A1 Security System

Department of Electrical Engineering and Computer Science
University of Central Florida
Dr. Lei Wei

Group 4

Timothy Henry	Computer Engineer
Brandon James	Computer Engineer
Jonathan Chew	Electrical Engineer

Table of Contents

1. List of Figures

2. List of Tables

3. Executive Summary

According to the US Department of Justice, there are more than 2.5 million home intrusions are reported annually. 75% of burglaries occur on residential property. In addition to the total amount of break-ins, 30% of all reported burglaries occur when homeowners leave the front door unlocked/unattended. To put this into perspective, every year more than 750,000 family owned properties are left completely vulnerable to burglars because the owners simply forgot to lock their doors. If families can have the ability to access the lock on their front door by a push of a button anytime and anywhere this will undoubtedly reduce the number of intrusions. In the world of technology, Smart Home Security Devices are quickly becoming a necessity for the average family household, however, because of high prices for these systems, families have long delayed this expense until their first break in. With all the smart security system devices available to consumers, an affordable and fully equipped security device seems to still be missing from the market. As society's demand for all-in-one security device continues to grow, this necessity has inspired us to create a product that will contain all the features a homeowner desires in a security system. Compared to the isolated single function security devices currently on the market, our design will work parallel with several security peripherals and mobile application capabilities to meet all the security needs for the homeowners. Our design will guarantee low cost, user friendliness, easy installation, and most importantly, safety to families and their belongings.

The main objective of this project is to integrate several essential hardwares together to form an all-in-one security system that will operate seamlessly, and in some instances, hands-free. The hardware will include both a Wi-Fi and Bluetooth features, LCD display, microcontroller (ESP WROOM-32), microprocessor (Raspberry Pi 3), camera module, PIR sensor, and a fingerprint scanner. In addition to the hardware, will produce a mobile application that shall support the security system's interface. The mobile application will allow users to lock and unlock doors, view camera pictures, and be able to record a comprehensive list of entering or exiting activity. The mobile application that shall have full interaction with the electronic door lock as well. The security system will run only on the mobile Android operating system for this project. Over the course of the semester the application will be developed, completed, and presented to the faculty on the designated presentation day. There will be two options for the user to communicate wirelessly with the security system. The Wi-Fi module will allow users to correspond with the security system remotely, as long as there is a stable network connection. However, even in the case of no internet connectivity, users of this system will still be able to wirelessly interact with security device via bluetooth transmission. A Raspberry Pi 3 will be communicating with our main microcontroller in order to interface a camera module. The Raspberry Pi 3 will be the appropriate microprocessor for efficient image processing. The camera NoIR module is built specifically for the Raspberry Pi 3 and will be responsible for capturing and presenting live images as guests arrive at the front door after a

PIR sensor senses movement. The camera module shall implement facial recognition as a security feature as well. The PIR sensor main task is to detect movement within a few walking distance from the security system. The camera module shall intake data using its high resolution pixel lens that will be capable enough to implement facial recognition. The microprocessor will receive digital data from the camera and store images in memory for later use. The Raspberry Pi 3 shall be able to send signals of information to the main microcontroller when receiving a valid facial recognition scan or digital data from images that have been taken. The security system will also incorporate a fingerprint scanner that is capable of remembering 20 different scans.

The developers will implement a low power consumption model to decrease costs for consumers and increase the operating lifespan. The group has decided to use a rechargeable battery pack that is capable of outputting 12 volts DC at 6000 mAh. After calculations, the consumers should be capable of using the security system for three weeks for an average family after a full charge. A huge drawback with batteries is that they can only supply power for a duration of time. The users are then held responsible to charge the batteries whenever the end of the battery's life approaches. The microcontroller will monitor battery health when in active mode and display battery percentage on a LCD display. The users will have plenty of notice before the battery health depletes entirely. The 16x2 LCD display shall show users the locking status along with battery percentage. The LCD display will be mounted onto the outer case for simple viewing. The security system will be using a door locking solenoid that remains in locked position when no power is being drawn. To unlock the security system, the microcontroller will control a switch to run power through the solenoid that will retract the metal beam. The security system is required to have power in order for the user to have the ability to enter/exit. The security system will not be able to be opened using physical key, however a backup battery will be used to operate the security system for a short limited time.

For our project, the group will collaboratively construct a security system device that shall emulate similar products on the market today. The way this project will stand out is by gearing the design towards a more dependable, inexpensive, low power consumption, and easy quick installation procedures. The security system will guarantee a more secure home by eliminating the use of a physical key, and use other biometric ways to ensure a safe identity before entering. The system will be try to implement a plug and play aspect as much as possible to help consumers install our product. A goal the group will like to reach is to keep the security system's materials cost to be below $200. Some security systems currently charge monthly for their features or cost way above the $500 mark. Our final goal is for the security system to appear as a product that could potentially be on the market someday. With adequate research, careful development and hard work, the group will create the A1 security system.

4. Project Requirements and Specifications

Specifications and requirements have came forward during the development and research process. For A1 Security System to be the most effective and secure system on the market, our group members will need to meet all specifications by the end of this developmental process to ensure a complete successful project. Specifications and requirements must be explained in thorough detail to provide all the information on functionality for the project. The specifications will be divided into three parts: system, hardware, and software.

4.1 System

- Shall only be installed on doors that have a deadbolt lock.
- All main components of security system must be enclosed in protective casing.
- Finished product shall be able to mount behind door to ensure safety from outside weather and theft.
- Finished product shall weigh less than 5 pounds for easy packaging including the door lock.
- Shall be battery powered.
- Shall implement a low power mode for battery life conservation.
- Shall implement a pressable button for fast and easy exiting that will be exposed on security system casing.
- Shall be able to communicate with security system through mobile application
- Shall implement fast startup times of less than a 1 second.
- Shall be able to lock/unlock door incase of power system failures using a physical master lock key.
- Shall implement facial recognition and fingerprint scanning for easy unlocking.
- Shall enter low power mode after 30 seconds after being idle.

4.2 Hardware

- Main controller shall control all peripherals autonomously after proper system installation.
- Main microcontroller shall sync all components to a main clock.
- Main microcontroller shall to be able to receive inputs from PIR sensor, bluetooth, and wifi module when in low power mode.
- Main controller shall display all text messages onto LCD display including battery health and door locking status.
- Main controller shall be able to power door lock servo for locking/unlocking functions.
- Main power source shall run on a rechargeable battery power bank.
- The main power source will be backed up by a temporary battery pack to ensure the system will never have any power failures.
- PIR sensors shall turn on system when sensing motion

- Camera module shall have minimum high resolution for accurate facial recognition.
- Wifi module shall allow users to communicate with security system with no distance limitations.
- Bluetooth module shall allow users to communicate with security system at close distances less than 10 feet and for devices with no internet connection.
- Fingerprint scanner shall be mounted on the door handle for easy access for users.
- Fingerprint scanner shall have an easy setup and capabilities for memorizing 20 fingerprints at a time.
- PCB design shall deliver power to all components to the security system.

4.3 Software

- Microcontroller shall be programmed in C language.
- Mobile application shall operate on android operating system.
- Mobile application shall be able to lock/unlock door over wifi and bluetooth connection.
- Mobile application must be able to fulfill requests if a guests requests access for entrance.
- Mobile application must be able to receive live feed from camera module
- Mobile application will have option to receive push notifications when security system has been tampered with.
- Mobile application will be user friendly with simple interface displaying controls for the security system.

5. Related Standards and Design Constraints

5.1 Design Constraints

An engineer will undergo constraints in every project that will ever be attempted in his/her career. Constraints are conditions where engineers are required to make happen or would like to happen for a particular design. Constraints will appear always in the real workplace and must always be accounted. They set boundaries on what the outcome can and cannot be achieved. For a senior design project, there are many constraints that our group will have to encounter and realize before attempting any research. Time constraints cause a major set backs on the capabilities our project can ultimately become. Thorough projects in the industry will require months of researching, manufacturing, developing, and testing, which will equal years of work. The time frame for our project must be

completed in 7 months. Agreeing to finish the project in consecutive semesters, Spring and Summer, our group will lose almost three weeks worth of time compared to other sections. With the limited amount of time, our group has allocated each month for certain tasks to ensure a successful project.

First and second month will be spent finalizing a project idea, formulating requirements and specifications, and gathering research on all the functions and parts needed for the overall design. Third month is spent documenting all research that has be completed and ordering all parts to be tested. Fourth month, the group shall test all ordered parts to verify their functionality. Group members shall be able to build design onto breadboard. PCB board will have to be in the process of developing on Eagle CAD software, and mobile application will be in the beginning stages of development. All documentation needed to finish project will be recorded and completed at this time. Fifth month, the PCB board design shall be finalized and sent to manufacturing company for professional development. This process may be time lengthy, so our group must account for this constraint. Mobile application shall be almost completed are ready to communicate with security system. Sixth month, the group will have to test and simulate security system. This step process will take up the majority of the time. The option to purchase or 3D print a proper case will be determined on status of the project fully connected and running smoothly. Seventh month, the group will finalize all work and prepare for presentation. The group must be able to follow this strict time schedule to ensure a smooth (success synonym project).

Economic constraints limit the parts that will be purchased to fully maximize performance. This project is not sponsored by a company, therefore, is fully student funded. As a group, we have agreed to purchase only what we need and must also account for mistakes if they do occur. Our spending costs will accumulate quickly and must stay within our budget. When establishing a budget of $150 per group member, the budget has set a constraint on where we decide on allocating the money spent. Economic constraints will vary the overall performance, but not the functionality.

Safety constraint is placed that has steered our design to operate at low voltages. Instead of pulling 120V from power grid, the security system is powered by 9V D batteries. High voltage levels will raise a great amount of concerns especially with electrical engineers with few experience. Working at low voltages will maintain the development process safe for the creators, and final product safe for consumers. A software constraint limits the ability to create a mobile application for all mobile devices. Apple products contain licenses that need to be purchased in order to create an application for IOS devices. Android OS is open sourced based, which allows our group to design an application without additional costs. With these constraints stated in full detail, we can continue the research and development process.

5.2 Related Standards

5.2.1 Wifi IEEE Standards

Standards	Max Speed	Frequency
802.11	2 Mbps	2.4 GHz
802.11a	54 Mbps	5 GHz
802.11b	11 Mbps	2.4 GHz
802.11g	54 Mbps	2.4 GHz
802.11n	300 Mbps	2.4 / 5 GHz
802.11ac	1300 Mbps(5 GHz)	2.4 / 5 GHz

Table 1 - WiFi IEEE Standards

Wi-Fi currently has 5 standards: a,b,g,n, and ac, in order from oldest to newest, with 802.11 being the oldest standard of all. In 802.11, which was first introduced in 1997 by the Institute of Electrical and Electronic Engineers(IEEE), the maximum supported speed was 2Mbps. Following 802.11, are 802.11a and 802.11b, both of which expanded on what 802.11 had to offer. 802.11b supported max speeds of up to 11 Mbps in the 2.4 GHz frequency. 802.11a, which was developed at the same time as 802.11a , had a max speed of up to 54 mbps in the 5GHz frequency, however, because it was so expensive, it was more prevalent in the business community rather than in homes.

Next, 802.11g was introduced in 2002, with the hopes of bringing 802.11a and 802.11b together into one standard. 802.11g supports a speed of up to 54 Mbps, but in the 2.4 GHz frequency, unlike 802.11a. It was also backwards compatible with 802.11b. Following this, 802.11n(Wireless N) was launched in 2009, with a mas speed of up to 300 Mbps. It also included a greater signal than its predecessors. Lastly, the newest and most powerful standard yet it 802.11ac. This standard supports a max speed of 1300 Mbps in the 5 GHz frequency and a max speed of 450 Mbps in the 2.4 GHz frequency.

5.2.2 Bluetooth Standards

The Institute of Electrical and Electronics Engineers, or IEEE, is a group of professional engineers that focus on the advancement and educational purposes

of computer, electronics and telecommunication subjects. It is an organization that complies of over 420,000 members, most of which are electrical or electronics engineers but over the course of years it has grown to expand disciplines ranging from computer engineering, computer science, mathematics, physics, and information technology to name a few. Of all standard making organizations across the globe, IEEE is by far one of the biggest and most credible. Their standards and protocol functions span many industries which include information technology, wireless communication systems, transportation, and even healthcare. Some of the most well known and recognized technology standards today are the internet and network protocol standards in the 802 sections which comprise 802.11 for wireless local area networks.

Bluetooth was standardized by the Institute of Electrical and Electronics Engineers with the name of IEEE 802.15.1. However, what makes this technology and its documentation interesting is that the IEEE does not preserve the standard. The standard and the overall design and management of Bluetooth is maintained by the Bluetooth Special Interest Group, or SIG. The organization group was first established back in September 1998, which is relatively a baby compared to other standards making associations. This specialized group of individuals, maintain design requirements, it markets the technology across the globe, it supervises the research and development of Bluetooth, and it assures its own trademarks involved with the name. When a company or manufacturing business intends produce and advertise a good or device as a Bluetooth operating device, it must be up to par with the Bluetooth SIG set standards. Another thing of note about the Bluetooth Special Interest Group is that this faction of professionals are together for non-profit. They do not seek to make a revenue, but to educate, form camaraderie between industry professionals, and draft standards for Bluetooth. The association also does not manufacture any products, Bluetooth or not, nor do they make contracts to sell products.

5.2.3 Android Application Standards

When it comes to the Android Development, Google makes the standards that Developers should follow to ensure a well functioning application with a great design. In the instance of design, the currently recommended standard is Material Design. It has specifics on how an interface should look, transition, and animate across all devices. Firstly introduced with Android 5.0, it has quickly become the go-to standard for Android Development.

Furthermore, Google has Standards and Guidelines related to Core Application Quality. The standards that we are concerned about are Visual design and user interaction, functionality,compatibility,performance, and stability, security. In Visual Design and user Interaction, the group must ensure that the application uses common UI patterns and Icons, while not changing the expected behavior of systems icons, like the back button. Along with this, we must confirm that the

application supports standard system back button navigation, while also making all the dialogs dismissible with the press of a back button. Lastly in this section, we must make sure that notifications only persistent if an event is ongoing(such as music playing) and that they do not contain advertisements. All of these can be found in the Visual design and user interaction section, under the IDs of UX-B1, UX-N1, UX-N2,and UX-S1.

In terms of Functionality, we must ensure that the application only makes requests for the minimum amount of permissions needed, does not use services when the application is running in the background and not needed(this can cause a drain of battery), and also we must ensure that the application state is preserved when opening and closing the application. These can be found in the in the Functionality section of the Core App Quality Standards, under the IDs of FN-P1, FN-S1, and FN-S2.

In the area of compatibility, performance and stability, we must ensure that the application does not crash, force close, freeze, or function in any unusual way,that the app is compatible with the newest Android SDK and also the minimum target SDK that is selected when starting the project, and that the app displays visual UI elements without pixelation, distortion, and blurring. All of these standards go a long way in guaranteeing that the application is an enjoyable experience for the user. All of these standards can be found in the compatibility, performance, and stability guidelines with IDs PS-S1, PS-T1, PS-V1, and PS-V2.

Lastly, we have the category of security. To follow the standards of Android Security, we have to make sure that all private data is stored in the application's internal storage, all network traffic is sent over SSL, all intents and broadcasts follow secure best practices, and all libraries, dependencies, and Software Development Kits are up to date. All of these aforementioned items certify that the application is a reliable and guarded experience. The last thing we would want is for the user's data to be stolen. These standards can be found in the Security section of the Android Core App Quality Guidelines with IDs SC-D1, SC-D3,SC-N1,and SC-U1.

6. Hardware Research

6.1 Similar Projects

The first part of research that was conducted was to revisit previous Senior Design security system projects that have been completed in other semesters. This will allow us to create new ideas that have not been implemented before. Viewing previous projects will give us a foundation and clearer idea on what other groups were capable of completing for their final product. Two projects were chosen for research due to similar requirements and features that our team want to be implement.

Home Observable Monitoring Entry System (HOMES) was created in Spring 2015. The senior design group members are Colleen Caffey, Bruno Calabria, and Ricardo Georges. The HOMES project has many functions that our security system would want to implement. Sensors to active the system when it senses movement. Facial recognition and fingerprint scanning will grant access to the system. We differ from the HOMEs project because of our facial recognition approach. Our security system will incorporate facial recognition within the mobile application. This will allow us to use existing processing power from our phones to create this spectacular feature. Another difference between the two projects is our security system will be able to lock and unlock the door handle through wifi. Does not matter where the user is, as long as there is an internet, the user can communicate with the security system. HOMES project uses RFID and Bluetooth are used for access as well.

The other previous project we have researched is the Close to Home finished in Spring 2014. The creators for the project are Joshua Early, Marc Garcia, Daniel Krummen, and Nicolas Godfrey. This project is designed for home automation for the entire home. That includes checking statuses for home appliances, windows, and controlling house temperature and ceiling fans. They have implemented a central hub microcontroller to control all of their peripherals along with an android mobile device to create their mobile application. One feature that will be implemented from this project is the door lock mechanism, and the mobile application functionality. The door lock used as a servo motor with low voltages of 6V which is very beneficial to the design because this allows a less stronger power supply. The mobile application features include easy communication between user and security system. This security system requires a direct power source so a power outlet is necessary for functionality. Our design will guarantee low voltages and run on strictly batteries. The goal is to maintain the cheapest battery alternative along with high power outputs and long lifespans. Rechargeable batteries will be a great alternative if possible due to cutting major costs for users in the long run.

Because these senior design projects were both sponsored, the cost for the projects had a high budget of $1500+ for both projects. This is considered a very expensive final product. Our team will like to reduce the cost of production for the final product to be less than $150. The total cost for researching and developing will most definitely costs more than $150, however, the final product will be able to be listed at a market price of $150 or less. We will also like to improve the all-in-one aspect with overall easy installation. The previous projects have many components that need to be installed around the household in order to function properly. Our design will be centralized with no detachments.

6.2 Products In Market

Products that are similar to our project are generally much more expensive. They can range up to $450 for the package or charge $50 monthly for the security services. For a customer that agrees to paying $50 a month for these security services can run them up to $600 a year. There are similarities that are provided in the existing market like a touchscreen interface, wireless communications, and easy customization. The Simon XTi Wireless Home Security Touch screen Package is marketed at $450. This product acts like a central hub with a touchscreen display that can control all of its peripherals. The system supports live streaming through its camera module. There is an alarm feature that will go off when security system is being tampered. The interface can support up to 40 electronic devices. The system is equipped with 4 sensors to be placed around the house for extra security for easy accessible entrances like windows and backdoors. The camera module can retain all images taken are saved in memory. The product has lighting control and voice recognition. This product is ideal for the project our design would like to replicate without the high costs.

6.3 Main Microcontroller

First we will discuss what a microcontroller is and what they are responsible for, also what these things called microcontrollers are possible of doing. A microcontroller is kind of like the brains of an integrated electrical circuit, it has the ability to control everything on a circuit board. We have definitely heard of the CPU before, Central Processing Unit, the unit that reads instructions and makes computations and logical decisions based on what the program says in its code. The CPU is a control unit and a processing unit and it is all stationed within a microcontroller. These devices are specialized devices that do only certain things specifically well. Microcontrollers, however, nowadays often come with complete systems on a chip. What that means is that the board that the microcontroller comes embedded on is usually already connected electronically to different components around the board. It could be connected to various peripherals like a digital input, radio signal components, and maybe an analog input. Sometimes systems on a chip come preinstalled with things like GPUs, graphics processing units, Wi-Fi modules built and manufactured to the board, or maybe they come with multiple CPU chips called dual-core or quad-core chips. So in general a good majority of microcontrollers in today's market are “system on a chip” microcontrollers in which the boards they are embedded on come connected to different peripherals. Those peripherals typically include:

- The microcontroller or microprocessor itself
- a memory module for ROM and/or RAM, flash memory
- Timers
- USB (Universal Serial Bus)
- Ethernet
- Voltage and/or power management components

- SPI (Serial Peripheral Interface)
- UART (Universal Asynchronous Receiver Transmitter)

For this project specifically, the team will conduct and use one robust microcontroller to be in direct on control over the various components that to transmit and receive data from and to the microcontroller. We have a few requirements and desirables that we would like to see from the microcontroller we choose to use as our main microcontroller. Throughout the beginning of this semester our team has set out goals they would like to see from the main microcontroller. Our design has been changing constantly from the beginning not because of anything negative but because of new concepts, new ideas and new research that we have been conducting to get our ideas out of our heads and into reality. During our research we have found many viable options from across the world and across the net that can meet our specifications. So we have decided to pick our top four microcontrollers that can meet those standards while also being reasonable for the team and compare and contrast them so we can pick a clear winner for use as the main microcontroller for the Smart Integrated Home Security System.

6.3.1 Arduino Due

The Arduino Due processing board is one of the most powerful boards ever devised by the computer hardware company called Arduino based out of Italy. The company has been an open source program from its start and the software and hardware are apparently smooth and burdenless to use for up and coming young technologist. For years upon years, Arduinos have been placed to head hundreds and hundreds of projects across the world. One of the main arguments for utilizing an Arduino microcontroller over the many other microcontrollers out there is that the Arduino IDE, or Integrated Development Environment, is cross-platform. The IDE can be run on Windows, Apple's MacOS, and Linux which is opposite to what most microcontrollers IDE's run on which is Windows. Arduino boards are relatively cheap compared to other microcontrollers, some really low cost boards can be amassed together by hand.

The Arduino board the team is considering to use as our main microcontroller to use as the brains of our system is the Arduino Due. The Due is a more powerful and enhanced board than the very popular Arduino Uno. This board is the first board by the Italian based company to have come with a 32-bit ARM CPU to run the instructions on the Arduino Due. Arduino itself said on is website that the board with all of its many inputs were made for more larger scale projects and we believe this project is extensive enough to employ this board for our project. The Due has 54 general digit input and output pins and 12 of them can be used as PWM (Pulse-Width Modulation) pins. This powerful board has 4 pairs of UART pins useful for situations where data can be received and transmitted to and from the board to the many peripherals that we plan to use through our design. There is a 84 MHz rated clock on the board, and power jack, erase and reset buttons

located on the board. The major thing that our group will have to consider and deliberate on is the fact that the Arduino Due board completely operates with a maximum of 3.3 volts only. So if we as a team forget that important specification for the board and place a 5 volt input into the board we could see some issues, where the board can be severely damaged. Here are some of the major specifications of the Arduino Due:

- 32-bit Atmel SAM3X8E ARM Cortex-M3 CPU
- 54 digital pins
- 12 Analog pins
- 3.3 Voltage operation
- 512 KB of flash memory
- 96 KB of SRAM
- USB Powered connection

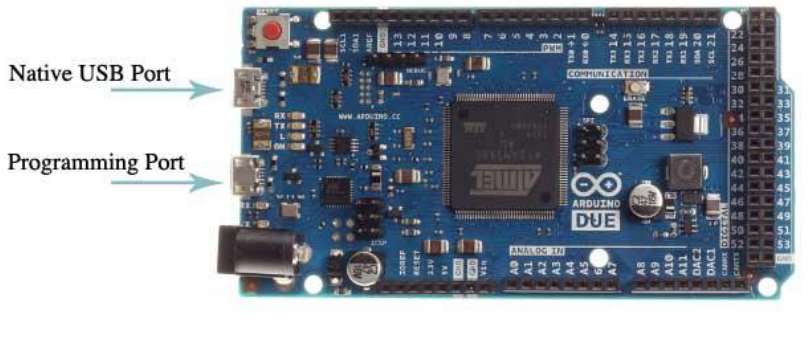

Figure 1 - Arduino Duo Development Board
Pending Permission from arduino.cc

6.3.2 BeagleBone Black Wireless

The BeagleBone Wireless is a dynamic and fully capable board to complete even the most demanding of projects for hobbyists around. The board was constructed by the BeagleBoard.org Foundation, a group that is non-profit and seeks to educated and push the passion of technology to youngsters. The BeagleBoard.org Foundation is a combination of like minded individuals from the Fortune 500 company called Texas Instruments and other companies to create trailblazing, innovative and unconstrained devices for anyone. On the Beagle website there are forums for persons to ask questions and look at board documentation, free of cost. Their boards are said to be fanless and reasonable cost for the amount of processing that you need to complete your project. All of the Beagle boards are ran by low-powered Texas Instruments processor, like for example the ARM Cortex series of processors.

The BeagleBone Black Wireless is essentially the upgraded version of the BeagleBone Black which was released back in 2013. The boards are basically

the same, it's just that the BeagleBone Black Wireless got rid of the 10/100 Ethernet port and now comes with a built-in Wi-Fi module (802.11 b/g/n 2.4 GHz Wi-Fi) and Bluetooth 4.1 plus BLE. This board has third party support for Android and Ubuntu operating systems. When programming the BeagleBone Black Wireless board one must plug in a USB cable from a computer to the USB hub attached to the board. The USB hub embedded on the board utilizes USB 2.0 which means it has a maximum signal rate of 480 Mbits/sec. Once plugged in, a program will pop up called "Cloud9 IDE". This is the software environment that one will use to write code and instructions to the board. The coding language that is used to program the BeagleBone board is JavaScript. There are four LEDs on the board that are blue, a mini HDMI port for connection to an HD monitor, and there are 3 buttons, power button, boot power, and reset button. The rest of the specifications on the board are:

- Octavo Systems OSD3358 1GHz ARM® Cortex-A8 processor
- 512 MB RAM
- 4 GB flash storage
- 3D graphics accelerator
- HDMI
- 2.4 GHz Wi-Fi

6.3.3 Arduino MEGA 2560

The MEGA 2560 was designed and released by the Arduino company, the same company that delivered the Arduino Due. The Arduino Due as we can recall is another microcontroller that we are comparing in this section. Like the Due, this board is similar in power and can see through to the end of project that are demanding and complex. On the Arduino site they say that this microcontroller is a remarkable one for robotics projects. Just like the Arduino Due and all other Arduino boards, this board can be programmed in the Arduino Software IDE. Arduino has a way of simplifying conditions for their customers with a central hub of software to get jobs done.

The board comes with an extensive amount of digital connection pins, 54 to be exact which can be used as input or be utilized as output. This value is exactly the same amount of pins on the Arduino Due. Interestingly enough the pins on the Arduino MEGA 2560 operate at 5 volts each which is higher than the Due, operating at 3.3 volts across the board. The MEGA has four pairs of UARTs, transmitter and receiver pins where the appropriate amount of important data can be shared between components. Having a decent supply of Rx and Tx pins cannot be understated in terms of our project, we have sensitive data that must be able to pass through our system. Also there is an added layer of preservation built in within the Arduino MEGA. For instance, the USB port on your computer has protection inside of it but this board comes with a what they call a resettable polyfuse which will break the connection up till when the overburden is no long

putting a stranglehold on the system. The MEGA board can be equipped with 6 volts to 20 volts from external sources but according to our research, the board is more suitable for a voltage range of 7 volts to 12 volts to run smoothly. A resource of less than 7 volts will cause the input/output pins to supply voltage of less than five. Now a source of more than 12 volts can work, but it won't work for long as the voltage regulator can overheat and extensive damage can then not be avoided. An important list of documented information is listed below:

- 8-Bit ATmega 2560 CPU @ 16 MHz
- Operating Voltage 5 Volts
- 54 Input/Output pins
- 256 KB of flash storage
- 4 pairs of UARTs for serial connection
- USB port
- Reset Button
- Power Jack
- 8 KB SRAM

6.3.4 ESP-WROOM 32

The last system on a chip that the team is considering for use as the main microcontroller is the ESP32 by Espressif Systems. Now Espressif Systems, which is located in Shanghai Park, administers small current sapping devices to hobbyist and newbie alike around the world. The company Espressif not only makes microcontrollers and wireless connectivity modules, but they conduct cutting edge research and development strategies. This potentially means that the kind of technology that Espressif outputs, are goods that have been tried and tested, things that the group has stated they appreciated. Espressif has created a multitude of products, their Internet of Things (IoT) can be found in diversified products extending from DVD players, home appliances, smart television sets, and automation vehicules. They have a mission to provide innovative robotics and solutions but what's interesting is their goal to reduce Wi-Fi and Bluetooth manufacturing waste.

Espressif's ESP32 has, what we believe, the features it takes for a device of this nature to be a force to be reckoned with. The microcontroller is the upgraded, newer version to the ESP8266, which was reviewed by many as a terrific board, but had a slew of shortcomings like features and versatility. This board is a comprehensive beast that can handle the many modern day demands of projects. Integrated within the ESP32 are two major wireless connection modules that are embedded, Wi-Fi and Bluetooth. The Wi-Fi chip inside the board is incorporated with 802.11 b/g/n latest protocols. The Bluetooth comes with the newer Bluetooth Low-Energy with adds to the marketing claims by Espressif saying that this microcontroller ultra low power. Another upgrade that the ESP32 retains above the ESP8266 is the number of GP input and output pins. The

ESP8266 had only seventeen while the more advanced ESP32 has thirty two pins. On the board lies a Micro-B USB port which can be used to connect to the user's computer to program and govern the microcontroller. This port additional can be used to power on the all of the components on the board. For further power management, the ESP32 is also laced with an infrastructure for single cell lithium polymer batteries for the board and a lithium polymer charger. It comes with a two pin JST connector for the batteries which will benefit a project to make it more appealing to some.

The Espressif IDF is the official Internet of Things development framework for the ESP32 microcontroller. This is an open source library hosted on github. The code is written mainly in C. It also contains content for making changes to the flash storage on the microcontroller. The framework contains necessary c functions to communicate over wifi and bluetooth. This includes setting up a wifi access point, connecting to a wifi access point (including enterprise), http requests, openssl components, coap server… Without this the microcontroller would be almost useless as we would have to reverse engineer all the programming and drivers for the board. With openssl already implemented we have the tools for provide the security that a lock needs to operate effectively over network communications. Additionally, there are also a plethora of examples pertaining to the use of the framework.Major features and designations are listed:

- Dual-core Tensilica LX6 microprocessor
- 802.11 B/G/N Wi-Fi
- Dual-mode Bluetooth and BLE
- 240 MHz clock frequency
- 32 GPIOs
- 520 KB SRAM
- 16 MB Flash storage
- 2.2V-3.6V Operating Voltage

6.3.5 Choice of Main Microcontroller

So we have come to pivotal point in the development of this Senior Design project, choosing which system-on-a-chip that will be the brains of our system. We have done our research in seeking information across the web, within educational engineering publication, engineering and industry magazines, and by word of mouth between professionals and friends alike. Many microcontrollers with different specifications and designations were recommended from others and many forums that we read online advised us on the kind of microcontrollers that we should be looking for and to be aware of. Doing the research on microcontrollers was very interesting in that there was so much different microcontrollers in many different shapes and sizes. The fact that we were looking at so many peaked our interest because coming into this class, we had very few to no knowledge what a microcontroller was or what it can do. So doing

research on this subject has really benefitted the team on what they can do and now we feel like we can apply our knowledge into choosing the correct microcontroller that is best for what we want and what we foresee.

What we want from our microcontroller is mainly a painless system to incorporate with the rest of the components in our scheme. We want a microcontroller to have the requisite amount of input and output terminals to that the many different peripherals can connect properly to the microchip. We want it to be able to interface, receive data and be able to transmit data to multiple peripherals. One main requirement to have a microcontroller that has multiple UARTs (universal asynchronous receiver and transmitter) for serial communication such that the communication can be adjusted by speed and format. Plenty of the microcontrollers that we saw online while doing research only had one set of receiver and transmitter connections embedded on the board. Not to say those microcontrollers are useless, they are used by thousands of people, but they didn't offer want this specific project needs. So we looked harder, there are far more microcontrollers with only one set of Rx/Tx pins than those with multiple. The controller that we would get would have to be able to interface with the fingerprint scanner, bluetooth module, Wi-Fi module, and maybe an additional camera if needed, that alone means our requirement is at least four sets of UART pins need. The board that we will obtain would also have to have about 20 pins at least to connect to the board through input and output.

The search for the right board has persisted for a decent amount of weeks and we feel that we have found a good set of boards to choose from. All of the boards that we found, we feel can adequately work for us with our project. Later we will compare and contrast the boards we found that can potentially operate for us to the detail that we want it to. The some of the biggest factors that will go into the choice of our main microcontroller will be cost, type of processor, speed of the processor, special features of the board, digital input and output pins, memory and the programming language that will be used to program and write instructions to the system. We must factor in cost because that is one of the biggest impacts on any type of device that is manufactured. If the market value of a device is too much for the consumer, the consumer will likely not invest in such a device. What about the type of processor embedded onto the board? Who was it made by? How many bits does the processor work with? What's the operating voltage range of the CPU? These are the different things that we as a group must discuss between ourselves and make an educated decision on. Then what about the speed at which the central processing unit handle instructions. How many millions of instructions are processed per second by the core processor? We believe that we must have a board that can conduct and deal with the demands of our senior design project. We will have great deal of inputs and outputs to and from the system, we will entail that it can give us back the necessary outputs on time from the multitude of peripherals we have in our system.

Other things that will factor into the choice of the microcontroller will be the features that are included with the board. Added features probably won't necessarily be used or may be used right away, but we feel that it could be a resource we can use if we further expand upon this project in the future. This can only be a positive for us especially if an added feature is included onto the board at only a little extra cost. Then another considerable deal for is the number of pins that are on the board. If there aren't enough digital pins located on the microcontroller then that is an obvious deal breaker for us. Now if we were changing the scope of this project, perhaps making the project smaller, thus those speculations could be examined, however we are far too deep into this senior design project to scrap our plans. It is just very valuable to have our board with a decent amount of pins for our components, this amount will weigh heavily into our choice of the main microcontroller for our security system.

Memory is an another key selection that the group will have to decide upon when the time is right. We have been asking ourselves questions like how much memory do we actually need? How can we figure out how much memory the system needs to compute all numbers and outputs accurately? Memory is highly valuable, if we don't have it or if we don't have it in abundance relative to our system, the system will not be taking into account all of the code that the microcontroller must follow. All of the microcontrollers that made our final cut have the appropriate amount of memory we feel to operate our security system exceptionally.

Finally, the last major factor that will lead into the ever important decision into the choice of the home security lock system is the type of programming language that is used to program the microcontroller. As stated in the past sections, we have mostly little to no experience with microcontrollers or even a project to this size, therefore we have came together and decided that it would be nice to get a microcontroller that can be written in a language we are comfortable with coding in. Languages we are comfortable with as a group are: C, Python, and Java.

Microcontroller	Arduino Due	BeagleBone Black Wireless	Arduino MEGA 2560	ESP32
Price	$49.99	$55.00	$45.95	$8.95
Features	Equipped with pulse-width modulation pins, reset button, erase button, Arduino software, Android ADK	It has a next gen ARM core, 3D graphics accelerator, Boot Linux in less than ten seconds, Wireless connections available	Connect fast with pulse-width modulation pins, crystal oscillation, power jack, reset button, USB connector located on board, HDMI output capable	Bringing convenience it has both Wi-Fi and Bluetooth in one form factor, dual-core chip, ultra low power solution, touch sensor pins

	platform			
Processor	32-bit SAM3X8E ARM Cortex-M3	Sitara AM3359A ARM Cortex-A8	ATmega2560	ESP-WROOM-32
Clock Speed	84 MHz	1 GHz	16 MHz	160 MHz
Memory	SRAM 96KB	DRAM 512MB	SRAM 8 KB	SRAM 120KB
Total Number of Digital Pins	54	65	54	32
Operating Voltage	3.3 volts	5 volts	5 volts	2.2-3.6 volts
Weight	36 grams	39.68 grams	34.9 grams	2.0 grams

Table 2 - Main Microcontroller Comparison

Looking back at this comparison table, we can see that the finalist for the main microcontroller are all really good options to choose from. Out of all the research the team has done, we found these five microcontrollers as the best viable and powerful choices to choose from for our project. All of these options are robust and engineered to compete against the best MCUs on the market today. Sadly we can only pick one to be the operational engine of our system.

When we first started to brainstorm for a senior design project to work on, we thought about the possibility of creating a system that is easily accessible to anyone that would desire to possess an integrated security system. The predominant problem with that situation is that most home integrated lock systems, whether it be online or in stores, are relatively expensive for people on a budget. Most of the best products that can connect with most consumers in the market are items that are very useful and items that also don't break the bank. We want to produce a decently priced system and that starts with the microcontroller. The BeagleBone Black Wireless is a very attractive microcontroller for us, it brings strength, versatility, and many outputs and inputs. However, at a price point of $55 we all feel that it is too high to begin our project with considering all of the other components that will be purchased. We also are choosing to go a different route because although the features of the BeagleBone Black are interesting, many of them will go unused and we don't want to spend unwisely.

Our system is a very integrated body of work which has been stated many times before. We would need a processor that can respond and communicate with

other peripherals in a timely manner. Because of the nature of our project, some users of the system might desire to get into their house quickly, therefore a powerful processor is required. The Arduino MEGA 2560 is a great board to start out with for newer hobbyist getting into programming embedded devices. It contains many good features like a power jack, a convenient operating voltage of five, and 54 pins but with the lower clock speed of 16 MHz it limits the desirable requirements of our design.

The one microcontroller's specifications we haven't reviewed yet is the Espressif ESP32. This microcontroller has some serious potential as an option for our main microcontroller. It is very compact, small-scale package that is 18mm by 25.5mm, it has a keep out zone at the top of the chip that is 18mm by 6mm. This keep out zone will not be that much of a hindrance as of the date of this. This microcontroller is also extremely light. With a weight of only two grams, this presents the team with flexibility when designing a circumspect project. With a lightweight project, it can only be a benefit to the designers and to the people that will be using the system. The thing that stands out the most to the team about the ESP32 is the Wi-Fi and Bluetooth inclusion in one single chip. This solves the Wi-Fi and Bluetooth integration that we want in our system and takes care of the compatibility and synchronization issues that could show put should we use separate Wi-Fi and Bluetooth modules. ESP32s are also very cheap, we found some for what we think is a very advantageous $8.95. This is exactly what we want collectively, a useful yet low cost system that many people can afford. Lastly, the chip offers what could be a trump card against the other microcontrollers in contention, a low power mode. The average operating current draw of the ESP32 is 80 mA which is pretty compared to other controllers but the light-sleep mode on the chip operates at 0.8mA. There's even a lower mode called Hibernation mode where the chip uses only 5μA.

The Arduino framework for the ESP32 microcontroller is also open sourced and hosted on github under the official Espressif user. This library is a C++ wrapper to the Espressif IDF with further implementations and simpler function usage. For example: Wifi.begin("ssid", "password); will attempt to connect the lock to the wifi network identified by the given ssid (first param in function). A biggest advantage to using this framework is the handling of errors, OTA (over the air updates), and file system handling. OTA is very complex and a lot of things can go wrong, using optimized methods and tested code will reduce the possibility of errors for this and everything else. This will further increase our productivity and efficiency. The arduino framework seems to handle errors from the base framework (Espressif IDF) and provides a layer of abstraction. This layer of abstraction being maintained by the maker of the microcontroller and the base framework is reliable; Thus, if the base library changes we will not have to change our code as the Arduino framework api should not change but the code inside the api's calls will adapt keeping us up to date.

ESP32 has an onboard hardware encryption feature that can secure you program and proprietary data. This feature can turned on and off. This encryption uses AES256 bit and the encryption key is located in efuse block 1 and is read- and write- protected. The key is tweaked with the offset address of each 32 byte block. When using this encryption for flash it is important to use esp_partition_read() as it will always produce decrypted data whether reading from the encrypted flash or in an un-encrypted partition. As esp_partition_write() should be used to automatically encrypt data written to flash in an encrypted partition. Although using this encryption will limit the amount of serial flashes available else it will no longer be encrypted. It will permanently disable the encrypted flash feature. This limit is 4 including the original serial flash.

This a huge disadvantage when the group with be in the testing process. Having the ability to only reprogram the ESP-WROOM 32 with a limited five times will create a huge constraint. The code that will be flashed onto the microcontroller must be perfect every time. There is a development board, which starts at $15 each, that is offered for the ESP-WROOM 32 which will require soldering the microcontroller onto it. Testing each peripheral with the microcontroller seems almost impossible. Mistakes will occur plenty of times which will result in buying more ESP32 and development boards and cost of production will increase by a lot.

6.3.6 Final Decision On Microcontroller

Doing all of this research has lead us to see what microcontrollers are and what they can do and what they can be used for. So the search of a microcontroller that can manage our system has been an interesting and useful experience. After all of the digging we have done, we singled down all of the controllers we looked at down to five. We discussed the last five microcontrollers we examined into great detail and we came out the other side with a consensus decision. The team has chosen Espressif's ESP32 module to be the main microcontroller for our home security system. The choice came down mainly from the fact that the ESP32 had an integrated Wi-Fi/Bluetooth system that was precisely the resource the team wanted. Also the hardware was completely there, over thirty input and output pins that is functional for that different components that will be connected. The UART communications that we also wish for are there, three pairs that will go a long way. We are confident in this choice and we feel like there is no better option than the ESP-WROOM-32.

6.4 Power Source

The power source must be able to power all components on and off the PCB board. All components require different amounts of voltage and current in order to become active. Below is a table for all components needed for the design and what are their voltage and current ratings.

Component Name	Voltage Rating	Current Rating
ESP WROOM 32	5 - 12 V	< 20 mA
Raspberry Pi	3.3V	< 250 mA
LCD Display	4.8 - 5.2 V	< 200 mA
Electronic Door Lock	12 V	< 500 mA
Finger Print Scanner	3.3 - 6 V	< 130 mA
PIR Motion Sensor	5 - 12 V	< 40 mA
Magnetic Switch	< 100 VDC	< 500 mA

Table 3 - Component Voltage and Current Ratings

Three options were taken under consideration when deciding on how to deliver power throughout the design. Solar panels, batteries, and the 120V power source supplied from the power grid are all compatible to the security system, but all options have their imperfections. Solar panels are an excellent power source by the means of renewable energy. The process of charging photovoltaic cells that turns solar energy into usable electricity could ultimately power up the design, however, not as dependable as batteries and the 120V power source. A security system should always be dependable, so solar panels are not the most reliant during consistent cloudy weather.

Another option for receiving power would be to connect the security system to a 120V power outlet. This method would require more resources in order to be considered an option for power. A step down transformer is mandatory to obtain the low voltage needed for the project. The 120V power source is an AC signal which requires rectification, smoothening, and regulation in order to be compatible for our design. Diodes are needed to create a full wave bridge rectifier for a consistent positive voltage along with capacitors charging and discharging that will smoothen out the AC signal. Lastly, the 120V AC signal must be regulated through a voltage regulator to eliminate fluctuations within the power signal. Purchasing an AC to DC converter would also be a possible alternative. The AC to DC converter will properly step down the voltage to 12 volts as well as converter the power signal from AC to DC. The converter will also be able to send the power signal through a barrel jack connector to the power management board. This will remove a lot of extra concerns about converting the 120VAC to 12VDC. Both methods will increase the cost of production, however, will benefit the design in terms of more functionality and disregard for low power approach.

An advantage would be a guarantee constant supply of power whenever the system is connected to a power outlet. Continuous power from the power grid provides the most dependable option as well as eliminates the cost of replacing and repurchasing batteries. The main disadvantage that disapproves this technique is the extra labor work that is needed if no power outlet is within distance of the security system. The possibility that users might have to invest more money on installation tools/materials and time will reflect a poor power solution. The 120V power source from the grid will make a requirement for a power outlet to be within reach of the system for operation.

After researching for the proper power source for the design, batteries have seemed to be another great option. The disadvantages for using batteries is the need to continuously replace batteries overtime along with the cost to properly dispose them. Batteries will always have these limitations, therefore the design will have to accommodate them by managing its power consumption very carefully. A low power approach will have to be implemented in order to achieve maximum efficiency and usage when using batteries. The main advantages for choosing batteries is to allow the security system to have an easy and quick installation, inexpensive low power source, and almost instant power delivery throughout the device. Batteries will reduce installation time because there will be no extra wiring required. The consumer has to simply mount security system and insert batteries for full functionality. Batteries are affordable and easily available for consumers.

Batteries have the ability to deliver power almost instantaneously, which is a characteristic needed to operate a low power approach. All services provided by the security system is to be switched on once PIR sensors detect movement, or when the security system is interacting with mobile application. Otherwise, only the bluetooth and wifi module will be drawing energy from the power source. Therefore, the requirement for split second power delivery is vital to the design. Batteries are beneficial to the design because they are considered an almost noiseless power source, which will help improve the accuracy for communications within the system.

The power source that will drive the security system will be the 120 volts from the grid. A few important factors helped solidify the decision for the power source. The system requires a constant need for power when using bluetooth and wifi communication and PIR sensor. The LCD display and electronic lock has the potential to draw large amounts of power from the source when active. The second best option would have been batteries. The critical problem with batteries is the possibility of losing power all together due to dead batteries. As discussed in previous section, the security system will be implementing a fail safe door lock that remains in locked position when dormant. This door lock also prevents a hard master key because the door lock is placed in the deadbolt opening. The result for having no access with a physical key has steered the project design to use a constant power supply to guarantee functionality at all times. The security

system will then implement a backup battery source that will run parallel with the 120V main power source during power loss from the main power grid. The backup battery will only be activated when sensing the main power source has been turned off.

6.5 Battery

The security system is going to be powered entirely from batteries. The battery must be able to supply current to the low voltage components (Wifi module, PIR Sensor, etc.) continuously for the design to properly function. The batteries must be able to supply enough voltage for powering up the 12V door lock as well as all the other peripherals that are going to be connected. The batteries will be purchasable in most convenient stores. The batteries will be connected in series for a greater voltage, however, not affecting the output current. The batteries must be able to withstand all of these conditions.

The first process when selecting the appropriate battery was determining the cell type. Standard cell types include AA, AAA, C and D are used all around the world. AA and AAA are considered low voltage batteries with a nominal voltage for 1.2 volts. They are usually used for devices that require few amounts of current. An advantage for these types of batteries is the ability to fit in small portable devices. With smaller sized batteries, the AA and AAA batteries have the ability to be stored neatly into the overall design. They are both rated with the same voltages. The key difference between AA and AAA batteries are the size differences. The AA outputs a stronger current due to its greater size compared to the AAA. Although these batteries are lightweight and easy for integrating, they are not capable of supplying enough current to the overall design. C batteries are much greater in size compared to AA and AAA batteries and have the ability to output higher voltages. The greater size results in a much longer duration for supplying current. The C battery is too large and heavy to be incorporated into the design, so C cell types will not be used. D batteries are able to output 12V, however, very bulky and heavy so these type of batteries will not be used. Another factor to consider when choosing a battery is the milli-amps-per-hour (mAh). This measurement determines the amount of electric power it can output overtime. The higher the mAh the longer the time of output. When looking up batteries for the power supply, we will try to use the average amount of mAh for batteries.

Our Calculations:

$$\frac{2500mA * h}{500mA} = 5hours$$

An average AA batteries will run at 2500 mAh. The solenoid door lock draws the most current of about 500 mA for operation. We will use this as the amount of current that will be drawn from the battery every time the security system is in active mode. The solenoid current will serve as a reference to get a close estimation. By dividing the mAh of the battery by the amount of current being drawn from the load, it will equal the amount of hours the battery will operate. Five hours is a good estimation of operation time.

$$5hour * \frac{60min}{1hour} * \frac{60s}{1min} * \frac{1}{30s} = 600$$

Next we calculate how many seconds are in 5 hours. Having the total time the battery will supply power in seconds, we can now divide the total time by the time the security system is active. The result will equal how many times the security system can remain in active mode for 30 seconds until the battery life runs out. This is a very rough estimate because there will be other functions constantly running in the background, however, we can conclude that the security system can operate at least 450 times.

$$450 * \frac{1day}{10} = 45days$$

Using a statistic from the US Census Bureau, it states that the average number of family members in a household is 3.16 (2016). We can assume that the average family will access the security system about ten times everyday. After calculations, we can conclude that our security system, if running on a battery with 2500 mAh, can last the security system about 1 1/2 months.

Battery chemical content is also important to take under consideration. Common substances include alkaline, lithium, carbon zinc, nickel cadmium (NiCd), and nickel metal hydride (NiMh). Alkaline are inexpensive and provides decent amount of voltage. The downsides are the high tendencies for leakage and poor performance in when drawing high currents. Lithium batteries are long lasting, expensive, and have great performances with high drain devices. Carbon Zinc are considered very cheap and perform slightly worse than alkaline batteries. Nickel cadmium and nickel metal hydride are opposites of each other. Nickel cadmium will output low power densities but for a much longer duration of time, while nickel metal hydride releases high power densities within short period of time. Lithium ion batteries will be the best option for the security system due to its high power density capabilities and being lightweight. However, they are too expensive so we will not be using these batteries. Something more practical would be using nickel metal hydride because we will need high output to operate the solenoid for short periods of time, and they are inexpensive and common to purchase.

Battery Type	Chemical Content	mAh	Cost	Rechargeable	Operation usage
10 1.2V AA batteries (12V)	Nickel Metal Hydride (NiMh)	2200	$22	no	~ 420
HitLights Power Bank	Lithium Ion	3500	$24	yes	~ 700

Table 4 - Battery Options

The first option is a bundled pack of 10 1.2V AA batteries. The batteries are connected in series to reach the 12 VDC needed to operate the security system. Using this as the power supply will be very expensive overtime. Users would be required to constantly purchase 10 AA batteries once system runs out of power. The batteries will have a difficult time to find room within the interface since they will appear much bulkier. Using 10 batteries would require multiple battery holders to be mounted which requires much more space. The batteries are rated 2200 mAh which probably supply power to the security system of about 420 times, from using the equation above. In the end, this power source is not the best solution to the security system.

The second option that can be done is using the HitLights rechargeable Lithium Ion 12V power bank. This power bank comes with a charging kit so users are able to recharge the battery once battery life has diminished. The power bank's price is listed at $23.99. This is cheap because of the total lifetime for the power bank will eventually save plenty of money compared to non-rechargeable batteries. This powerbank is rated at 3500 mAh, which is much higher than the average 2500 mAh. The power bank will increase the number of times the security system can be activated. The power bank consists of lithium-ion, so it will be capable to supply the solenoid. The power bank has an AC adapter which can be integrated into our design by attaching a barrel jack to the main PCB design. There are great benefits when using this rechargeable battery pack, so the group has decided to go with this option.

6.6 Electronic Door Lock

When researching for an appropriate electric door lock for the security system, two different algorithms are used to create a locking function with electricity, fail safe and fail secure. Fail secure is an approach where the door lock will remain locked when drawing power. Guests will be able to pass through once the lock loses a power signal. The door lock remains in unlocked position until it draws power from its supply again. An advantage with fail secure technology is for

safety purposes during emergency situations. When power is lost, the lock can guarantee people to enter/exit freely without having any malfunctions with the lock. A disadvantage is the large amount of power this method consumes in order to create a locking function. The second approach is the fail safe. Fail safe will remain locked at all times until a power signal is received. This method would be very ideal for our project because it will consume the least amount of power. A flaw to this algorithm is that failsafe creates a possibility for the doorlock to remain in locked position when power is lost during emergency situations. The huge advantage is how little of power fail safe consumes compared to fail secure.

There are a few requirements that needed to be met when choosing the ideal door lock for the security system. The electronic lock should be easy to install, affordable, compatible with most doors, strong enough to maintain locked position, and compatible with our power design. We have gathered four potential door locks during the research process that could be integrated in the security system.

Name	Cost	Power	Installation Difficulty
Generic Fail Secure NO Mode Electric Strike Lock	$28	12 VDC	Difficult with extra wires to system
Signstek Keyless Door Lock	$50	4 AAA Batteries	Simple and includes doorknob
Kwikset 92640-001 Electronic Single Cylinder Deadbolt	$55	4 AAA Batteries	Simple but requires a deadbolt opening
Lock-style Solenoid - 12VDC Solenoid	$12	9-12 VDC	Easy and compatible with most door designs

Table 5 - Electronic Door Lock Options

The first option is the Generic Fail Secure NO Mode Electric Strike Lock. This model is considered fail secure which acts like a latch that only opens for a few moments once power is lost. This lock is to be installed at the opposite side of the door knob. Installation will require some screwing and extra wiring to the constant power supply. In order to incorporate this model into our project design, we will need a step down transformer to reach a voltage of 12V DC, and a separate microcontroller to switch on/off the power supply to the door lock. This microcontroller will be communicating with our main hub microcontroller through UART connection. Because our design is trying to achieve a low power system, this electronic door lock will not work because it is going to require a continuous

power signal. The costs for integrating the fail secure door lock will not work for our project.

The second option will be the Signstek Keyless Door Lock. The electric door lock provides simple and quick installation. An internal servo motor that drives the locking/unlocking function for the door lock is embedded in between the two sides of the door handles. This door lock does not require being compatible with other different types of door knobs because the door knob is incorporated in the design. The installation will not require any more modifications to other hardware because the door lock will fit in all standard door knob openings, as well as have the ability to be mounted on doors measuring 33 - 50 mm in width. The door lock can be installed with using just a screw driver. The door lock has the flexibility to be configured for left hand and right hand doors. The door lock receives it's power from four AAA batteries. The design prevents more costs by reducing the amount of resources needed to operate. Therefore, this lock will be provide less complications when powering up, simple installation, and no extra costs. An advantage for being powered by batteries gives the design a smooth integration into the power management PCB. The door lock also provides a 0-9 keypad for supporting a password security feature along with LEDs lights for night use.

The third option is the Kwikset 92640-001 Contemporary Electronic Keypad Single Cylinder Deadbolt. This door lock model has the same specifications as the Signstek Keyless Door Lock, however, will be able to lock and unlock with a key incase of power failure. The door lock has assimilated a lock cylinder as the locking mechanism, and battery operated for easy integration to project design. This door lock model requires a deadbolt opening in order to be mounted properly which limits its ability to be adaptable to different types of doors. The deadbolt lock is usually a second locking mechanism found on doors, which differ from spring locks found within the door knob/handle because a deadbolt can only be moved to the open position by rotating the lock cylinder with a key or motor. The deadbolt design provides a more secure and stronger connection making it extremely difficult for intruders to break through.

The last electronic door lock is called the Lock-style Solenoid. This lock is the most inexpensive door lock option. The solenoid consists of a copper wire coiled up attached to an armature (the metal bar). Once the solenoid receives a power signal, the coil pulls the armature into the lock. This lock is implementing a fail safe method, so the lock will remain in closed position until it is energized. The lock has an operating voltage range of 9-12 VDC. We will be able to draw enough power from our 12V battery to operate the locking solenoid. This door lock is also not adaptable to different types of door knobs, so it must be installed in the deadbolt opening. The solenoid will be easy to integrate with our design because we can run a wire connected to our main hub microcontroller's GPIO pins. The doorlock is fail safe, so the security system will remain in locked mode when the microcontroller is asleep.

The Lock-style solenoid is the electronic door lock that will be integrated into the security system. It is able to communicate directly with the main microcontroller. The solenoid is able to operate for a few moments rather than constantly drawing power to operate. Installation is easy for users because it will fit easily into the deadbolt lock opening. The solenoid is also the cheapest alternative that will require no extra costs towards the final product. The door lock will be most appropriate fit for our specifications. The one requirement that has risen was the security system must have power at all times in order for the security system to fully function.

6.7 Camera Module

In our project, the camera module is an important device that serves a myriad of purposes, so finding the right camera module was quite a significant task. The camera module is responsible for taking images and/or video of whoever is at the door so that the image can be sent to another device, such as an Android phone.We looked at many modules to find one that would meet our requirements. But before we could pick one, there were many different aspects to consider including the microcontroller that is chosen, the power usage of the camera, and also the interface in which the camera will connect to the microcontroller. We also needed to take into consideration the resolution of the camera, along with the frame rate of video that is recorded. Taking all of this into account we considered the following camera modules.

Camera	Price	Max Static Resolution (pixels)	Max FPS	Power Usage
2.8mm 8510 Mini Camera HD 700TVL	$12	720x576	60fps	80mA
Raspberry PI 5MP Camera Board Module	$22	2592 x 1944	720p/60fps	250mA
Raspberry Pi NoIR Camera Module V2	$28	2592 x 1944	720p/60fps	250mA
OmniVision OV5642 5MP Camera	$40	2592x1944	720p/60fps	70mA

Table 6 - Camera Module Options

6.7.1 2.8mm 8510 Mini Camera HD 700TVL

The first camera module we considered was the Mini Camera HD 700TVL. This is a camera with a 1/3rd inch CMOS image sensor, a 720x576 resolution, and a max frame speed of 60fps, and a power consumption of 80mA. However, as a team we felt that the camera resolution was a bit too low, whether it be for facial recognition, pictures, or video. We did love the low power consumption of the module and the fast frame speed. These would ensure that feeding power to this particular camera module would not be a huge concern and that video would be smooth as needed.Also, another great aspect of this camera module is that it is $12, which aligns with our goals of making a product that is cheaper than others on the market. But In the end, this compact and small module seemed to be great for simple tasks, but not powerful enough for the tasks we needed to accomplish with it.

6.7.2 Raspberry PI 5MP Camera Board Module

The second camera module we looked at was the Raspberry PI 5MP Camera Module. The first caveat we noticed with this camera was that it was a module that could only be used with the Raspberry Pi. It is custom designed, with a short ribbon cable specifically made to connect to the Raspberry Pi using a dedicated CSi(Camera Serial interface). Aside from this limiting factor, the Raspberry Pi 5MP camera is packed full of features that would be beneficial to our project. It beat all of the previously analyzed camera modules in nearly every single category. It has a 5 megapixel sensor that is able to take static images of 2592 x 1944 , and also supports 1080p video at 30 frames per second, 720p video at 60 frames per second, and 480p video at 60 or 90 frames per second. What this means is that this camera was capable of not only producing clearer and more detailed pictures, but also smoother video at a higher resolution than any of the other camera modules.

Furthermore, this module has automatic exposure control, automatic white balance, automatic band filter, and automatic black level calibration(ABLC), while also supporting JPEG, JPEG + RAW, GIF, BMP, PNG, YUV420, and RGB888 formats. However, we discovered all these great features come at a cost, and at $22, it is more expensive than the Mini Camera HD 700TVL. But surprisingly, even though it has better specifications, it is less than the Lumenier CS-600. One last thing that did bring up concerns was power usage of the module, considering that 250 mA is required to be able to power it. In the end, despite the camera concern, we felt as if this module was definitely the strongest candidate.

6.7.3 Raspberry Pi NoIR Camera Module V2

Even after being so confident about the Raspberry PI 5MP Camera Board Module, further questions emerged, with the biggest question being: how will we be able visitors who come to the door at night? This is where the Raspberry Pi NoIR V2 camera module comes in. The Raspberry Pi NoIR V2 module, unlike the normal camera module allows you to use infrared light as a light source in conditions with low or no light at all. The normal camera would not be able to produce clear images or video in these situations. Also, unlike the Raspberry Pi 5MP module, when using this module it is recommended to have at least a 2 amp power supply, so this begs the question, is the rise in power usage worth it for the ability to see in darker conditions? This question became one of the most important, if not the most important aspect to consider when comparing the camera modules in the end because it was a decision that would affect which microcontroller we used, while also affecting the reliability of our facial recognition.

6.7.4 OmniVision OV5642 5MP Camera

Following the Raspberry Pi NoIR Camera Module V2, the last camera we considered was the OmniVision OV5642 with OmniBSI and embedded TrueFocus technology. We needed to have another camera choice that met our expectations if we did not use a Raspberry Pi, and this was it. This camera has everything that we need, including a 5 megapixel (2592x1944) maximum static image resolution and 1080p/30fps and 720p/60fps video quality, which completely matches the previously analyzed Raspberry Pi camera modules. Furthermore, this camera has Automatic Exposure Control, Automatic White Balance, Automatic Band Filter, and Automatic Black Level Calibration. Lastly, we were quite intrigued by the variety in output formats with there being RAW RGB, RGB565/555/444, CCIR656, YUV422/420, YCbCr422, and compression.

6.8 Wi-Fi Module

The WiFi module is a monumental component to any device providing wireless communications because, based on the IEEE 802.11 standards, it allows connections over large distances using the 2.4GHz or 5GHz band, so when picking this part, we knew we had to do very careful research on all the pros and cons of using each Wi-Fi module. This module is responsible for communicating with the internet to complete tasks such as sending an image to a user’s phone to allow him or her to see who is at the door and allowing a user to connect to the lock to control functions such as registering fingerprints. We had to make sure we had a chip that has compatibility with a variety of modern electronics and older electronics, preferably something that supported wireless a,b,g, and n with ac being a feature that would be nice to have, but not necessarily required.

Furthermore, we had to decide if we were going to depend on the Wi-Fi chip on the board or use a separate, external chip.

6.8.1 AT Command Set

The AT Command Set, also known as the Hayes Command Set, is a special type of command language that is specifically used for programming modems. Called the Hayes Command Set because it was first used by Dennis Hayes to program the Hayes Smartmodem 300 in the late 1970s, this language uses text strings, that when put together, can construct commands for activities like changing the framework of a connection, or activities such as small as hanging up or initiating a connection. While this language was the foundation of the earliest modems, new variations of this type of language have emerged with the addition of new commands. However, nearly all of these variations share the structure and syntax of the original language.

6.8.2 2.4 GHz vs 5 GHz

When it comes to Wi-Fi there are 2 bands in which wireless signals are transmitted in, one is 2.4 GHz and the other is 5 GHz. Both of these bands have their pros and cons and I'll provide a breakdown of each.

2.4 GHz was the first band that Wireless Local Area Networks(WLAN) used, and is also used by a myriad of other products, including garage door openers and cordless phones, just to name a couple. What makes the 2.4 GHz band great is that the waves produced by it are longer than 5GHz. What this actually means is that the band can travel longer distances and is able to penetrate walls and other dense objects as needed. So all in all, 2.4 GHz is the band with the most reliable coverage over distance.

5 GHz is the newest band that is being used by WLANs. What makes it a great band is the fact that there are less devices that are using this band, therefore once connected you should be able to have a more reliable and stable connection. Along with this, you will get higher speeds with the 5 GHz band due to it being a higher frequency. But unfortunately, these higher speeds come at a cost. The 5 GHz band is less able to penetrate walls like the 2.4 GHz band is able to, which results in a smaller range. So to summarize the 5 GHz band, it is able to provide faster and more stable connections, but at shorter distances.

In our project we plan to rely on the 2.4 GHz band over the 5 GHz band, as we would rather have a stronger connection at greater distances, over a faster connection. Of course, we will test multiple conditions to ensure that this is the correct path to take, but our initial decision is 2.4 GHz and Wireless N.

Module	Wireless Standards supported	Flash storage	Price	Power Consumption
ESP8266	802.11 b/g/n	1 MegaByte	$7	< 1.0 mW.
ESP-WROOM-32	802.11 b/g/n	4 MegaBytes	$9	< 5 microAmps

Table 7 - WiFi Module Options

6.8.3 ESP8266

The ESP8266 WiFI Module supports 802.11 b/g/n and comes ready with an AT command set firmware, so you do not have to worry about getting AT commands working on the board when you receive it. The board has support for APSD for Voice over Internet Protocol applications and bluetooth co-existence interfaces. Furthermore, it has a self-calibrated RF, which eliminates the need for external RF parts and allows it to work under any operation conditions. Also, it has a flash disk size of 1 MegaByte, supports Wi-Fi Direct(Peer To Peer), an integrated TCP/IP protocol stack, and a low power 32-bit Central Processing Unit that can be used for as an application processor. Two important aspects that caught our eye were the fact that the chip could wake up from sleep and transmit packets in less than 2 milliseconds and that it had a standby power consumption of less than 1.0 mW.

6.8.4 ESP-WROOM-32

The ESP-WROOM-32 is a combo Bluetooth and Wi-Fi chip that supports 802.11 b/g/n at 2.4 GHz. It also features two low-power Xtensa 32-bit CPU cores with a clock frequency that can be fine tuned to be anywhere in the range of 80 Mhz to 240 Mhz and a very power efficient coprocessor that monitors other components on the board for events and changes. This chip even has a sleep current of less than 5 microAmps and 5 different power modes: Active mode, Modem-sleep mode, Light-sleep mode, Deep-sleep mode, and Hibernation mode. Having all 5 of these modes is essential because of the concern of power usage in our lock.

Moreover, the WROOM 32 has an output power of 22 dBm and can a maximum speed of 150 Mbps. One fantastic positive of module is the fact that it actually supports over the air(OTA) updates. This would help considerably in our development process as we fine tune the chip for our project. In addition to ota capabilities, it beats the ESP8266 in the area of Flash Storage, with 4 MB of flash

storage on board. After our analysis of both of these boards, we considered the ESP-WROOM-32 to be the more efficient and capable wireless module out of the two.

6.9 Fingerprint Scanner Module and Relevant Technologies

In our project, as previously discussed, one of our components for security will be the fingerprint scanner. This module will allow for users to place his or her finger on the module, unlocking the door near instantaneously. First and foremost, we want this module to be able to scan the user's finger as fast as possible, while also remaining as accurate as possible. Our second requirement we were looking at was low power consumption. Our third, and last requirement, was that it was able to be connected to rest of our components without any conflicts or compatibility issues.

6.9.1 SmackFinger 3.0 Algorithm

SmackFinger 3.0 is a fingerprint scanning algorithm developed by the Beijing Smackbio Technology Company. This algorithm has False Rejection Rate of less than 0.01 % and a False Acceptance Rate of less than 0.00001 %. It requires 3 scans of a fingerprint for the fingerprint to be successfully registered and produces image sizes of 256 x 256 pixels, or 403 dpi.

6.9.2 False Acceptance Rate and False Rejection Rate

The False Acceptance Rate(FAR) and the False Rejection Rate(FRR) are two metrics that play a role in determining how accurate a fingerprint scanner is when it reads fingerprints. The False Acceptance Rate is the measure of the likelihood that a biometric security system will incorrectly accept an access attempt by an unauthorized user; This is calculated by the ratio of the number of false acceptances divided by the number of identification attempts. The False Recognition Rate is measure of the likelihood that the biometric security system incorrectly reject attempt by an authorized user. This is calculated by the ratio of the number of false recognitions divided by the number of identification attempts.

6.9.3 UART Protocol

UART, or Universal Asynchronous Receiver/Transmitter, is a microchip that allows a programmer to communicate with serial devices, such as modems. So basically, what this means is that the primary goal of the UART is to send send and receive serial data. To do this, the UART converts the bytes it receives from the computer along with parallel circuits into a single outbound transmission. When it comes to inbound transmission, it translates the serial bit stream into bytes that a chip can understand. The UARTs of today even include the ability to buffer data, allowing serial devices and the processor have some level of coordination

Module	Identification Speed	Fingerprint storage	Power Consumption
GT-511C1R	1.5 seconds	20 different fingerprints	3.3V - 6V & < 130 mA
ESP-WROOM-32	1.5 seconds	200 different fingerprints	3.3V - 6V & < 130 mA

Table 8 - Comparison Fingerprint Modules

6.9.4 GT-511C1R

The GT-511C1R Fingerprint is the first module that the team researched. It features 360 degree recognition of fingerprints, a UART protocol, communicates over TTL Serial, and uses the SmackFinger 3.0 Algorithm, and is around the size of a United States quarter. Also, this module has it's own database in which it can read and write fingerprint data from users. However, the database can only store about 20 different fingerprints. Something that is a plus is the ability for us to download the database of prints from the board. Powering this module is an ARM Cortex M3 Core CPU, and the board uses 3.3V - 6V in operating voltage and less than 130 mA in operating current. Other positives that the team noticed were the identification time of 1.5 sec when a user's finger is placed on the scanner, a False Acceptance Rate of less than 0.001 % and a False Rejection Rate of less than 0.1%. Coming in at $31.95, the GT-511C1R is definitely a solid fingerprint scanner module that meets all expectations of scanning speed, capabilities, and power efficiency, so we were impressed, but we decided to consider others options to ensure that this was a good choice.

6.9.5 GT-511C3

The next module we looked at was the GT - 511C3 scanner. This module is actually the newer, but more expensive version of the GT-511C1R Fingerprint Scanner Module. This newest module has one major improvement over the older model: the ability to store 200 fingerprints in the database, which is 10 times more than how many the GT-511C1R can store. Other than that, the newer model is practically identical to the older model, including the SmackFinger 3.0 Algorithm and 360 degree fingerprint recognition. At $49.95, this brings about the question: is the ability to store 180 more fingerprints worth spending $18 dollars more? Because we anticipate out smart lock being used on houses with average sized families and not in public areas, we feel as if a 20 fingerprint database is more than enough.

6.10 Magnetic Contact Switch

If our lock does not have its own sensor for detecting whether the door is open or closed then we will use a magnetic contact switch. This is a type of, reed switch, electrical switch controlled by a magnetic field. A reed switch is made up of a glass tube with high electrical resistance and two or separated magnetizable, flexible, metal reeds sealed on opposite ends. When a magnetic field is strong enough to push the power source reed to or away from the ground reed depending on how the reed switch was produced. The magnetic switch we are purchasing has a open circuit when not affected by a magnetic field. To utilize this there will be a magnet on the door. When the door is shut the magnet should be less than 13mm or .5'' away causing the circuit to close with a line coming off parallel to the ground into an input on the microcontroller. The security system will know whether the door is open or closed. The microcontroller will receive two inputs when to acknowledge the door status. Input will be a one if the microcontroller senses the door closed, and a zero signal will be sent to the microcontroller digital pin when door status is open. The magnetic switch is capable of drawing up to 500 mA and 100 volts which is well above over what the security system is going to operate at. The magnetic switch is to be mounted with screws onto the door and door frame to be able to sense separation of the two plates properly.

6.11 LCD Display

The LCD display will be programmed to display text messages for the security system. The display shall state the status for the locking device. “Locked” and “Unlocked” text messages will appear when the microcontroller senses the positioning of the locking motor. “Unlocking…” and “Locking…” will be shown on the LCD display when transitioning between locking statuses. The LCD display shall also present a message for the battery life percentage. There are a few things to account for when choosing the appropriate LCD display. The LCD must be large enough to display the text messages needed for the system. The LCD must be able to operate at low voltage levels. The fewer number of pins needed for full functionality would be ideal for a simpler design. LCD display must be able to be mounted onto security interface when fabricating the final product. We have narrowed down our LCD display options to these last three:

Name	Voltage	Screen Resolution	Screen Dimensions	MPU interface
Standard HD44780U LCD	5 VDC ±0.04%	Single LED Backlight	0.9" x 2.7"	4/8 - bit

16x2				
Adafruit 2.4" TFT FeatherWing	3.3 VDC	240x320	2.6" x 2.1" x 0.4"	16 - bit
Standard HD44780U LCD 20x4	5 VDC ±0.04%	Single LED Backlight	1.02" x 2.7"	4/8 - bit

Table 9 - LCD Display Options

Adafruit 2.4“ TFT FeatherWing is a touchscreen display device with 240x320 pixel resolution. The FeatherWing was chosen due to its affordability compared to other touchscreen devices. The display is controlled by a FeatherBoard, a stand alone microcontroller manufactured by Adafruit. The Feather Board is required for operating the LCD screen due to the increase of data that will be needed to be processed. The LCD operates on 3.3 volts and capable of drawing up to 100 mA. With touchscreen capability, the overall design will allow consumers to interact with action items displayed on the screen when pressing onto the onscreen options. Action items will include door locking functions, display battery health, and requesting access to open door. The FeatherWing is a great option that would give the design better human interaction capabilities, however, it will increase the cost of production. After much consideration, the team has decided to pursue a more concise and inexpensive LCD display.

The next LCD display options are the Standard HD44780U LCD 16x2 and Standard HD44780U LCD 20x4. The LCDs have operating voltages ranging from 4.8 - 5.2 volts and drawing a maximum of 200 mA. The LCDs are very similar except for the amount of characters that can be presented onto the screen. The 16x2 is able to have 16 characters on 2 rows, and 20x4 is capable of 20 characters on 4 rows. The downside for these two options is the inability to interact with the user without creating more inputs elsewhere. Inputs will be assigned certain output messages that will be displayed when active. In order for the user to view a message, the design will have to connect extra buttons to the main microcontroller. Each button will output a text message tied to it’s input. With these extra inputs that must be interfaced with the system, the overall design for incorporating a LCD screen will require the use of more GPIO pins. Addition to the 8 or 11 pins needed for functionality depending on which MPU interface is used, the pins needed for human interaction will require about 11 - 14 pins. The extra pin additions has steered our design away from the human interaction approach. The most simple and cost friendly option is to implement an LCD screen that is capable of displaying all the text messages at once. A requirement for the LCD is to be sizeable enough to display battery health and door lock status at all times while the security system is active. With the 20x4 screen, the design will have plenty of room for displaying the messages needed for the security system.

6.12 Motion Sensor

The Smart Home Integrated Security System will be a resourceful and an intelligent system built to fulfill the consumers needs. Features upon features many not necessarily be used all the time by the customer, but we believe that the features list will peak their interest. The system will have Bluetooth and Wi-Fi integrated into the system for communication connectivity, but another headliner that the team is excited to add is the ability for the system to sense motion. The team is planning on having the security lock system sense motion directly in front of it, say an individual wanting to get inside of the house, then the motion sensor will send a signal to the controller and then the controller will turn on the LCD display.

The LCD display will show things like maybe the time, or possibly the weather, or even maybe the remaining battery left status. We are still considering whether we will have the motion sensor scan the area, sense movement, then if that movement is detected for more than twenty seconds with no attempt to open that lock via Wi-Fi or Bluetooth or fingerprint scanner, then the microcontroller will turn on the camera to record a ten second video. Then the design will send the user of the system some kind of notification that motion was detected without attempt. We believe this is an adequate security measure that not many other projects in the market can offer at a low cost.The type of motion sensor that we found that could be useful for us is the PIR motion sensors. A PIR sensor, or Passive Infrared sensor, reads the infrared rating emitting from hard objects in a centralized scan of view. How it works is that the sensor can sense heat being radiated from a living organism, say a human or animal, then a signal from the sensor is set to high. Although PIR motion sensors can become aware of heat, it cannot calculate or judge the amount of heat being given off. The reason why this type of motion sensor is named “passive” is because the sensors neither produce or radiate any power for detection reasons. These sensors are very different from other sensors like switches, pressure sensors, or speed sensors because there is a lot of variables to these pieces of equipment. The lens alone can alter the field of view, range, width of view, or amount of light absorbed.

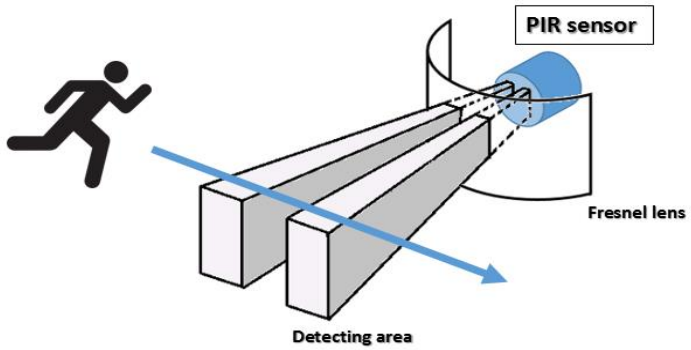

Figure 2 - How Motion Sensor Works

Just like the microcontroller section, we are going to reveal the final parts we are considering for the motion sensor component. We will go into detail to explain each component we are thinking about using. Once each part has been gone over, a structured and detailed chart will list the important, relevant specifics to each respective motion sensor. Then a detailed explanation as to why a certain element of the project was chosen.

6.12.1 PIR Motion Sensor

The PIR sensor are reliable sensors that can be used in almost any situation, whether it be in a home, business, factory, or in schools. These systems are very meager and modest and can be placed in most cramped locations. The PIR sensors don't draw a large amount of power contrary to popular belief. It has a wide angle of focal length and in addition to that, the PIR sensor is what we hear very simple and uncomplicated interface to interact with. The newer generation of PIR sensors now have an adjustable setting for sensitivity of the sensors. This compact chip is equipped with a three pin layout that will connect the motion sensor to the VCC power, the ground for the system, and the digital out pin. The VCC voltage for the PIR motion sensor is recommended to receive no less than three volts and no more than five volts. At above five volts, the operation of the sensor could be compromised and damage could be done to the board. The digital out pin for the board is the connected pin that will go high when motion is detected and back to low when it is not. There is also a voltage regulator on the board for an extra wall of protection if excessive voltage is feed to the motion sensor. The motion sensor also comes with a BISS0001 microchip. The chip actually grabs or receives the output from the sensor and then turns the analog signal it receives and converts it into a digital waveform to be sent out.

6.12.2 Mini PIR Motion Sensor Module

This motion sensor is in general, basically the same motion sensor the was just mentioned previously. However, the major difference between the two motion sensors is that the Mini PIR is obviously much modest in stature. The dimensions of the Mini are as follows: 28mm by 13mm by 13mm. As the numbers show, this is indeed a miniature device, small enough to fit on the bottom of an American 25¢ coin. However, we cannot say that this motion sensor is not as reliable just because the Mini is smaller and more diminutive. This sensor boosts the ability to get back a high sensitivity reading back to wherever the data needs to go and instant reaction measures that are beneficial for quick responses. It is surprisingly able to handle a reported direct current voltage of five to nine volts, which is more than the previous motion sensor. It can detect objects from up to

seven meters away, or 23 feet. The widest angles for detecting objects in front of the sensor is about 100 degrees.

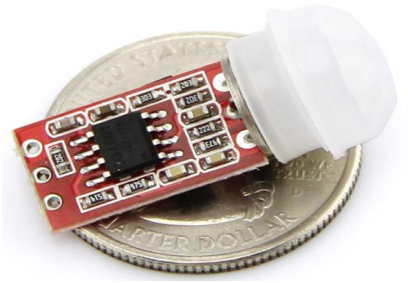

Figure 3 - Mini Motion Sensor
Pending Permission from seeedstudio.com

6.12.3 PIR Motion Sensor - Large Lens

The last sensor the team has considered for integration into the home security lock system is a motion sensor that is very similar to the others reviewed, the only major difference is the large lens. This version of the PIR motion sensors can of course do what is expected of it to do which is to discover infrared movement in front of the sensor. But this variant however, is fitted with a large dome such that more infrared from even wider angles can be observed. This more extensive dome cap increases the angle of view to 120 degrees, more than the Mini and PIR motion sensor. The motion sensor comes with a set of three pins, like the rest of the sensors, all of which are 2.54mm connectors which is standard. The operating voltage of the Large Lens PIR sensor is between 3.0 volts to 5.5 volts and one of the features that was listed of this motion sensor is said to be that it is low power consuming. A representation of a Large Lens PIR motion sensor is listed below this. Make sure to capture the size comparison of the sensor relative to the American quarter used for currency.

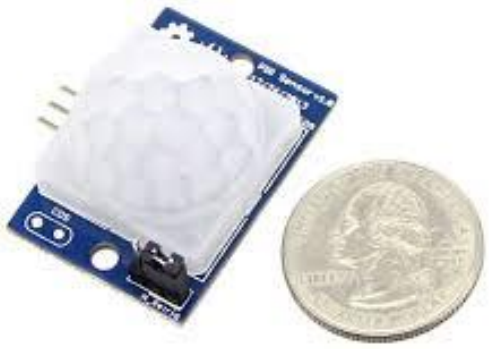

Figure 4 - Large Lens Motion Sensor
Pending Permission from seeedstudio.com

Motion Sensor	PIR Motion Sensor	Mini PIR Motion Sensor	PIR Motion Sensor - Large Lens
Operating Voltage	5-12 Volts	5-9 Volts	3-5.5 Volts
Detection Distance	20 ft (6 m)	23 ft (7 m)	20 ft (6.1 m)
Detection Angle	110 degrees	<100 degrees	120 degrees
Dimensions	32.2 x 24.3 x 28 (mm)	28 x 13 x 13 (mm)	36 x 26 x 21 (mm)
Cost	$9.95	$5.90	$12.99

Table 10 - Motion Sensor Comparison

6.12.4 Motion Sensor Decision

Looking over the scope of this graph we can clearly see the advantages and disadvantages for all of the components that are being considered to be utilized for the motion sensor for our system. To understand which motion sensor will be chosen, a defined scope of the use of a motion sensor needs to be understood. The smart home security lock will have a motion sensor to determine if anyone or thing makes an approach to the front door. Once a clear cut, obvious motion is scanned the sensor will notify the microcontroller that there has been motion detected near to the front door and that a certain response may or must be taken. If motion is indeed detected by the front door, the system should then turn on the LCD screen, turn on most off the peripheral components on standby, and especially turn the camera on standby just in case a video feed or photograph is necessary. The constraints of the design of the motion sensor are another pivotal aspects of the decision that needs to be taken into account as well.

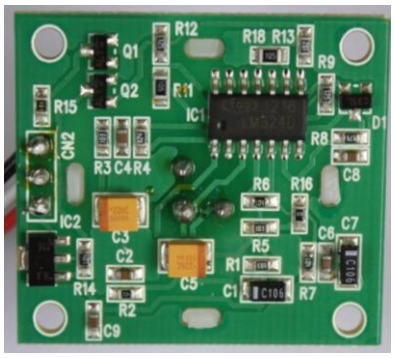

Figure 5 - PIR Motion Sensor Board

All of these devices could be great decisions to pursue for this important project. Looking at every detail is also important starting with voltage. The operating voltage of this component is crucial. One must select the right voltage to have it be similar or as close as possible to the other components. Having all of the systems components at or almost equal to all of the other system components within the system could be a huge advantage to the power management of the system. When all of the components are similar in operating voltage to the other components, voltage difference doesn't have to be such a worry anymore. Most of the system components operate between three and five volts, so choosing a motion sensor within that range could be wondrous for the team. Looking back at the stats, it seems like all of the three components in consideration are within the operating voltage we set out to be our standard.

The distance that the motion sensor module can accurately detect movement is also a heavy factor in the choice of the right sensor. This another huge constraint of this project, can the motion sensor pick up motion, not just any motion but the right one, from a significant distance? Pondering this idea is not a far fetched one because for some homes, the walkway to the front door is really long is terms of distance. Some walkways stretch from the street to the actual front door of the home. The motion detect should be able to detect such movement systematically with almost no error. Now examining the table of important factor for these motion sensors, once again it is clear that they all are able to scan a considerable distance. Each sensor can scan a distance of at least twenty feet or six meters in front of where the motion sensor is placed. This distance is in general is more than enough to begin detecting movement far in front of the home security system such that the appropriate signals can be sent and processed in time. They need to be sent in time before the user of the system begins to interact with the system. We can see that the smaller Mini PIR Motion Sensor has the furthest ability to scan motion than the other components in comparison, it can scan up to 23 feet or seven meters away.

Each motion sensor also has a set and defined range of detection angles they can observe motion at. The infrared rays are shot out and establish a certain range of detection as seen in the figure above. Once an object or human enters into that field range, a signal is set out of the digital output pin to the microcontroller. This signal is generally like a Boolean variable, it sends out a signal at the operating voltage to the microcontroller, once the microcontroller sees the signal, that means true in this case. The microcontroller will act appropriately to this response by the code and instructions that were written to it. If there is nothing that enters into the field of view from the motion sensor, then no signal will be sent from the motion sensor to the microcontroller chip. Usually the signal sent will be equal to the operating voltage, but when there is nothing scanned, the microcontroller will only see a result of zero volts. When the output is zero volts, it's as if the microcontroller can't see anything and nothing will be acted upon by any of the systems. The first motion sensor we looked at has a

degree range of 110 degrees. It will have no problem detecting objects or individuals coming in from an acute angle to the door. The second PIR motion sensor was the convenient mini sensor. This sensor has great use despite its miniature stature, its field of view can scan a width of up to but less than 100 degrees. Now for the last motion sensor in contention, the PIR large lens sensor. As mentioned before, if you have a sensor with a bigger lens the angle of view will be wider. This motion sensor in particular has a detection range of 110 degrees, which makes it the widest viewing motion sensor that is being considered for use for the security system.

When figuring out what sensor to use, cost of the component will also drive the choice for which one will be used. The team wants to have a system that will not break the bank and go over a certain budget. Being in college also limits the capability for the project to get to a point where the cost is not a significant burden. Also, a reachable and tangible goal from the team is to produce a security integrated system that will be priced reasonable for a family to purchase one. Examining the market, there has been no to very few items that can conduct the capabilities that this project can scope while also being estimated at a decent price. Every family should be able to afford at least a small amount of security. In today's world, security is an immersive subject that has be lobbied and gone over many times in federal and local government. Sometimes security is a source that isn't always provided by government all of the time, so it should be up to the individuals to arrange decent protection for themselves and for their loved ones. The cost is a major constraint to this project, so one must adequately prepare for it. The first motion sensor has a reasonable cost of $9.95. The mini PIR sensor that is so small compared to the other motion sensors has a retail cost of only $5.90. At that price that provides a lot of head way to put those cost savings elsewhere into the project. Now the last motion sensor is priced at $12.99. So as you can see, the PIR large lens sensor will be a decent investment in the security aspect of the project. The reason for this higher cost is of course because of the viewing angle capacity of this specific motion sensor, the larger lens play a pivotal role in the price.

The next thing that must be looked at is how large is the motion sensor, because this device will have to be packed into an electronic cover. The device must be able to fit into a certain given area of space while also not being a burden getting the other components into the system. These are hard constraints that are present simply given the type of design by the project. The overall design is limited by space so if some component can't fit into space or is blocking another component, then some hard changes must be made. The hard changes that will be made will be completely removing that system from the project and considering some other device that is more compact that will not disrupt the overall design. The mini PIR motion sensor obviously has the smallest footprint of any of the other sensors. This can be both a positive and a negative, positive because the device will give a lot of room for wires and cables to run to and from within the system without there being much of a hassle. However this can be a

negative because a smaller device means a smaller area for the printed circuit board to house all of the requisite material that runs the sensor. The size of the mini sensor is 28 x 13 x 13 in millimeters. Now for the large lens motion sensor, the area that it encompasses is 36 x 26 x 21 and this is listed in millimeters. With these stats, we can see that this particular sensor is the largest sensor. This might be a pain point because it may very well cause an issue with the constraints of the design. The width of the lens which must be protruding the design may cause an overall design shift that may be a hassle for everyone involved. However, it's not all bad with this specific sensor. The large lens provides better viewing angles for heightened security for any infrastructure in the business.

6.12.5 Final Choice of Motion Sensor

The purpose of a motion sensor in the home security integrated project is to add another level of security that the other components of the system can't provide. Beyond these new and added capabilities, the sensor will work as a wake up device. The plan is to have the motion sensor detect motion and send an alert to the microcontroller that says: "hey, movement has been detected, wake up!" to paraphrase. Obviously, it wouldn't be advisable to have the entire system running all the time, that would be a security risk and that would use great deal of power. The liquid crystal display alone just definitely isn't something you would want to leave running every second of the day. So the main job of the sensor is to detect movement, but also importantly wake up the integrated system. So with that said, choosing a motion sensor is very important. The PIR motion sensor is a very attractive sensor because of its price point and because of its distance it is able to scan. It doesn't have the furthest distance able to scan by grade of the three motion sensors but once again the price is a great solution. The Large Lens PIR sensor has the best wide angle viewing for movement detection, but what limits this device as a solution, is the price for it. This sensor costs the most, yes it does have the better angles for detection but not by much. Both the PIR sensor and the mini sensor have about an angle of 100 degrees or more, but the large lens is only ten more degrees at 110 degrees. The mini PIR sensor is a great option considering its size and cost but it is limited by its viewing angle at less than 100 degrees.

The motion sensor that will be used in the home security system will be the Passive Infrared Motion Sensor. This was chosen because of it has a great viewing angle of over a hundred degrees, 110 to be exact. It's not the cheapest, the mini is, but it is also not the most expensive. So this device is kind of like the best of both worlds, not the best but also not the worst. What the team is getting back for the price that will be paid for the device is well worth it when acknowledging the overall value of the motion sensor.

6.13 Bluetooth

Looking past, the funny name, Bluetooth is one of the premier foundations for wireless communication between two individual devices. Bluetooth, when it was first introduced to the world, was a sort of technology that was never seen like on Earth. It transformed the way we used technology then, however it is still changing the way we use technology now. Bluetooth was initially not even called Bluetooth was it was first created. The creation of Bluetooth was first named “short-link” radio technology by Nils Rydbeck and with the help of Johan Ullman, Rydbeck is the Chief of Technology Officer at Ericsson Mobile in Sweden. Their main goal for creating this type of technology that has never been done before was to make wireless headsets. Bluetooth is based on frequency-hopping spread spectrum technology.

The construction of the name, Bluetooth, was actually made in honor of a Medieval king in the Scandinavian kingdom. His name was Harald Blåtand, which if translated to English, is Harold Bluetooth. Now King Bluetooth is renowned for bringing all of the neighboring kingdoms under one rule, that new nation became part of what is now present day Denmark. The man responsible for this name change is Jim Kardach. He made a system that was able to allow mobile phones to communicate with computers. The whole idea of calling this new technology Bluetooth, was because of what King Bluetooth did for the Danish people and also what the technology can do for remote devices, which is united them wirelessly.

Bluetooth usually is conducted between a range of frequencies to allow for wireless communication between a certain two or more devices. The set value of frequencies that Bluetooth runs at is between 2.4 GHz and 2.485 GHz. There are also guard bands of 3.5 MHz at the top of the interval and 2 MHz at the bottom of the interval that are not used but have a great reason for being there. Guard bands, which are used in wireless and wired technology, stops nearby neighboring frequency bands from interacting with the same radio point. Between the frequency range of Bluetooth, there is division amongst the other 79 or 80 channels on the range. For classic Bluetooth, every channel is sliced into packets of 1 MHz, this is what you would call the bandwidth. The Bluetooth that will be utilized in the home security project, uses Bluetooth Low Energy which was found anew in version 4.0 of Bluetooth. Bluetooth Low Energy, or BLE, slices up the frequency range into forty channels. So, if there is forty channels between the frequency range, that means the channels have a bandwidth of 2 MHz. The current version of Bluetooth technology is on generation number 5.0, from number 4.2 just recently. This type of communication resources are in constant renewals for specifications and reversions in the market. The needs and the uses of Bluetooth are constantly changing. In today’s world, technology is constantly evolving to meet ever developing demands from the people that use these systems. Moore’s Law states that computing power and machines and computers will all advance to get smarter and faster as time goes on. With that

said, it should be no surprize that Bluetooth technology is steadily evolving. What this new version of Bluetooth brings to the modern table is speed, more connectivity, and more speed. Bluetooth 5 offers twice the speed of the older Bluetooth 4.2 by increasing the bandwidth to 2 Mbps. The ability to double the total volume of data that will be given to receiving systems, allows for higher data transfer rates between receiver and transmitter. Also, Bluetooth 5 technology improves the range of Bluetooth coverage by up to four times providing better range. With this better range, this can allow for communication with devices over the distance of a small business or a family home. The range can be of an advantage for Bluetooth developers that may produce things like smart home security systems. The version 5 does not eliminate the other previous like version 4.0, 4.1, or 4.2, but what is does is add upon the already existing attributes.

However, all of the Bluetooth modules that were to be considered don't have the newer version 5 of Bluetooth just yet. They all have either version 2.0 or version 4.0. The Bluetooth modules with 2.0 had implementations from Bluetooth Basic Rate and Enhanced Data Rate. Early in the life of Bluetooth, data rates were much slower than they are now so what at the time Bluetooth Basic Rate increased the data bit rate to 1 Mbsp. The Enhanced Data Rate upped the ante by being able to function with data rate at up 2 Mbsp. When Bluetooth 2.0 was introduced, it allowed for customers to get the ability to add Bluetooth devices manually from a drop down selection type menu. Bluetooth Low Energy took Bluetooth technology into another generation which no focused on availability and sustenance. It was introduced alongside Bluetooth 4.0 and 4.1 and 4.2 as this technology looked at advanced and unfamiliar ways of getting a device to run on power sources efficiently. This was the next step for Bluetooth as the community for it grew large and demanded a more adaptive system that can be used in hobby projects and Internet of Things (IoT). Bluetooth Low Energy is a concept that has a really low draw of energy during peak usage, and an especially low and minimal draw of power in idle modes.

The microcontroller chip that the group will be utilizing, Espressif Systems's ESP-WROOM-32, has a Bluetooth module embedded within the chip that runs on Bluetooth version 4.2. This specifically will use Bluetooth Basic Rate and Bluetooth Enhanced Rate what was discussed earlier in the section above. Of course it will also come with Bluetooth Low Energy to support the chip's different power modes that can be chosen for certain use cases. This version of Bluetooth technology, Bluetooth 4.2, was announced on December 2, 2014 and it packed resources for Internet of Things. Another feature that version 4.2 brought to the game was version 6 Internet Protocol Support Profile (IPSP) which allowed for better smart connected things, like a smartwatch or smart home technologies. It brought IP connectability to devices that support it so things like smart lightbulbs can connect to the internet. This technology changed the market for smart products that essentially robotized the homes in an interesting way. Bluetooth 4.2 brought added security measures such that a standard connection between two hotspots cannot be tracked physically. This is a feature that will go along nicely

with the security measures we would like to see realized in the integrated home security lock.

6.14 Software Development Environment

6.14.1 EAGLE

For the purposes of this project, our team will utilize the effective and productive computing software of EAGLE to produce our schematic designs. EAGLE printed circuit board creation software was created by the well renowned company of Autodesk. What they do is provide software development tools for designers, programmers, engineers, or anyone that wants to build something using expert software to assist in those plans. “Make anything” is one of Autodesk’s major slogans and it’s largely true. You could end up making a replica of a high rise building that you admire, say the Empire State Building, a phone that you use on a day to day basis, a fast vehicle, or even movie making. Whatever you choose to make or design Autodesk most likely has the software resources you need to complete the task you desire.

Autodesk provides a multitude of software packages for one to utilize to construct and build most projects. They offer more than the software that we will use to produce this project’s schematics. Outside of EAGLE, Autodesk provides software like the well known AutoCad software that can be used to create 2D or 3D sketches for engineering projects. AutoCad is a software system that many professionals in the engineering industry work with, and is also a skill that is in demand for the work force. They also have Maya, which is the same software that was used to create video games like Electronic Art’s FIFA franchise and Bugie’s Halo franchises as well. Maya software is also used to create digital effects that appear in Hollywood; Pixar movies, The Matrix, Spiderman, Finding Nemo, Avatar. The software have created visual effects for shows the small screen like Game of Thrones, South Park, and The Walking Dead. So Autodesk software has been appearing in many media sources behind the scenes that many of us don’t realize. The company has also had an indirect hand in the engineering sector as it has developed software that benefit and support designers all over the world every day. Based on Autodesk’s track record and what they have done, we feel safe and secure that their EAGLE software is exactly what we need to help to create the correct outputs.

EAGLE offers great features for all electrical projects like modular design blocks that is instituted to keep the edits made to a design and printed circuit board stay the same. An enormous advantage of using EAGLE also, is that it has the ability to organize multi sheet schematics. Now what multi sheet schematics are, is various schematic designs combined together to form one schematic. This feature is exactly what we need as an overall system schematic is what is required. Features that can help us with our electric circuit theory are also included within this pivot software. EAGLE offers a feature they happen to call

“electrical rule checking”. So what this feature can do is verify that all of the printed circuit board wiring is connected to the right areas and also, that it makes sense electronically. One can set the electronic theory to verify and when that electronic rule should be checked. This gives the designer more freedom to put more thought and brainstorming elsewhere while the system does its required work for the user. Real time design synchronization is a similar feature to the modular design blocks previously discussed that keep all of the design packages the same. With this feature however, every single edit that is made inside of EAGLE editor is automatically synced. What is actually synced together is the changes made on the printed circuit board layout files and the schematic files. This feature provides a way for a user of this printed circuit board layout software to avoid trivial lost of time adjusting for changes in both types of files. As new users of this type of software, we can think of another system that affords us this advantage.

EAGLE provides it’s users with a simple and straightforward schematic editor that can make near and orderly connections. The design tools that come standard with this editor are professional with many tools being used by those in the industry. Sometimes a user who may be designing a project may strict draft constraints like size. To combat those constraints EAGLE has 3-D modeling capability to create a life like structure so the user can accurately determine what the constraints would look like given a particular decision. The modeling feature allows for one to devise their printed circuit board and the package that it could possibly go into. Parts for a certain project can be selected and ordered within EAGLE. The software links its components with the manufacturer's website, so these selections can be done efficiently.

Operating System	System Prerequisite
Microsoft Windows	Windows 7 and later is required 64 bit operating system is required
Linux	Runtime libraries: libssl.so.1.0.0, libcrypto.so.1.0.0, and CUPS are required Linux on kernel version 2.6 Needs a 64 bit-operating system and libc.so.6 with sub version GLIBC_2.14+
Mac	Apple® Mac OS® X version 10.10 or higher for Intel based central processing units
All operating systems	There is a minimum graphical resolution of 1024 by 768 pixels

Table 11 - EAGLE System Requirements

Another reason why we choose to use the printed circuit board editor EAGLE by Autodesk is because it was free to use. Cost restrictions play a large role in determining a system to use for getting a precise and detailed schematic for the whole team to go by. Getting such a component for free was a enormous convenience for us as we look to get all of the requisite resources but to also not spend a fortune in the process. The fact that we can do all of these calculations and build and construct these type of files for free is simply amazing. Autodesk has gone far and wide to cultivate such a useful tool, not to just professionals in the work force but for also amateurs getting their feet wet, so to speak, in project design.

Word of mouth was also a determining claim to use EAGLE software to assist the group with the home security project. Classmates and associates have raved about the usefulness of the software product as well. Past students have also used this product when operating in the senior design class, even past senior design products that were similar to this project have utilized EAGLE printed circuit board software. The professor of the class has made suggestions not once, but multiple times to use this computing tool to generate our project schematics. Thankfully we have choose EAGLE as the team's main software tool to develop and house our design schematics. This tool can be used not only for this year's round of senior design projects, but should also be recommended for future projects for the time being. For example, EAGLE can take care of assembly design tools, routing tools that can be used today like USB-C, and very intuitive in the way the software can handle the most demanding PCB design.

6.14.2 Arduino IDE

We have gone over the Arduino company and the type of electronics they provide for engineers and hobbyist from novices to skilled professionals, but what is an IDE? The first thing that is important to know is that the acronym stands for an Integrated Development Environment. So what does this environment provide us, it equips the programmer with a place to write, develop, and harvest the instructions her or she wants to run within a software application. It is a suite of software built to house all of the tools developers need to make and write source code. Within the GUI or, Graphical User Interface, the window that the user of a computer system looks into, there you can usually find the editor, the compiler, and the debugger. Some of the most popular integrated development environments are Netbeans, Eclipse, and Microsoft's Visual Studio. Now when it comes down to microcontroller development, one of the most well-known commonly used IDEs is Arduino's Arduino IDE.

The Integrated Development Environment that Arduino has created was a place for developers with Arduino boards to write and control the Arduino microcontrollers. It's an open-source IDE tool that was conceived to simplify the process of developing software that is and intended to run on Arduino

microcontrollers. The IDE from Arduino is open-source, which that means that the software is a system that has been collaborated and worked on my a community of people. Open-source has been the way to go lately for computer systems because those systems tend to be very user-friendly and also tend to save companies thousands of dollars of software maintenance. Independent research groups in the past have reported cost savings into the millions ($USD) for software companies because of open-source adaption.

Arduino products are already in high demand, which obviously makes the Arduino IDE in steep demand as well. Once the IDE is installed, it already has all of the resources and libraries for every Arduino product right there for the user to quickly start coding for their specific controller. Other important reasons why the Arduino IDE is highly attractive to users is because it can push code to development boards that are non-Arduino products. So even though the development board that will be used to test the components of this project, isn't an Arduino product of sorts, it is still possible to establish connection and integrate it with the IDE. This is very convenient for the team as the group would not have to go out of its way to find an interactive environment suited towards the test development board. Having one integrated development environment system that is this versatile cannot be taken for granted.

A resource like this is rare and the fact that this software can be utilized at cost of nothing means that there is little to lose by trying it out. Online, one can find many learning materials to help with figuring out how to work within the integrated development environment. Tutorials after tutorials that encompass a wide array of topics can be found when first starting out with this system. So that is a humongous support for helping the team to understand the ins and outs of Arduino IDE. Going along the lines of how adjustable this system is, the integrated development environment by Arduino can be used by multiple and different operating systems. The table below will show more of the Arduino IDE specifics for the latest build.

Operating System	System Requirements
Microsoft Windows	Windows 7 or higher Ability to handle zip files for non-admin users
Mac	Mac OS X 10.7 (Lion) or higher
Linux	Linux 32 bit or Linux 64 bit or Linux ARM

Table 12 - Arduino IDE System Requirements

7. Software Design

7.1 Version Control Software

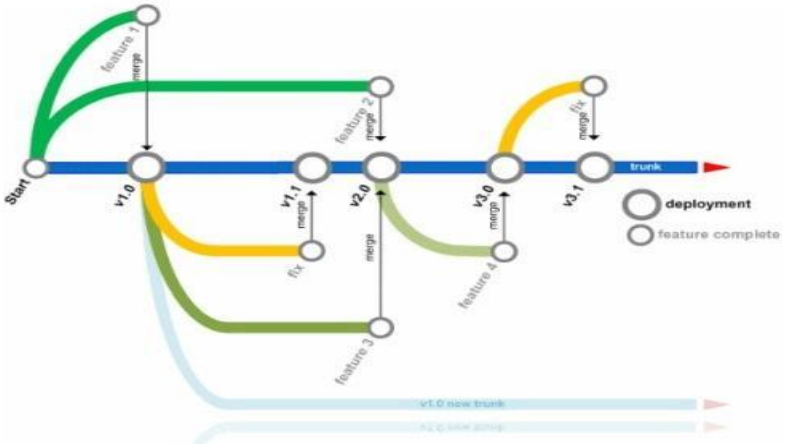

Figure 6 - Version Control Flow

When there are multiple developers working on code, a tool needs be used to keep final code consistent. This tool must also allow protection against team members tampering with each other's code. In other words, we need some form of Version Control and the tool chosen for this is Github. With Github everyone can work on his or her own tasks on separate branches avoiding any conflicts, until the chance of conflicts arise when merging everyone's code. Along with separate branches for everyone to do work on, there will be another standalone branch that will be considered our stable branch. Here, only code that has been tested and passes our standards for quality will be available. This is also the branch where all code will have to be merged into. Furthermore, there will be a repository for every different part of our software, whether it be the Android Application or the microcontroller.

7.2 Android OS

Google's Android Operating System is one of the most widely used mobile operating systems in the world. With there being more than 1.4 billion active Android users, we believed that if we were going to reach the largest audience with our application, Android is the way to go. Not only is it one of the most popular operating systems in the world, there are also has a variety of different form factors that support it. While there is Android OS for the phone and tablets, there is also Android Wear for watches, Android Auto for the car, and Android TV for the TV.

7.2.1 Why We Chose Android

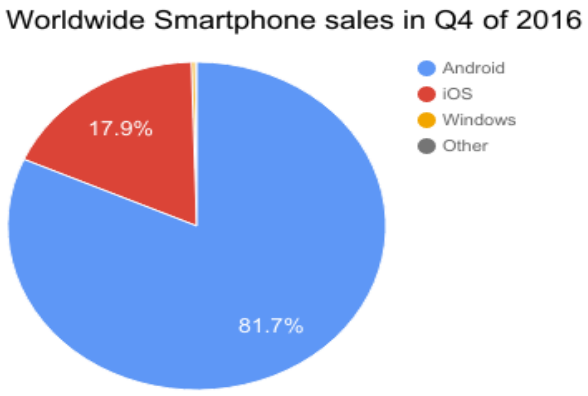

Figure 7 - Worldwide Smartphone sales in Q4 of 2016

One of the most important aspects of Android and Android OS is its openness.Unlike when developing for Apple's iOS, Android Development is accessible across all of the platforms: Windows, Linux, and Mac OS. This eliminates the problem of team members not having access to the development tools of the mobile application.

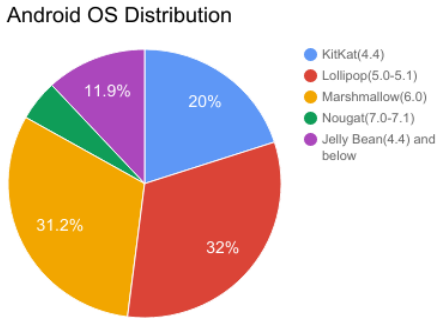

Figure 8 - Current Android OS Distribution

In addition, we felt more comfortable with Android's large amount of third party support and libraries. Yes, the actual Android Software Development Kit is great and will most likely have anything and everything the team needs, but there is no guarantee that the methods of the SDK will be the most understandable or simplest to use. In many cases in software development you find that libraries can take what is in the SDK and can wrap methods around these functions to make day-to-day operations much easier and sometimes these third party libraries can even fix problems in Google's own code. Of course there are pros

and cons to libraries and some can even cause more problems than they fix, but we enjoy the different options for application.

Finally, we chose Android because it was the mobile Operating System with which the team had the most experience using for development. We felt as if starting from scratch in learning how to use the development tools of another OS would have caused serious setbacks in our project roadmap.

7.3 Java

Furthermore, Android development is predominantly done in Java. Java is the language that is the most emphasized in our programming classes and the second most-in-demand programming language of 2017 according to codingdojo.com and indeed.com, so naturally those in the group that are Computer Engineers are the most comfortable with it. Java itself is an Object Oriented Programming(OOP) Language created by Sun MicroSystems that is so well-liked because of its numerous quality features that make it a complete package as a programming language. One reason why java is so loved is because of its portability, in other words it is platform independent. Java can run on any Operating System, without the developer having to worry about having a specific compiler for the system that they are running it on.

Additionally, it is a very flexible language. Java can be used for phones, servers, desktops, and other devices; its reach seems to have no limit. Moreover, Java has amazing tools that assist in making your life easier when programming in java. Some of these great tools are the feature-packed and free Integrated Development Environments that are currently present. There is NetBeans, Eclipse, and IntelliJ just to name a few. The features that I have expanded on are just a few of the characteristics that make Java such a special language to work with. Along with the previously stated reasons, java also has great, in-depth documentation, concurrency, excellent support, and extensive third party support that can allow you to do some extraordinary things that you otherwise could not do.

7.4 Purpose of the Android Application

The main purpose of the Android Application in our project is to be the primary bridge of communication between the the user and the actual locking system itself, whether it be through Wi-Fi or Bluetooth. With the app, the user will be able to easily complete the initial set-up for our device. One of the many ways it will assist in creating a more streamlined setup process is that it will allow the user to train the lock’s fingerprint scanner to recognize his or her fingerprint from the app. The UI will make it easy for the user to see if errors are being made in the scanning process or if the finger needs to be positioned correctly and the app will

provide feedback for each of the different cases. The initial setup will also allow for the user's phone to be able to communicate with the lock through Wi-Fi or bluetooth, simplifying the process of unlocking the door in the future.

7.5 Android Application User Interface

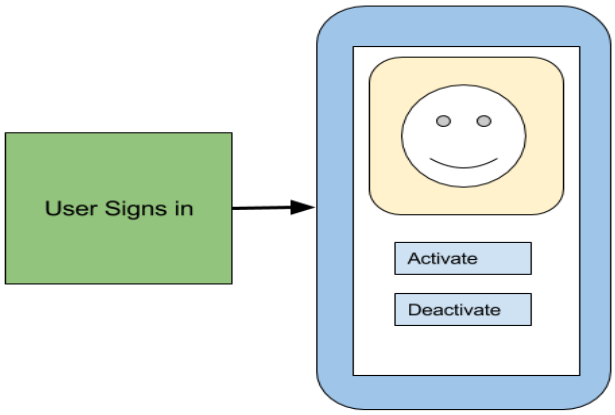

Figure 9 - Android UI

For our application, our goal is to have a clean, simple, and intuitive user interface. When a user gains access to the app with one of the 3 forms of authentication, we do not want to obscure any of the important features or functionality behind menus or different screens, so the main functions will be presented instantly on sign in. On this main page at the top of the screen the most recent image taken by the locking system will be shown if the user was notified because of a unrecognized visitor at the door. Furthermore, the user will have the options to activate and deactivate the locks on this screen in the application. Behind the scenes, in menus and on other screens, we will have the features that we do not expect a user to user very often. These will include things such as changing login credentials, setting up new forms of authentication, and much more.

7.6 The Android Application and Visitors

Along with assisting with the initial setup process, the app will play a key role in alerting user's of a visitor at the door, whether the user is known or unknown. When our system senses a visitor at the door, a picture of the visitors face will be taken with our camera. The picture will then be sent to the user's phone where the process of facial recognition will be offloaded and occur in the app. From here users will be notified of a presence at their door and whether or not the system recognizes the face of the visitor. If the user is recognized and does not have access to unlocking the door, the user will be given the option to unlock the door for the visitor, this will be able to happen over bluetooth or Wi-Fi. If the system happens to recognize the visitor and the visitor has a means of unlocking

the door, because he or she is a user of the system, then other users of the system will be informed that the aforementioned user has arrived. However, if the user does not recognize the visitor, all users that are registered with the smart locking system will be alerted of the unrecognized user. This means that all users will be able to see the picture that is taken of the visitor and even a live video feed of the visitor. From here, users can determine if the unrecognized visitor is a threat and will even give the user the option to report suspicious activity.

7.7 Unlocking the Door with an Android Device

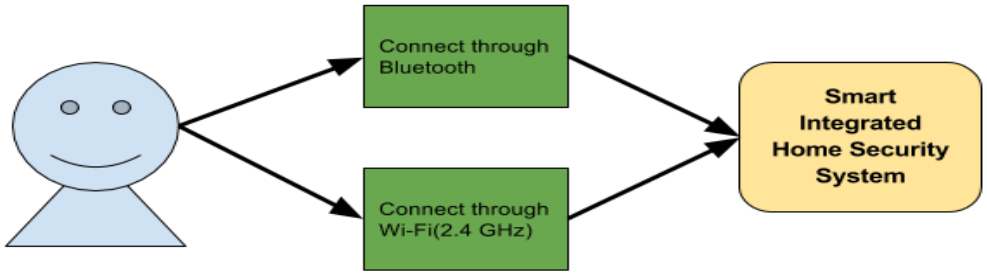

Figure 10 - Android App Connectivity

There will be two methods for unlocking the door from a user's Android device, but first the device will have to be connected to either bluetooth or Wi-Fi. With Wi-Fi the user will be able to connect to the Smart Lock System from anywhere there is internet access, with bluetooth the user will be able to connect to the locking system while in a certain proximity of the door. Both options have their pros and cons but we felt that user's should have both options as a choice.

Once a user is connected, whether through bluetooth or through Wi-Fi, the user will have the option to activate or deactivate the locks in the system. If the user is opening the door for an unrecognized visitor, the user will be able to see a picture that was taken of the visitor just moments before they were notified of a presence at the door. We would like to make this process of unlocking the door as seamless as possible, especially as a user walking up to door, so that they can open the app and press one button and they're able to walk inside. However, there will have to be some sort of authentication when signing in on the application for the purpose of keeping the users lock system safe from those who are unauthorized. We will further expand on these forms of authentication and how they will be utilized in the next section.

7.8 Security in the Android Application

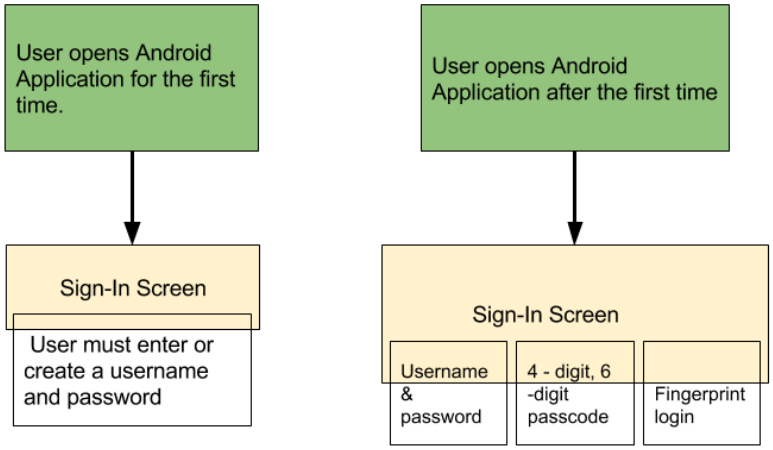

Figure 11 - Authentication Options

To keep those that are unauthorized from using a user's application and taking control of the system, we will implement 3 security measure. The first one will be a username and password combination. These will primarily be used for verification when the user is first signing up and setting up the locking system. Along with this, these will also be used as fallback just in case other forms of authentication fail, the system notices suspicious activity with too many incorrect attempts, or a user just happens to forget his or her passcode. Having a username and password is mandatory for a user, as they will be needed at some point or another.

The second, and optional form of security we'll introduce to the application is the passcode. This passcode can only be set once the user has signed in at least once with his or her username and password and it will be available in two lengths, 4 digits or 6 digits. Once this has been set up and confirmed, the user will be able to bypass inputting the username and password and gain access to the app more quickly. We believe this will be the most widely adopted method of authentication throughout our whole user base.

The third, and optional form of security for users that are able to utilize it, will be the use of the phone's fingerprint scanner. This will by far be the quickest way to access the app and control your system. However, this option will not be available to all users of the app because not all phones actually have a fingerprint scanner. But for those that do, this form of security will be, what we believe, the most widely preferred method of gaining access to the locking system.

7.9 Facial Recognition in the Android Application

There will 2 options for facial recognition in our system with our first method being facial recognition through the actual Android Application. In the Android method, a photo will be sent to the phone using Wi-Fi and once the phone receives the picture, it will be able to process facial recognition algorithms on the phone itself. Most of this work will be done by using a third party Android Library called Kairos.

7.9.1 Kairos Android SDK

The Kairos Android SDK is the Android Client of the Kairos Facial Recognition API, which allows for Face Detection, Face Identification, Face Verification, Emotion Detection, Age Detection, Gender Detection, Multi-face Detection, Attention Measurement, Facial Feature Detection, Sentiment Detection, Face Grouping, and Ethnicity Detection. Kairos itself is an artificial intelligence company located in Miami, Florida. Furthermore, they have expertise specifically in facial recognition.

The API has a plethora of useful and amazing abilities. First, there are three modes of operation in the SDK: Recognize method, Enroll Method, and Detect Method. In the Recognize Method the API takes a picture and compares it to all images in a specified gallery. Then, a list of IDs for each subject is returned and also confidence values are returned for each ID. With this method of recognition, the user's image will have to be stored in some gallery that will be used when comparing faces . And along with this, multiple pictures of a subject will be needed for the best accuracy. In the end, as long as the confidence value for any ID at least 80%, the system will see the visitor as a recognized user. To circumvent the inevitable algorithm errors, the user will be able to confirm if the facial recognition match is correct. If not, the visitor will be denied entry.

In the Enroll Method, the SDK allows you to register faces for future face recognition. This goes hand in hand with the Recognize Method, in which these enrolled faces are scanned through to produce a confidence value. To enroll a face, Bitmap image, or String image, String galleryId, String subjectId, etc are needed. This method would most likely be used during the setup process, so that the user can train the system.In the Detection Method, the SDK can be used to track and see attributes of a face. These attributes include the exact location, or coordinates, of facial features including the eyes, nose, and mouth. This can be helpful in the identification of a visitor's face in a still image on the app's home page.

This library was chosen due to the fact that it was free and also because of the extensive and well-written documentation that many libraries seriously lack. It was also the most feature packed of the facial recognition libraries that could be

used on the Android Platform. The Kairo SDK also has a MIT license, which assuages the fears of copyright problems.

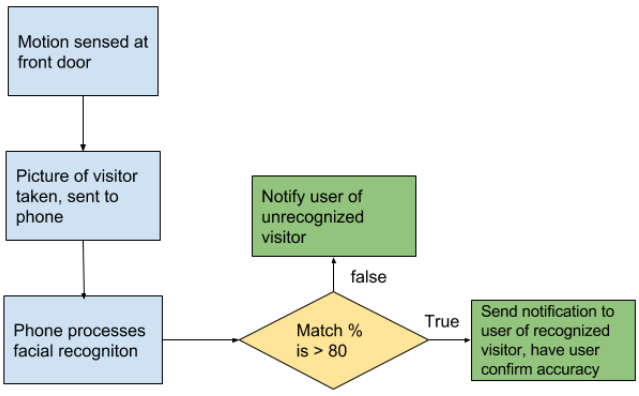

Figure 12 - Android Facial Recognition

7.10 Raspberry Pi

7.10.1 Raspberry Pi 3 Model B

This single board computer was developed by the wonderful people over at the Raspberry Pi Foundation in the United Kingdom. Their original goal or mission was to help create a new creative learning environment for youngsters all over the world. They wanted and have been attempting to spread the interest of computing science while also not having to break the bank. The foundation provides low cost and tremendously powerful chips for use for teaching and educational purposes. The Raspberry Pi Foundation has provided substantial resources to assist students and adults alike with free tutorial for computer learning, training for teachers, and community outreach.

The Raspberry Pi 3 Model B system on a chip board is one of the most powerful boards ever constructed. The reason why this board is so popular with the computing and do-it-yourself communities is because of the amount of money you are putting down for the amount of processing power you are receiving. The third generation of the Model B now comes with a brand new 1.2GHz 64-bit quad-core ARMv8 CPU to control the logic on the broad. The CPU on the model B system is said to be ten times better than the Pi 1 and twice the processing power of the Pi 2. The board comes with a 802.11n Wireless LAN chip which was highly anticipated to be on the previous generation but sadly wasn't included is here now with the third iteration of the board. Another difference of the Raspberry Pi 3 Model B versus the previous generational model is the presence of a newly embedded Bluetooth 4.1 module which also supports Bluetooth Low Energy (BLE). Everything else included on the board is the same as the second version of the board like:

- 40 GPIO (General Purpose Input/Output) Pins
- 1GB RAM
- 4 USB Ports
- HDMI Port
- Ethernet Port
- Micro SD Card Slot
- VideoCore IV 3D Graphics Core
- 3.5mm Audio Jack

7.10.2 Raspbian

In order to use the Raspberry Pi, an operating system must be installed on the device itself. Luckily, there are plenty of free operating systems online that can be obtained to install on the Raspberry Pi - 11 to be exact. These OSes are Raspbian, Ubuntu MATE, Snappy Ubuntu, Pidora, Linutop, SARPi, Arch Linux ARM, Gentoo Linux, FreeBSD, Kali Linux,and RISC OS Pi. However, out of all of these choices, we chose Raspbian.

Raspbian is a free operating system was built upon the foundation of Debian, except it is optimized for the Raspberry Pi hardware. One reason why we chose Raspbian is because of how complete the software package is. Raspbian includes more than 35,000 packages that allow you to perform some of the most complex functions with ease. And even with these 35,000+ packages, Raspbian is known for it's efficiency and amazing performance. The second, and most monumental reasoning for picking Raspbian has to do with the fact that it is actually officially supported by the Raspberry Foundation. This is huge because the Raspberry Foundation is the foundation that is actually responsible for producing the Raspberry Pi. If the makers support the operating system, you can guarantee that it will be the most problem-free and reliable OS that can be installed on it.

7.10.3 Python

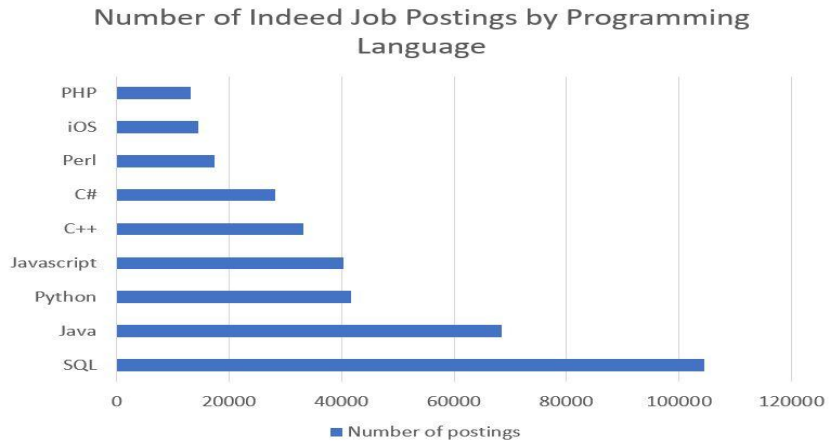

Figure 13 - Most Demand Languages

There are a multitude of programming languages that can be used with the Raspberry Pi, but for our purposes we will be using the Python Language. Python was actually created in the 1980s and got it's name from Monty Python. Since the 1980s it has exploded in popularity and demand. And as of February 2017, it is the third most in demand language in terms of the number of job postings on Indeed.com. Python itself is a strongly-typed, object-oriented, dynamic, and multi purpose programming language that has a myriad of purposes. Python is used in Data Analytics, Machine Learning, Web Scraping, and Web Development just to name a few. Also, outside of Java, Python is the next coding language that the group feels the most comfortable with.

7.11 Programming on a Raspberry Pi

The Raspberry Pi, other than the mobile phone, will be one of our main sources of facial recognition in the application, but in order to integrate it into our whole system and have it communicate with other components, it must programmed. There are a couple of ways to go about programming on the Raspberry Pi:

One method of programming Python on the Raspberry Pi is by using the a text editor and command line combo. The user can use a text editor such as Vim, Nano, or Leafpad to type the code and then run code from the command line as a Python script All the user has to do is go to the directory that has the saved file and run the command line arguments from there. The other method of programming is to use IDLE.

7.11.1 IDLE

IDLE stands for the Integrated Development and Learning Environment in Python. It is cross-platform, uses pure python, and has many features including:

- Searching within any window, replacing, and using grep(allowing you to search through many files)
- Includes a debugger with features such as breakpoints and stepping. While also including the ability to view namespaces.
- A shell for Python that contains input, output, and error messages.
- A multi-window text editor that color codes key words and has other features such as auto-completion, and suggestions.

IDLE actually has two types of modes, also known as window types, which are are the Editor Window and Shell Window. In the Shell Window you'll find features such as the Shell menu, Debug Menu, Edit Menu, Options Menu, and Window

Menu. In the Editor Window, you'll find the File Menu, Edit Menu, Format Menu, Options Menu, Windows Menu, and the Help Menu.

7.12 Facial Recognition on the Raspberry Pi

As previously stated, the Raspberry Pi's primary purpose will be that of processing facial recognition software. The Pi, combined with a 5MP Raspberry Pi NoIR camera, will be able to scan a face using facial recognition algorithms and match it to a specified person. Unlike the Android method, this process of facial recognition will happen in real-time, there will be no overhead of having to wait for a picture to be sent to the phone before the facial recognition is processed. However, all this cannot be done on the barebones Raspberry Pi by itself. To do all of these intensive facial recognition tasks, some type of third party library is needed. And in this case, the library that will be used is OpenCV.

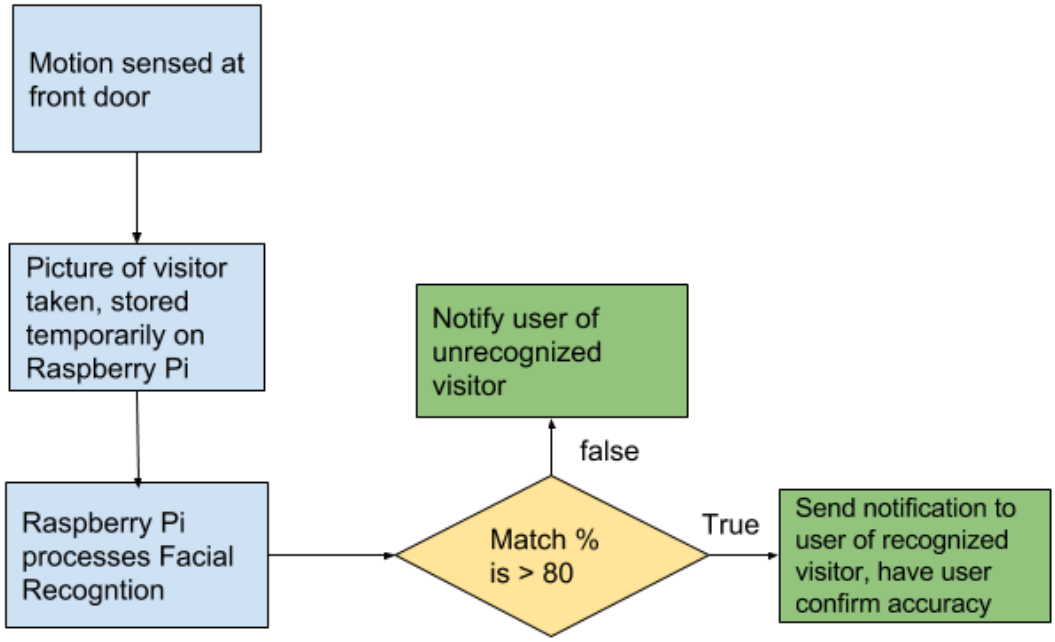

Figure 14 - Raspberry Pi Facial Recognition

7.12.1 OpenCV

OpenCV, or the Open Computer Vision library, was created by Intel in 1999 and is a free to use library that can be used with C, C++, Python, and Java, while also supporting Linux, Windows, Mac OS, iOS, and Android. The library itself is actually written in C/C++ ensuring that the library if optimized and can utilize multiple cores for the processing of algorithms and data. Furthermore, it is one of the most popular Computer Vision Libraries in the world with about 47,000

people in the user community and over 14 million downloads. It has many wide-ranging purposes including robotics, and art.

Facial Recognition, recently added in version 2.4 of OpenCV with the FaceRecognizer class, currently uses one of three algorithms to complete its task, Eigenfaces through createEigenFaceRecognizer(), Fisherfaces through createFisherFaceRecognizer(), and Local Binary Patterns Histograms through createLBPHFFaceRecognizer().

In the Eigenface method was constructed by Sirovich and Kirby in 1987 and was founded on the basis that each human face can be represented as percentages of a set of “base” face, or in this case eigenfaces, and along with this, this method tries to maximize variation. The eigenfaces themselves are ghastly land blurred images.

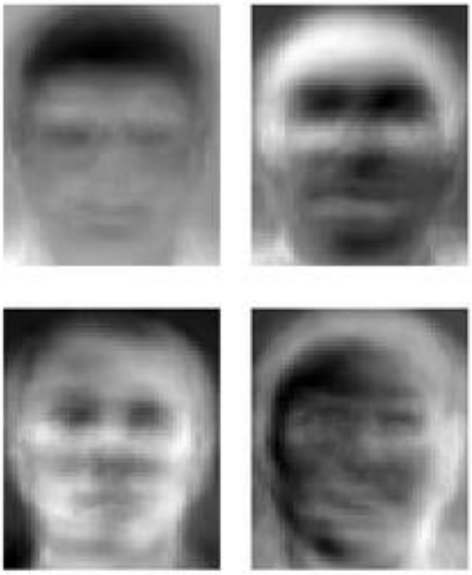

Figure 15 - EigenFace examples
Pending Permission from research.att.com

Luckily for the team, OpenCV has been ported over to the Raspberry Pi where it has been optimized to run on this device. With this comes the abilities to track faces and to also recognize faces. OpenCV is essential to the goal of bringing facial recognition to our project, and there is no better library to do that with.

7.13 WiFi and Bluetooth Configurations

The bluetooth thread will loop indefinitely. First the thread will initialize a response queue for received messages and check if the lock is registered in the status byte; If not, it will only accept wifi setup commands. Once registered the thread the rest of the commands will open up. The main program will hold a

hashmap for users. These users will be verified while wifi is enabled. As incoming messages are viewed a user will be attached with a particular encryption attached. If these users have been granted access then it will be filled and hashed on board. These incoming bluetooth messages will first establish a secure connection per user, this is discussed below. Then the user may send commands. Bluetooth only commands:

- Admin user soft key gen (usable only when lock is not connected to wifi source) : An authenticated admin will select a pre-connected unauthenticated user to grant access to open/close the lock and the time period to which this user will have open/close privileges. Then the selected unauthenticated user will be sent a message on his/her already bluetooth connected device. This will be a string of digits. The admin must then enter those digits as a confirmation to authenticate the user. Once wifi is reconnected this information will be registered with the server. If the user is not registered the key will be deleted immediately; This situation should be near impossible considering the client on the device had to go through the authentication process described below and must be logged in to access the client application.

- Admin key revoke: This is simple. The admin selects a user and revokes his/her key. The key will no longer allow the user access to control the lock regardless of how much time was previously left on the key. This information is sent to the server upon reconnection.

- Unlock: listed in general.

The wifi loop, main loop, will have a lot more to it considering that a connection with probable authentication must occur and may or may not be available at all times and even if available and connected there may still only be connection to local devices and the internet inaccessible. The loop will begin by initializing a response queue and checking the status bit to see if a wifi configuration has been established, this will be achieved with a simple and operation on the status byte. If configuration is established then wifi will proceed to try and connect to the network. After several unsuccessful attempts to connect to the configured access point the microcontroller will scan to see if any other locks have an ssid to avoid a matching name when establishing its access point to which there will be no password and the ssid will begin with a constant string then a random skew of numbers. This can be used to set up a new wifi configuration. The same thing will occur if no wifi configuration was saved. Although if a configuration is saved, it will retry to establish a connection once every so odd minutes.

Once wifi connection has established then the registration bit will be checked. This is done the same way as before. With a simple logic operation on the status byte. If the lock is not registered then it will attempt to connect to the server. If unable to reach the server then the lock will be at a stalemate till such a time that it can be registered. Once registered the wifi will allow all other commands and

one should be able to see one's lock on one's device. Details about registration are described in another section.

Wifi will use the same user map as bluetooth. Once a day while connection to the server is active it will try to update the programming on the microcontroller. If the microcontroller is updated a restart will take place and a small window of downtime will occur. This downtime will be negligible. This will end the wifi loop.

7.13.1 Registration

Registration begins when the Owner first makes an account with the server. Then proceeds to continue by registering the lock. Assuming that wifi is setup and connection to the server has been established. The server will identify the lock by its serial number/id and each id will have an associated set of digits that will be on the server and included with the lock. He/She will use those to prove he/she is the Owner for the lock and register it as his/her own. Granting that person full control.

7.13.2 General Commands

For the following commands wifi is connected and there is access to the server, if sent through bluetooth the microcontroller will be a medium to the server.

- Add User Key Gen: An Admin that has been authenticated with a secure connection sends a message to the server to grant a key to a user for a specified period of time. This user could be in their contacts, registered with a specific email address, or by id. The server generates a key and adds it to the database for that lock and sends a message to the lock letting it know to add that user authentication key for a specified amount of time starting at a specific time. This user now has access to control the lock until the key expires.

- Revoke User: An Admin that has been authenticated with a secure connection sends a message to the server to revoke access for a user. This destroy the key for that user in the database and the server will send a message to the lock to do the same regardless of the time remaining on the key. The user will no longer be able to control the lock.

- Make Admin: An Owner that has been authenticated with a secure connection sends a message to the server to grant a user Admin rights. The owner selects a user and grants him/her the right to not only control the lock but grant other users the ability to control the lock and an indefinite key. This is sent and recorded in the server database. The server then sends this information to the lock.

- Delete Admin: An Owner that has been authenticated with a secure connection sends a message to the server to revoke a user's Admin rights. This

also takes away the indefinite key and control of the lock to that user. This information is sent to the server and deleted from the database, echoed on the lock.

- Status: Shows the current status of the lock recorded in the server.
- Unlock: A user request the lock to open. Sends his/her key. If the key is valid and active then the lock opens. The time the lock remains open is temporary and set by the admin. The User who unlocked the door and the time are noted. This information is sent to the server and logged in the database.

7.13.3 Passkeys (also referred to as key)

The only way to unlock the door is with a granted passkey. There are three ways for a person to have a passkey. Someone can be an Owner or Admin and have an indefinite key. Someone could be a user with an indefinite key. Someone could be a user with a temporary key. These keys may be updated after a certain time or certain amount of uses if indefinite to hold security even though after a secure connection is established and authentication has been conducted. A User must still have a key which is 256 bits of raw randomly generated data. A chance of 2^256 of guessing a key and that is not taking into account user authentication. A lock is about security. If that is not provided it has lost its general purpose. Thus the passkeys length. That being said over 30 passkeys can fit in 1 KB which is small amount of space for a ridiculous amount of people having a key for a house at one time.

7.13.4 Secure Connection and Authentication

Both the wifi and bluetooth will run under the same security measures. First a sha256 of the client public rsa key and server public rsa key are hardcoded. These will change with every update and will be stored in a database on the server. A standard Diffie–Hellman key exchange to achieve a shared secret:

1. Lock sends message to server to start connection
2. Server/client send p and g, p is a prime number of 600+ digits and g is a primitive root of p
3. Lock selects a large secret int a and sends g^a % p
4. Server/client selects a large secret int b and sends g^b % p
5. Lock computes shared secret = (g^b % p)^a % p
6. Server/client computes shared secret = (g^a % p)^b % p
7. Now server and lock have the same number shared secret (ss)

This shared secret is now taken to encrypt the communication between the two parties. This is done using AES (Advanced Encryption Standard). As the ss number will be a modulus of 600+ bits. The ss will be hashed to 256 bits using sha256 this will make it small enough to use AES 256. All further information will be encrypted by AES256(sha256(ss)).

8. Lock sends version number
9. Server/client looks up RSA for version number and sends the public key
10. Lock then checks the public rsa key by performing sha 256 on the decrypted data and checks it with the hardcoded value. If it is a match then the client/server is authenticated and communication can continue but now All further Information is encrypted RSA(AES256(sha256(ss))).
11. All security measures for basic communication have been met and data can flow

7.13.5 Server

The server has multiple parts as It will have to maintain a client communication, a web interface, and communication/synchronization with all locks. A mysql database will back all data for services. A server also has to make sure that digit sets sent out with locks are matching the locks serial/id number. The web interface will mirror the android/ios clients. The entire backing interface will primarily be written in java for easy deployments and updates. The driving web engine behind java will be a glassfish server. This can easily produce database classes and beans for JSF (java server faces) through reverse engineering and is highly used in commercial software.

8. Hardware Design

8.1 Power Supply

The power supply is the most important aspect for any project. To power all components seamlessly can become very complex when dealing with multiple components operating at different voltages. Engineers must give plenty of thorough contemplation before implementing onto a PCB. Using a constant supply of power, which was decided in the research section, has narrowed the approach for the required parts needed to keep the security system operating. This section will explain the group's design process for creating the power management PCB.

The first step is to acknowledge every necessary voltage level and current supplied needed to power up all of the components for the security system. After reviewing all of the operating voltages for the peripherals, the voltage levels the power management board must supply are 12 volts, 5 volts, and 3.3 volts. 12 volts will be the first voltage to be achieved because the design will be easier and simpler to step down in voltage rather than amplifying the signal to higher voltages. 12 volts will be supplied from a rechargeable battery pack that is rated 12 VDC with 6000 mAh. The rechargeable battery pack can output 12 volts DC through a male barrel jack adapter. A female barrel jack adapter will be needed to connect with the male connector for power to be transmitted to the security

system. A breadboard friendly 2.1mm jack barrel adapter is going to be used as the female connector, which will be easily implementable into the design. The adapter has considerably thicker leads, which will raise concerns when soldering onto through holes in PCB. Therefore, this barrel jack adapter will only be used during the testing and developing process. For the final PCB design, a surface mounted jack barrel adapter will be used. Common developmental boards on the market implement the same technology to receive power.

As a power signal is being received from the barrel jack, the 12 volts line will be used for powering on the door lock solenoid. The 12 volts line will be directly connected to the solenoid and a component that will be capable of bringing down the current voltage to 5 volts. Voltage dividing, linear voltage regulator, switching regulator, and switching controller can all be used for obtaining a lower voltage. The design will implement a linear voltage regulator by texas instruments called the LM7805CT. The LM7805CT is an a fixed 5 volts voltage regulator capable of receiving input voltages between 5 volts to 18 volts and outputting current at 1A or less. For the project design purposes, the LM7805 will be receiving an input power signal of 12 volts DC and outputting 5 volts for the next voltage line. A schematic will be shown on the recommended layout for regulating the input voltage. Capacitors are used to ensure ripple rejection and stable transient response. Diodes are placed to for the capacitors to safely discharge through the low impedance path to avoid voltage regulator damages.

The last voltage level to reach is 3.3 volts. The most least expensive way for achieving this voltage level can be reached by the means of two resistors. The resistors values are chosen to properly divide the 5 volts down to 3.3 volts. However, the voltage will not be regulating and the resistors will draw up way too much current and will lead to more complications, so this method will not be used. The next option was to use another voltage regulator that is also manufactured by Texas Instruments called LM1117DT-3.3. This voltage regulator is used specifically for the step down 5 volts to 3.3 volts conversion. The LM1117DT-3.3 will require a 5 volt input in order to output 3.3 volts.

How efficient the regulators are when outputting voltages can become another area of concern that must be accounted for when designing the power management board. If planning to connect both voltage regulators in series to reach 3.3 volts down from 12 volts, the output performance will most likely produce very poor efficiency. The LM7805CT and LM1117DT-3.3 are both rated at 95% efficiency. The 3.3 volts will only be (0.95%*0.95% = 0.9025%) efficient due to the current topology. The best option to receive a 3.3 volt rail is to use another LM7805CT voltage regulator drawing from the 12V rail. Therefore for the most efficient stable design for reaching the 3.3 volts is having the LM7805CT in parallel with the LM1117DT-3.3. The resistance in the output terminal of the LM1117DT-3.3 can be adjusted to acquire the appropriate amount current to be drawn. A schematic is shown on how the voltage regulating circuit will reach the 3.3V limit. The schematic includes the 5 volt circuit and will be outlined as shown.

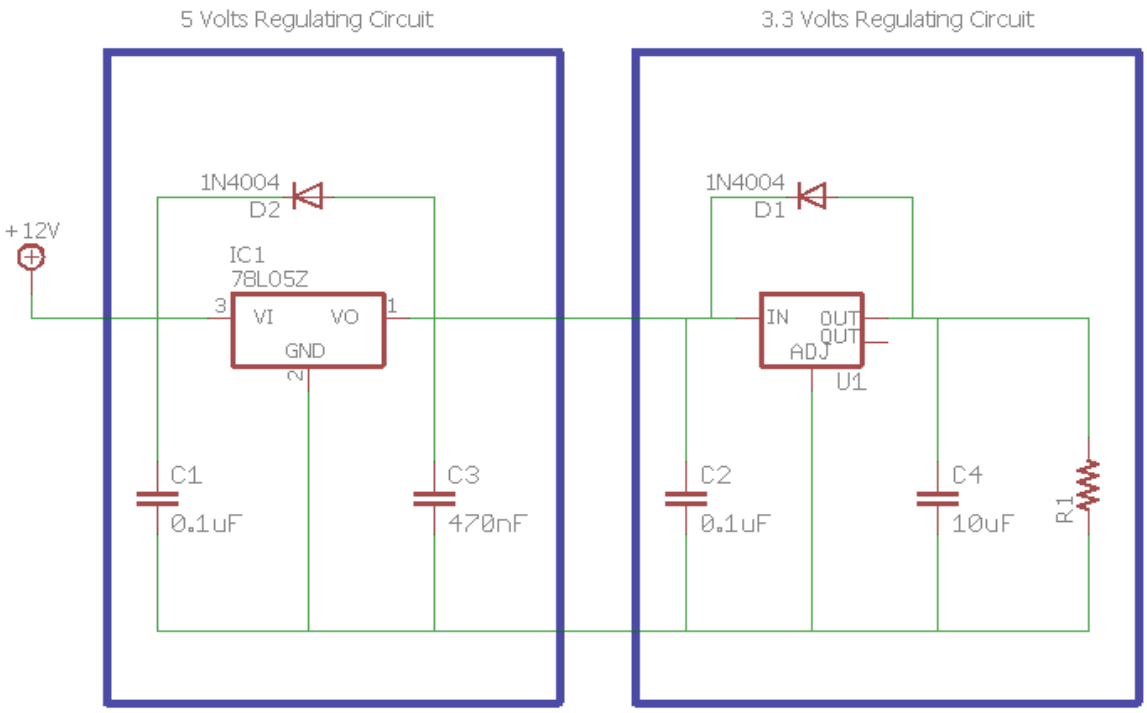

Figure 15 - Power Management Schematic

All of the main components that will be integrated into the power management PCB have been mentioned in this section. A block diagram will illustrate the architecture for the power management PCB in figure 16.

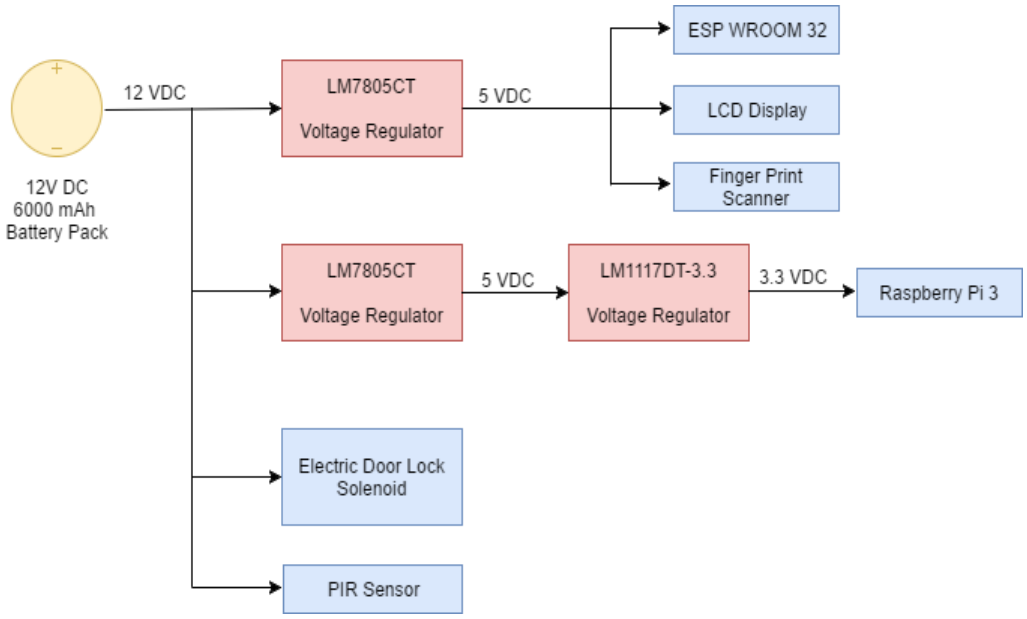

Figure 16 - Power Management Architecture

8.2 Monitoring Battery Health

The biggest limitation the security system will be facing is conserving battery power. The security system shall be designed to be as efficient as possible. There is a phenomena that occurs when a power supply drops below a certain voltage. If this voltage is below the load's operating voltage, the load will draw large amounts of current. This transfer of large current is called inrush current. When the inrush current is greater than the nominal current rating of the load, the inrush current can cause huge damages to the circuits connectors and traces. The security system is going to prevent inrush current from damaging the door lock solenoid and other circuitry by monitoring the battery power source. Usually most electrical components have a ±10% voltage and current rating tolerance. This allows the electrical component to be in safe operation if just a little more voltage or current is being received. Inrush current will be preventable by detecting when the battery's voltage is about to drop below the 10% operating voltage for the load. The following table will show the voltage levels at each battery life percentage till reaching 0%. These are the voltages that will be monitoring to indicate what levels the 12 volt battery is around. The yellow and red areas are the voltage levels that would cause inrush current to flow into the circuit causing damages. Ideally, the battery level at 100% will be outputting 12.7 volts and 11.9 volts at 0% charged for the security system to operate safely.

Percentage Battery Charged	12 Volts Battery Output
100%	12.7 VDC
90%	12.5 VDC
80%	12.42 VDC
70%	12.32 VDC
60%	12.2 VDC
50%	12.06 VDC
40%	11.9 VDC
30%	11.79 VDC
20%	11.58 VDC
10%	11.31 VDC
0%	10.5 VDC

Table 13 - 12V Battery Charge Percentage

The ESP WROOM 32 will be used to monitor the battery health. Multiple analog to digital converters are embedded in this microcontroller, which will be a key component to sensing the battery's health. For this process, the design will only require one ADC pin. The ADC has a 12-bit resolution, and the voltage level can be divided into 4096 equal parts. The pin that will be reading in the battery voltage levels must have a voltage divider tied to the pin. As for all electrical components, the input voltage should not surpass ±10% voltage rating values. The 12V battery must be at least below the operating 5 volts for this function to properly monitor. The design will have a reference voltage, which is usually the supply voltage to compare with the battery's voltage. The reference voltage that can be used is the 5 volts being supplied to power up the ESP WROOM 32. The design will require a code program to assign which ADC pin is being used, what pin will be reading the input voltage from the battery, and what pin the reference voltage will be. The following formula can be used to calculate the levels of the battery. After calculations, there will be a specific range that the ADC will tolerate before shutting down all operations before any damage is conflicted onto the circuit.

$$ADCvalue = 4096 * \frac{Vin}{Vref} = 4096 * \frac{Vsupply}{5V}$$

The resistors used for the design must divide the voltage being monitored below 5 volts as reference. As a safe voltage for operation, the voltage divider should divide down to around 3 volts. The design will use common resistor values, 10 k-ohm and 33 k-ohm, to reach a voltage at around 2.953 volts. The next step is to calculate the ADC range for when the battery is fully charged and once the battery is about to dip under the 40% mark from Table 12. The voltage range can be obtained by calculating the voltage difference between the highest and lowest acceptable voltage before shutting down. There is a 0.8V difference for the operating voltage, and the next step is to divide the voltage range into ten equal parts. The voltage levels will decrease from 12.7 to 11.9 in intervals of 0.08 volts to properly scale the battery health in increments of 10 percent. The following will display new values when the ESP WROOM 32 reads the battery health.

Battery Voltage	Divided Voltage	Battery Health Percentage	ADC Value
12.70 V	2.953 V	100%	~2419
12.62 V	2.935 V	90%	~2404
12.54 V	2.916 V	80%	~2389
12.46 V	2.898 V	70%	~2374
12.38 V	2.879 V	60%	~2358

12.30 V	2.860 V	50%	~2343
12.22 V	2.842 V	40%	~2328
12.14 V	2.823 V	30%	~2313
12.06 V	2.805 V	20%	~2298
11.98 V	2.786 V	10%	~2282
11.90 V	2.767 V	0%	~2267

Table 14 - New Battery Monitoring ADC Values

From the new table that was produced after some calculations, the ADC value range for safe operation is from 2419 through 2267. The microcontroller will have to be programed to read these ADC values. The ADC values will help distinguish how much the battery life percentage is by associating the values to a particular percentage. Once a ADC value falls below or equal to a certain threshold, the microcontroller will be able to transmit a text message to the LCD display to show what the battery percentage is.

Another consideration that must be accounted for is the amount of power the battery monitoring will draw from the system. Although the battery monitoring is considered low voltage, the battery monitoring process will be consuming the most power once the microcontroller enters deep sleep mode. Because the design is be as power efficient as possible, the only way to fix this issue is to somehow only monitor the battery health when in full active mode. This can be done by having the microcontroller activate a switch, for this case it will be a logic level p-channel MOSFET (FQP27N06L), to allow power to flow whenever the security system is not in sleep mode. An n-channel MOSFET (FQP30N06L) shall be used as the level shift to drive the p-channel. When the p-channel is operating in off mode, it acts as an open circuit. Having the both MOSFETs in this particular configuration, the ESP WROOM 32 can control the switch to monitor the battery's health. With all the considerations taken into account for, the following schematic will represent the battery monitoring circuit in full detail.

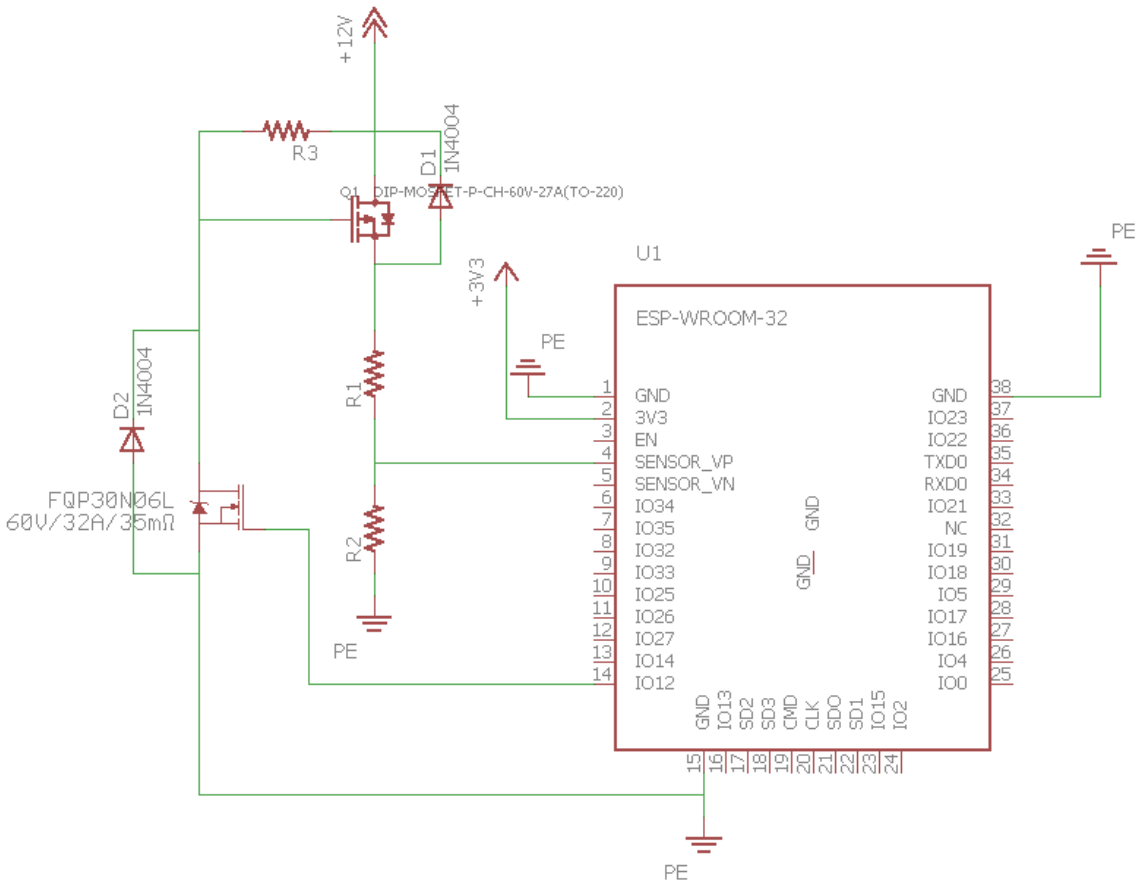

Figure 17 - Battery Monitoring Schematic

8.3 ESP WROOM 32 Interface with Raspberry Pi 3

The main function for the Raspberry Pi 3 is utilize its processing power to implement facial recognition as a security access feature. The ESP WROOM 32 must be able to communicate with the Raspberry Pi to be able to do so. There are a few methods to interface between the two modules. Communicating through a serial, I2C connection or USB are all common arrangements that the group has considered employing. The design process for this interface will be explained in the following sections.

I2C communication is supported on both the Raspberry pi 3 and ESP32. The ESP32 can support 2 I2C devices through any of its GPIO pins. The ESP32 is considered the master and the raspberry pi will be the slave, and this implementation will remain consistent for both technologies. Since the ESP32 has 3.3 volt logic levels rather than Raspberry Pi's 5 volts, a logic converter is needed between these two connections. The signals needed for these connections are SDA and SCL pins on both of the microcontrollers. The Raspberry Pi and ESP32 will require coding to establish the master and slave

I2C connections. Communication through serial GPIO pins approach is very similar I2C. The logic converter will still be used because of the differential voltages. In order establish the proper bridge between both devices, the process to configure both microcontrollers will require coding as well. The serial connection is going to require Tx and Rx pins on both microcontrollers in order to create this connection. The group has decided to not to apply these two approaches because of logic converter that is required for the master slave communication. The ESP 32 must be the master for the security system and there was a potential issue that could arise because this voltage difference.

The best option for connecting these two microcontrollers was by a serial USB cable. This method demands the least amount of extra hardware and simply uses the micro USB cord that comes with the ESP WROOM 32. The development board that was purchased for the testing and production process includes a micro USB connection, so this will be used temporarily for the beginning stages of this project. After building a bridge between the two microcontrollers, a micro USB female connector will need to be implemented in the final PCB design. The micro USB connector will have to be surface mounted and connected to the program ports of the ESP 32. In order to be able to communicate properly between devices, the design will use a package called pySerial. pySerial allows the developers to access serial ports through python properties. The developers are able to directly read and write to the serial port using Python language. Establishing a dependable connection between these two devices is vital to the security system's image processing functionalities. Communicating through serial USB cable is going to be the best option to ensure the most simplest yet strongest connection between the two microcontrollers.

8.4 Magnetic Contact Switch Integration

The magnetic contact switch will be incorporated into the design to sense the door closed/open status. Being able to sense when the door is open or closed is important for how the locking system algorithm is going to function. A wire is going to be connected from the magnetic switch to one of the digital pins on the ESP WROOM 32. The main microcontroller will output a digital signal to the electronic door lock circuit to remain active (unlocked mode) when receiving an input of 0 from the magnetic switch. This means that the security system will continue to remain active as the door is left in open position. The microcontroller will receive an input of 1 when sensing that the magnetic reeds are in close contact of each other. The microcontroller at this moment knows that the door is in closed position and will discontinue supplying power to the solenoid. The magnetic contact switch will also incorporate a piezo buzzer connected in parallel that will sound off when the door is open. This sound feature shall help remind users to keep the door closed because the piezo buzzer is going to continuously emit noise until the magnetic switch is in contact (door in closed position). The following schematic is simply the connections for the buzzer and magnetic

switch. There will be a full schematic with the microcontroller connections connected to the switch and electronic door circuit in the test section.

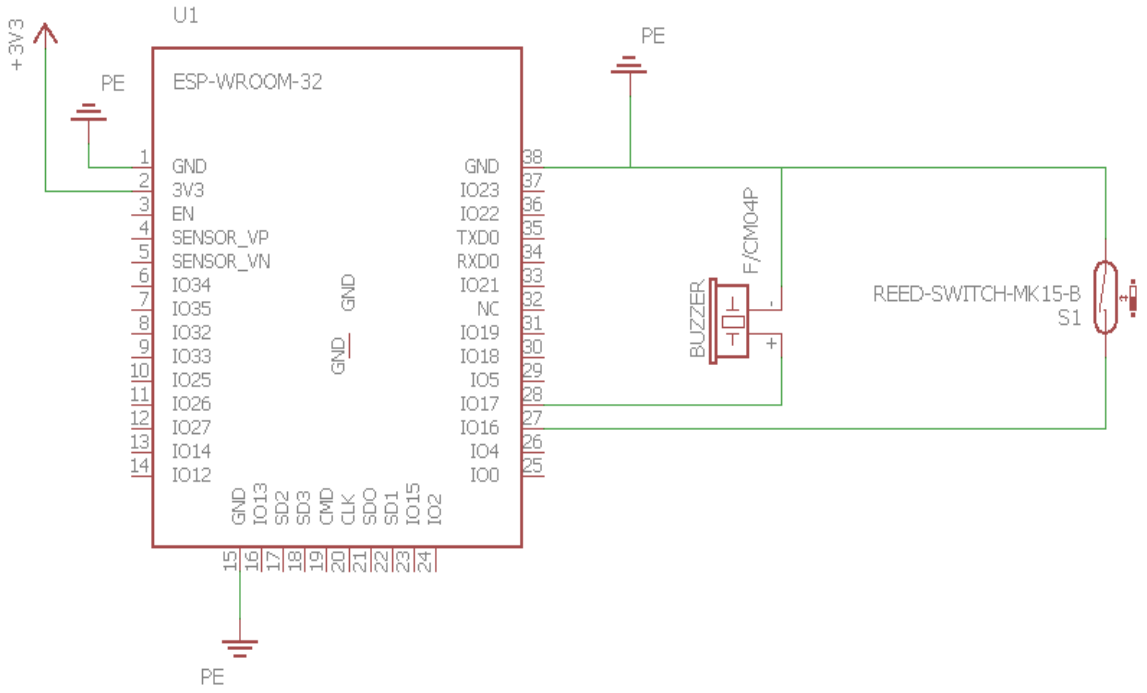

Figure 18 - Magnetic Switch Schematic

8.5 Electronic Door Lock Solenoid Integration

The electronic door lock solenoid has a operating voltage rating at 12 VDC and a rated current of 500 mA. The solenoid retracts the metal into a chamber within the solenoid once the coil inside is excited with electrons. The solenoid remains in outward position when no power is flowing through the solenoid's coil. For these reasons, the solenoid makes the perfect ideal lowest power consumed door lock. The electronic door lock will be powered by a 12V DC, from the power management board rail supplied by a 120 VAC to 12 VDC wall adapter. The solenoid will be mounted into the deadbolt opening, which is normally above the door handle. The solenoid will have to expose its wires to the inside of the door in order to connect to the main security system hub. The solenoid will be interfaced with the ESP WROOM 32 through the means of a switching circuit. The approach of how the solenoid functions clarified the need to have a switching behavioral circuit that is going to be able to turn off/on the flow of current almost immediately.

8.5.1 Switching Characteristics

This switching characteristic will be controlled by the ESP32 sending a digital signal to a N Channel TTL MOSFET that will control the current flowing through the solenoid. The N channel TTL MOSFET that will be used is Fairchild's FQP30N06L. The design will not incorporate a bipolar transistor because the switching will not be as easily controlled by a GPIO pin from the microcontroller compared to a logic level MOSFET. The solenoid load is turned on when V_{GS} = 3.3 volts from the ESP WROOM 32 GPIO pins. The solenoid load is not draining any current when V_{GS} = 0 voltage. Since a solenoid load is considered an inductive load, a flywheel diode is necessary to be placed parallel with the solenoid load to ensure protection from back EMF for the MOSFET. The FQP30N06L already has a built in diode to protect itself from back EMF, so that will be one less thing to worry about. The following schematic is just a representation on how the ESP WROOM 32 will be connected to the electric door locking circuit. The testing section will combine the circuits designed in the hardware design portion.

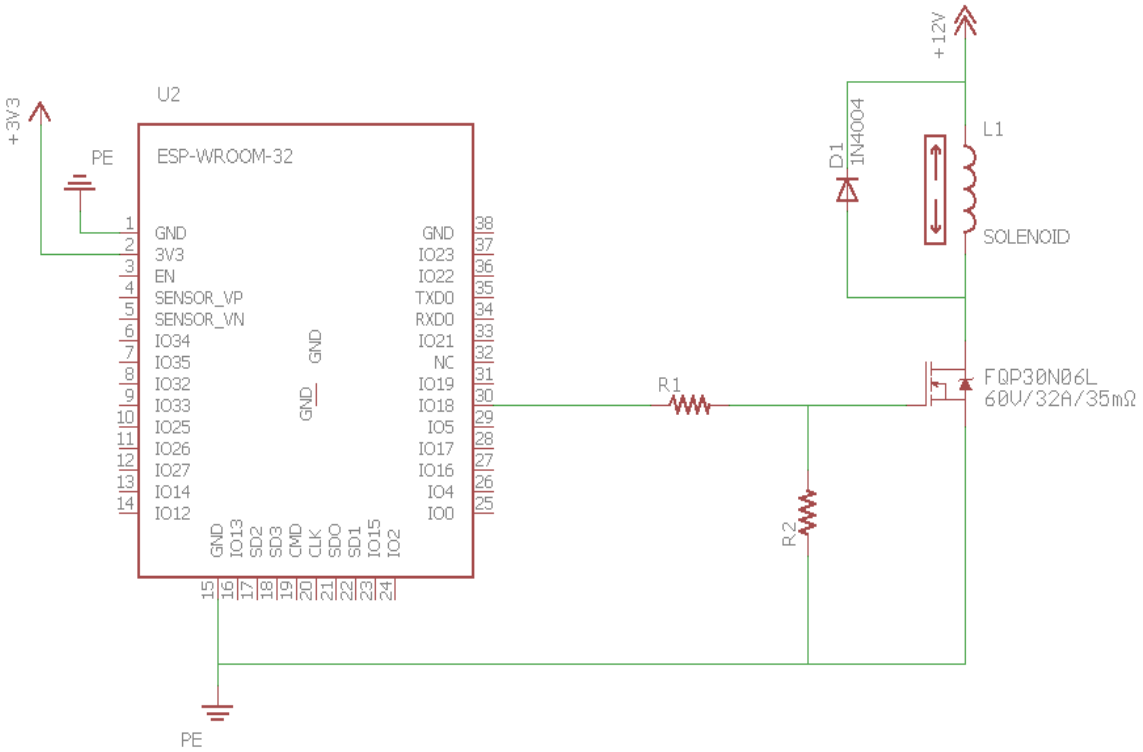

Figure 19 - Door Locking Solenoid Circuit

8.6 LCD Display

The LCD display is going to be an important part of the security system because it is going to help users indicate battery life and door locking status. The LCD display is going to be mounted on the outside frame of the security system.

When manufacturing the case that will be enclosing the system, the enclosure shall have a small section cut out where the LCD display can simply be placed. The users will be able to easily view what will be shown on the screen. The LCD will be only displaying text message when in full active mode. The LCD display will draw a lot of power from the battery, so it is necessary to limit the amount of time on as well as limit the brightness. The LCD display is able to adjust brightness of the backlight by using a potentiometer. A potentiometer has a special characteristic that allows its internal resistance to be varied by turning a knob. The potentiometer is a three terminal device connecting to 5 volts Vss, ground (GND), and Vo (the backlight power pin). The 10k-ohm potentiometer will be set to the appropriate resistance that will limit the voltage and current that is used up by the backlight. The potentiometer will be set to a higher resistance to perform this task. In figure 20, it shows how the ESP WROOM 32 is interfaced with LCD display with the varying potentiometer connected.

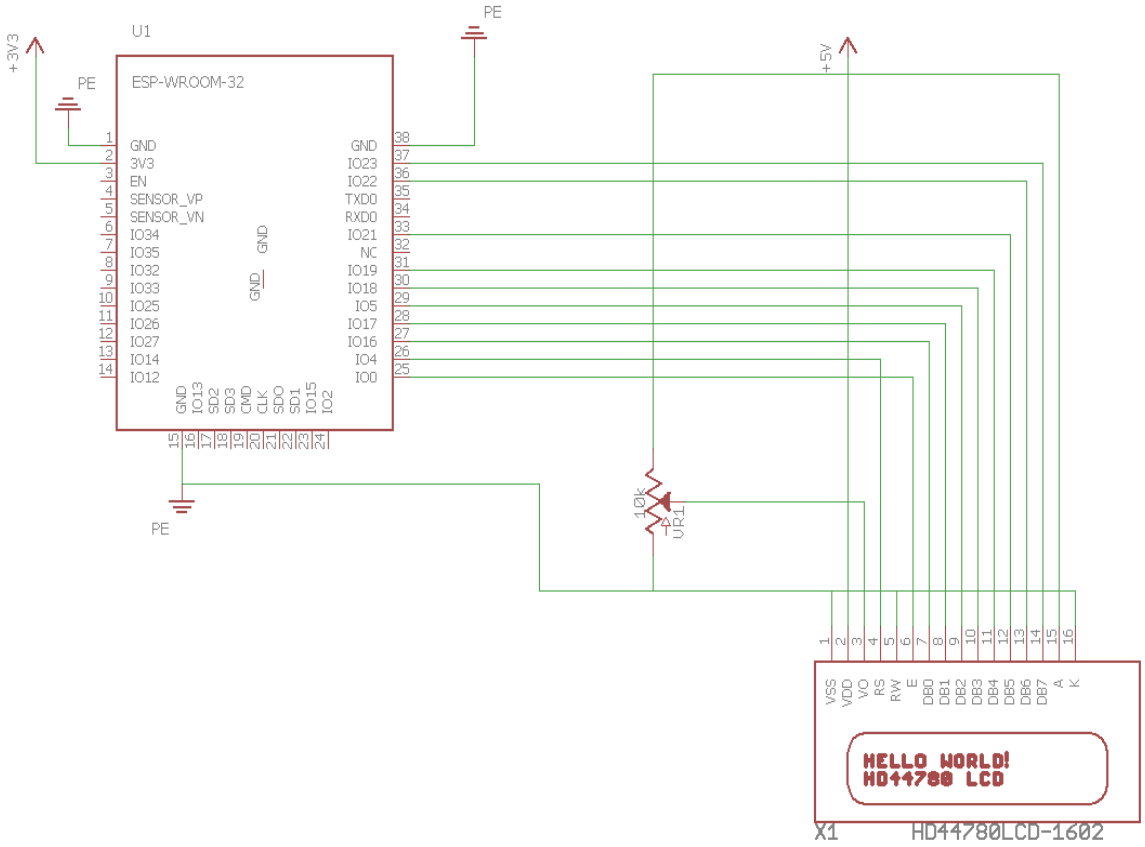

Figure 20 - LCD Display Schematic

9. Mechanical Design

When designing a product, the developer must have a clear understanding of possible all factors that can affect the success of the design. One major factor that creators must take account for is the environment. The environment can

steer a design in a particular direction because of the inevitable forces that will be in contact with. For the security system, the environment will be placed indoors at room temperature. The main controls for security system will be away from outdoor factors like sunlight, wind, and rain. The camera and fingerprint scanner will be exposed to the outside forces. To deal with this exposure, there will be a cover to block environmental factors to the electrical components. After understanding how the environment will affect the security system, the designer can now proceed to incorporate other mechanical details to the finish product. The security system is limited to a number of things. As the designer, the best option for the security system to function properly and to have the easiest installation is to mount the system on the inside of the door where the deadbolt lock is placed. The following statements will explain how this conclusion was made.

The camera module that will be integrated has a wire length of 1 foot. Because the camera is used for capturing video and pictures outside, the camera must somehow be able to reach the opposite side of the door. The designer's best option is to run the camera with its wires through the deadbolt spacing. This will eliminate the use of drilling and other hardware modifications. The fingerprint scanner along with the camera must run its wires through the deadbolt because it too needs to be exposed to the outdoors. To manage this problem, a separate mounting board will be needed. The mounting board does not require much area. Measuring at around 3 inches x 3 inches, a square 3D printed board can be used to mount solely the fingerprint module. The mounting board will have a small hole where the camera and finger scanner can feed their wires through. The small mounting board will have to be secured onto the door using screws. To protect the fingerprint scanner from water, a plastic cover will be made that will surround the mounting board. The cover will appear as a simple box. The plastic cover will have the freedom to rotate in an upward/downward motion for easy access to the fingerprint scanner. The plastic cover will have a small incision for the camera lens to be housed. A thin clear plastic sheet will be placed above the lens to ensure no water encroachment. The following figure will present a clearer idea of the fingerprint and camera lens housing.

For the remaining of the system, it will be mounted onto the opposite side of the door which faces the indoors. The security system will be able to fit all of the electrical components into a small case. The design will choose a case that covers more area but becomes less bulky. The weight of the system will be distributed much better in this fashion, which will help installation purposes. The case interfaces with the rechargeable battery bank externally. This allows easy attaching/detaching the battery power bank when needed. The case will also have to be large enough to house a back up battery supply. The following figure will present a clearer idea for mounting the main system.

Figure 21 - Inside A1 Security System Mounting

Figure 22 - Outside A1 Security System Mounting

10. Testing

10.1 Raspberry Pi NoIR Camera V2

Purpose:
Ensure Raspberry Pi Camera functions as should and produces a clear image without artifacts or any other blemishes.

Materials:
1. Raspberry Pi 3 Microntroller
2. Raspberry Pi NoIR Camera V2
3. Computer

Procedure:
1. Connect the NoIR Camera to the Raspberry Pi microcontroller via the Ribbon that comes attached to the camera.
2. Enable camera support in Raspbian.
3. Capture an image in normal lighting using the Python prompt.
4. Capture an image in low lighting conditions using the Python prompt.
5. Record a video in normal lighting conditions.
6. Record a video in low lighting conditions.
7. View each of the outputted filed to ensure that quality is as it should be.

Results:
The images produced by the camera at all resolutions were the expected quality. No defects or artifacts were seen in the produced files. Furthermore, all video looked as it should. There were no problems with command line arguments not working or anything else of the sort.

10.2 Facial Recognition

Purpose:
Test if the Raspberry Pi 3 Microcontroller is able to recognize faces using the NoIR camera along with OpenCV.

Materials:
1. Raspberry Pi 3 Microntroller
2. Raspberry Pi NoIR Camera V2
3. Computer
4. OpenCV

Procedure:
1. Install OpenCV on the Raspberry PI Microcontroller

2. Add OpenCV to libraries to your code, along with the facial recognition API.
3. Ensure that recording of video still functions as should from the camera.
4. Ensure that the video recording is grayscale. This allows for facial recognition to work as it should
5. Take a picture of yourself and train the algorithm on this image.
6. Capture a live video feed with the facial recognition running simultaneously.
7. Ensure that the facial recognition algorithm recognizes your face with a square and an ID.

Results:
After training the facial recognition algorithm the user's face, it was able to recognize the user in the video live feed. This was able to happen in normal and low light conditions.

10.3 Mobile Application

Purpose:
Make sure that the Android Application lives up to quality standards and is able to communicate with the lock efficiently.

Procedure:
1. Install latest Android Application build on to device.
2. Ensure Log in/Create account work as should by creating an account, then signing in for the first time.
3. Confirm that security features function as they should. This includes too many incorrect authentication attempts.
3. Set up a pass code log in and fingerprint log-in. Check to see if they both authenticate as they should
4. Once logged in, ensure the user can see the most recent picture taken by the Raspberry Pi.
5. Connect to door through bluetooth. See if unlocking and locking work.
6. Connect to door through WiFi, confirm that locking and unlocking work.
7. Verify that the user is sent a notification when the system is notified of a visitor.

Results:
At the time of this writing, code for the Android App has not been written yet. However, the app shall be thoroughly tested for the best quality once it has been completed.

10.4 Electronic Door Lock and Magnetic Contact Switch

Purpose:
Test functionality of electric door solenoid using the ESP32 microcontroller along with sensing the magnetic switch open/close status.

Materials:
1. ESP WROOM 32 Microcontroller Development Board
2. 2 Resistors
3. Logic Level N Channel MOSFET (FQP30N06L)
4. Door Lock Solenoid
5. Magnetic Contact Switch
6. Piezo Buzzer

Procedure:
1. Build the schematic design for both electric circuits on breadboard
2. Install the magnetic on door and door frame using screwdriver and screws
3. Connect temporary 12VDC power supply to breadboard friendly female barrel jack connector.
4. Connect 3.3V power supply to the ESP WROOM Development Board. Aiglent E3630A Triple Output Power Supply will be used as a temporary power supply for testing purposes.
5. Measure current being supplied from the power supply to the solenoid load. Verify that current should be running at about 500 mA.
6. Measure the correct voltages at all critical points. Critical points for this test would be the supply voltage powering the ESP32 microcontroller, 12VDC supply voltage, and digital pin voltages transmitting to the magnetic contact switch and MOSFET.
7. Program ESP32 to read input voltage from magnetic switch. If 1 voltage, door status is closed => do nothing and if 0 voltage, door status is open => send signal to MOSFET. ESP32 shall continuously output 3.3V to MOSFET to open switch. Cut supplying signal to MOSFET once ESP32 reads 1 voltage.

Results:
The results for the combined circuit proved to be working appropriately. The ESP32 was capable of reading when the magnetic switch was open or closed. The magnetic contact switch status determined how the ESP32 output controlled the switching for the Logic Level N Channel MOSFET (FQP30N06L). The piezo buzzer was functioning properly as well emitting sound continuously whenever the microcontroller sensed that the magnetic contact switch is left in open position.

Schematic Layout:

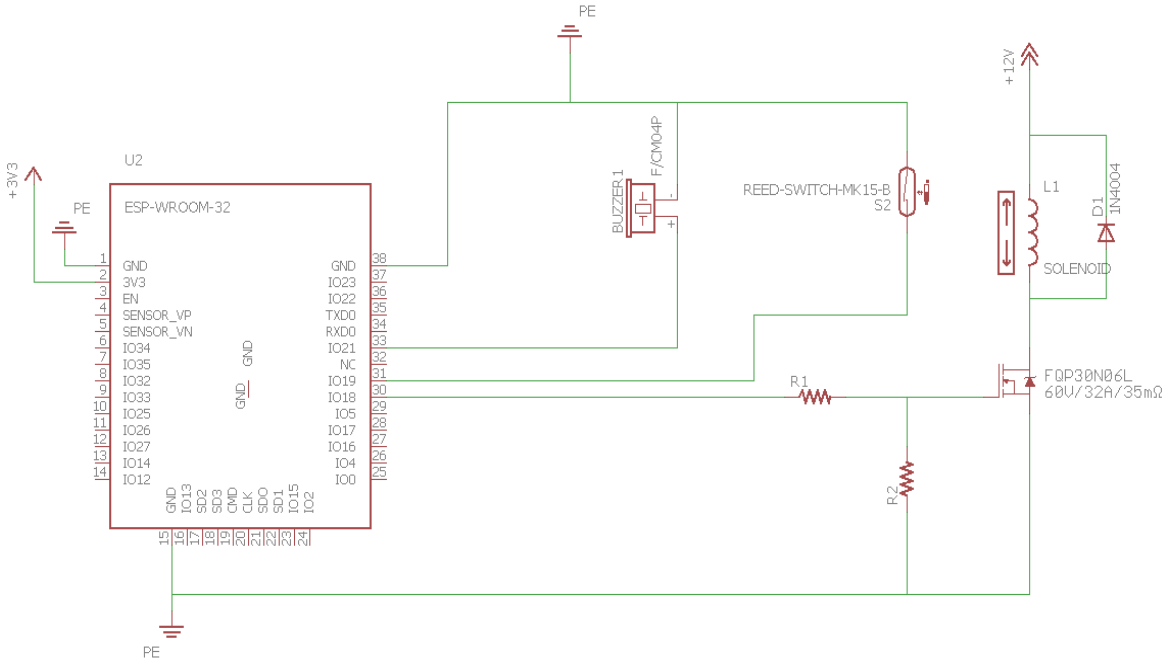

Figure 23 - Magnetic Switch and Door Locking Solenoid Test

10.5 Communication between ESP WROOM 32 and Raspberry Pi

Purpose:
The main purpose for using the Raspberry Pi 3 module is to be able to have image processing functionality. The ESP WROOM 32 (Master) and Raspberry Pi 3 (Slave) will communicate through serial USB connection. Python application, pySerial, will be used to read and write to the serial port.

Materials:

1. ESP WROOM 32 Microcontroller Development Board
2. Raspberry Pi 3 Microcontroller
3. Micro USB cable
4. Arduino IDE

Procedure:

1. Connect ESP32 to computer by Micro USB to be ready for programming
2. Upload code in Arduino IDE. Code consists of python programming language to configure connection to its USB serial port.
3. Send small text message ‘Hello’ to the Raspberry Pi 3 through terminal
4. Power up Raspberry Pi 3 and connect to the ESP 32 through serial USB cable.
5. Test connection between both devices by checking if Raspberry Pi 3 is receiving text message ‘Hello’.

Results:
The ESP WROOM 32 was properly communicating with the Raspberry Pi 3. The simple program uploaded was able to display test message ‘Hello’ onto the computer terminal to verify an established connection between the two devices.

10.6 PIR Sensor

Purpose:
Properly interface the PIR sensor with the ESP WROOM 32.

Materials:
1. ESP WROOM 32 Microcontroller Development Board
2. PIR Sensor
3. Light Emitting Diode (LED)
4. Jumper cables
5. Agilent E3630A DC Power Supply

Procedure:
1. Develop and upload code program into ESP 32 through Arduino IDE. The program shall properly read the output voltage transmitted from the PIR sensor when detecting movement. The ESP 32 will transmit a power signal through another GPIO pin that will power an LED.
2. Build the circuit from the schematic layout design.
3. Power all electrical components. The ESP 32 can remain powered through USB from the computer. The PIR will be powered by a DC power supply at 5V.
4. Test the PIR sensor and ESP 32 interface is properly functioning. Create sudden movements in front of the sensor, and observe if the LED is emitting light to verify full functionality.

Results:
After constructing and simulating the PIR sensor for a few tests, a conclusion was made that the PIR sensor does in fact work properly. The group has verified that LED has emitted light whenever the PIR sensed hand movements. Since the PIR sensor has an operating voltage range from 5 VDC to 20 VDC, the group varied the input power of the PIR sensor and observed that sensor performed much better at around 12 VDC. The sensor was able to sense at much greater distances at this operating voltage. This has changed the power distribution design.

Schematic Layout:

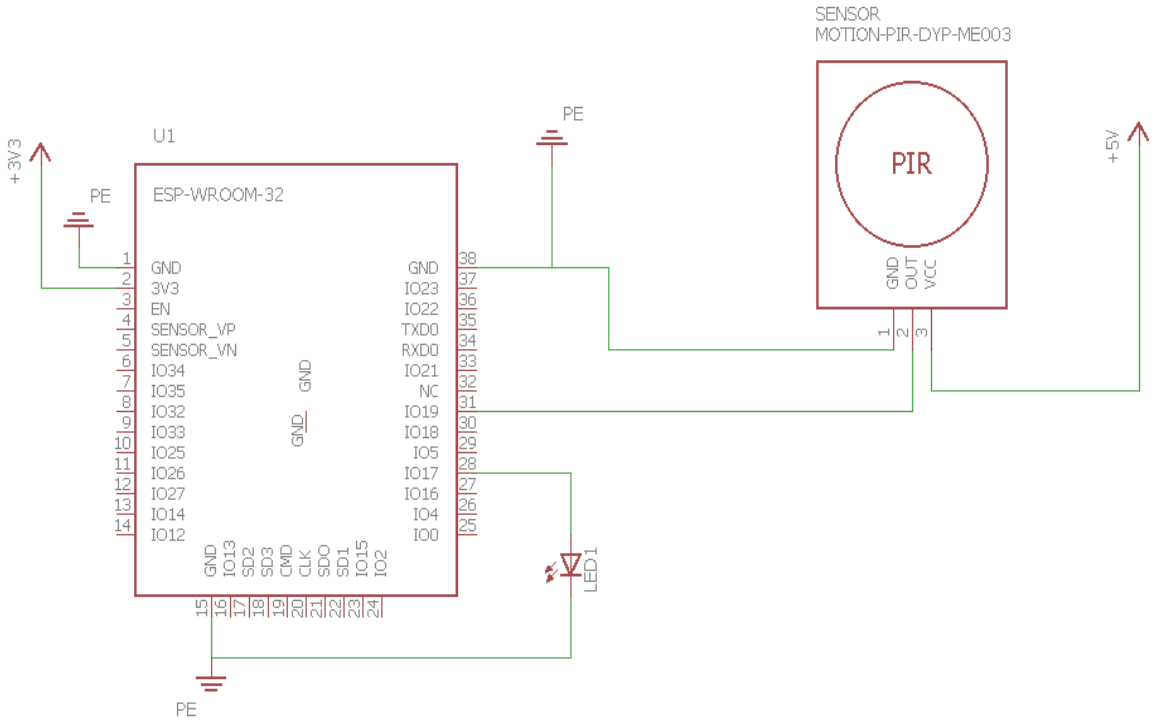

Figure 24 - PIR Motion Sensor LED Test

10.7 LCD Display and Fingerprint Scan Integration Test

Purpose:
Properly interface LCD display and fingerprint scanner with ESP WROOM 32. The microcontroller shall be able to display simple text to display locking status, and transition statuses when reading a valid fingerprint scan.

Materials:
1. ESP WROOM 32 Development Board
2. 20x4 LCD Display
3. Jumper Cables
4. Potentiometer (10 K-ohm)
5. Fingerprint Scanner
6. Breadboard

Procedure:
1. Connect all necessary connections between the LCD display, fingerprint scanner, and ESP 32 development board using jumper cables and breadboard.
2. Initialize fingerprint scanner with a valid scan through Arduino IDE.
3. Vary potentiometer resistance to check the brightness of the backlight on LCD display is working correctly.

4. Develop and upload code to display door locking status as a text message onto LCD screen. The code shall also communicate with the fingerprint scanner through serial communication. When receiving a valid scan, ESP 32 shall display “Door Open”. “Door Closed” shall appear after 10 seconds from opened position.
5. Observe if fingerprint scanner is able to read valid scan.
6. Observe if code is functioning correctly by verifying the correct message on the LCD display, after valid fingerprint scan.

Results:

This test required a few extra steps that proved proper functionality to important aspects of the security system working together. A step taken was to check the backlight brightness adjustment function. By varying the potentiometer resistance, the backlight on the LCD display was able to get dimmer and brighter accordingly. The higher resistance the dimmer the backlight appeared. The less resistance resulted in a much brighter screen. The next step was to prove that the LCD display was working parallel with the fingerprint scanner. The test was to simulate the microcontroller to display text messages on door locking status whenever the ESP32 received a input for valid entry from the fingerprint scanner. The microcontroller will then output “Door Closed” after 10 seconds of displaying “Door Open” message. The group has concluded that the LCD display is working normally and as expected. The 8 bit LCD display was able to show “Door Closed” and “Door Open” text messages whenever the microcontroller received access from the fingerprint scanner.

Schematic Layout:

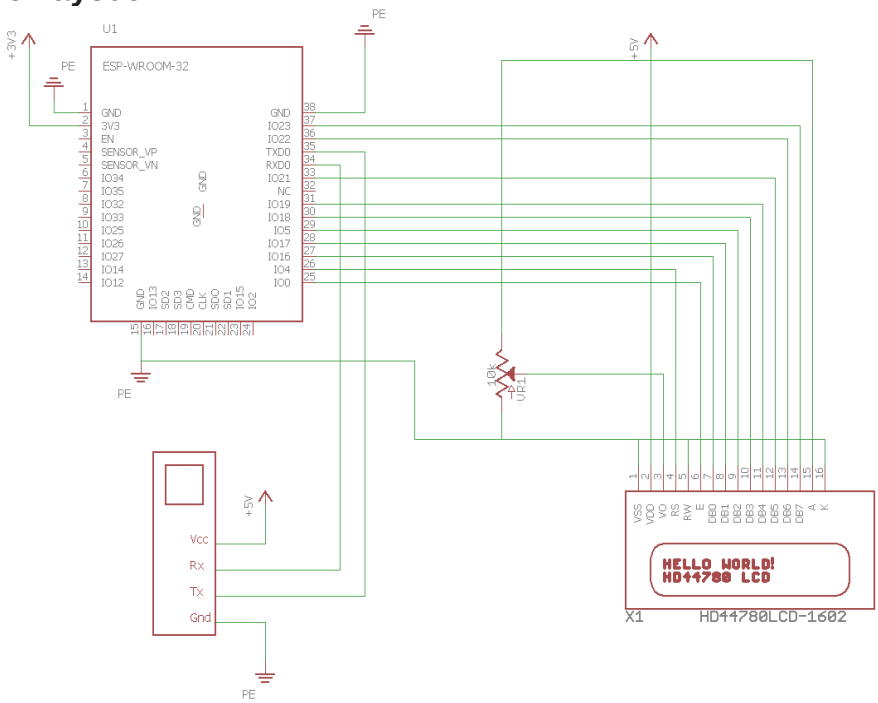

Figure 25 - LCD Display and Fingerprint Scanner Schematic

10.8 Power Management Board

Purpose:
The purpose for this test is to make sure all voltages and currents are reached in order to power all electrical components in the security system.

Materials:
1. Agilent E3630A DC Power Supply
2. Capacitors and Resistors
3. 2 1N4004 Diodes
4. 1 LM7805CT Voltage Regulator
5. 1 LM1117DT-3.3 Voltage Regulator
6. Jumper Cables
7. Digital multimeter

Procedure:
1. Build the 12V - 5V regulating circuit on breadboard.
2. Configure the power supply to output 12 volts and connect it to the input of the regulating circuit.
3. Measure the voltage from the output terminal of the voltage regulator circuit.
4. Measure the current being drawn from the output terminal of the voltage regulator to the load resistor.
5. Remove the load resistor and connect the 3.3V voltage regulator along with the electrical components needed for functionality.
6. Repeat steps 3 and 4 to test the circuit if the correct voltage and currents are being reached.

Results:
After conducting the power management tests, the results can conclude that all the voltage and current levels have been reached using the voltage regulating circuits. The circuit in Figure 26 shows that the 5 volts is being outputted from the voltage regulator and the load is drawing the 200 mA needed to power up the LCD display, fingerprint scanner, and ESP WROOM 32. Resistors can be used to limit the amount of current that will be drawn into these components. If the current drawn is over the electrical components current rating capabilities, the part will destroy its circuits. This is very crucial and must be taken into account when powering up electrical components. After verifying the correct current and voltage being received, the 12V-3V circuit can be simply built by just connecting the LM1117DT-3.3 in parallel with the existing layout. The voltage and current is measured to be 3.294 Volts and drawing 200 mA, which is enough to power up the Raspberry Pi 3. In Figure 27, the simulation verifies the design.

Power Management Board Simulations

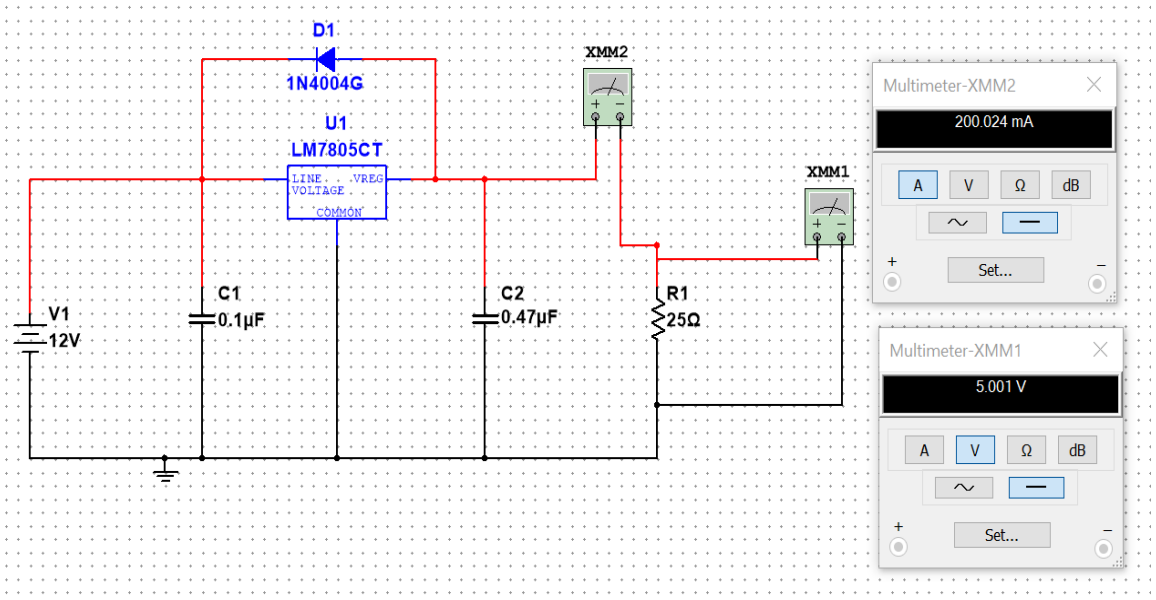

Figure 26 - 12V-5V Regulating Circuit Test

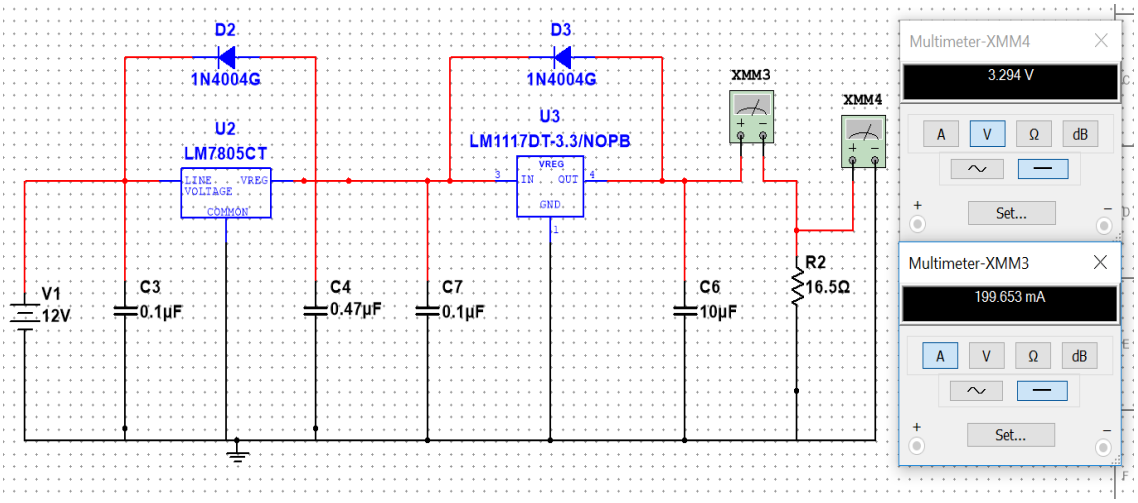

Figure 27 - 12V-3.3V Regulating Circuit Test

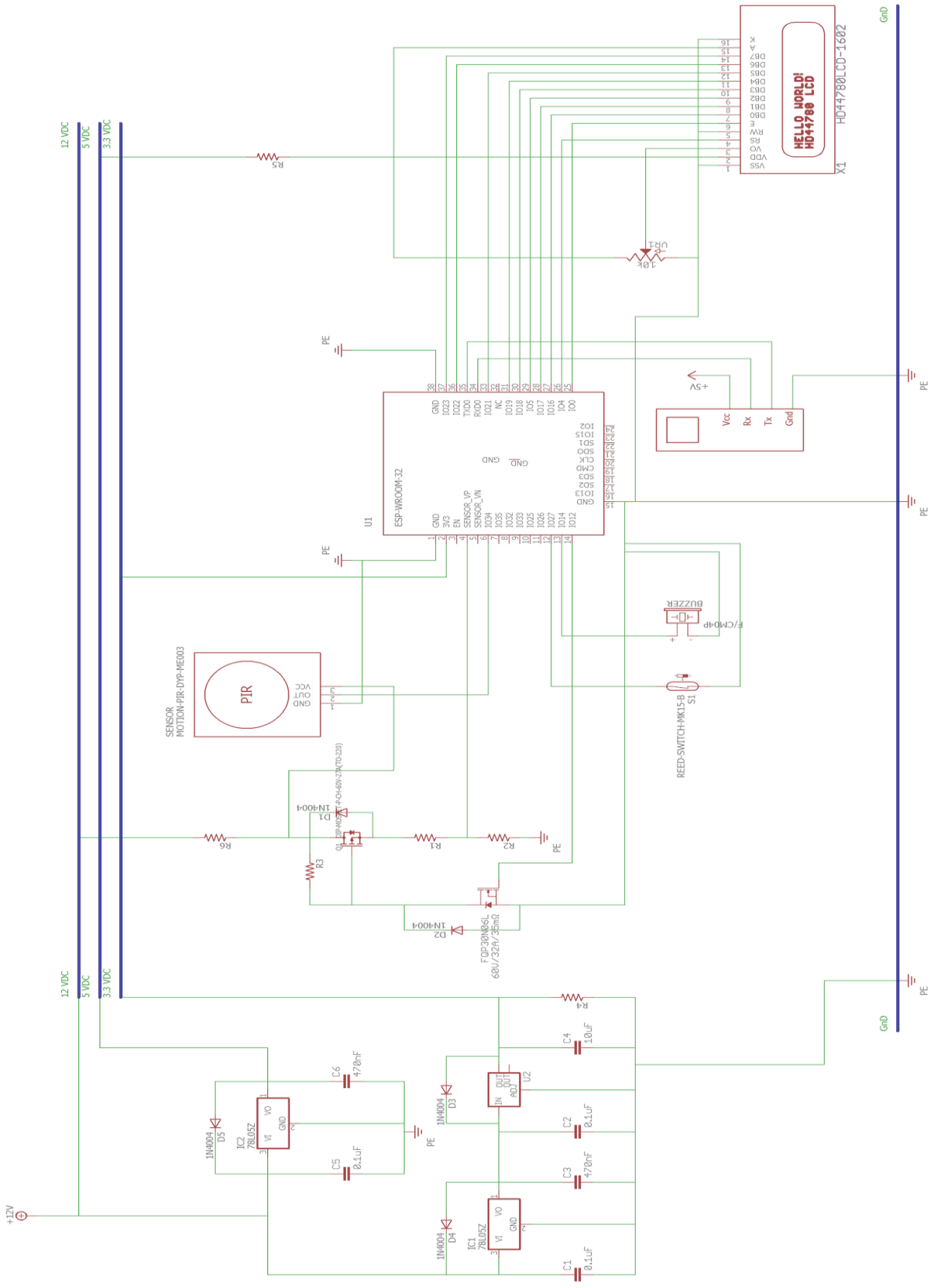

Figure 28 - A1 Security System Schematic

11. Administrative Content

11.1 Project Milestones

Task	Start Date	End Date	Status	Responsible
Project Brainstorming	1/17/17	1/27/17	Finished	Group
Initial Document - Divide & Conquer	1/27/17	2/3/17	Finished	Group
Table of Contents	2/17/17	3/24/17	Finished	Group
1st Document Submission - 15 Pages Each	2/17/17	3/24/17	Finished	Group
2nd Document Submission - 25 Pages Each	2/17/17	4/14/17	Finished	Group
Final Document Submission - 30 Pages Each	2/17/17	4/27/17	Finished	Group
Acquire All Parts	3/24/17	4/21/17	Finished	Group
Test Project Components	4/24/17	5/15/17	Ongoing	Group
Research & Development	2/3/17	6/16/17	Ongoing	Group
Build PCB	5/15/17	5/31/17	Pending	Group
Begin Prototype Construction	5/22/17	6/23/17	Pending	Group
Final Documentation	6/12/17	7/7/17	Pending	Group
Prototype Testing	6/26/17	6/30/17	Pending	Group
Complete Final Product	7/3/17	7/7/17	Pending	Group

Table 15 - Milestones Tracker

11.2 Bill of Materials

The A1 Security System was not able to get a company to sponsor the project, therefore, is funded by it's group members. With a small budget of $100 per group member, the group wanted to construct the most affordable and most featured security system as possible. The parts that were acquired for this project has been bought through Amazon, Adafruit, Sparkfun, and Texas Instruments. All the materials are in hand and ready to be assembled for Senior Design II. There was no software licenses that were needed to purchase for this project. All software related materials are considered open source, which are free for the public use. The following table shows descriptive detail on how the group managed their budget.

Part	Unit Cost	Quantity	Total Cost
Magnetic Switch	$2.95	1	$2.95
Piezo Buzzer	$2.50	1	$2.50
Battery Power Supply	$30.00	1	$30.00
Micro USB female connector	$1.50	1	$1.50
Door Lock Solenoid	$12.99	2	$25.98
PIR Motion Sensor	$5.79	1	$5.79
Breadboard	$7.99	1	$7.99
Jumper Wires 120pcs	$6.99	1	$6.99
ESP WROOM-32	$3.95	1	$3.95
Makerfocus ESP32 Dev Board	$15.99	1	$15.99
GT-511C1R Finger Scanner	$32.00	1	$32.00
Raspberry Pi 3 Module	$40.00	1	$40.00
LCD Display	$10.00	1	$10.00
Electrical Circuit Components	$35.00	1	$35.00
Raspberry Pi NoIR Camera	$25.00	1	$24.99
Hardware Door Demo Materials	$40.00	1	$40.00
Total Project Cost			**$285.32**

Table 16 - Bill of Materials

Figure 29 - Door Lock Solenoid, Power Bank, and Raspberry Pi 3

11.3 Personal Responsibilities

In this section, the following table will provide a thorough breakdown of all the group members contributions to the A1 Security System. The project responsibilities have been divided into four sections: Research, Design, Testing and Miscellaneous. All the responsibilities will be highlighted in the table.

Group Member	Content

Jonathan Chew	Research:
	- Similar Projects
	- Projects in the Market
	- Electric Door Lock
	- Power Source
	- Battery
	- LCD Display
	- Magnetic Contact Switch
	
	Design:
	- Power Supply
	- Magnetic Contact Switch Integration
	- ESP WROOM 32 interface with Raspberry Pi
	- LCD Display
	- Monitoring Battery Health
	- Electric Door Lock Solenoid Integration
	- All Schematics Layouts
	- Mechanical Design
	
	Testing:
	- Electric Door Lock and Magnetic Contact Switch
	- Communication between ESP WROOM 32 and Raspberry Pi 3
	- PIR Sensor
	- LCD Display and Fingerprint Scanner Integration
	- Power Management PCB Board
	
	Miscellaneous:
	- Executive Summary
	- Design Requirements and Specifications
	- Design Constraints
	- Table of Contents and List of Figures/Tables
	- Final Formatting
	- Administrative Content
	  - Bill of Materials
	  - References

Brandon James	Research: - Microcontroller

	- Development Boards - UART - Solder - GPIOs - Motion Sensor - Wi-Fi - Bluetooth/BLE - EAGLE - Arduino IDE - IEEE Software Design: - Arduino IDE Testing: - ESP 32 Development Board - PIR Motion Sensor - LEDs Miscellaneous: - Bluetooth Standards - Solder Development Board Pins - Wiring/Breadboard - Milestones - Appendix Permissions/Requests - Overall Formatting
Timothy Henry	Research: - Camera Module - WiFi Module - AT Command Set - SmackFinger 3.0 Algorithm - UART Protocol - Fingerprint Scanner Software Design: - Version Control - Android OS - Java - Python - Android Application - Application,A1 System Communication - Application Security - Facial Recognition on Android - Facial Recognition on Raspberry Pi - Kairos Android SDK - Raspbian - OpenCV - Diagrams

	Testing: - Camera Module - Facial Recognition - Android Application Miscellaneous: - Wireless Standards - Design Requirements and Specifications - Project Summary and Conclusion - Related Standards

Table 17 - Personal Contributions

12. Project Summary and Conclusion

Our group had a plethora of motivations for developing the A1 System, but our most significant reason for working on this is the lack of affordable smart locks currently in the market. Smart locks are largely unattainable by the masses, resulting in a slow spread throughout the market. The world is moving in the direction of smarter devices, so why shouldn't an upgrade to a crucial household item, the mechanical lock, not be expensive?

Furthermore, the group has the goal of allowing multiple methods of control and authentication, as seen in other smart locking systems, at an affordable price. These methods of control and authentication: the fingerprint reader, facial recognition, and the Android Application will allow for an intuitive and hassle-free experience of gaining access to the household or maintaining security of the household. Our group envisions walking up to the door and, with a tap of the button, the user gains access. Also, we envision the user having the ability to walk up to the door and having facial recognition allow or disallow access.

Of course, as a group we've run into a multitude of problems, especially when dealing with the practicality of some additions we were hoping to make and also the ability to see some of the proposed additions through to completion. Down the line, in the more technical parts of the project our group is sure that there will be more obstacles to face, but we have no doubt these obstacles will be overcome.

All things considered, so far with this project we have had the ability to apply all that we've learned inside and outside of the classroom to the process of developing this product. We believe this will be a product that can be influential in the market and to those who are attempting to work on a similar device in the future. As said before, our main goal is to create an affordable smart lock that can reach the masses and we have no doubt that we will be able to meet this goal while also having an impact that stretched beyond Senior Design.

13. Appendix A: References

Battery Monitor
- http://www.egr.msu.edu/classes/ece480/capstone/fall13/group06/files/everdeen_appnote.pdf
- https://e2e.ti.com/blogs_/b/fullycharged/archive/2016/01/15/simple-battery-monitoring-in-ultra-low-power-applications

Managing Inrush Current
- http://www.ti.com/lit/an/slva670a/slva670a.pdf

Arduino and Raspberry Pi 3 Interface
- https://oscarliang.com/connect-raspberry-pi-and-arduino-usb-cable/

Magnetic Contact Switch Design
- https://learn.sparkfun.com/tutorials/reed-switch-hookup-guide

Door Locking Mechanism
- https://www.adafruit.com/product/1512
- https://www.amazon.com/Signstek-Keyless-Digital-Electronic-Security/dp/B00F4TU7V4/ref=pd_sim_60_1?_encoding=UTF8&psc=1&refRID=QC3J37JHYCADZJEXX26T
- https://www.amazon.com/Generic-Secure-Electric-Strike-Control/dp/B00JWDE98K

Previous Security System Projects
- http://www.eecs.ucf.edu/seniordesign/sp2015su2015/g12/
- http://www.eecs.ucf.edu/seniordesign/sp2015su2015/g05/files/whcs-sd1-report.pdf
- http://www.eecs.ucf.edu/seniordesign/fa2013sp2014/g23/
- http://www.eecs.ucf.edu/seniordesign/su2012fa2012/g10/

Power Management Board Materials
- https://www.adafruit.com/product/373
- https://www.sparkfun.com/products/107
- http://www.mouser.com/ProductDetail/Texas-Instruments/LM1117DT-33-NOPB/?qs=X1J7HmVL2ZHOT670myqy2w%3D%3D

LCD Display
- https://www.adafruit.com/products/181
- https://www.adafruit.com/products/198
- https://www.adafruit.com/products/3315

Image Processing Microcontroller

- https://www.amazon.com/Raspberry-Pi-RASPBERRYPI3-MODB-1GB-Model-Motherboard/dp/B01CD5VC92/ref=sr_1_2?s=pc&ie=UTF8&qid=1488907334&sr=1-2&keywords=raspberry+pi

Wifi Module
- https://www.sparkfun.com/products/13678
- https://www.amazon.com/HiLetgo-ESP8266-ESP-12E-Transceiver-Wireless/dp/B010N1S5WK/ref=sr_1_33?ie=UTF8&qid=1489169347&sr=8-33&keywords=esp8266

Fingerprint Scanner
- https://www.amazon.com/Fingerprint-Scanner-TTL-GT511C1R-cable/dp/B00EZCIX8U
- https://startingelectronics.org/articles/GT-511C3-fingerprint-scanner-hardware/
- https://www.sparkfun.com/products/11792

Camera Modules
- https://www.amazon.com/Raspberry-Pi-NoIR-Camera-Module/dp/B01ER2SMHY/ref=sr_1_2?s=pc&ie=UTF8&qid=1489082194&sr=1-2&keywords=raspberry+pi+camera
- http://m.gearbest.com/multi-rotor-parts/pp_361920.html?currency=USD&vip=760925&gclid=Cj0KEQiA8orFBRCEpODivaOft_EBEiQAy3mlfdEHAGZH_-hv_gacSl9pWS8IMZi7M2_yA0Uw1oN_pA8aApIX8P8HAQ

Bluetooth Module
- https://www.amazon.com/HC-05-Bluetooth-Pass-through-Wireless-Communication/dp/B01G9KSAF6/ref=sr_1_fkmr0_1?ie=UTF8&qid=1489166498&sr=8-1-fkmr0&keywords=Bluetooth+Module+HC+05
- https://www.amazon.com/gp/product/B00J1D6UBA/ref=as_li_ss_tl?ie=UTF8&linkCode=sl1&tag=intorobo-20&linkId=5bdb86acc3e7767b574e74b840a7fe33

Main Microcontroller
- https://beagleboard.org/black-wireless
- https://www.arduino.cc/en/Main/arduinoBoardMega2560
- https://www.adafruit.com/product/3320

Motion Sensor
- https://learn.adafruit.com/pir-passive-infrared-proximity-motion-sensor/overview
- https://www.seeedstudio.com/Mini-PIR-Motion-Sensor-Module-p-1729.html
- http://www.digikey.com/product-detail/en/parallax-inc/555-28027/555-28027-ND/1774435

14. Appendix B: Use of Copyright Permissions and Requests

1. PIR Motion Sensor Images - Granted

Brandon James <brandonantjam@gmail.com> 5:37 PM (47 minutes ago)

to meccanismo.com.

Hello,

To whom it may concern, I Brandon James on behalf of my team would like to make use of a couple of your images. like to formally request permission to reprint and reuse some of your material. All images will be correctly credited wi to you.

Thank you,
Brandon James

Meccanismo Complesso 5:43 PM (41 minutes ago)

to me

Hi James,

In this case, it is ok for me. Just keep me informed about the reference.

Fabio Nelli

2. Mini and Large Lens Motion Sensor Images - Requested

Brandon James <brandonantjam@gmail.com> 6:00 PM (30 minutes ago)

to order

Hello,

To whom it may concern, I Brandon James on behalf of my team would like to make use of a couple of your images. I would like to formally request permission to reprint and reuse some of your material. The images that we will use is of the Mini PIR motion sensor and the Large Lens PIR motion sensor. All images will be correctly credited with respect to you.

Thank you,
Brandon James

3. Eigenfaces - Requested

Brandon James <brandonantjam@gmail.com> 6:16 PM (17 minutes ago)

to research-info

Hello,

To whom it may concern, I Brandon James on behalf of my team would like to make use of one of your images. I would like to formally request permission to reprint and reuse some of your material. The eigen facial detection image will be used. All images will be correctly credited with respect to you.

Thank you,
Brandon James

4. Indeed Job Postings Chart - Requested

[Request received] I am a current student - Brandon James

Inbox x

Rajan Selvan (Coding Dojo | Contact Us) <support@codingdojo.zendesk.c 6:08 PM (29 minutes ago)

to me

##- Please type your reply above this line -##

Your request has been received and is being reviewed by our support staff,

In the meantime, you can learn more about the Dojo with these helpful resources:

Visit our campus >> codingdojo.com/visit-our-campus
Join our one day HTML/CSS Workshop >> codingdojo.com/intro-to-code-workshop

Meet our alumni >> codingdojo.com/success-stories
Financing & scholarship opportunities >> codingdojo.com/tuition-and-scholarships

This email is a service from Coding Dojo. Delivered by Zendesk