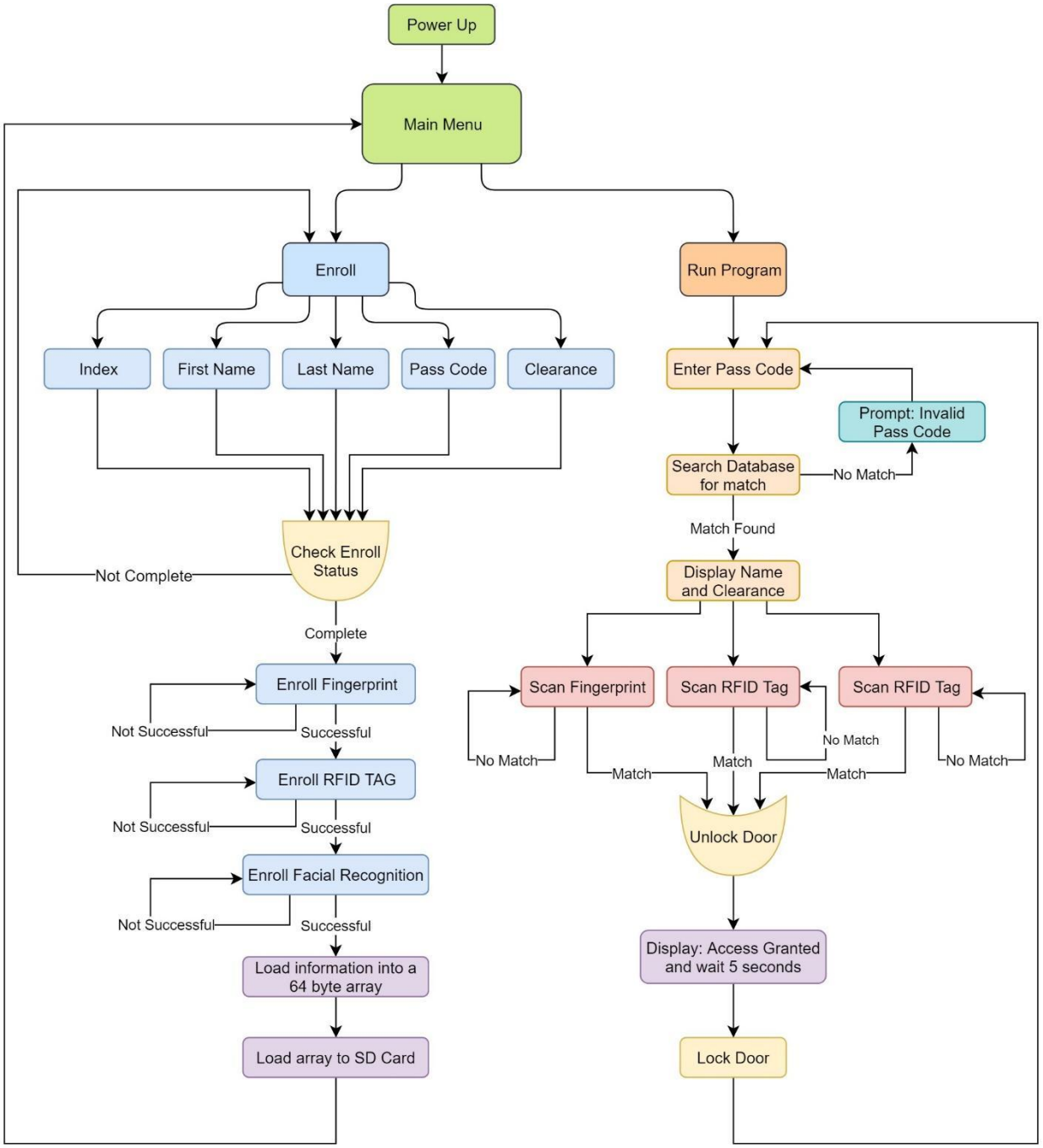


Figure 35 Embedded software design

The program architecture, as shown in Figure 27, is designed to allow the processor to idle within a while loop most of the time and is brought out of its infinite loop using an interrupt that triggers a variety of interrupt service routines. A boolean is used to keep the program This approach was chosen because the TFT touchscreen interface sends a low signal to its interrupt pin whenever the screen is touched so it is a convenient way to wait and respond to a touch command.

For the graphical interface, several scenes are developed. The first scene is the Menu. This screen gives the user the ability to enroll a new person or run the Smart Lock program. When the screen is pressed, an interrupt is triggered and since the program is on the menu screen, an interrupt service routine that corresponds with

the menu is executed. During the interrupt service routine, the program reads the x, and y registers and compares. Depending on the threshold the coordinates fall within the program determines if the Enroll button is pressed or if the Run Program button is pressed.

When the Enroll button is pressed, a sub-menu is loaded that allows the user to select which information to enroll. The user can select an Index number which is the number slot to enroll the account in, the Smart Lock can Support up to 100 Accounts. The user can numberpad screen is loaded. This screen is used to input integers from 0-9. Figure 33 shows how the program decides if the number 1 has been pressed after taking a reading following an interrupt. The interrupt service routine begins by asserting the Touch Screen chip select pin, then entering the command to read the X, Y, and Z registers. If the x value is greater than the threshold value that is between the first and second column and the y value is greater than the threshold between the first and second row, the program decides that the number 1 has been selected. An array is used to store the values that the user enters. For the Index, the value must be between 0-100 otherwise the program displays a prompted that said “invalid entry”.

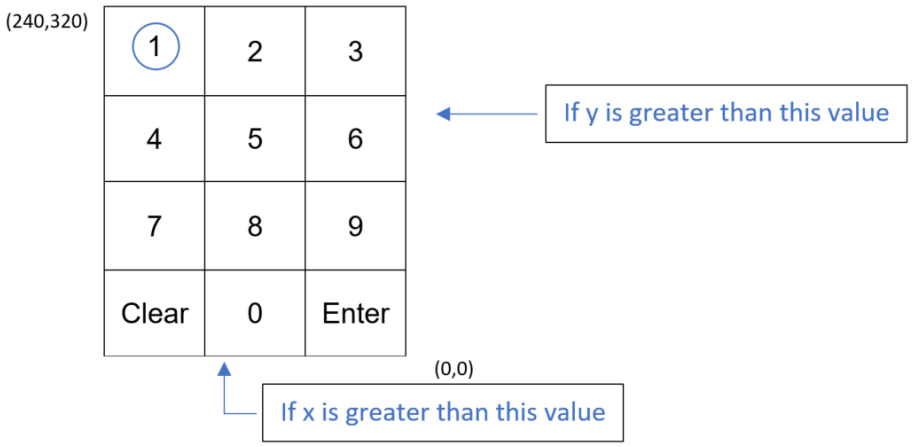


Figure 36 Touch Screen Number Pad

After the user selects an index, the user should enter the First Name. This is done on a similar screen but instead of numbers, the alphabet is divided into 3 different screens. Letters A-I are on the first letters page, J-R on the second letters page, and S-Z on the third. A character array is used to store the user’s entry of the first and last name.

Next the user enters a 6 integer pass code and then is asked to verify the pass code by repeating it. If the repeated pass code differs from the original pass code entered, the program returns a prompt saying invalid entry and asks the user re-enter the password. After 3 failed attempts, the program will ask the user to enter an entirely new pass code then verify it.
Lastly the clearance level can be selected by entering 1 integer. 0 means no clearance and grants zero access. 1 means low level access and grants only entry at specified times. 2 means mid-level access and grants anytime entry. 3 means top secret clearance and grants anytime entry and the ability to enroll users.

When the correct data loads into each of the arrays, the menu page will update and new buttons will appear allowing the user to either enroll the data or return to the main menu.

After the information is enrolled, the program will ask the user to place a finger on the finger print sensor and it is scanned. After a successful scan, the program asks the user to lift their finger and place it back on the fingerprint scanner. After a successful second scan, the program asks the user to lift their finger and place it back on the fingerprint scanner for the third time. If successful, the 3 scans will be enrolled into the index number slot of the finger print sensor's database.

The program then will then ask the user to scan the RFID tag that they would like to enroll for the account. A successful RFID scan will lead the user to then enroll facial recognition data. The user will stand directly in front of the camera and the on board feature detection algorithm will extract facial feature data and store it on its on board database chosen by the index.

After the facial recognition enrollment is complete, all of the information gathered is loaded into a 32-byte array. This array is then uploaded to an offset position within a slot on the SD card and the user receives a prompt that the enrollment is complete. This process is repeated for additional accounts.

When the Run Program button is pressed, a prompt asking the user to enter their passcode is loaded to the LCD screen then the number pad is loaded. After the user enters a 6 digit pass code and selects Enter, the program retrieves the first 1024-byte block from the SD card into an array then parses the array for a sequence that matches the entered passcode. If there is no match, the program retrieves the second 1024-byte block from the SD card and repeats the search. If no match is found, the program retrieves the third 1024-byte block from the SD card and repeats the search for the third time. If no match is found, the program displays a prompt saying "Invalid Entry", then displays another prompt asking the user to enter a valid pass code. When a valid pass code is entered and the program finds a match within the data base, the program displays a welcome prompt and retrieves the first name, last name, and clearance of the user and displays it. The program then powers on the Fingerprint Scanner, the RFID radio antenna, and the facial recognition camera then begins polling to see if a finger is placed on the scanner, if an RFID card is near the antenna, or if a face is detected. If any of these conditions are true, the program checks to see if the scanned fingerprint, RFID, or face matches the enrolled data for that account. If a match is determined, the program displays a welcome prompt and grants the user access as defined by clearance level. After the program grants access to the user, the program will wait for 5 seconds then lock the door and return back to the number pad scene. awaiting a user passcode.

Table 19 Member Array Data Structure

Pass Code	Index	First Name	Last Name	Clearance	RFID UID
6 Bytes	1 Byte	10 Bytes	10 Bytes	1 Byte	4 Bytes

The member array structure as shown in Table 1 details the way user data is organized in the SD card. The first 6 bytes of the array is the user's pass code, used to identify the user. The 7th byte is the index that the user was enrolled in and can hold a value of 0-100 and is used to verify the fingerprint of the selected user because the index will correspond to the index of the user's enrolled fingerprint. Bytes 8-17 hold the first name of the user, and bytes 18-27 hold the last name of the user. Byte 28 holds the user's clearance level. Bytes 29-32 hold the RFID tag's UID number and is used to verify the user when the RFID tag is canned.

8 Administrative Content

Working as a team to develop a smart lock has proven to be a challenging and rewarding experience. The administration of our group was facilitated by use of a shared drive where each of the teammates published their work. Additionally, a WhatsApp group chat was created to ensure that all teammates were able to communicate with each other. These tools allowed everyone to stay on task and report any findings, issues, or doubts as it pertains to the development of the project.

Tasking was assigned on a weekly basis for each team member so that deadlines were met and assignments were submitted on time. By setting tasks it was able to allow for additional time should there be any setbacks due to time constraints or personal matters. By communicating effectively we were able to help each other achieve our goals and work towards finding a compromise when multiple options were found in the design of the product.

As the conclusion of the research and designing phase of the project nears, preparation for the building phase has begun. Meetings have been scheduled to begin to work out equipment ordering and planning for construction of the model that will be used to demonstrate the functionality of the smart lock. Also, a testing plan will be devised so that once products have arrived; they can be tested to ensure that they have been received in working order so that programming can commence. To help with planning, milestone discussions have been noted and will be used throughout the progress of the project.

8.1 Milestone Discussion

Milestones were set from the beginning of the project in order to ensure that deadlines were met according to the course syllabus. By setting milestones the smart lock was kept on schedule in terms of research and design. Along with the milestones our group devised a weekly schedule in which each member had to submit a minimum of 5 written sheets to ensure that the required 30 pages per person was met before the deadline. To make sure that everyone was able to complete their tasks time incorporated in the design for time spent correcting anomalies found during the developing phase which required that additional research be made to correct the observed problem. The senior design 1 and 2 milestone tables outline the task descriptions and dates for which they must be completed by to ensure that they are submitted before the deadline.

Table 20 Senior Design 1 Milestone

Senior Design 1 Milestone		
Description	Week #	Dates
Brainstorming	1	May 14 - May 21
Project Selection	2	May 21 - May 29
Divide and Conquer 1.0 & 2.0	2	May 21 - May 29
Research and Documentation	4	June 7 - July 7
Table of Contents	6	7-Jun
Writing	6	June 7 - July 7
Senior Design 1 Draft	7	7-Jul
Research and Design	7	7-Jul
Finalizing the Paper	8	13-Jul
Final Document	10	20-Jul

Table 21 Senior Design 2 Milestone

Senior Design 2 Milestone		
Description	Week #	Dates
Build Prototype	4	Aug 21 - Sep 21
Testing & Redesign	2	Sep 21 - Oct 5
Finalize Prototype	2	Oct 5 - Oct 20
Peer Presentation		TBA
Final Report		TBA
Final Presentation		TBA

These tables hold absolute dates for which we must complete each task. The reason why the dates are strict is because failure to complete the task by the deadline may result in setbacks that will prevent the submission of the required work by the deadline.

While currently in senior design 1, the absolute dates for senior design 2 have not been obtained as the class has not started and work submission deadlines have not been appointed, thus the dates listed on this table are estimates for what we believe

will be the time frame allowed to submit our work. This table will be updated accordingly once the senior design 2 course has begun and the due dates provided.

8.2 Budget and Finance Discussion

The smart lock project does not have a third party sponsor which means that the team will need to supply the funds necessary to purchase all of the equipment needed. To lower the cost for the parts that are needed for the build, research has been done to find the lowest priced equipment that will satisfy the requirements of the project. The equipment price list is a summary of the parts needed along with the best price found.

Table 22 Smart Lock Cost Analysis

Smart Lock Cost Analysis	
Equipment	Cost
Locking Mechanism [2]	$69.00
Image Processing Camera [2]	$24.16
RFID [2]	$19.99
Finger Print Sensor [2]	$50.00
PCB Design [5 pieces]	$35
PCB components [2 times] [BOM]	$50
Prototype [hardware]	$50
LEDS [10]	$2.99
TFT 2.8" Touchscreen [2]	$30
Batteries (9V Alkaline) [3]	$20
Total Cost	$351.14

Development cost for 2 prototypes will cost the team $351.14 each. Because we expect that not all equipment will work we have purchased extra supplies as shipping times can often delay the team. While this brings up the cost, it will ensure that we are able to meet our deadlines without having to stress for parts to arrive as quickly as possible. Once the smart lock has been tested and is in working order, the cost for each unit will greatly decrease, as additional parts will not be necessary.

9 Appendices

The appendices section lists the appendices that reference the media used to support and develop the smart lock project.

9.1 Appendix B: References

[1] [Online]. Available: https://www.elprocus.com/i2c-bus-protocol-tutorial-interface-applications/.
[2] [Online]. Available: https://www.allaboutcircuits.com/technical-articles/the-i2c-bus-hardware-implementation-details/.
[3] [Online]. Available: http://www.circuitbasics.com/basics-of-the-i2c-communication-protocol/.
[4] [Online]. Available: https://www.allaboutcircuits.com/technical-articles/the-i2c-bus-hardware-implementation-details/.
[5] [Online]. Available: https://www.electronics-tutorial.net/Digital-CMOS-Design/CMOS-Inverter/.
[6] [Online]. Available: https://en.wikipedia.org/wiki/I%C2%B2C#Reference_design.
[7] [Online]. Available: https://i2c.info/i2c-bus-specification.
[8] [Online]. Available: https://www.i2c-bus.org/i2c-primer/clock-generation-stretching-arbitration/.
[9] [Online]. Available: https://techterms.com/definition/lcd.
[10] [Online]. Available: https://en.wikipedia.org/wiki/Liquid-crystal_display.
[11] [Online]. Available: https://electronics.howstuffworks.com/lcd4.htm.
[12] [Online]. Available: https://forums.anandtech.com/threads/active-monitor-vs-passive-monitor.2373904/.
[13] [Online]. Available: https://www.lifewire.com/truth-about-so-called-led-televisions-1847935.

[14] [Online]. Available: https://www.crutchfield.com/S-D8BFesQwIHl/learn/oled-led-tv.html.
[15] [Online]. Available: https://www.techwalla.com/articles/what-is-a-tft-touch-screen.
[16] [Online]. Available: https://www.electronicsnotes.com/articles/electronic_components/electrical-electronic-relay/what-is-a-relay-basics.php.
[17] [Online]. Available: https://www.galco.com/comp/prod/relay.htm.
[18] [Online]. Available: https://www.explainthatstuff.com/howrelayswork.html.
[19] [Online]. Available: https://www.allaboutcircuits.com/technical-articles/basics-of-ssr-solid-state-relay-the-switching-device/.
[20] [Online]. Available: https://www.pickeringtest.com/en-pk/kb/hardware-topics/relay-reliability/choose-a-reliable-reed-relay-construction.
[21] Kubo, in 2014 7th International Conference on Intelligent Computation Technology and Automation, Changsha, China, 2014.
[22] [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification.
[23] [Online]. Available: https://www.epc-rfid.info/rfid.
[24] [Online]. Available: https://internetofthingsagenda.techtarget.com/Definition/transponder.
[25] [Online]. Available: https://www.camcode.com/asset-tags/what-are-rfid-tags/.
[26] [Online]. Available: https://www.amazon.com/Mifare-RFID-Electromagnetic-Arduino-Raspberry/dp/B0722M7M63.
[27] [Online]. Available: https://www.dhs.gov/biometrics.
[28] [Online]. Available: https://www.sciencedirect.com/topics/computer-science/biometric-technology
[29] [Online]. Available: https://computer.howstuffworks.com/fingerprint-scanner2.htm
[30] [Online]. Available: https://www.researchgate.net/publication/224382169_Review_of_ finger_print_sensing_technologies.
[31] [Online]. Available: https://internetofthingsagenda.techtarget.com/definition/transponder.
[32] [Online]. Available: https://www.ieee.org/about/corporate/governance/p7-8.html
[33] [Online]. Available: https://www.dicardiology.com/content/fda-says-rfid-devices-cause-malfunctions-pacemakers-icds
[34] [Online]. Available: https://www.maximintegrated.com/en/app-notes/index.mvp/id/2031.
[35] [Online]. Available: http://www.kicad-pcb.org/.
[36] [Online]. Available: https://www.autodesk.com/products/eagle/overview.
[37] [Online]. Available: https://learn.sparkfun.com/tutorials/designing-pcbs-smd-footprints/all.

[38] [Online]. Available: https://www.quora.com/What-does-a-%E2%80%9Cfootprint%E2%80%9D-mean-in-PCB-design.
[39] [Online]. Available: https://www.quadcept.com/en/manual/common/step6pcb.
[40] [Online]. Available: http://kicad-pcb.org/libraries/klc/.
[41] [Online]. Available: https://maker.pro/pcb/tutorial/how-to-make-a-printed-circuit-board-pcb.
[42] [Online]. Available: https://www.theengineeringprojects.com/2018/11/use-of-silk-screen-technology-in-printed-circuit-board-pcb.html.
[43] [Online]. Available: https://www.autodesk.com/products/eagle/blog/printed-circuit-boards-10000-feet-introduction-electronics-beginners/.
[44] [Online]. Available: http://www.robotroom.com/Silkscreen-and-Solder-Mask-1.html.
[45] [Online]. Available: https://www.google.com/search?q=copper+in+pcb&oq=copper+in+pcb&aqs=chrome..69i57.3734j0j1&sourceid=chrome&ie=UTF-8.
[46] [Online]. Available: https://www.raypcb.com/heavy-copper-pcb/.
[47] [Online]. Available: https://www.indiamart.com/proddetail/copper-clad-pcb-19966857891.html.
[48] [Online]. Available: https://www.theengineeringprojects.com/2018/04/rigid-pcb.html.
[49] [Online]. Available: https://blogs.mentor.com/jimmartens/blog/2015/08/11/why-impose-pcb-design-constraints/.
[50] [Online]. Available: https://www.tempoautomation.com/blog/pcb-thermal-design-for-manufacturing/.
[51] [Online]. Available: https://macrofab.com/blog/picking-right-trace-width/.
[52] [Online]. Available: https://electronics.stackexchange.com/questions/5403/standard-pcb-trace-widths.
[53] [Online]. Available: https://en.wikipedia.org/wiki/Printed_circuit_board.
[54] [Online]. Available: https://www.dummies.com/programming/electronics/components/switches-in-electronic-circuits-poles-and-throws/.
[55] [Online]. Available: http://resources.uwcsea.edu.sg/UWCSEA_DT_East/Electronics/Electronics/Switches.html.
[56] [Online]. Available: http://resources.uwcsea.edu.sg/UWCSEA_DT_East/Electronics/Electronics/Switches.html.
[57] [Online]. Available: https://evatronix.com/en/offer/pcb/pcb-layout-design.
[58] [Online]. Available:https://layout.alimb.us/50-how-to-make-pcb-layout-fv0x/how-to-make-pcb-layout-how-to-design-a-pcb-layout-circuit-basics-2/.
[59] [Online]. Available: https://www.elprocus.com/different-types-printed-circuit-boards/.
[60] [Online]. Available: https://www.theengineeringprojects.com/2018/03/single-sided-pcb.html.
[61] [Online]. Available: https://heracolights.com/2014/03/07/led-vs-smd/.
[62] [Online]. Available: https://www.electronics-notes.com/articles/electronic_components/surface-mount-technology-smd-smt/what-is-smt-primer-tutorial.php.

[63] [Online]. Available: https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C1R_datasheet_V1%205_20140312.pdf
[64] [Online]. Available: https://en.wikipedia.org/wiki/Eclipse_(software)
[65] [Online]. Available: https://www.buydisplay.com/download/ic/XPT2046.pdf
[66] [Online]. Available https://firebase.google.com/docs/database/
[67] [Online]. Available https://savvyapps.com/blog/firebase-realtime-database-vs-cloud-firestore-for-your-app
[68] [Online]. Available https://softwarehut.com/blog/how-to-communicate-small-arduino-device-with-android-phone-via-bluetooth/
[69] [Online]. Available http://www.electronics-lab.com/project/arduino-communication-android-app-via-bluetooth/
[70] [Online]. Available https://medium.com/blueprint-by-intuit/native-mobile-app-design-overall-principles-and-common-patterns-26edee8ced10
[71] [Online]. Available https://devtechnosys.com/know-about-industry-standard-for-app-development
[72] [Online]. Available https://developer.android.com/guide/topics/connectivity/bluetooth
[73] [Online]. Available https://developer.android.com/guide/topics/connectivity/bluetooth-le.html
[74] [Online]. Available https://examples.javacodegeeks.com/android/android-bluetooth-connection-example/
[75] [Online]. Available https://www.tutorialspoint.com/android/android_bluetooth.htm
[76] [Online]. Available https://www.thedroidsonroids.com/blog/flutter-in-mobile-app-development-pros-and-cons-for-app-owners
[77] [Online]. Available https://hackernoon.com/whats-revolutionary-about-flutter-946915b09514
[78] [Online]. Available https://medium.com/asos-techblog/flutter-vs-react-native-for-ios-android-app-development-c41b4e038db9
[79] [Online]. Available http://www.ipc.org/TOC/IPC-2221.pdf
[80] [Online]. Available https://www.schneider-electric.com/resources/sites/SCHNEIDER_ELECTRIC/content/live/FAQS/176000/FA176928/en_US/Degrees%20of%20protection%20IP,IK,%20NEMA.pdf
[81] [Online]. Available https://www.cui.com/catalog/resource/iec-62368-1-an-introduction-to-the-new-safety-standard-for-ict-and-av-equipment.pdf