HOMES

(Home Observable Monitoring Entry System)

Sponsored by:

Group 12

April 30th, 2015

Colleen Caffey
Bruno Calabria
Ricardo Georges

Table of Contents

List of Tables

1.0 Executive Summary

The purpose of senior design is to give engineering undergraduate students the opportunity to create and build a project that will give them real life engineering experience. In order to make a successful product one must first examine the market and find a niche that must be addressed. As a group, we decided that one such niche is adding technology to home monitoring and entry. In 2014 only 15% of Americans had an alarm system in their home. This means that most of the United States has no technology protecting or monitoring their house. However, the alarm security industry has been increasing their revenue with a 3.0% increase in 2014 to 2015. This provides a window for home security and monitoring; since the alarm security industry is increasing it is obvious that Americans want home alarm systems. It is possible that the main reason more homeowners don't have a security system is either that they are too expensive or they do not trust the security of their home to an automated system. Our project is a home observable monitoring entry system, or HOMES. We choose HOMES in order to provide homeowners with a cost friendly, reliable solution to home entry and monitoring. We also choose it as our project to learn about all the different systems we want to incorporate into making a complete system. We want to learn how to make our own printed circuit board (PBC) from scratch and how to design a mobile and web application also from scratch. Lastly, we want to learn how to work well as a team to write papers and complete a finished project together.

HOMES will use several different methods of entry. These methods are facial recognition, fingerprint scan, Bluetooth, and a mobile application. Such approaches ensure that the homeowner has numerous choices on how to enter their home. For example, if they forget their phone then they can still open the door via facial recognition or their fingerprint. Children can be given a keychain to emit a Bluetooth signal to HOMES and enter the home that way. Even pets can have a collar that emits Bluetooth signals that will unlock a pet door. This is no less safe or reliable than a key. With a battery backup system in place, HOMES will continue to work even if the power goes off. Also with home monitoring modules at every external entry point of the home, HOMES will allow users to see if a door or window has been opened through a mobile application. This will also be convenient for when the homeowner leaves for a while and wants to make sure all doors and windows are shut. It will also provide a web application for homeowners who do not have a smart phone that will give the user the same abilities as the mobile application. HOMES will alert the homeowner's application when someone approaches the front door and sends them a picture of the guest. If it is not a resident of the home who can unlock the door themselves via one of the many ways, then the homeowner has the option of allowing the guest entry to their home via the application. This is extremely convenient if there are guests visiting and you are out. It is also helpful for people who visit your home on a regular basis such as a nanny or a contractor. HOMES will eliminate the need for exchanging physical keys and is safe and reliable.

2.0 Project Description

2.1 Motivation

The focus of our senior design project is to create an innovative and modern home observable monitoring entry system (HOMES) that will be low in cost and simple to use. The system will function with all entry points of your home including doors, windows, and even pet entrances. The user will be able to grant or prohibit access to the home via the system panel, wearable devices, fingerprint, facial recognition, or remotely via android device app. We plan to have an LCD panel mounted to the outside of the front door to display a list of options for your guests to interact with the system. The options will include but are not limited to leaving a voice message or a text message, unlocking the door by facial recognition or by fingerprint, and ringing the doorbell. When a guest approaches the door, a motion sensor will detect the movement and activate a camera and if the lighting is low it will also activate a light. The camera will then record and capture images that will be sent to the homeowner to be viewed in the application. The system will be able to send notifications via android device app, text message, or email when the doors open, lock or unlock, and monitor the entry or exit of all entities in your household, all at the request of the user. This is a complete and comprehensive solution to monitoring and controlling all entry points in a home.

Humans need shelter to survive, but a home is more than just a place to survive. It is a place of comfort and relaxation, a place for family. When people arrive home at the end of a long day and should feel happy, relieved, and secure. This place where everyone goes every day to relax and unwind has the least amount of technology. Our homes are accessed with a key, what happens if that key is lost? Call a locksmith or hope you can get ahold of that friend that has a spare key. Imagine a world where we need a key to access our phones or our laptops. Instead we use passwords, fingerprints and security codes to gain entry into our phones and computers. If one of these is forgotten the process for replacing it is significantly easier than calling a locksmith. It seems that everybody would like a smart home to go along with their smart phones, smart TVs, smart cars, etc. but most of our homes are still technologically lacking. We can operate our cars, television sets, and other devices remotely so why not our homes?

When friends and family, and even strangers decide to contact us we are notified, especially if we were unavailable. Whether we missed a voice call, video call, text message, or email, we are able to see a picture or at least a name of who is trying to contact us, but what about the people who visit our homes? If someone rings a doorbell and no one is home how will the homeowner know? When we get a phone call and it is someone we don’t want to talk to at that moment we have the option to see who is and decide if we want to answer. This doesn’t happen with a front door. When someone rings the doorbell we have no choice but to answer and see who it is. Wouldn’t it be nice to be able to look on your phone after the doorbell rings and see who is there? Why can't we use the technology we have for everything else and use it to help us gather more information about who has been trying to see us?

These questions and the answers to these questions are the motivation behind our project. We as a group do not feel comfortable with the lack of knowledge of who may have approached our homes while we were away. We also feel like a key and lock are extremely outdated technology and that it is time to increase the level of sophistication of home entry and monitoring. Therefore we've decided to create a system that will provide the monitoring and security features you need at your fingertips.

2.2 Objectives

After careful consideration of our project and the motivations behind choosing a smart entry monitoring and controlling system we have outlined the key objectives for the development of HOMES that will guarantee a successful project as well as help all team members gain experience in several engineering and business aspects. These objectives will help us shape HOMES into a comprehensive solution. They are the following:

- Experience in design and implementation of electrical devices
- Experience in design and implementation of a power supply
- Experience in design and implementation of printed circuit board
- Experience in the selection and integration of commercially available parts
- Experience in the writing of a technical paper
- Experience in working as a group to a common goal
- Experience in presenting our finished project
- Camera display & capture at request
- Lock and unlock door via android app
- Motion sensor camera/light activation
- Detecting the opening of other entry points
- Flawless communication between all components of our project
- Sleep function / low power mode
- Access via wearable device
- Access via fingerprint scan
- Access via facial recognition
- Pet collar wearable
- Pet door unlocking mechanism
- Fully functional face recognition
- Fully functional user interface for the system panel
- Fully functional lock and unlock mechanism

3.0 Specifications and Requirements

3.1 Hardware Specifications and Requirements

Following the consideration of our project and all the functionality that is desired, we completed the subsequent list of specifications and requirements for the hardware of our system.

- Create a locking/unlocking mechanism that will respond to a signal that will then lock or unlock the front door.
- Front door will have a motion when a person comes within 2 feet of the door.
- A light will turn on if there is low lighting and the motion sensor has detected movement.
- Motion sensor will activate a camera that will take a picture of the individual at the door and send it to the homeowner's phone via an android application.
- A LCD touch screen will be on the outside of the door and will list options to the guest. These options will be to unlock the door, ring the doorbell, or leave a message. If unlock the door is selected it will display three options: to unlock via facial recognition, fingerprint, or wearable.
- Camera must be high quality to allow for facial recognition.
- Fingerprint scanner must be next to LCD screen for maximum user availability.
- Wearable receiver must also be next to the LCD screen.
- Homeowners will be given 2 wearables that will unlock the door via RFID, Bluetooth, or NFC.
- If the home has a pet door it will be fitted with a lock/unlocking mechanism that will unlock when the homeowners pet comes within 1 foot of the door via RFID, Bluetooth, or NFC and then lock after the animal enters or leaves the home.
- Create a small PCB that will be installed at all other external entry points to the home including windows and back doors that will send a signal when they are opened.
- Create housing that will store the main board, the LCD screen, the wearable receiver, and the fingerprint scanner that will be weather resistant.

3.2 Software Specifications and Requirements

In order for the hardware to work and communicate with each other we need software. After bearing in mind the motivations and objectives of our project we prepared the following list of software specifications and requirements.

- A user interface for the LCD screen that will display options to the guest in an easy to read and efficient manner.
- The options for the LCD screen will be facial unlock, ring doorbell, and video call.
- Android/iOS application for the homeowner to send and receive signals to the front door.
- Application will also send notifications to homeowner when an external entry point is accessed.
- Application will also enable homeowner to lock or unlock their front door.
- Web application for the homeowner to view the status of their front door and entry points from any web browser.
- Ability to send signal to locking/unlocking mechanism to lock or unlock the front door.
- Ability to receive signals from small PCBs at the external entry points if one has been accessed.
- Ability to use facial recognition to gain entry to the front door.
- Large enough memory to store database of faces for comparison.
- Ability to use a fingerprint to gain entry to the front door.
- Enough memory for a database of fingerprints for comparison.
- Ability to receive a signal from a wearable: NFC, Bluetooth, or RFID.
- Logic to grant/deny entry to front door depending on if the method of entry was passed or failed.
- User interface description of status. “Come in” if the method of entry passed and “Please try again” if the method of entry failed.
- Ability to leave a message to the homeowner and forward the message to their android/iOS application.
- Ability to receive signal from pet wearable and will then unlock the pet door.

3.3 General System Specifications and Requirements

There are more than just hardware and software specifications and requirements for our project. There are several items we wish to address that fall outside of these two categories. They are the specifications and requirements of our system as a whole. They are as follows:

- User friendly system as a whole.
- Easy to install and maintain.
- No less reliable and safe than a key and lock.
- HOMES will need constant internet access.

4.0 Research

4.1 Similar Projects and Products

The idea of a smart home has become ever more significant as we continue to advance in technology. However, most homes and apartments use the ancient technology of a lock and a key to open their front door. Also with our smart phones we are notified of everything like when someone messages or emails us or when a package is delivered. But we get no notifications about our home, if someone tried to visit or if the back door was opened. This knowledge is crucial to a safe and high tech home. There are many products on the market that try and revolutionize home entry. Here we discuss but a few past senior design projects and current products that are similar to HOMES.

4.1.1 Projects

4.1.1.1 KEES (Keyless electronic entry system)

KEES is a previous senior design project completed in the spring of 2014 at UCF by Chris Condella, Jason Wagner, Joshua Baxter, and Samuel Demole. This senior design project incorporates many of the same functionality as HOMES. The motivation of KEES was to make a lock that was accessible anywhere and did not use keys. They allow users to lock or unlock their front door via a mobile application, RF technology or a secret knock. The makers of KEES used an electronic strike lock and built a small door to demonstrate the functionality.

As can be seen from the specifications and requirements of HOMES, we have added to this project by providing different ways of home entry such as a fingerprint as well as monitoring other entry points, making HOMES a comprehensive solution for the entire home. We plan on having multiple ways of entry including the mobile application, fingerprint, facial recognition, and a wearable. HOMES also will provide a wearable for the family pet that will make animal entry and exit easy and secure. This makes HOMES versatile and convenient for homeowners as they can choose how they wish to unlock the door. KEES also built a mobile application and a web or browser application, both of which is planned for HOMES. KEES however has a way of unlocking the door that is not present in HOMES which is the secret knock using a piezo sensor.

The use of an electronic strike lock was interesting and could easily be incorporated into HOMES as our lock. An electronic strike lock will make it easier to implement locking and unlocking of the front door because the lock is already electronic and already takes a signal, there is no need for a servo or motor or to build anything that physically turns the lock. A comparison of this type of lock versus other types will be discussed in the following research section. Another thing we learned from researching KEES is that facial recognition/image processing/video streaming take up a large amount of processing power as well as a large amount of memory. In fact, KEES had to cut video streaming out of their final project because they did not have the capability. Using this knowledge we can better plan for the processing power and memory that image processing and video streaming takes.

4.1.1.2 Close to Home

Close to Home is another previous senior design project from UCF. It was completed in the spring of 2014 by Joshua Early, Marc Garcia, Daniel Krummen, and Nicholas Godfrey. This senior design project aims to give homeowners a system that can monitor their home, guarantee security, and control some aspects of their home in order to save on energy usage. They monitor if there is someone is in a room to determine which items should be "on" and use this to conserve energy. They also have a mobile application that lets the homeowner lock/unlock the front door as well as monitor the energy consumption of their home.

HOMES takes away the energy consumption part of this project and adds a more comprehensive way of entering a home and monitoring all entry points. Also, our project adds a web interface for those who do not have a mobile device capable of an application. This is an advantage because the website can be accessed from anywhere such as a hotel room, library, or home computer. The bulk of Close to Home focuses on energy savings which is quite different from HOMES and they do not focus too much on front door entry, they only have one way to open the front door besides a key which is with a mobile application. The focus of HOMES is on safe, keyless, easy home entry and monitoring. While we do want low power consumption of our system in order to best optimize it, this is not our goal nor is energy monitoring.

Close to Home had the same communication issue between different components as we face now. They researched Bluetooth, Wi-Fi, and ZigBee. One of these wireless communication methods can be implemented in HOMES to connect with all our different components including the main board and the small PCB boards that monitor external entry points, the wearable receiver and the main board, and the camera and the main board. Close to Home choose to use ZigBee for their project because it only uses intermittent communication which is ideal for their project and it also has low power consumption. ZigBee can be easily integrated into our project as our communication system. A comparison of the different types of wireless communications will be discussed in the research section. Close to Home also built a lock module for the unlocking or locking of the front door via the mobile application. To do this they used a battery powered servo that used the MSP430 microcontroller to check the status of the lock and to send a signal to the servo to lock or unlock the door. To detect the status of the door they used a micro switch. All of this can be easily implemented in HOMES as our unlocking/locking front door module. In fact, the research completed on this can be seen in a later section.

4.1.2 Products

Similar products are different from the projects in the section above because these products are on the market and selling. We can take what we learn from these products and use it to make HOMES a user friendly and marketable system. The two following products are good examples of a marketable smart lock that we can use to make our lock safe and secure.

4.1.2.1 August

August is a keyless lock that uses Bluetooth and mobile devices to unlock the front door. August gives the homeowner full control over who is allowed in their home or not. By use of a user friendly mobile application, the homeowner can send invitations to those who they wish to allow in their home and they have the option of setting a time frame of how long that person is allowed to be inside the home and the option of taking away the ability to get in at any time. This allows for the homeowner to easily give people the ability of accessing their home, even if they are out of town or away. August will unlock the door once the homeowner is within range so there is no need to fumble for a key or get a smart phone out and unlock it via the application. August has a slick look and a very user friendly apparatus and mobile application.

August is a product that is focused solely on secure and simple front door entry and exit. It is very simple to install because it fits into the existing deadbolt and it has low power consumption and runs on batteries. This is convenient because if the power goes out it will still work and be secure. Also to unlock the door all a user needs is their smart phone which most people carry around with them anyway. August does keep a log of who came in and out of the front door but it doesn’t inform the users about the rest of the home. This is one of the functionalities of HOMES. Another functionality of HOMES is that it is possible to gain entry to the home without anything but the user’s finger print or their face. This makes it convenient if the user forgot their phone somewhere then there is another easy way to gain entry to their home.

August installs right over the existing deadbolt in the front door by replacing the thumb turn then will turn the dead bolt in to lock or unlock position via a motor. This can be used in our project for our locking and unlocking mechanism. Also to send signals to the lock that someone is approaching with permission to enter August uses Bluetooth. As was mentioned earlier we will be discussing Bluetooth later in the research section of this paper and comparing it with other kinds of wireless communication. This too could be easily implemented in HOMES and be the way we send wireless signals from one part to another.

4.1.2.2 Kwikset Keyless Lock

Kwikset is a manufacturer or many different kinds of smart locks. They have locks that use a keypad and a smart code to gain entry to a home without the hassle of keys called smartcode locks. They also have a product similar to August called

Kevo in which the user's phone becomes the key. Kevo works by first the user tapping the lock, then it scans the immediate area for a Bluetooth signal that matches one that is allowed access to the home, and if it finds one then it will unlock. They also provide a key fob for children or anyone who doesn't have a smart phone. The smartcode locks use different technology. They are simple key pads that the user must enter the correct combination to gain entry. The advantage of this model is if the user forgot their smart phone or key fob somewhere, it doesn't matter because the key code is in their head and they don't need anything else to gain entry.

As with August discussed above, Kwikset locks are focused only on secure home entry, not complete home entry monitoring like HOMES. Also besides a key given to customers for backup purposes, there is only one way to enter the home. With Kevo it is via the Bluetooth on a smartphone or key fob, or with a smartcode lock via a numerical code. If the user forgets their phone or the code they have no other way of entering their home. With HOMES there is a way to enter with only your person, no smart phones or codes. Kevo does have an application that will also the homeowner to grant people access to their home as long as they have a compatible smart phone. This is done via the Kevo mobile application. This is similar to our plan for HOMES in that the homeowner will get a notification to see who is at their door and then grant the guest permission or not to enter the home.

Kevo uses Bluetooth which as mentioned above can be easily implemented in HOMES for communication between the different modules of our project, including the wearable that will be given as both a wristband and a collar for a pet. As for the smartcode lock we considered at the beginning of our planning phase using such a lock but decided that either a regular lock with a servo or motor attached or an electronic strike lock would be better alternatives. Since a keypad with a code seems unnecessary because the purpose of HOMES is to create not only an easy, save, and efficient home entry system, but also to have a system that can be accessed via facial recognition or fingerprint and since a keypad makes the need for these methods unnecessary, we decided to look at other options for the door lock. The key fob used for the Kevo lock is the same concept of the wearables in HOMES. Kwikset uses Bluetooth to transmit a signal from the fob to the lock to gain entry into the home. This could be easily implemented in HOMES as our wearable communications system.

4.2 Hardware Research

We have many good ideas about what we want to do with HOMES. The following section will explain our thought process on the hardware we want to use for our project. Some of the hardware is very complicated and therefore before we begin to design or build HOMES we must do an adequate amount of research on all the different hardware technologies we can use so we can make well-informed design decisions. In this section we will explore many different methods of completing a module and weigh the advantages and disadvantages. A sufficient amount of research will also ensure that any troubleshooting will be smooth because we will be so similar with the hardware.

4.2.1 Power

A power supply provides energy to an electric load. There are several different types of power supplies, they are the following: DC, AC, switched-mode, programmable, uninterruptable, and high voltage. The basic description for these supplies is shown in table 1. Most boards need a continuous voltage so DC is used. However, AC-to-DC adapters make it easy to convert the power from an AC source such as a wall outlet to the DC energy needed to power the board. The type of power supply needed depends on the particulars of the system.

There are many factors to take into consideration when choosing a power supply such as efficiency, cost, size, and mobility. It might be cheaper to make our own power supply instead of purchasing one that is already made. It might also be a hassle for the user to have to constantly replace the batteries for the system so perhaps a power supply that has access to a continuous stream of energy such as a wall outlet would be more user friendly.

The main power supply will be for the single board computer that will control our system. However there are several parts of the system that are separate from this board and need their own source of power. The external entry point monitors, the wearables, the locking mechanism and possibly the camera all need their own power source. The power sources for these fragments will be discussed in their section. It is possible that we can use a small power PBC to supply power to the components that are near each other such as the locking mechanism and the single board computers. The other components that are out of reach for this PBC will have to have their own source of power.

Another option for the power supply is solar power. Solar power converts sunlight into electricity usually by using photovoltaics or PV. PV cells do this conversion using the photovoltaic effect. The photovoltaic effect occurs when light hits a material causing the electrons in the valance band to absorb energy jump to the conduction band. These electrons then move toward a junction and into a different material, which creates an electromagnetic force or electric energy. Another way to perform this conversion is through the use of concentrated solar power or CSP. CSP systems convert light into energy by using a large amount of mirrors or lenses. Power is generated when the light is converted to heat, which then runs a heat engine which is connected to a power generator.

For HOMES we would need to use a PV cell because they are smaller and more affordable. Usually CSP systems are used for large scale solar power needs such as for a home or a building. Since HOMES is a small system that only mainly needs to power the single board computer, a PV cell will be the best option.

PV cells can be relatively inexpensive; a small cell that outputs 3VDC is only around $4.00. Depending on which single board computer we decide to use in our design, this may or may not be enough power. If it is not enough we will simply need to find a PV cell that outputs the correct voltage. We could also step up or down the voltage from the PV cell using a small voltage regulator circuit.

Table 1: Power Description

Power Supply	Description
DC	Offers direct current to the system
AC	Offers an alternating current to the system
Switched-Mode	Takes AC power, filters it, and then turns it into DC voltage
Programmable	Can be easily adjusted to fit the needs of a specific system
Uninterruptable	Takes power from two sources at once so if one fails the other can pick up the slack
High Voltage	Outputs a voltage in the hundreds or thousands
Solar Power	Electric power from sunlight

4.2.1.1 Raspberry Pi Power Supply

The Raspberry Pi needs a 5V micro USB 2.1A power supply. This energy can be supplied via a battery or an AC adapter. Powering the Raspberry Pi via battery can be risky if there are USB devices connected to the Pi. The best way to use a battery to power a Raspberry Pi is to include a converter that converts battery power and delivers into 5V stabilized, regulated to 5%, and able to deliver approximately 2.1A. A safer route to power the Raspberry Pi is via an AC adapter. This technique offers better protection for the board and less of a chance that it will short the power supply or harm the power input fuse.

4.2.1.2 BeagleBone Black Power Supply

The BeagleBone Black uses a 5V 2.1A DC power supply. This can be done via an adapter or a battery pack. A battery pack is essentially a set of batteries that can be used to deliver a desired voltage and current to the system. These batteries can be recharged or replaced however this can be a hassle for the user to do. A DC adapter though can be connected to a power outlet and left alone.

4.2.1.3 Arduino Uno Power Supply

The Arduino Uno uses a 7-12V power supply. This energy can be supplied be either a battery or an adapter. The current for each I/O pin is 40mA and the current for the 3.3V pin is 50mA. Since there are 14 I/O pins they draw approximately 6.4A. If we include the 3.3V pin current then the total current needed for the Arduino Uno is 6.9A. The best way to provide this power is via a battery pack or an adapter. As with the BeagleBone black the battery pack could be potentially non-user friendly, while the adapter can allow for continuous power to the system and is very user friendly.

4.2.1.4 Power Sources

We looked at several different ways to get a power source. Some are mentioned above as using a battery or using an adapter. There are other ways to supply power to the board. One option is by tapping in to the power that is given to the doorbell. By connecting to this power we can then regulate it to the voltage needed to power the board. Another option is using a battery to power the board, while this may at first seem like a flawed idea because the user will have to be constantly replacing batteries, it could work if the board is allowed to go into a low power mode, sleep mode, or completely off while not in use and then when it is needed turned on to the full power mode.

All houses and most apartments have doorbells. In order for a doorbell to work it has to be supplied power. This power comes from the standard 120V electrical box, which is a lot of power so doorbells use a transformer to step down the voltage into a useable range. This range is typically 16-24V. This is plenty of power for us to tap into and divert to a regulator to power the board. One problem with this method though is that in order to get to this power source we would need to drill through the wall of the house. This makes installation of our project more complicated. Another problem is that in order to get and install this project the user must have a doorbell. If not then we would need to add our own transformer to step down the 120V from the electrical box and then run a wire from that to the front door.

Perhaps the better option would be to power the board using a battery and then putting the board into a low power mode or off while it is not in use. This can be done be creating a microcontroller that controls the on/off power to the board. When a user triggers the system, by walking up to the door, a signal will be sent to the microcontroller to power on the board. Then after some time of inactivity, the microcontroller can turn off the board and wait for another signal. Of the three boards we are researching, the Raspberry Pi does not have a low power or sleep mode, therefore it must be completely turned off when it is inactive. The Arduino does have a low power mode so instead of completely cutting the power to the board it can just be put into this mode when inactive and wakened when needed. The BeagleBone black is like the Raspberry Pi in that it does not have a low power board and must be turned off when inactive. A battery can be used then to power both the microcontroller and the board. Since the microcontroller will be small it will have low power consumption and therefore not need new batteries frequently. Also because the board will only be using power when it is on and needed, this can drastically increase the total amount of power used and enable us to use a battery to power the board.

As discussed above it is another option to use a solar PV panel to provide power to the system. A solar panel would eliminate the need to connect to the homes power and thus if the power goes off the system will continue to work. There can still be a battery backup system in place that can be used if the PV cell runs out of energy. This would most likely happen at night.

4.2.2 Motion Sensor

HOMES will detect when a guest has arrived at the front door using some kind of motion sensor. When the motion sensor goes off we want the camera to take a picture of the guest and send it to the homeowners application. We also want the motion sensor to turn on the light if it is dark and it senses motion. In this section we will discuss how motion sensors work and analyze different kinds.

4.2.2.1 Passive Infrared Sensor (PIR Sensor)

PIR sensors do not emit infrared energy but seek changes in infrared energy in the encompassing area. While most of the thermal radiation emitted by objects near room temperature is infrared, we will be looking for significant changes such as the movement of body heat. Detection is made when there is a break in “normal” temperature in the field, the PIR sensor returns to its normal state when the field returns to its “normal” temperature.

An advantage of PIR sensors is their ability to be applied to a large area. Giving that varies heat sources will interfere with the PIR sensor, outdoor detection or placement near windows, will not seem suitable due to the infrared rays produced by sunlight. The maximum sensing range falls around 30 feet at an angle of 15º.

4.2.2.2 Active Infrared Sensor (Photoelectric Sensor)

Photoelectric sensors emit an infrared beam using a dual setup. One side with an emitter for emitting an infrared beam, the other side with a receiver for receiving the beam. Detection is made either when the receiver receives the emitter signal or when the receiver does not receive the emitter signal. Photoelectric sensors may incorporate a multiple beam setup to reduce false alarms. Since the photoelectric sensor is not looking for changes of infrared energy in the environment, it is suitable for outdoor point-to-point detection. The different types of photoelectric sensor arrangements that have been researched are the through-beam sensor (Figure 1a), retro reflective sensor (Figure 1b left), and proximity-sensing or diffused sensor (Figure 1b right).

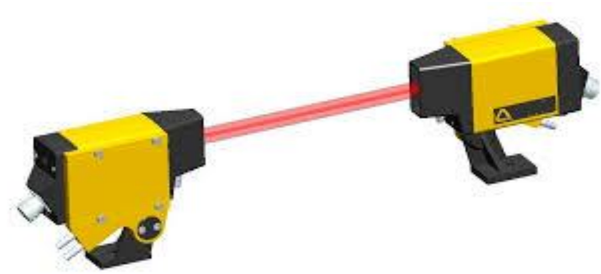


Figure 1a Through-beam Sensor
With Permission from: Carl’s Electronics

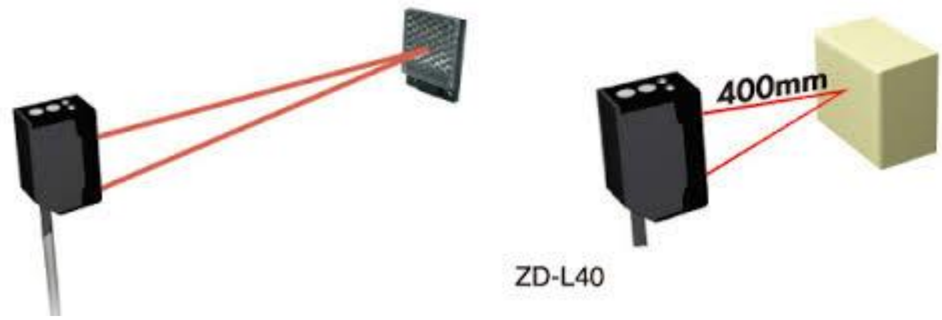


Figure 1b Retro Reflective sensor (left) and Diffused Sensor (right)
With Permission from: Carl's Electronics

A through beam arrangement consists of a receiver located within the line-of-sight of the emitter. In this mode, an object is detected when the light beam is blocked from getting to the receiver from the emitter. The maximum sensing range is 300 feet, which is the longest and still very reliable and accurate. The disadvantage of using the through-beam setup is the cost and having to install two components.

A retro reflective arrangement places the emitter and receiver at the same location, in one unit, and uses a reflector to bounce the light beam from the emitter to the receiver. A target is sensed when the light path is interrupted and fails to reach the receiver. When the target no longer blocks the light path the sensor returns to its normal state. The maximum sensing range is 35 feet.

A proximity-sensing (diffused) arrangement places the emitter and receiver at the same location, in one unit, and uses a reflector to bounce the light beam from the emitter to the receiver. This setup is one in which the transmitted radiation must reflect off the object in order to reach the receiver. In this mode, a target is detected when the receiver sees the transmitted source rather than when it fails to see it.

4.2.3 Camera

In our project we are using a camera for several purposes. First, when the motion sensor is triggered the camera will take a photo of the person at the door and send it to the home owner's phone via the application. Second, we are going to be use it for facial recognition and if the person is in the database then the door will unlock. Lastly, we are using the camera for real time video streaming to allow the homeowner to see what is happening at the front door via the application. There are many factors to consider on choosing a camera including cost, mobility, and quality. Table 2 shows a comparison of the different types of cameras discussed in the following sections.

4.2.3.1 Raspberry Pi Camera Module

The Raspberry Pi has a camera module, which can be used to take both still photographs and high quality video. Obviously this camera can only be used with the Raspberry Pi. It uses a CMOS sensor for the camera and is a 5-megapixel camera. The Raspberry Pi camera module can even detect motion using command line motion software and can be programmed to take picture or video when motion is detected. It is easily connected to the Raspberry Pi via a ribbon cable. This means that the camera and the Raspberry Pi need to be in very close proximity of each other and therefore restricting where we can put the camera. However it is small and light weight subsequently making it easy to place as long as it is near the Raspberry Pi. This module is powered by the Raspberry Pi and therefore uses whatever power supply is being used for the board. It is reasonably priced, only about thirty dollars. This is less than our projected price of a camera for our budget.

Some advantages of using the Raspberry Pi camera are that the software for the module makes use of RPi GPU, which is the Raspberry Pi graphics processing unit and thus uses less CPU. Also the camera is fairly high quality; however it has approximately the same megapixels as webcam. Since it has a high amount of megapixels the module takes high quality daytime pictures and videos. Nevertheless, nighttime pictures and videos require a strong light to be able to be seen. Another disadvantage of the module is that it is connected to the board via a ribbon cable which can be viewed as fragile.

4.2.3.2 Raspberry Pi NOiR Camera Board (Infrared-sensitive camera)

The Raspberry Pi also has an infrared camera module. This module is almost the same as the regular camera module except it has no IR cut filter. This makes it ideal for nighttime camera and video. As with the camera module discussed before this can only be used with a Raspberry Pi. Similarly like the regular camera module it uses a CMOS sensor. It also is a 5 megapixel camera and it is capable of taking 2592x1944 pixel still images. However during the daytime this module will take pictures and videos with odd colors. A possible option for fixing the daytime photos would be to add an IR filter during the day and then take it away at night. Even at nighttime the subject of the photo or video need to be lit with infrared light. As with the regular camera module the NOiR camera board is powered by the Raspberry Pi. Also like the regular camera module, it costs about thirty dollars.

4.2.3.3 Webcam

Yet another option for the camera is a regular webcam. This can be cheaper in comparison to the Raspberry Pi module and it has approximately the same megapixels depending on the camera bought. There are many choices for a webcam; yet we only need a basic one that will allow us to take photos and videos. The photos must be of a high enough quality to be used for facial recognition. A webcam can be attached to the Raspberry Pi via a USB cable. This can give more flexibility to the length and therefore the distance the camera can be from the Raspberry Pi. Most webcams can use the same software the Raspberry Pi camera module uses to detect motion and can be used as a motion sensor as well. As with the Raspberry Pi camera module a webcam is good when there is plenty of lighting. So during the day this camera will have no problem. But at night we will need to make sure there is plenty of light or else the camera will not be able to pick up on anything and facial recognition will be unworkable.

Some weaknesses of using a camera are that it uses more CPU than the Raspberry Pi module. Also average webcams have fairly low quality video capabilities. However, strength of a webcam is the price. They cost about 15-60. Depending on the video and photo quality a webcam could be more cost effective than the Raspberry Pi camera modules.

There are several ways we can power the webcam, we can connect it to the board using USB and therefore not only providing power to the webcam but also establishing a connection from the board to the camera. This way we can send the images captured on the camera to the board. The board can then run the facial recognition program and/or send a picture of the guest to the homeowner's phone via the app. However, we could use a battery to power the camera and then communicate to the board via Wi-Fi. This might be useful if we find that the board power is not enough to implement all the functionality that is desired.

Table 2: Comparison of Cameras

Camera	Photo quality	Video Quality	Price
Raspberry Pi modules			
Camera module	5 megapixels	1080p30 720p60	$29.99
NOiR camera module	5 megapixels	1080p30 720p60	$29.99
Basic webcams			
Logitech HD webcam C310	5 megapixels	720p	$49.99
Creative Live! Webcam	5.7 megapixels	720p	$39.99

4.2.4 Single Board Computers

The single board computer will be the brain of our system. The controller we use for this will have to handle a large amount of processing and it will also need to be able to hold large amounts of data. The single board computer will be in charge of every aspect of our project and it will control the entire system. Here we will discuss several possible options for a single board computer.

4.2.4.1 Raspberry Pi 2

Is the recently release upgraded version of the Raspberry Pi B+ it comes equipped with a new Broadcom BCM2836 quad-core ARM Cortex-A7 CPU (Promising about 6x the performance of the original Pi) and equipped with a 1GB LPDDR2 SDRAM. The Pi would be a great choice for our project due to its capability to handle OpenCV; it also has 40 GPIO pins we can use to control our locking mechanism, and other components we may use. These pins and their functions are shown in Figure 2.

The Pi has its own optimized versions of Linux, has great peripheral support including Touch Screen LCD attachments, custom cameras, cases, and many other breakout chips. In addition the Pi has 4 USB 2.0 ports, 10/100 Ethernet Port, HDMI, 3.5mm audio out, microSD card slot 2 onboard ribbon slots for camera and display, and is backwards compatible to B and B+ board. It does all this for about $35 to $45 dollars.

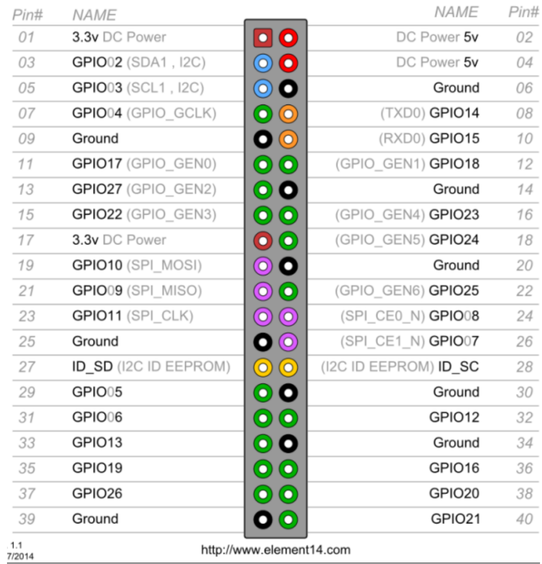


Figure 2 Raspberry Pi 2 Pins
With permission from element14

4.2.4.2 Raspberry Pi B+

The earlier version of the Raspberry Pi this the exact same layout as the newer Pi with the same amount of GPIO pins, USB 2.0 ports, ribbon slots, and all other things found in the Raspberry Pi 2. The main difference comes with the weaker 700MHz Broadcom BCM2835 CPU and 512 MB SDRAM running at 400MHz. With the ability to overclock this chip to about 900MHz relatively easily it might also be able to handle OpenCV face recognition but the low amount of memory (512 MB to be divided between the GPU and CPU) might prove to be a bottleneck.

Overall this board is slightly more affordable then the Raspberry Pi 2 now costing about $25 to $35, due to this not being that significantly cheaper this board will probably only be used if a Raspberry Pi 2 cannot be acquired or if significant budget cuts are needed.

4.2.4.3 BeagleBone Black

As of the major contenders in current market for low cost single-board computers the BeagleBone Black comes with a powerful TI Sitara™ AM3358 1GHz ARM® Cortex™- A8 CPU, 512 DDR3L DRAM, and 4 GB of 8-bit eMMC Onboard Flash. It has 1 USB port, 1 Ethernet port, 2x 46 pin headers, 2 32-bit 200MHz PRUs, HDMI, 3D graphics accelerator, and has over 100 capes (external add-on boards). The BeagleBone Black is picture with a mapping of its pins in figure 3.

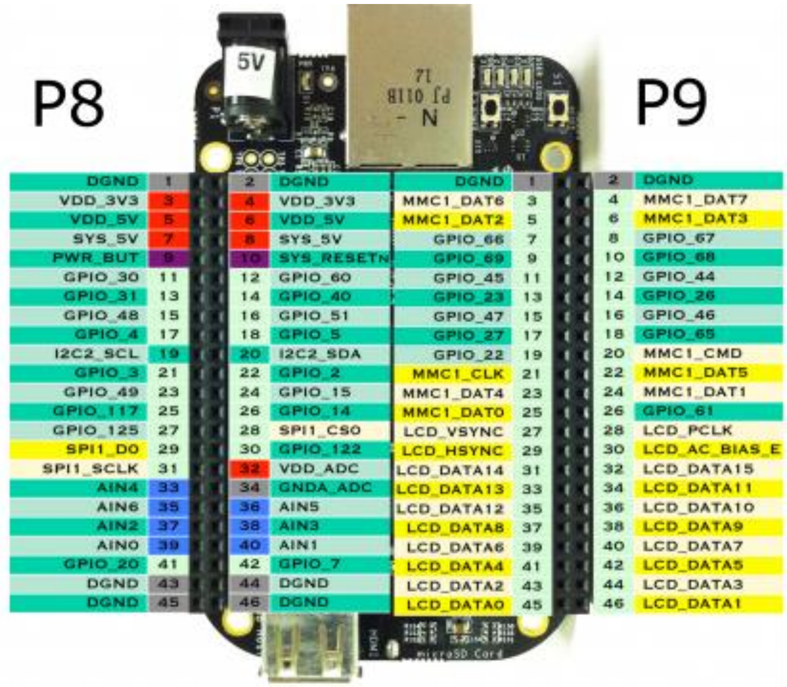


Figure 3 BeagleBone Black
With permission from: Let's make robots

This board is more than capable of running OpenCV with its 1 GHz processor, and DDR3 RAM, Wi-Fi can be added by a simple dongle, and with Linux coming pre-installed along with a helpful suite for programming bundled with its default distribution, and along with that it has a JavaScript library called BoneScript to make it programmable even by JavaScript. The GPIO ports also make it very convenient to control all other sensors used in our project and the two Programmable Real-time Unit subsystems (PRUs) allow for faster and more efficient power usages when reading sensors or anything else on the GPIO pins.

4.2.4.4 Arduino

The Arduino is a popular hobbyist board that are great for interacting with the environment around them via the use of I/O with sensors, motors, and any other hardware of the sort. The Arduino family of boards encompass a wide range of sizes and performances, but none of them has the performance necessary to run OpenCV natively. This doesn't include the upcoming Arduino Tre board, which is a collaboration with BeagleBone and has the benefits and connectivity of an Arduino with the power of the Sitara AM3359AZCZ100 (ARM Cortex-A8).

Overall the Arduino platform would be great for any part of the project that doesn't rely on face recognition or video. But in the end it can't keep up with the competition in terms of processing power, memory, and even in price $20 to $40 doesn't make it any more affordable a Pi or Beagle Bone.

4.2.4.5 Intel Edison
The Edison is Intel's attempt a small single board computing, and it packs a lot in a tiny package. The Edison comes with a dual core 22nm SoC that includes a 500 MHz Atom CPU accompanied by a 32-bit Intel Quark microcontroller at 100 MHz In addition it packs a 1 GB LPDDR3 POP memory (2 channel 32bits @ 800MT/sec), 4 GB eMMC storage, Wi Fi, and Bluetooth 4.0. Along with this it has 40 GPIOs that can be configured as 1 SD card interface, 2 UART controllers, 2 I2C controllers, 1 SPI controller, 1 USB 2.0, and an additional 12 GPIO with 4 of them capable of Pulse Width Modulation.

Performance wise the Edison's dual core Atom should be more than capable of handling our OpenCV, it can run Windows Linux, and even interface with Arduino shields. With the separate Quark microprocessor it can use its GPIO pins without using the Atom CPU. Overall it seem a great board with a good deal of potential a good support forum, but the only drawback is the Edison chip alone costs $50 plus the additional breakout boards would place it a >$60 price range with no reason to pick it over the Pi or BeagleBone for our project.

4.2.4.6 Conclusions
Overall the decision ultimately comes down to Raspberry Pi 2 vs. BeagleBone Black (BBB). Both would meet the needs for our project so it now we must take into consideration the differences in the other features, reliability, ease of use, and resources available

Starting off the Pi is better with multimedia and GUI related tasks, while the Bone is mainly focused on connecting and integrating with electronics. This is evident when comparing the choices in processors (the more multimedia/GUI focused Broadcom as opposed to the control and communication focused TI Sitara) the, and availability and uses of their various I/O pins for which the BBB has the definite advantage with its 7 channel 200kHz 12-bit ADC, 8 PWMs, 4 UART, and its two 200MHz, 32-bit RISC PRUs for extremely low latency to I/O pins.

In terms of reliability the main concern is with the possibility of SD card corruption on the Pi due to it booting and writing to the same device, although the BBB also faces that problem the eMMC is seen as more stable and a SD card for data can be used as well.

When it comes to ease of use the Pi requires a SD card containing Linux which may need to be installed while the BBB comes with a version of Debian already pre-installed in its eMMC. In addition the BBB comes with extra convenience features straight from the box such as USB client and boot from USB/serial direct, while the Pi needs a separate Serial/USB cable to match that functionality. Additionally the BBB's hardware is open-sourced as opposed to the Pi, which for our purposes does not affect us.

Lastly the available resources are what will have the most weight to our decisions. While the BBB has been around since 2011 and has had several books, articles, and tutorials the Pi still has a greater range of community support, peripherals, expansion boards, and tutorials. The shear popularity of the Pi has led it to become the first choice for the enthusiast looking for a powerful and affordable Single Board Computer.

4.2.5 Communication

There are several different modules in HOMES that will need to communicate with each other. The main computer will be physically connected to the motion sensor, the camera, the fingerprint scanner, and a receiver of some sort to handle communication with the wearables. Also the external entry point modules must be able to communicate with the main board to convey that it has been opened. The following sections will discuss the different methods of communication.

4.2.5.1 RFID/NFC

Radio-frequency identification is the wireless use of electromagnetic fields to transfer data. Radio frequency (RF) communication has three different forms. The first form is simplex. This is one way communication only, such as a TV or a radio. The second form is half-duplex. This is a two way communication such that both parties can send and receive information but not simultaneously. Lastly, the third form is full-duplex. This is a two way communication such that both parties can send and receive information simultaneously.

There are three kinds of RFID tags: Active tags that rely on internal batteries to power its internal circuits and broadcast its radio waves to a reader with a range of up to 100 meters, Semi-Passive tags have about 10 meters range but also rely on batteries to power their circuits but still need the reader to supply its power to broadcast. The most common and affordable type of RFID tags is the passive tag. The Passive tag relies on receiving the power from the reader which lets them be cheap and compact.

Near Field Communication (NFC) is a subset of RFID technology that is intended as a close proximity wireless technology based of electromagnetic induction that operates at 13.56 MHz at around 106 to 424 Kbit/s. The NFC can both be used as RFID with an initiator generating an RF frequency to power a passive tag, but it can also function in a peer-to-peer mode where both devices are active and can exchange information. The average tag holds from 96 to 4096 bytes of information and is usually read-only but can be rewritten.

For our project a passive RFID tag such as a card or a fob can be used by the user to gain entrance. We are also exploring RFID as an option for a pet collar to control the pet door entrance, although it would rely on finding a reader and tag combo that have a consistent range of >1 meter. The downside of using RFID is the relatively short range of affordable readers, in addition there is the extra security concern on the possibility of cloning or spoofing tags.

There are three different RFID modules that we are considering for our project, each come from a different distributors and has its benefits. The first one we are considering is the *Parallax Read/Write RFID module* it is intended for reading 125 Khz passive tags, with the ability to store 116 bytes and 2 LED lights for confirmation. This is a straightforward module that costs around $50 and will communicate via Serial.

The next modules are Sparkfun’s ID 3LA/12LA/20LA RFID readers costing about $26/$30/$35 respectively. These handy affordable modules take in 2.8-5V and can read 125 Khz tags. For our purposes we wouldn't need anything more than the affordable and super compact measuring only 19 X 21mm 3LA and its range of up to 30 cm with the addition specialized long distance RFID cards and antenna.

Last but not least is Adafruit's PN532 NFC/RFID controller breakout board. This is the most adaptive board we are considering, for the $40 price it does all we need and more it has both the ability to act as a NFC device, or a reader for NFC or 13.56 MHz RFID tags. In addition it provides the flexibility of communicate via I2C (by default) ,SPI, or TTL UART at any baud rate. It’s only downside is it’s relatively bigger dimensions 51mm by 117.7mm, and its price in comparison to the ID 3LA.

4.2.5.2 Wi-Fi

There are many ways to connect you embedded device to the internet of Things, some are a bit more simple while others are a tad more complex to implement. Overall Wi-Fi is great for transferring a lot of information at high speed, but for this reason it’s not as power efficient as the other methods.

The first item is the Electric Imp it’s an all in one solution to the challenge of making an IoT device. The Imp is an all-inclusive platform that includes the hardware, firmware, IDE, and cloud software. One of the biggest benefit of the imp is its BlinkUp technology that allows it receive all the Wi-Fi network settings information with device authorization codes from blinking the screen on a phone or tablet via a photosensor on the imp card this allows for quick and easy set up for a Wi-Fi-enabled device. The hobbyist version of the imp comes in two forms the SD card format imp001 (figure 4a) with built in photodetector and 6 GPIO pins, or the imp002 (figure 4b) with 12 GPIO pins with on separated on board antenna and the option of overriding the onboard LEDs and photodetector. The Imp would work wonderfully as part of the window/entrance monitor.

Figure 4a Electric Imp001 SD card
With permission from: Electric Imp

Figure 4b Electric Imp002
With permission from: Electric Imp

If we decide to go a more customized route we can utilize TI CC3200 chip, it is a full solution Internet on Chip. With an onboard ARM-Cortex M4 and Wi-Fi MCU this board is capable of controlling an embed design while taking care of the details and complications of implementing our own Wi-Fi stack, in addition it makes use of Texas Instruments' SimpleLink Platform which allows it the ability to be programmed over a IOS or Android application.

ESP 8266 is a newcomer to the IoT chips; it's a low cost module that satisfies the need of connecting embedded projects to Wi-Fi. It has a microcontroller and flash memory, which allows it to drive the project itself or it, can go into AT mode and be driven by a separate microcontroller. While it definitely the cheapest of all the options it is a lot harder to program or reprogram, and in addition its only supported by the community rather than an established company so if we were trying to take our project into production it would definitely be a hindrance to us.

4.2.5.3 Bluetooth

Bluetooth is another wireless standard used to exchange data over relatively short range via UHF radio wave at frequencies between 2400 to 2483.5 MHz. This was a technology initially developed by Ericsson in 1994 but has evolved via its open platform and support of major companies such as Intel, IBM, and Nokia into the defacto standard for short range non Wi-Fi data transfer with the 4.0+ versions reaching a data rate of up to 24 Mbit/s. Bluetooth devices work with a Master/Slave model inside their own networks usually called piconets. With the Master/Slave method one master can connect to up seven slaves while the slaves can only be connected to one master. While connected the master can send and request data from any slave, but slaves can only send and receive from the master and not any of the other slaves.

The process of connecting two devices using Bluetooth progresses through three states. The first step is *inquiry* in this step the devices send out inquiry requests and if any other device receives said request it will reply with its unique 48-bit Bluetooth address (BT_ADDR). The next step is *paging* here the devices attempt to initiate a connection with exchanged addresses. The last state is *connection*, once the devices successfully connect they can actively exchange data or it can go into a sleep state to conserve power until a signal or a set period of time. Depending on the purpose of the connection the device can be in active mode where it regularly exchanges data, it can be in sniff mode where the device will sleep and will only listen to a transmission after every certain period of time (usually around 100ms). If more power saving is required the device can go into hold mode which it sleeps for a predetermined interval of time before going back into active mode, or it can go into Park mode where the device a slave in this case will go into deep sleep until told to wake up by the master.

The Bluetooth standard has been constantly evolving, the latest major standard is Bluetooth 4.0 and it was a big step forward in the use of Bluetooth in low power applications. With the 4.0 Standard Bluetooth now is comprised of three separate standards: Classic, High Speed, and Low Energy. For the purposes of our project we are considering the application of Bluetooth as a form of user authentication in the form of their smartphone, or perhaps a fob or a wearable. This range and pairing abilities of Bluetooth also make it a strong candidate for use in the pet access door since the range would be much better the RFID/NFC. Regardless of whom will be using it we will still be taking advantage of the Low Energy version of Bluetooth to make a fob that will last a significant amount of time on battery life.

The master in our system would be the Single board computer and it would connect to Bluetooth via a generic 4.0 Bluetooth USB dongle found almost everywhere for around $10.

For use in the dongle the list gets pretty complicated, we would need a device with a Serial Port Profile that would send the master an identification code. The documentation for this type of application is pretty slim. The modules under consideration are the following.

Adafruit Bluetooth LE nRF8001 Breakout, a breakout for Nordic semiconductor's nRF8001 this tiny board can act like a UART interface for a controller. Sparkfun has a variety of modules such as the BR-LE 4.0-S3A or RN41 in a variety of breakout boards none of which would work without modification for our purposes. Lastly TI CC2541 is a promising low power module that has some great documentation behind it and a couple demo boards from TI displaying

The LightBlue Bean by PunchThrough is a great all-in-one BLE solution for our needs for our wearable. The LBB is a platform powered by an AtMega 328p chip to harness the power of LBM313 BLE module (which is powered by TI's CC2540 chip). The benefit of the LBB platform is its seamless wireless BLE programming, the open source design, and it purpose as a low power device running on a button cell. For our project we would use the LBB as a prototyping platform and then make a custom design using the just LBM313 if possible (as opposed to using the

LBM313 and AtMega 328p) to cut down on chip size, power usage, and cut costs on sensors we wouldn't need.

4.2.5.4 ZigBee

ZigBee is an open global wireless standard for the Internet of Things that provides communication for smart objects and enables them to work together. Currently ZigBee is used in cable and telecommunications such as Comcast and several other such services. Its range is between ten and a hundred meters, which is more than the range for Bluetooth and a simple Wi-Fi adapter. It is easy to install because all it uses is the ZigBee module attached to a board. ZigBee is the language for many smart home devices so it can be easily implemented into the home and can communicate with numerous smart devices. ZigBee operates in unlicensed bands such as 2.4 GHz, 900 MHz and 868 MHz. It also has a low duty cycle which means it is power efficient.

Sending data through a ZigBee application is incredibly simple since it will automatically decipher how to send information in the quickest way with the least chance of being lost. Data requests are sent out by the application and a data confirm is returned. The data confirm will tell the application whether the request was a success or a failure. This process is shown in figure 5.

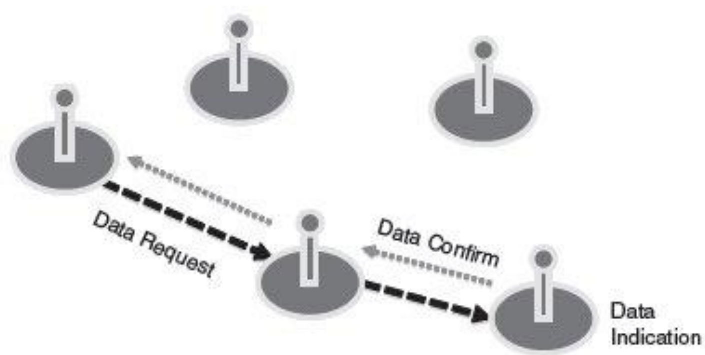


Figure 5 ZigBee Data Request
With permission from: EE Times

There are four main options of data requests unicast with end-to-end acknowledgment, unicast without end-to-end acknowledgment, broadcast, and multicast. Unicasts go from one node to another. End-to-end acknowledgement means the unicast will try three times before it gives up on the request. Broadcasts go from one node to all the nodes in the network. Multicasts go from one node to certain nodes. For our project we will only be utilizing the unicast request. We will most likely be using end-to-end acknowledgment. Further, ZigBee is asynchronous which means any node can both send and receive data at the same time. This is not necessarily needed for HOMES since all we care about is sending data from a wearable or entry point module to the main board. However it may be convenient to get information back from the board that tells the original sender if the data was sent properly.

In figure 6, the ZigBee is sending data to a node that is several nodes away. As is displayed on the figure for each node there is a 10ms delay. This means that end-to-end acknowledgement will not return with a data confirm until 80ms. This is a long amount of time and it can take a retry 1.6s to send the data again. This large amount of latency can be a problem and could cause a user attempting to enter their home via a wearable to wait at the front door for a few seconds while the ZigBee is attempting to send information over and over again.

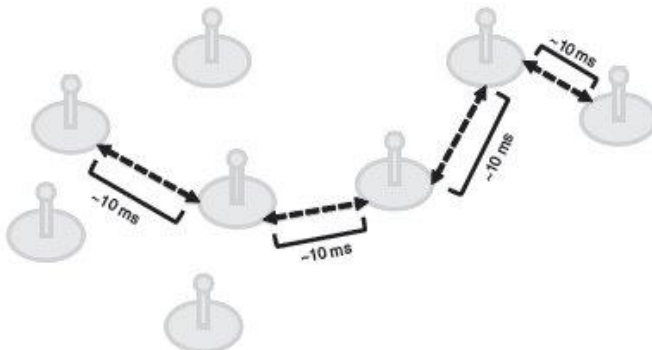


Figure 6 ZigBee Latency
With permission from: EE Times

4.2.4.5 Radio Frequency Transmitter-Receiver (RF Module)
An RF module is a device which is used to transmit and receive radio signals using a transmitter and receiver. It is widely used in embedded systems as a medium of communication. RF signals can travel large distances and through any hindrance or obstruction present in between transmitter and receiver making it a better choice compared to that of infrared signals which require a line of sight.

RF Communication works on the principle of Serial Communication, a general RF communication block diagram is shown below on figure 7, therefore a microcontroller or serial encoder are used to convert the conventional TTL (transistor-transistor logic) level n-bit input data into serial data. RF transmitter modulates the signal using ASK (Amplitude shift keying) or FSK (frequency shift keying) modulation and sends the data to the RF receiver via an antenna. The RF receiver demodulates the signal and sends the data to the microcontroller or serial decoder, which is then converted back to TTL level logic user input data.

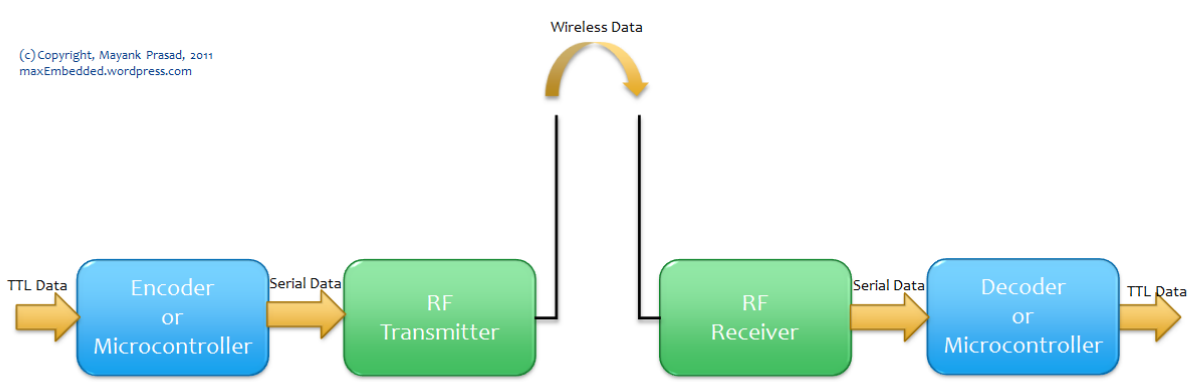


Figure 7 RF Communication
With permission from: maxEmbedded

RF modules use defined protocols for RF Communication such as Wi-Fi, Bluetooth low energy, or ZigBee. In the commercially available RF modules, several carrier frequencies such as 433.92 MHz, 315 MHz, 868 MHz, and 915 MHz are used because of the Regulatory Requirements governing the use of radio for communication which dictate the maximum allowable Transmitter power output, Harmonics, and band edge requirements.

4.2.4.6 Summary

As far as communication from the external entry points to the main board goes, once the sensor has detected that the entry point has been opened, it will need to communicate with the board to relay the information. There are several ways of communicating with the board. Since these sensors will be placed throughout the home at the entry points it doesn't make sense to use wired communication to the board at the front door. Instead we will use a form of wireless communication to relay information from the sensors to the main board. There are several different technologies that allow for the wireless communication of material as was just discussed. For external entry points Wi-Fi would probably be the best option because it has the best capability for data transfer with the maximum chance of success.

As far as communication from a wearable to the main board goes, we won't need anything very complicated, simply a transmitter and a receiver that can send a signal to the main board if the transmitter comes within a certain distance with the receiver. The most efficient means of this communication is Bluetooth. Also since most smart phones have Bluetooth, we can also allow residents to use the Bluetooth from their phone to unlock the door as well as wearables. In this way we can enable the homeowners to save the wearables for children or guests who don't have smart phones.

Table 3 shows a comparison of the major technologies discussed in the previous sections.

Table 3: Comparison of Communication Technologies

Specification	Bluetooth	Wi-Fi	ZigBee
Frequency band	2.4 GHz	5 GHz	915 MHz
Bandwidth	24 Mbit/s	6.93 Gbit/s	250 Kbit/s
Distance	10 meters	10 meters	10-100 meters
Line of Sight	No	No	Yes

4.2.6 LCD Touch Screen

HOMES needs to have a screen outside the door to display options to any guests. We want to use a LCD touch screen to display these options and to show the user the status of their request. There are several types of touch screens that will be compared in the following sections.

4.2.6.1 LCD TFT

A liquid-crystal display (LCD) is a panel that uses the light modulating properties of liquid crystals between sheets of polarizing to display an image once a current is passed through. A LCD panel is pictured in figure 8. The main type of LCDs that can be used in our project are thin film transistor (TFT) LCDs which a variety of display that use a special type of transistors embedded within the panel that help reduce crosstalk between pixels creating a sharper and more stable image.

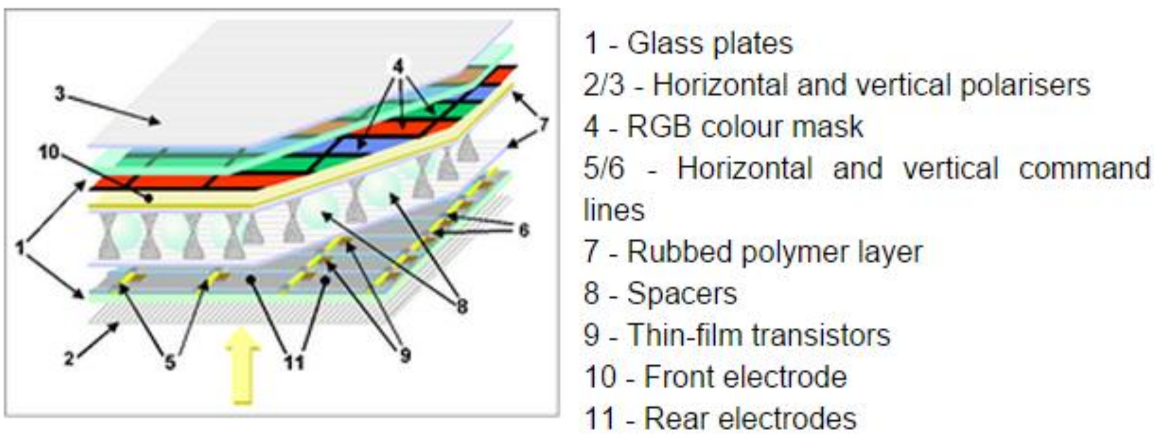


Figure 8 LCD Panel
With permission from: Creative Commons

4.2.6.2 Touch Screen - Resistive vs. Capacitive

The two most common technologies used in touchscreens available in the market today are Resistive or Capacitive technologies. Both allow the user to directly interact with what is being displayed, but they achieve this quite different ways.

The Resistive touchscreen uses two flexible sheets coated with a resistive material and separated by an air gap or microdots. It works by having a voltage gradient applied to one sheet and whenever pressure is applied to the screen causing the sheets to touch the voltage is then measured in the second sheet and used to find the distance along the first screen it represents giving the first axis value, this is then repeated with the voltage being on the second sheet to find second axis. The main advantage of the resistive screen is ruggedness, it can receive any kind of input be it a finger, a stylus, or anything else that can exert enough pressure to be sensed by the screen, as well as being able to be. In addition they're relatively cheap and capable of producing high resolutions. The biggest downside is the lower sensitivity as compared to the capacitive screens most phones, tablets, and computers use. Other than that the flexible material used on the resistive screens tend to feel less refined and usually have a slight haze due to the materials not being 100% transparent.

The Capacitive touchscreen is usually made of a glass that has been coated with a transparent conductive material on one side that has a small voltage running through it, when a conductor like skin comes into contact with the other side of the glass the electrostatic field present on the screen is distorted and a change in capacitance occurs that can be measured and interpreted to pin-point the location of the touch. The advantage of capacitive screens is the responsiveness and ability to sense multiple touches at a time. The downside is that compared to resistive screen they're more fragile and won't work with gloves or any nonconductive surfaces or in the presences of liquid, dust, or smudges.

4.2.6.3 Raspberry Pi

There are several touchscreens that are compatible with the Raspberry Pi. The following two sections briefly discuss the two touchscreens that are under consideration for use in HOMES.

4.2.6.3.1 PiTFT Plus 480x320 3.5" TFT+ Resistive Touchscreen for Raspberry Pi

PiTFT Plus is a 3.5" 480x320 LCD + Controller meant for the Raspberry Pi 2 it has 16-bit color pixels, and is capable of resistive touch. This display is sold by Adafruit for $45 and uses the SPI pins on the Pi.

4.2.6.3.2 PiTFT Plus 320x240 2.8 " TFT + Capacitive Touchscreen

The PiTFT Plus is a 2.8" 320x240 LCD + Controller meant for the Raspberry Pi 2 it has 16-bit color pixels, and is capable of single touch capacitive sensing. This display is sold by Adafruit for $45 and uses the I2C, and SPI pins on the Pi.

4.2.6.4 BeagleBone Black

This cape sold by Sparkfun uses a 4.3" Resistive touch screen by 4D Systems to create a that works seamlessly with the BeagleBone Black (running the latest Debian build), without need of a separate power supply or extra cables. In addition to the LCD the cape also includes 7 onscreen buttons that can be used as manual navigation for our project. The one foreseen downside of using this is that all the pins of the BBB get plugged in to the cape but it does not breakout the unused GPIO pins thus if this was to be used we would need to wire it manually and breakout the unused pins for the rest of our project. This screen costs about $65 and comes assembled. There is also a 7" version from the same manufacturer that costs $100.

4.2.7 Light

When motion is detected around the front door, the camera will take a picture of the guest. In order to do this the area must be well lit. The type of light needed for this project depends on the kind of camera we choose. If we use an infrared camera such as the Raspberry Pi NOiR camera module then we need to use infrared light. But if a non-infrared camera is used then we can use a regular light or LEDs. There are many tradeoffs to be considered when choosing a light for the project. LEDs are more expensive however they are more energy efficient and they can last almost 50,000 hours, which is almost six years. A regular light bulb lasts only about 1,500 hours or just over 2 months. In the long run however in the six years it takes for an LED to go out, the regular light bulb will need to be replaces 36 times. At one dollar per bulb this comes out to 36 dollars. As will be shown in the following section, the LEDs will cost 65 dollars. Therefore cost wise, a regular light bulb is better.

4.2.7.1 LEDs

LEDs are simple PN-junction diodes. When a voltage is applied the PN-junction emits light at a certain wavelength. This wavelength depends on the bandgap of the materials used in the PN-junction. If the bandgap is large, then the wavelength will be small and vice-versa. LEDs are quite small and are also usually more energy efficient than a regular light however, they can be quite powerful and are generally cheaper than a light bulb for instance.

An array of LEDs will brighten the desired area to be photographed. If a regular camera is used then at night or during a time when visibility is low then the LEDs can turn on and shed light on the guest so the camera can see them. They use less energy than a regular light bulb and their lifetime is enormous. However, LEDs cost about fifty cents apiece and while they produce about 45milliwatts that means the amount needed to roughly equal a 60 watt light bulb is 130 LEDs. The total cost would be about 65 dollars.

4.2.7.2 Infrared LEDs

Infrared LEDs are only needed if an infrared camera is used. Infrared light has a wavelength that is not visible to the human eye, about 760nm. Infrared LEDs are at the basic level regular LED's only with a different wavelength. This different wavelength is obtained by having a fairly large band gap. Most infrared cameras use an infrared detector to convert infrared energy to an electrical signal that can then be made into an image. The infrared camera being considered for this project is a regular camera that has no infrared filter. This means that in order to get a proper image the area to be photographed must be illuminated by infrared light. This also means that during the day time regular light can distort the picture. Infrared LEDs are a little more expensive than regular LEDs by about 10 cents apiece. This would put the cost of about 130 of them to 78 dollars. In terms of efficiency it depends on the type of camera, the infrared camera needs infrared LEDs and the regular camera needs regular LEDs.

4.2.7.3 Light Bulb

A regular light bulb can be used to illuminate the area to be photographed at nighttime. The basic light bulb produces light by running electric current through a wire filament. While this does the job it is not very energy efficient compared to an array of LEDs that uses very little energy. However this option is much cheaper than LEDs. A 60 watt light bulb costs around one dollar compared to the over fifty dollars spend on LEDs.

4.2.7.4 RGB LEDs

A RGB LED isn't one LED in a package but three LEDs along with a small computer to drive them. The LED is made up of red, green and blue LEDs each of which can be controlled by a microcontroller capable of Pulse-Wave Modulation (PWM). Since the two legs on the LED that supply the power are connected to the microcontroller and not the LED elements a current limit resistor is not required.

The microcontroller is able to turn each of the colors on or off, so if the red LED is turned on then the output from the color changing LED is red. When the blue LED is turned on it is blue, if both the blue and red LEDs are turned on then the color changing LED is a shade of purple (magenta). Similarly combining red with green gives yellow and blue & green gives cyan.

Although the color changing LED uses the six colors mentioned above, it slowly changes from one to another. This is still done using the three basic red, green & blue elements. If the red LED is combined with the blue LED, but the blue LED is only driven at 50% of its normal brightness then a color half way between red and magenta is generated. While the red LED is left turned on, if the blue LED is slowly taken from 0% brightness to 100% brightness then the color will gradually change from red to magenta.
If a standard LED is turned on and off very quickly, say 100 times every second then as far as the human eye is concerned it looks like it is constantly on. If the amount of time the LED is on for is the same as the time it is off for then it will be on for 50% of the time and 50% of its full brightness.

This same method can be done with the three LED elements inside the color changing LED. This means it is possible to combine any amount of the red, green and blue to give the desired color. Looking once again at the change from red to magenta, if the blue LED starts mainly turned off, goes to being on and off in even amounts and then to mainly being on. Four pin RGD LEDs are a little different. They share a common Anode, but three separate Cathodes, one for Red, one for Green, and one for Blue.

LEDs do not tolerate variable voltage well. That means that if you apply too much voltage, they pop. That means if you apply too little voltage they don't work at all. The 'Goldilocks' zone is far more narrow than with an incandescent light bulb, and unlike the filament bulbs, you cannot control the intensity of the output with voltage, they either light up, or not.

4.2.8 External Entry Point Modules

The system will be monitoring selected entry points to the house besides the front door. This includes windows, back doors, pet doors, etc. What is meant by monitoring the entry points is when an entry point is opened or shut it will 'know' and send a message to the Raspberry Pi that will in turn send a message to the application that the homeowner can then view. As such there are several different things to consider when creating this portion. The sensor that will detect if the entry point has been opened or closed, the power supply, and lastly the communication to the board are all things that need to be resolved.

4.2.8.1 Sensor

There are a number of sensors that could be used to check if the entry point has been opened or shut. There are several requirements for the sensor. The type of sensor used should be universal, meaning it should work with any kind of entry point whether it is a window, pet door, back door, sliding glass door, etc. It should be able to be attached to the inside of the entry point so there is no need to get a water/weather resistant sensor. Finally, it should have relatively low power consumption.

4.2.8.1.1 Magnetic sensor

A magnetic sensor can be used to determine if the entry point has been opened by placing a magnet on the bottom part of a window for instance, and then another one on the part that will open. When the window is shut, the magnets will come together. However when the window is opened, the link will be broken. This is a universal solution that can be applied to all types of entry points, can be placed on the inside, and will have fairly low power consumption.

4.2.8.1.2 Displacement sensor

A displacement sensor can be used as well by measuring the displacement at time intervals and comparing it with that of a base value (which would be when the window is closed). If the displacement measurement is greater or less then the base value then the entry point has been moved. This sensor should be place on the segment of the entry point that moves if it is opened or shut. This is also a universal solution that can be applied to any entry point and it can be placed inside the home. However because this takes measurements at time intervals and preforms calculations it will take up more computing time and thus more power than a magnetic sensor.

4.2.8.1.3 Accelerometer

Lastly, an acceleration sensor can be used to detect an entry point opening or shutting. The sensor would need to be attached to the section of the entry point that will move if it is opened or shut. It will constantly measure the acceleration and check if it is greater than zero. If the acceleration is greater than zero then the entry point is moving and thus opening or closing. If the acceleration is zero then it is stationary and has nothing to report. This is a universal solution that can be applied to any entry point and it can be placed inside the home. However, much like the displacement sensor, it requires constant checking of the acceleration and constant calculations that will consume more power than a magnetic sensor.

4.2.8.1.4 Reed Switch

A reed switch is a type of magnetic switch. It is made of two ferromagnetic reeds placed in a glass tube with a small gap between them. This is effectively an open switch, which leads to an open circuit. When a magnetic field is introduced the gap between the reeds lessens until they are in contact with each other. At this point the switch is closed and the circuit is no longer open.

There are two main types of reed switches. There is a two-reed switch and a three-reed switch. The difference between these two is pictured in figure 9a. The two-reed switch is normally open, meaning the reeds or contacts initially do not touch unless a magnetic field is applied. The three-reed switch has both a pair or normally open reads and a pair of normally closed reeds. This makes it more interchangeable and more complex. For this project we will most likely only need a simple two-reed switch, which is pictured in figure 18b.

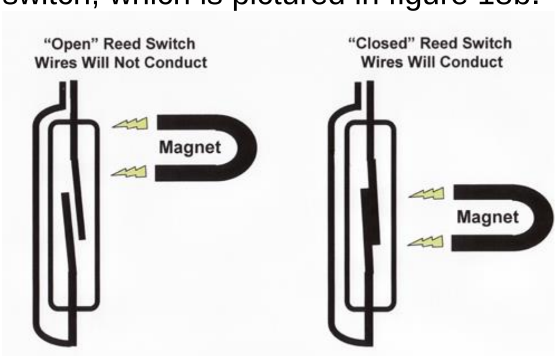


Figure 9a Open vs Closed Reed Switch
With permission from: Chicago Sensor

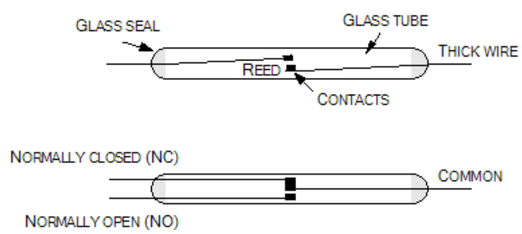


Figure 9b Two vs Three Reed Switch
With permission from: Electronics in Meccano

4.2.8.3 Power Supply to modules

The sensor and communication module will need some kind of power supply in order to function. Any of the sensors mentioned in the above section require low power. The acceleration and displacement sensor require more power than the magnetic sensor because they have to be constantly measuring and calculating. Even still they will not use much power. Also the communication module will need to be powered. All of the modules discussed in the above section have low power consumption, so the overall power consumption of the small PCB will be little. This means we can use a battery and a voltage regulator to supply the power to these components.

4.2.9 Wearables

As discussed in the RFID vs. NFC vs. Bluetooth section we discuss the difference in technology and begin to analyze which tool is better suited for our project. However, the wearable is what goes around the transmitter and makes it into a bracelet for the homeowner and/or their children and/or a pet collar. Then there is a receiver by the door that will pick up on the signal and unlock the door when the user is within a certain range. The human wearables do not necessarily need a wide range because the user can tap the wearable to the receiver in order to deliver the signal to the board to unlock the door. The pet collar on the other hand must be able to have a range because a dog or cat may not be able to learn that they need to walk right up to the receiver. Instead it would be more efficient to have a wearable that can send the signal and a receiver that can get the signal if the animal is only a few feet away.

There are programmable wearables out on the market to purchase, or we have the option of making our own and putting a transmitter inside our own creation. An advantage to obtaining a wearable is that it is ready to program without needing to build anything. Also it might be slimmer and more stylish than a homemade wearable. However, if we buy on that is already made we have little to no choice on the kind of transmitter inside the wearable. Whereas if we make our own we can choose the one that will best meet the requirements of our project, this gives us more flexibility. The price of a transmitter ranges depending of the type. However no matter what type of transmitter that is chosen, it will need to be powered. This can easily be done with a watch battery which are relatively inexpensive and have a fairly long life. All that is left after getting a transmitter and a watch battery is putting it inside the wearable. The most likely way of doing this is to put the transmitter and watch battery inside some kind protective casing and attaching it to either the inside of a bracelet or the inside of a pet collar.

Another option for the wearable is to make a small PCB that holds the power and the communication transmitter and then use a 3D printer to make a small housing for it. This way it will be more like a keychain than a wristband. Also this way it doesn't necessarily need to be fashionable, since no one will be physically wearing it. Instead it merely needs to be small enough to fit on a keychain and durable enough to endure the sometimes rough treatment of keys and key chains.

4.2.10 Lock

For our project we are considering three methods of providing access to the user, each having a different degree of price, ease of use, and ease of install.

The first option in providing access would be an electric strike shown in figure 19. The electric strike is a replacement for the usual metal faceplate doors have, instead it has a locking ramp surface that allows the door to close without problems, but has a latch bar that when activated does not allow the latch through to open the door. Once deactivated the latch bar pivots or unlocks allowed the door to be pushed open.

Electric strikes usually require 12 to 24 Volts in AC or DC current and come in two main configurations. Fail-secure in which the strike unlock only when the current is applied to it, due to this in case of power loss the door would stay locked and would still be able to open manually. Fail-Safe locks require the current to be constantly applied to the strike in order to keep it locked, although this is more power intensive allows the strike to remain open allowing continued access in case of power failure. For the purposes of our project we would want to be using a Fail-secure lock since we would want to door to stay locked in case of power failure or system restart.

The second option would be modifying an existing electronic deadbolt to be activated remotely by our system. Since electronic deadbolts come in many different shape, sizes, and functions; we would be considering affordable models that can still be manually locked and unlocked in case of power or system failure. The benefit of using a professionally made electronic deadbolt is that all the mechanical engineering aspects are already taken care of, and in some locks even have space for the addition of batteries. Additionally with these ready bought locks there would be a convenient way to run wires from the inside to the outside of the door for the other aspects of our project like the LCD. Thus we only need to wire in to control the locking mechanism. The only downside of this is in the added price since the lowest priced electronic lock is still around $60.

The last method to consider is using a servo and creating a module that would attach to a regular door deadbolt and open and close it by utilizing the servo to rotate the knob or possibly the actual spindle. This method would probably be the cheapest since it would use any regular deadbolt, and it would be the easiest for a user to utilize as well since it wouldn't require much modification to a user's door other than attaching the module to the deadbolt. The downside of this method is that a servo might not have enough torque to use any deadbolt especially one where the door needs to be pushed in for a smooth lock or unlock.

4.2.11 Fingerprint Scanner

One of the ways in which the user can gain entry to their home is through a finger print scan. As most people know, fingerprints are unique and adding this feature to the system provides a secure way for the user to enter into their home without the hassle of an actual key. The way a fingerprint scanner works is to obtain a picture of the fingerprint and then compare it to current fingerprints in the database. Obviously for our purpose the homeowner, family, and friends can all have their fingerprints stored in the database and when a user wants to gain access to the home all they need to do is scan their finger.

Fingerprint scanners can use two different types of scanning, optical and capacitance. An optimal scanner uses a charge coupled device, or CCD to take an image of the finger and is shown in figure 10a. LED's light up the finger and takes an image. Then the CCD inverts image so the dark areas represent the ridges of a fingerprint and the light areas represent the valleys. Then the processor checks if the image has enough exposure and is defined enough to get an accurate reading. In capacitance scanning, instead of using light and a CCD, current and a semiconductor chip are used. This scanner is shown in figure 10b. This scanner places conductor plates in an array and uses the fingerprint ridge and the valley, or lack of a ridge, as another conductor plate making a capacitor. In the case of ridges, which will be closer to the conductor, plate the capacitance will be larger than the case of a valley where the capacitor has some air between the finger and the conductor plate. This difference in capacitance translates into a different voltage that is delivered to the processor. It then uses these voltages to compile a picture of the ridges and valleys of a fingerprint.

After an image of the finger is captured the system software runs an algorithm that compares the captured print to prints in the database by comparing several points. If the fingerprint is in the database the door will unlock, if not an error will be displayed to the user on the LCD screen.

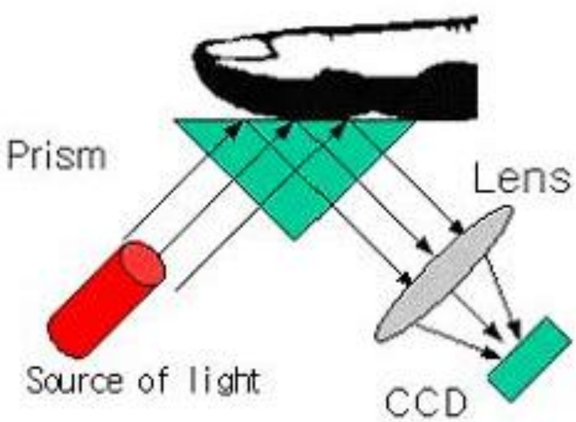


Figure 10a Optical Scanner
With permission from: Take off student

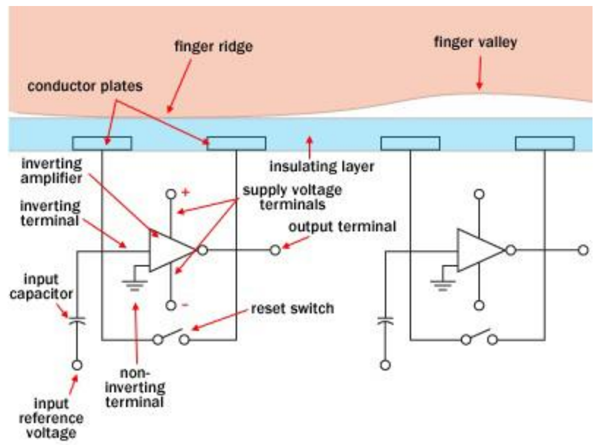


Figure 10b Capacitance Scanner
With permission from: Take off student

There are two options to obtain a fingerprint scanner, buy one or make one. As can be seen by the research above an optimal scanner would be easier to build, since this type uses a CCD and LED's to capture the image. Also there are fewer components so it would be more cost efficient to build this kind of scanner as opposed to the capacitance scanner that uses charge and conductor plates. A disadvantage of the optical scanner is that it could be less secure. Given that it uses a 'dark and light' image of the finger print it is possible to trick it using a photo of a fingerprint. The capacitance scanner will make it significantly harder to trick because it needs the actual 3D finger in order to compose the image. To make an optical scanner a CCD and LED's are needed. CCD's cost about ten dollars, and LED's cost around ten cents apiece. So building a scanner will cost about twenty dollars. The cost of a premade optical scanner is about $49.99, while a capacitance scanner is about $100.00 so there is a definite cost advantage to making out own fingerprint scanner. Our budget set aside $50 for the fingerprint scanner so even with the added security of the capacitive scanner it is our of the price range.

4.2.12 Microphone

Microphones are transducers that sense sound waves and then convert this into an electrical image. Basically the output of a microphone will be a voltage or current that represents the sound wave. There are many different types of microphones including dynamic, ribbon, and condenser. Dynamic microphones use a magnet and a coil of wire to detect pressure variations and then use these variations to generate a voltage that is representative of the original sound wave. Ribbon microphones use a round magnet and a metallic ribbon to detect the sound wave in the air. The output of the ribbon is a voltage signal associated with the sound wave. Condenser microphones use a battery, a resistor, and a condenser that acts like a capacitor. The pressure variations change the space between the condenser plates and thus the output voltage will change in accordance to the sound wave.

The system will give the guest an option to leave a voice or video message to the homeowner. To do this our project must have the capability of voice or audio. There are a few options for the microphone depending on which camera will be used. The Raspberry Pi camera modules do not have the capability of audio so a microphone, possibly a USB microphone must be used. If a webcam is used, it has the capability of audio and video. A potential issue with using a USB microphone with a Raspberry Pi camera module is that it will need to be synced with the video in order to leave a video message that has audio that matches with the video. Starting the video recording and the audio recording at the same time may prove to be off slightly. A solution to this problem is instead of leaving a video message to allow the guest to only leave a voice message. Then there will not be a problem of lining the audio with the video. A more comprehensive solution would be to use a webcam with video and audio capabilities.

4.2.13 Pet Door

We wanted HOMES to include a pet door because pets are the center of many households and we wanted to incorporate them into our project. HOMES will include a pet door that will lock and unlock when the homeowner’s pet comes within two feet of the door. To do this we plan on making a pet collar that has a wearable similar to the human wearable that was discussed earlier in the research section. Then we will put a small lock on the pet door to keep intruders from trying to enter through it. The door will unlock using similar technology to the lock that was discussed earlier in this section. Then the pet will enter through the door and after thirty seconds it will relock.

Most pet doors use some kind of aluminum sliding door to stop the flap from being pushed in or out. This means that the pet has to wait for the homeowner to come and lift the sliding door before they can use it. However, there are a few pet smart Doors that allow pets to unlock or lock the pet door so they can get out when they want to. This is similar to our idea for HOMES. Current electronic pet doors on the market use a variety of different communication technologies from Bluetooth to ultrasound. This can be applied to HOMES when we decide on how we would like the pet wearable (collar) to communicate with the single board computer.

To lock the pet door we will have a small bar slide into place in front of it in order to prevent it from opening. We will most likely do this by attaching a moor to the bar that will pull the bar out and push it into place when it receives a signal from the main single board computer. When the pet comes within two feet of the door the wearable on its collar will send a signal to the board. The single board computer will then send a signal to the motor controlling the small bar to slide away from the door allowing the door to be pushed through by the pet. After 30 seconds the bar will slide back into place therefore relocking the pet door.

4.3 Software Research

In order to be properly prepared to implement all the software aspect of HOMES we must first research the methods we intend to use. There are three different areas that we shall focus our research on: OpenCV face recognition, mobile application development, and web develop.

4.3.1 Facial Recognition

OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. It was made to create a common infrastructure and stimulate the use of computer vision in products. There are more than 2500 optimized algorithms included in the OpenCV library, and their uses span across various areas of computer vision such as face detection and recognition (our use for it) , object detection, camera tracking, motion tracking, extracting 3D objects from image, image stitching, eye tracking, and augmented reality. The OpenCV community is extensive and boasts more than 47,000 people in research, government, and corporate world. It supports Windows, OSX, Android, and Linux, although it is natively written in C++ but has interfaces in C, Python, Java, MATLAB, and has a CUDA one being developed.

4.3.1.1 Face Recognition
A major aspect of the user identification in our project is going to rely on the ability to match a detected face to a database of authorized faces. Fortunately OpenCV 2.4 now has a FaceRecognizer class that can use one of three algorithms for face recognition. These are based on Eigenfaces, Fisherfaces, or Local Binary Patterns Histograms but before using any of them first a database with at least around eight preprocessed images of each user you want to be able to detect.

4.3.1.2 Eigenfaces (Principal Component Analysis)
The theory behind using Eigenfaces is that not all aspects of the images are equally important and only a few actually meaningful. Using Principal Component Analysis the eigenvectors can be derived from the original training images or an image that is going to be compared against the database of Eigenfaces. When a new image is

received for comparison the Eigenface is first extracted then it is compared against all others to find one that matches more than a set threshold. The benefits of this method are mainly due to its simplicity which allows it to be easily coded up without being too computing resource intensive to use and allowing it handle a large database of faces easily. But the flaw with this method is that it's very susceptible to failing due to lighting, changes in facial expression.

4.3.1.3 Fisherfaces (Linear Discriminant Analysis)

While the PCA finds a linear combination of features that maximize the total variance in the data it may lose some important discriminative information because it's lack of considering classes. Linear Discriminant Analysis is used to perform a class-specific reduction of dimensions to eliminate all but the most important dimensions. It attempts to do this by maximizing the scattering between classes and minimizing the scattering of same classes. This helps mitigate the effect of illumination on finding good discriminative information.

4.3.1.4 Local Binary Patterns Histograms

While Eigenfaces and Fisherfaces take a general comprehensive approach to analyzing and recognizing features for facial recognition. Another method relies on extracting local features instead of treating the entire image a high-dimensional vector, from this idea the Local Binary Pattern (LBP) method was used. In LBP you want to create a summary of the local structure of an image from a comparison between each pixel and the surrounding pixels. This is done by taking each pixel value and seeing how it compares to each of the other surrounding it, if it is greater than what it is being compared to its marked as a 1 if not a 0, this results in an individual value for each of the pixels it was compared against or a single 8 digit binary number sometimes called *Local Binary Patterns*. These patterns can be used to detect various different kind of features depending on its value, and in addition this method works well regardless of lighting levels.

4.3.2 Mobile Applications

The mobile application will enable the user to communicate directly with the system. The user will be able to send commands to lock and unlock the main door, lock and unlock the pet door, or turn on and off the light. The user will receive pop up notifications for events such as the window or door being opened, guest arrivals, or entries and departures. The mobile application will have administration features that will require login credentials to gain access (Figure 11a). The admin user will be able to add users to the database, override access, and adjust notifications through the settings (Figure 11b).

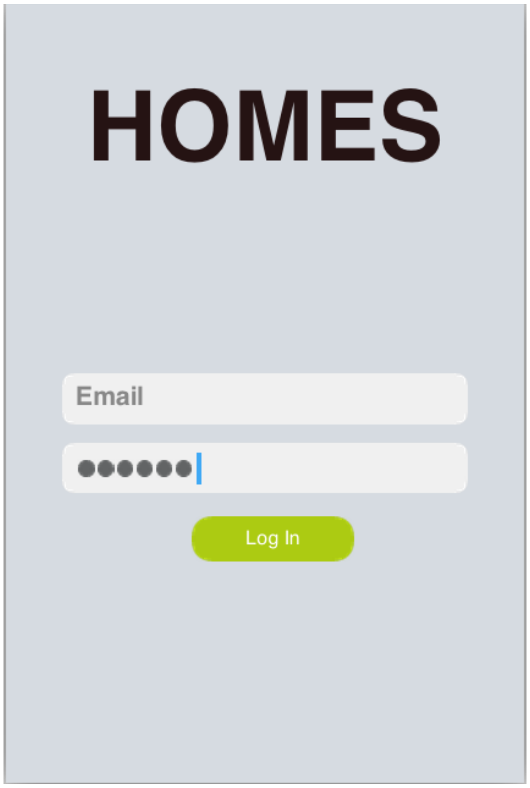


Figure 11a Mobile App Login Page

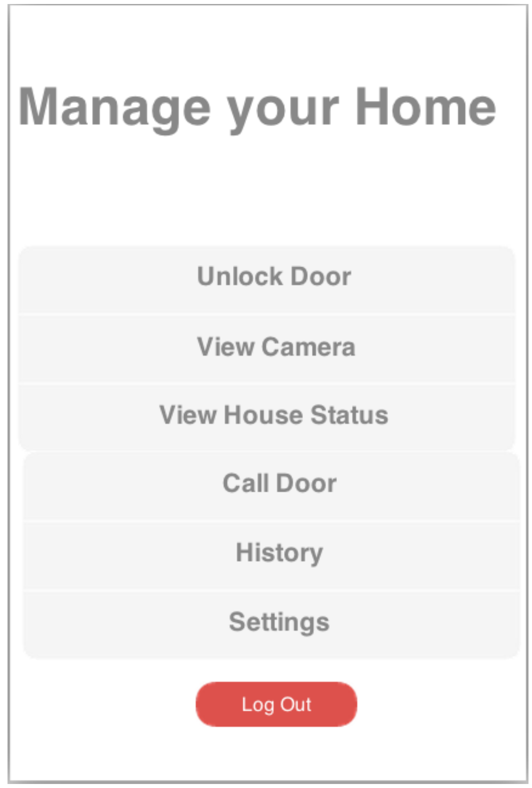


Figure 11b Mobile App Options

4.3.2.1 Environments

The following sections discuss the differences in Android, iOS, and windows mobile application environments.

4.3.2.1.1 Android

Android is a mobile operating system developed by Google. Being one of the most common mobile operating systems in the market, Android is an open-source platform meaning that the source code is made available with a license "[in] which the copyright holder provides the rights to study, change and distribute the software to anyone and for any purpose" (*Open Source Technology*). Open-source software is developed in a collaborative public manner which would allow anyone to create standalone Android applications that can be added to "Google Play", the digital distribution platform developed by Google and currently used as their official app store; allowing users to browse and download applications developed by users or published through Google. Android SDK "a set of software development tools which allows the creation of applications [aimed at Android]" (*Legacy Application Modernization),* utilizes the Java programming language. A onetime fee is required to publish a mobile application on "Google Play" store.

4.3.2.1.2 iOS

iOS is a mobile operating system developed by Apple Inc., currently the alternative to Android in popularity and market dominance. iOS is a closed-source platform were the source code is not made available and the user is given the right to use the software only under certain conditions, and restricted from other uses, such as modification, sharing, studying, redistribution, or reverse engineering. The App Store, "is the digital distribution platform for mobile apps on iOS, developed and maintained by Apple Inc. The service allows users to browse and download applications that are developed with Apple's XCode IDE." (*IOS-Unabridged Guide*) Apple's XCode IDE, an integrated development environment for creating applications for Apple devices using the Objective-C programming language. An annual fee is required to publish a mobile application to "The App Store."

4.3.2.1.3 Windows Phone

Windows Phone is a family of mobile operating systems developed by Microsoft. Windows Phone operating systems whether it be Windows Phone 8, Windows Phone 8.1, or Windows 10 have a much weaker presence in the mobile market and is usually last to be considered in comparison to Android or iOS running devices. Similar to iOS, Windows Phone is a proprietary software; parallel to Android there is a onetime registration fee to upload a mobile application to the Windows Phone Store, Microsoft's mobile app digital distribution platform. Development in the Windows Phone environment is done using Windows Phone SDK. The developer has a choice of several languages to program in such as C++, C#, and Visual Basic.

4.3.2.2 Summary

We've chosen to Android for our mobile application development due to several factors, target market size, development time and effort, and of course cost. A disadvantage of choosing to develop in Windows is its lack of popularity as compared to Android and iOS (Figure 12) therefore development in the Windows environment was quickly ruled out for this project.

Global Smartphone Operating System Shipments (Millions of Units)	Q2 '13	Q2 '14
Android	186.8	249.6
Apple iOS	31.2	35.2
Microsoft	8.9	8.0
BlackBerry	5.7	1.9
Others	0.5	0.5
Total	233.0	295.2

Global Smartphone Operating System Marketshare %	Q2 '13	Q2 '14
Android	80.2%	84.6%
Apple iOS	13.4%	11.9%
Microsoft	3.8%	2.7%
BlackBerry	2.4%	0.6%
Others	0.2%	0.2%
Total	100.0%	100.0%
Total Growth Year-over-Year %	48.9%	26.7%

Figure 12 Android vs iOS
With permission from: Strategy Analytics

An Android mobile application would use Java for development and seeing as how we each have previous Java development experience, the time required to learn, understand, and finally produce the application will be greatly reduced. iOS requires a current annual development fee of $99 on top of having to own a device that runs Apple's OSX, Android requires a onetime development fee of $25 which makes Android application development much more appealing.

4.3.3 Web Application

HOMES will provide homeowners with a web application that can be accessed at any time as long as there is an Internet connection. We want to create this for users who don't have a smart phone and thus cannot get the app, or for people who prefer using the web to an application. This way we are giving homeowners a choice.

4.3.3.1 PHP

PHP is a scripting language that one can use to build a web page. It is executed on the server-side rather than the client-side. It is very effective due to the many features that are designed solely for web pages, like POST and GET methods, and functions that work hand in hand with HTML. Building a secure web page where we would require a username and password before granting access would be ideal and with PHP the effort is seamless. PHP also works well with MySQL database so organizing, storing, and displaying collections of data will be unproblematic.

4.3.3.2 Python

Python is an object-oriented, interpreted and high-level programming language. Web Development using python was not an easy task until many special frameworks were created for this purpose. Web frameworks in Python have a lot of features, which allow developers to create faster, and more robust websites. A beginner may easily learn Python more quickly than other scripting languages such as PHP etc. The size of the code for a task is shorter than other languages due to its syntax so for smaller and common web tasks, Python is highly recommended. There are many options of web frameworks in Python like Django, Flask, Pyramid, and many more. A developer may use the right tools for their project and enjoy flexibility; Flask is mainly for small applications with simpler requirements while Pyramid and Django are mainly for larger applications.

4.3.3.3 Node.js

Node.js is a popular open source and cross platform runtime system for server side and networking applications. It has become the best choice for the JavaScript coders to build real time Web APIs. It uses an event based execution of server procedure instead of multithreaded execution which is used in PHP. By event based execution, it is meant that the execution for the program is determined by events. This type of execution is faster than the multithreaded execution.

It handles I/O efficiently by using event loop rather than waiting for I/O operations, through which it allows you to implement high concurrent web servers. With this feature high traffic on the website is easily handled. Node.js uses a virtual machine called v8 environment*, which* runs the JavaScript code. So it requires special web hosts that have the v8 environment.

5.0 Related Standards

The following list of standards were used in our project HOMES.

- NFC is standardized in ECMA-340 and ISO/IEC 18092
- RFID has standards on how data is stored by ISO 11784
- Bluetooth: IEEE 802.15.1
- Wi-Fi: IEEE_802.11
- ZigBee: IEEE 802.15.4
- Proximity sensor: IEC 60947-5-2
- Rechargeable battery: IEEE SA - 1625-2008
- Sensor: IEC 60947-5-2
- Network: IEC 62481 Digital Living Network Alliance (DLNA)
- Electrical Installations: IEC 60364
- Voltages: IEC 60038

6.0 Design Constraints

Every product or project has design constraints. These are limitations on the project by external factors. Some of these factors include economic, time, environmental, social, political, ethical, health, safety, manufacturability, and lastly, sustainability. In the following sections we will briefly discuss these constraints and how they apply to HOMES.

6.1 Economic and Time Constraints

An economic constraint is a restriction to a certain project or product by financial means. This could be a budget or a reason why a product is not selling like it should. The economic limitation on our project, HOMES, is mostly monetary. As is discussed in the budget and finance section at the end of this paper, we were partially funded by Boeing for about 66% of our estimated budget and as such we hope to not go too far over that funded amount. As for the funding agreement however, anything that we seek reimbursement for (anything we use the funding for) belongs to the university and therefore decisions must be made as to which parts we want to keep and which parts we don’t mind giving over to the University for future Senior Design students to use. Since HOMES is a project and not a product it is not being sold and thus doesn’t have any constraint or limitation as to selling it. If it were a product though the most important thing to emphasize is security, possibly one of the major reasons there aren't many smart front doors is because the general public is scared that such a system won't be as secure. The truth is that a lock and key aren't very secure either, they can be picked or broken down, or the key can be stolen. Since HOMES uses facial recognition and other systems that make sure only the homeowner and selected guests can gain entry to the home, this system is arguably more secure than a lock and key. We plan to enhance the monetary constraint by picking the most well priced parts as well as building certain things that will cost more to buy. We also plan to make our system as secure as possible so that the homeowner can feel safe leaving the entry of their home to our system.

A time constraint is a restriction to a certain project or product by the available period of time there is to complete it. The time constraint on HOMES is two semesters. The first semester, this semester, is focused on planning the project. This includes drawing schematics and preparing to build it. The second semester, next semester, is focused on actually building the project. This is also when we will test it and hopefully our plans and schematics are correct and the system will be fully functional. As is discussed in the milestones section below we split up the time we had into sections dedicated to research, planning, building a prototype, testing, and the final product. Also since we started the first semester in the spring (January through April) and the second semester is in the summer (May through August) that gives us 32 weeks total to complete both the planning phase and the building phase of HOMES. However, since it would be ideal to finish the project earlier so time can be spent writing papers and making presentations the time period is actually shorter than 32 weeks. In order to optimize the time we have we plan to implement the predetermined schedule perfectly and thus keeping on the correct timetable.

6.2 Environmental, Social, and Political Constraints

An environmental constraint is a constraint on a project or product by environmental factors such as safety and conservation of the existing environment such as animals or children. For HOMES we have to make sure that there are no external or exposed wires that could be dangerous. Whether an animal might find it and chew on it, or a child who gets a hold of it. We need to eliminate the possibility that someone could get electrocuted or hurt. HOMES plans on ensuring that this will not happen by creating housing for the main board and other components. This will hold all the equipment and wires in a nice, efficient, and safe manner. Another environmental constrain facing HOMES is the possibility of a fire hazard if a wire does get chewed through by an animal it could cause a short and then cause a fire. Again HOMES will mitigate the likelihood of this by creating a housing to protect the wiring. Lastly, HOMES needs to be weather resistant. Since the main board and other modules such as the Bluetooth receiver, the fingerprint scanner, and the camera will all be outside they must not be disturbed by the elements. The housing we will build to encase these items will help protect it from most weather elements.

Social constraints are limitations on a project or product by social factors such as security risks or safety concerns. Unfortunately as technology advances and things become more automated there is an increased likelihood that someone with ill intensions might hack in to a system. HOMES must be secure enough to put up a decent block for someone trying to force their way into the system. Homes will take several measures in the software to prevent people from pushing their way into the system such as a minimum amount of times you can attempt to enter the system before it sends a notification to the user and won't open unless the homeowner overrides it. Another security measure we are taking is via the hardware. By creating a battery backup for the system we are ensuring that if the power goes out the system will still continue to run undisturbed and can still monitor the home.

Lastly, political constraints are restrictions on a project or product by political factors such as rights and laws. One political constraint facing HOMES is the right to privacy. A guest has the right to their privacy which includes the right to not have their picture taken and sent to the homeowner they are visiting. In order to address this we will give homeowners a sign to put in their yard that will alert guests that there is a security system in place that will record and/or take their picture. Then it is at the choice of the guest whether they wish to enter the property or not. Also facing HOMES is the right to guard one's own property. As a homeowner or apartment owner deserves the right to protect and know what is going on their property even when they are not present. For example, in Florida a homeowner has the right to kill someone who is on their property and threatening them. This is a homeowners right to protect what is there. In fact, HOMES will lessen the probability that someone will be on the homeowner's property with ill intensions because it is advertised that there is a security system in place that will record or take pictures of any guests or intruders. In order to minimize the possibility that someone would question the legality of taking a picture of guests, the sign will explain the system and that after reading it the guest is proceeding at their own choice.

6.3 Ethical, Health and Safety Constraints

An ethical constraint is a limitation due to a moral or ethical problem such as cutting down trees to build a new building and thus destroying habitats of many animals. HOMES is very ethical, however as was mentioned in the political constraints section above, there is the dilemma of taking a picture of a guest without their knowledge and sending it to the homeowner's phone. Ethically speaking, a guest should be warned before the picture is taken and be able to make the decision of whether they are ok with it or not. If they are not ok with it then they have the option of not walking up to the front door. To face this constraint HOMES will provide homeowners with a sign to place on their property explaining that there is a security system in place that will take video and/or pictures of any guests who approach the front door.

A health constraint is one that confines a project or product due to health concerns. For instance, a medicine trying to get on the market must pass numerous health constraints before the FDA approves it. HOMES has almost no health hazards since most health hazards occur with a product that is consumed or has some kind of sharp part or radiates something. The only possible health constraint facing HOMES is any lose or exposed wiring could lead to a child or animal grabbing or chewing on it and getting shocked or electrocuted. However, we will be 3D printing housing for HOMES that will encase all objects and wires to eliminate this possibility.

A safety constraint is a limitation from a safety and well-being standpoint. For example, a building must address numerous safety constraints before it is deemed safe to go inside. Even if it is deemed safe it must still obey fire safety rules such as a maximum number of people per room. HOMES safety constraint is that the system must be secure enough so that an unwanted person cannot enter the home. The goal of HOMES is to make sure it is no less safe than a key which can be easily picked or stolen. A computer system is much harder to crack and requires a skillset that many people do not possess. HOMES will face this constraint by ensuring it is a secure system that only the homeowner or other residents are able to gain entry.

6.4 Manufacturability and Sustainability

HOMES is able to be manufactured quite easily. All that needs to be done is to put the parts together (the Raspberry Pi, the fingerprint scanner, the camera, etc.) and put a housing around it. Then a pre-programmed embedded system would most likely be a replacement for the Raspberry Pi. This would be fairly expensive to produce since it has so many modules and parts. However, it would be pretty easy to produce. Since it is expensive to produce it would probably cost a lot for customers to purchase.

HOMES is fairly easy to install since it is basically one main module. It is simply attached to the door and connected to the home power. Then the external entry modules are placed around the home at any points desired by the homeowner. Because of the simplicity of installation the price of HOMES would decrease since an installer will not have to take a long time installing one system.

Homes is very sustainable as long as the homeowner lives in a mild climate. If temperatures go to extremes it could cause HOMES to overheat, freeze, or take up more power. That can also affect how quickly the batteries lose power. However, since the battery is easily replaced and can be charged while there is power, that makes HOMES very effortlessly sustained.

7.0 Hardware and Software Design Details

7.1 Hardware Design Details

In the following sections we will discuss the design decisions and details of each section of out project. We will describe why a decision was made. We will also talk about how we plan to implement each module in our project. We plan on having most of the hardware including the light, camera, motion sensor, LCD screen, and fingerprint scanner outside the front door in a 3D printed housing that will mostly protect it from the elements. The single board computer will be inside the front door connected to a power supply printed circuit board. The external entry point modules will have their own power source and be placed at other doors or windows. There will be two kinds wearables, one for humans and one for pets. The human wearable will unlock the front door. The pet wearable will unlock the pet door.

7.1.1 Single Board Computer

To be the brains of our system we choose the Raspberry Pi 2, this was an incredibly tough choice since the other strong contender was the Beaglebone Black. Both boards provided a great hardware to work with and have enough RAM, GPIO pins, and processor speed to accomplish all the requirements for our system. What it really came down to is personal preference and supportive hardware both of which the Pi was superior. This was due in part because most of the group was familiar with the Pi and how it works so it felt more familiar, and the big reason the Pi was chosen is because the PiTFT touchscreens are vastly superior and more affordable than the alternatives found on the BeagleBone Black.

We will also be using the Arduino microcontroller for some things such as the PIR sensor, the RGB LED, and a few other items. The Arduino will be connected to the Raspberry Pi and will receive power from it. We needed to add the Arduino to our single board computer because it needed a little more processing power and it will be easier to program the separate systems instead of doing everything on the Raspberry Pi.

7.1.2 Motion Sensor

For many basic projects or products that need to detect when a person has entered, left, or approached the area PIR sensors are great. PIR Sensors are small, inexpensive, low-power, have a wide lens range, easy to interface with, and are pretty rugged don't wear out. Another benefit to PIR Sensors is that it comes in only one part so installation is only at one point and can be set up in an area where it cannot be reached. Furthermore, PIR sensors can be programed to only detect movement at a certain distance. Since we do not want the sensor to go off when there is movement far away, we want to restrict it only two or three feet.

Motion sensors tend to not be picky when it comes to what will set it off. Birds, animals, and even large insects can set of a motion sensor. Since we only want HOMES to sense motion when a human approaches the door we will want to program the PIR so that it only detects movement of large proportions. In this way we will eliminate the possibility of the homeowner receiving notifications to their phone whenever an animal crosses in front of the door. The PIR sensor will be physically connected to the Arduino microcontroller so there will be no need for wireless communication between the two.

7.1.3 Communication

There are two sections of our project that need wireless communication. One is the wearables, and the other is the entry point modules. As was discussed in the summary of the research on communications we will be using different wireless communications for both modules. For wearables we will be using Bluetooth. More specifically, we will be using the LightBlue Bean, which is a Bluetooth module that is powered by a watch battery and is small enough to be a keychain. For the external entry points we will be using Wi-Fi to communicate with the main board. We will be using the Electric Imp mentioned in the Wi-Fi research section for this communication. The Electric Imp will be prototyped on an imp breakout. At the same time as development on using the TI CC3200MOD chip for our project will be ongoing due to its low price (free samples from TI), and its powerful yet power efficient ARM processor it will be a great replacement for the imp but the lack of community/hobbyist use of it makes it difficult to assess its feasibility without hands on testing. The Electric Imp will be powered by the PCB discussed in the external entry point modules section and will only receive power if a switch is on indicating the door or window has been opened. For Wi-Fi we will be using an 802.11b/g/n dongle on the Raspberry Pi 2.

7.1.4 Camera

In the research part of this paper we discussed several options for cameras. These options were the Raspberry Pi camera module, the Raspberry Pi NOiR camera module, and a web cam. As was discussed earlier all three of these options had advantages and disadvantages and a number of factors need to be considered including cost, efficiency, and mobility. We decided to use a webcam because it has more flexibility than the Raspberry Pi modules.

The biggest advantage of using a webcam is the fact that it has video and audio capabilities. Neither of the Raspberry Pi modules have this ability. This allows us to do video streaming and video messages using the same component without the hassle of syncing a video with audio. Also a webcam can be easily connected to the Raspberry Pi using the USB port and can then be placed almost anywhere with relative ease. Lastly, a webcam can be cheaper if purchased from certain websites like Amazon. Overall, the webcam felt like a better option on all fronts.

We plan to take apart the Logitech C310 to the bare minimum of the camera and put it next to the LCD touch screen. This way the camera will be a part of the housing for the Raspberry Pi, the LCD screen, the fingerprint scanner, and the RFID receiver. Also this way the camera will be in an optimal position to take a picture of any guests that come within two or three feet of the motion sensor.

7.1.5 Light

We discussed several options for lighting in the research part of this paper. The decision was largely impacted by what camera was chosen. Since we decided to use a webcam as our camera we can eliminate infrared LEDs since we won't be using an infrared camera. Instead we will be using a regular porch light. This is the most common lighting apparatus and is therefore easy to attach to a motion sensor. It is also more price efficient compared to regular LEDs. Even though LEDs last longer, they are not worth the cost in this case.

We will be using a porch light purchased from amazon that runs on a 60 watt bulb. This will be enough light for the camera to take a good picture and for facial recognition to work. It will also be enough light for the homeowner to see who the guest is at the door if it is dark out. The light will only come on if the user turns it on via the application or if it is dark and the PIR sensor has detected motion.

7.1.6 External Entry Point Modules

The entry point modules will be using a reed switch. This switch will break the circuit when a magnet comes within a small distance. It will then send a signal to the Raspberry Pi via Wi-Fi. Then the Raspberry Pi will send a notification to the homeowner's phone via the mobile application and alert them that an external entry point has been opened. In order to implement this we will put a reed switch on a small PCB powered by a battery in series with a resistor. This will be mounted on the doorframe or window frame. Then a magnet will be attached to the moving part of the window or door and will therefore alert the user if the door or window has been opened (thus breaking the circuit). The circuit is shown in figure 13 was drawn using eagle. All that is left is to add a Bluetooth module.

This circuit was then tested in Multisim and is shown in figure 14. The output of the voltage regulator will be fed into the Wi-Fi module that needs 3.3VDC. This voltage will be supplied by the regulator and is shown on the multi-meter. Since there isn't a reed switch in Multisim we simulated it using a regular switch. When the switch is open the magnet is not within range, the circuit is broken and the Wi-Fi module is not powered. When the switch is shut the magnet is within range, the circuit is connected and the Wi-Fi module is powered and sends a signal to the Raspberry Pi.

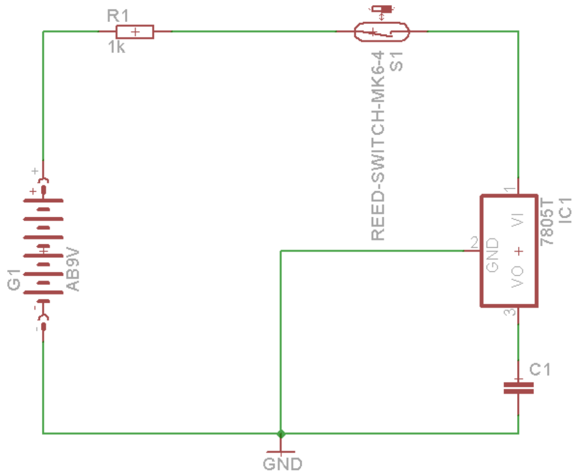


Figure 13a Eagle Schematic

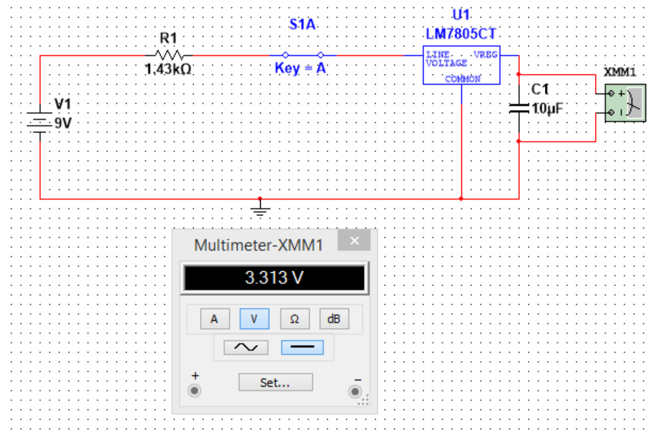


Figure 13b Multisim Schematic

7.1.7 Locking Mechanism

We decided to use an electric strike for our project purposes mainly due to budget constraints. Both the electric strike and the electric lock would be good and simple to use for our project since all either would need is a pin being set from low to high to operate the mechanism that sends the voltage through the strike or activates the motor in the lock. Thus the choice was one of the battery power, security and elegance of the electric lock versus the low cost and ease of set up of the electric strike. Ultimately we ended up using the electric strike since the purposes of our project is to make the entry control system and not necessarily a method of entry (i.e. lock or strike) and the extra cost would not be justified.

7.1.8 Power Supply

As discussed above we decided to use a Raspberry Pi as our single board computer. The Raspberry Pi uses 5V and 2.2A. This can be accomplished through a wall adapter power supply that outputs this amount from the 120VAC 60Hz power from a wall outlet. This will be how we supply power to the main board and through it the LCD screen, the fingerprint scanner, the camera, and the Bluetooth receiver. Also the electronic strike lock that requires 12V will be powered by this PCB.

The only down side to using this power supply is if the power goes out then the system will not work. Because of this we decided to make a backup system. This backup system will supply the Raspberry Pi with power from batteries when and if the power from the wall adapter power supply goes out. Then when the power comes back it will stop drawing power from the batteries and continue with the power from the wall adapter. In this way we can be sure that even if the power supply goes out the system will still work. Since the Raspberry Pi will be doing a lot of processing it will not be very long before the batteries run out. However, this can be easily remedied by changing the batteries. If the Raspberry Pi is using battery power and the batteries are dying then the homeowner will receive a notification via the mobile application that the batteries need to be changed or the power needs to be restored.

In order to make the PCB described above, we will need a voltage regulator. We want the output of the regulator to be 5VDC and 2.2A. The regulator that can accomplish this is the LM4805. We will use this regulator to switch between the power supply from the wall and the battery. The regulator takes a 12VDC to output 5VDC. This means our battery and wall adapter must output 12VDC. This PBC is pictured in figure 14, which was built in Multisim.

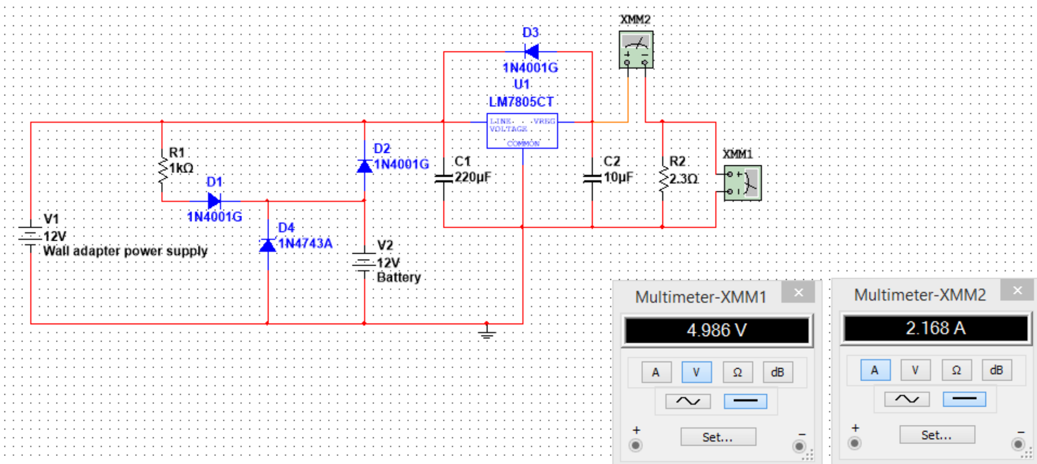


Figure 14 Battery Backup Circuit

As can be seen by the multimeter, the output of the regulator is 5VDC. If we disconnect the 12V wall adapter power supply we still get a 5VDC output from the regulator. This is shown in figure 15.

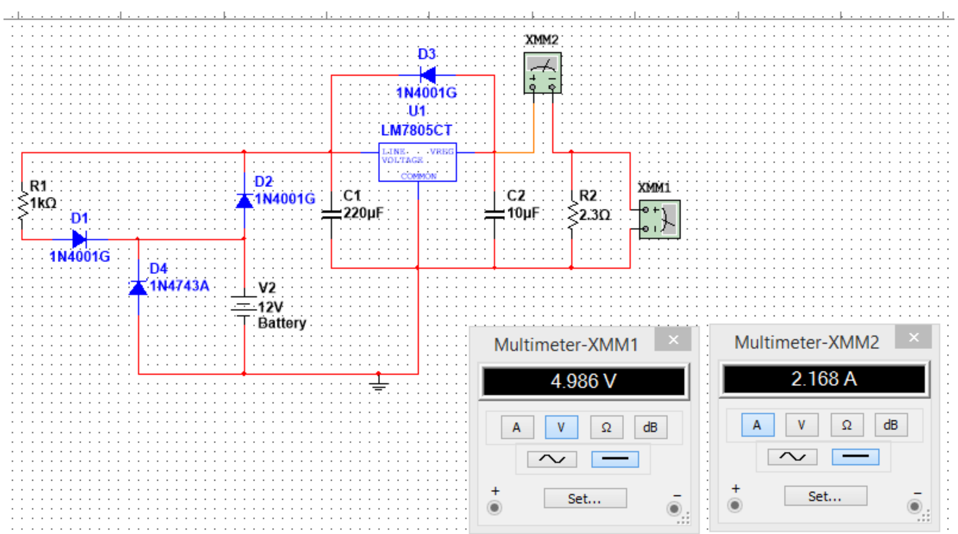


Figure 15 Battery Backup Circuit With No Power Supply

Also removing the battery has the same effect, the regulator still outputs 5VDC. This can be seen in figure 16.

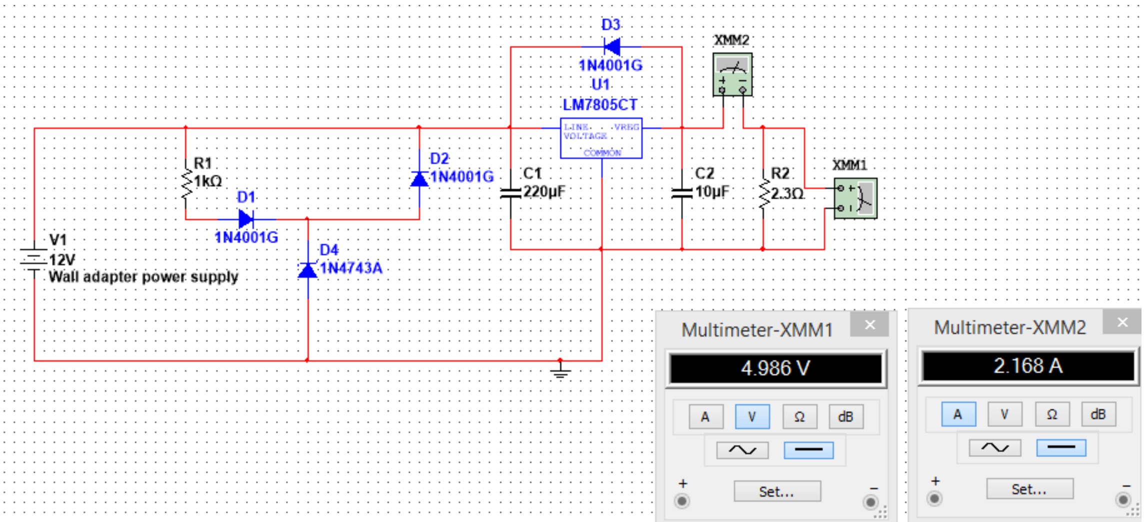


Figure 16 Battery Backup Circuit With No Battery

As for the battery we will be using a 12V lithium ion battery. We choose a lithium ion battery because it is rechargeable. The circuit in figure 16 will charge the battery while there is a power supply. Then when the power supply goes out the battery begins to supply power to the Raspberry Pi. It takes about 12 hours to fully charge a dead lead acid battery and it will probably only last a few hours with all the processing the Raspberry Pi will be doing. Nevertheless, as this is for emergency power outages, the above battery backup circuit will be sufficient.

7.1.9 Fingerprint Scanner

Upon looking further into building a fingerprint scanner from scratch we decided that it was within budget and easier to buy one instead. Therefore we are buying an optical scanner that will be connected to the Raspberry Pi via pins. The pin output for the fingerprint scanner is shown in figure 17.

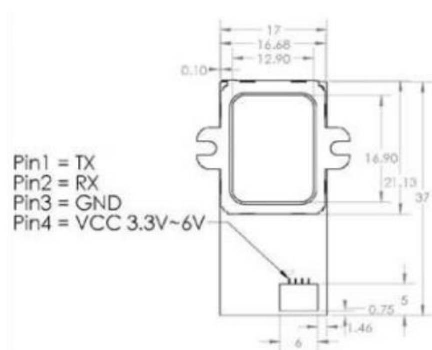


Figure 17 Fingerprint Scanner Pins
With permission from Sparkfun

The fingerprint scanner will automatically detect if someone has placed a finger on it and will take a picture of the fingerprint by lighting it up with LEDs. It will then compare certain points of the fingerprint to the fingerprints in the database and decide whether the user is able to gain access. That database will have two different types of users, those who are able to enter and those who are not. If someone who is not given permission to enter tries to use the fingerprint scanner then the system will not let them try again. However if there is no match for the fingerprint in the database then the guest will have two more tries to scan their finger. If both of these attempts still fail then the system will not let them try a fourth time.

7.1.10 Wearables

As for the wearables we will be using Bluetooth to communicate with the Raspberry Pi. More specifically we will be using the LightBlue Bean. It is low energy Bluetooth Arduino microcontroller as discussed in the research section above. The BLE (Bluetooth low energy) communication sends data out in pulses which is ideal for our project since all we need is a pulse to the receiver telling the Raspberry Pi that a wearable is near enough to unlock the door.

The LightBlue Bean is a small microcontroller that will be powered by a small watch battery shown in figure 30. It will need to be housed by something in order to make it visually agreeable and also protect it from external elements. In order to accomplish this we will be 3D printing a small housing for the board. This will be done for both the human wearables and the pet collar. The end product will look similar to a car remote.

7.1.11 LCD Touch Screen

The LCD choice was an easier one we knew we wanted a Touch screen capable LCD, and since it is intended for outdoor use we chose a resistive touchscreen instead of a capacitive screen due to its ruggedness and reliability. Once we compared the available screens for the Raspberry Pi vs. the BeagleBone it was clear that the PiTFT screens were better suited for our purposes due to its use of less pins and its breakout for the unused Pi pins. So the last choice we had to make was size and resolution, since we wanted something big enough to be interacted with but not so big that it be out of our budget we settled on the 3.5” 480x320 PiTFT from Adafruit.

The touch screen will display the user interfaced discussed in the software design details. It will allow users to choose from options and it will show them the status of the option they choose. It will be covered in a clear plastic film to make it water resistant. It will also be housed in a 3D printed housing with the camera, the PIR sensor, fingerprint scanner, and the Arduino microcontroller.

7.1.12 RFID Module

For the RFID Module we decided to go with Sparkfun's ID series module, more specifically the 3DLA version due to its small size and low cost. In comparison to the other modules we were considering this one doesn't write to the RFID card, or read and write NFC but since we have numerous forms of authentication we decided that this would be sufficient for our needs.

7.1.13 3D Printing

For our prototype we will probably be using 3D printed housing to provide a custom fit clean design, we currently are expecting to rely on the Innovation's 3D printer and if it is fixed one of our group members will have access to one at home as well. Otherwise there are two more 3D printers on campus, one being at Tech Commons and in the Business Administration building. If all else fails makexyz.com is a website where you can have local 3D printer owners print things for you from their own printers.

Cost wise it will be hard to estimate our total cost from printing due to it usually being in dollars per centimeters cubed or in some instances total printing time. From research in the cost of 3D printing the average material which either PLA or ABS costs from $0.20/cm3 to over $1/cm3 depending on the plastics color and property. If we were to do 3D on our own printer 1 kg of material goes for about $20-$45 depending on quality, properties, and color. Although it is not a direct measurement a kilogram of material should be able to produce from 500-900 cm3 of printed material. In the testing of a Makerbot 2 it was show that one kilogram of material should be able to produce around 400 normal sized chess pieces, thus for our uses I don't estimate using more than one kilogram roll.

7.1.14 Pet Door

As was discussed in the research part of this paper, HOMES will include a pet door that will lock and unlock using a sliding metal bar and will only unlock when a pet wearing a collar with a special transmitter comes within two feet.

The transmitter we will be using is Bluetooth. We choose Bluetooth because it is already being used for our human wearables so it made sense to use it for the pet wearable. This way only one communication receiver is needed for both types of wearables. For the Bluetooth transmitter we will be using the same module as for the human wearable, which is the LightBlue Bean. It is well priced and highly efficient. Also the LightBlue Bean offers a module that comes with a watch battery to supply power to the Bluetooth transmitter so we won't need to worry about powering it.

To power the small motor we will use a battery. We will connect the battery to a voltage regulator, which will output the correct amount of voltage needed to the motor. Also the board will have the LightBlue Bean attached for wireless communication to the Raspberry Pi.

7.1.15 Summary

The design project is heavily depended on the exact entry method we will use in the final project, but the diagram in figure 18 shows a general layout of the different modules and wiring assuming an electric door lock is used. In this diagram the Touch LCD screen and all the sensors are place in a 3D printed enclosure outside the door and wired through the lock to the Raspberry Pi that will somewhere inside. The Raspberry Pi would get power from the inside, and would also have control of the pet door via a hardwired connection, Bluetooth or Wi-Fi.

If the electric lock doesn't work out we can still use an electric strike or deadbolt opening servo in a similar manner by drilling the wires through an existing deadbolt or door handle. The electric strike would require an extra module to control the higher voltage it would require, and the deadbolt opening servo mechanism would require its own module over the preinstalled deadbolt.

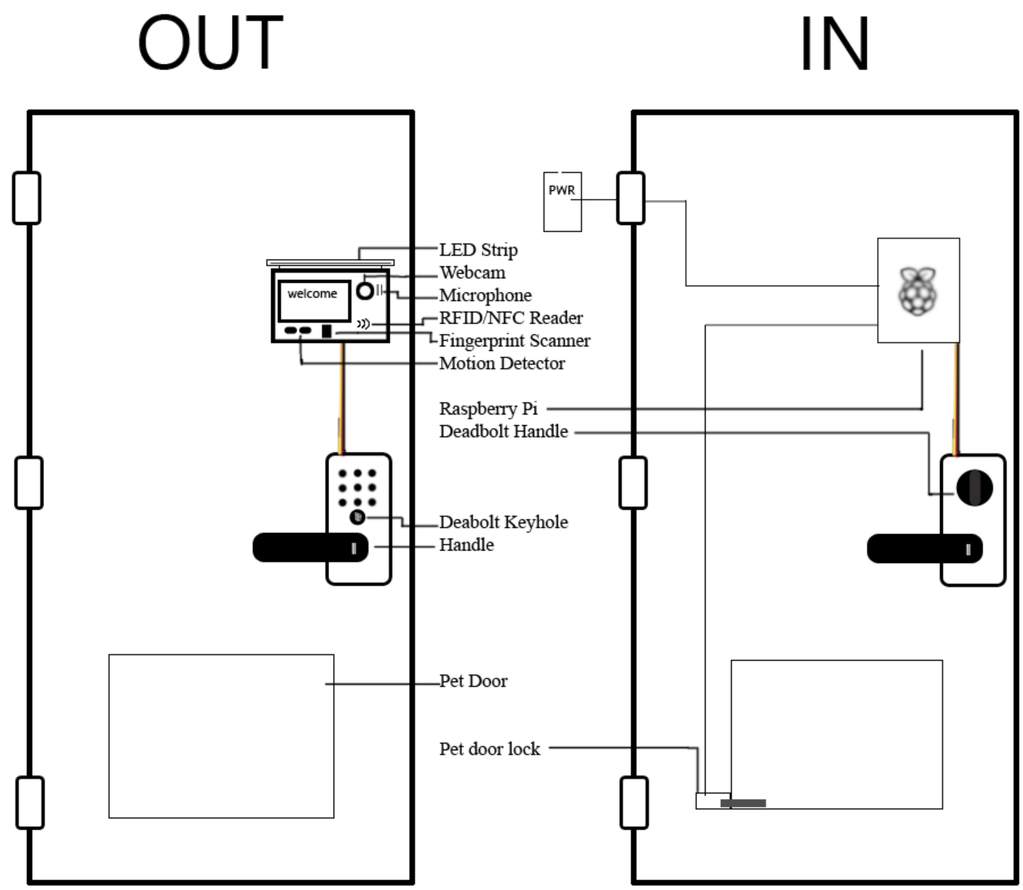


Figure 18 Hardware System Diagram

In summary of all the hardware systems we will be using in HOMES, the front door will have several ways of entering based mostly on hardware. These hardware options are via a wearable, fingerprint and facial recognition. There are other ways of entering which are mostly software and will be discussed in the software design details summary. The main computer will be a Raspberry Pi that will be powered via a power supply PCB. This power PCB will have a battery backup system in case the power goes out. The PCB will also charge the battery when the power is on to give the homeowner the maximum usage out of the life of the battery. Further there will be a locking mechanism that will lock and unlock the door based on a signal it receives from the Raspberry Pi. There will also be a way to sense if the door is locked or not so the homeowner can check if the door is locked. Also we will be making external entry point modules that will be small and battery powered and will use Wi-Fi and a reed switch to communicate with the Raspberry Pi and send a signal when it has been opened. There will be two RF communications available for users, Bluetooth and RFID.

7.2 Software Design Details

In the subsequent sections we will discuss the design decisions for the software portion of our project. We will explain the why a decision was made and how we plan to implement it in HOMES. There are five major software components: the mobile application, the web application, facial recognition, user interface, server, and client. We will discuss each of these modules in detail and talk about our plans for implementing them in our final project.

7.2.1 Mobile Application

There are four components in developing a mobile application for Android:
1. Activity
2. Service
3. Content Provider
4. Broadcast Receiver

An Activity in the android application is what the user interfaces with on the screen; it's what's going on in the foreground, it provides a window in which users can interact with in order to do something, such as dial a phone number, take a photo, send an email, or view a map. Each activity can then start another activity in order to perform different actions; for instance, a browser window opening up a map to view a location, your email activating your calendar to save a date, or your file manager opening loading up Adobe to view PDF files.

Services works differently from activities, a service is what's going on in the background while you are using the activity or interface. An example of services would be listening to music while browsing the web, downloading files while messaging a friend, or update apps while watching videos. Its job is to do work or complete tasks without interrupting or interfering with what an activity is doing.

Content providers manage data that can be shared through apps. They provide a bridge connection for when apps need access to use files or data such as images, calendar events, or contact information. Content providers are important for reading and writing unshared data for an app as well, as this data can be stored in an SQLite database, on the web, or any storage location your app can access.

Broadcast receiver responds to the broadcast announcements by system and the apps, otherwise known as notifications. For example, an announcement that the system's battery is low, a screenshot has been captured, or that a file or some data has finish downloading. The system also delivers various broadcasts that are not visible to the user like called system events, such as when the system boots up or the device starts charging. A broadcast is a message that any app can receive therefore an app may use this information to initiate a task when say your phone starts charging or your battery is too low. An example of an application's broadcast would be announcing that an update is available or needed, or any other task initiated by the app has completed. This flow is shown in figure 19 below.

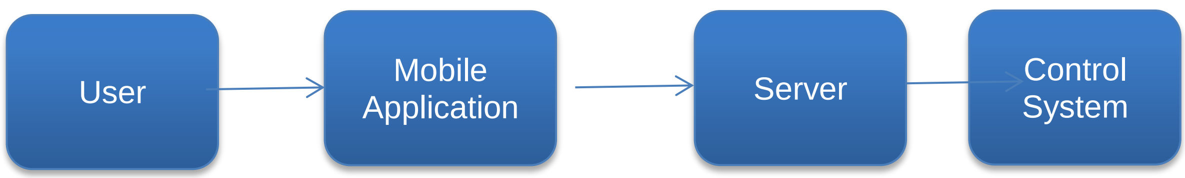


Figure 19 Mobile Application Flow

7.2.2 Web Application

Similar to how a user can control home automation features using a mobile app, a user can also control the same features with the click of a mouse. The website is meant to give the homeowner a more in depth control over their system. The website unlike the mobile app is designed for the homeowner exclusively, controlling the app's functionality and adding members into the database etc. (figure 20) shows a block diagram of how the user and web application interact with the system.

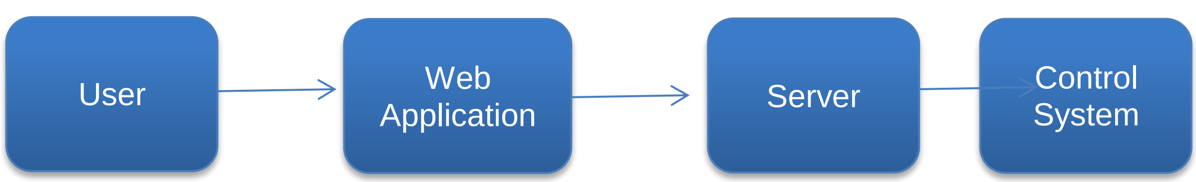


Figure 20 Web Application Flow

7.2.2.1 Login

In order for the website and mobile application to be accessible to an admin it is a requirement for the user to log into the system in a secure fashion (Figure 21). With the use of login credentials the user or homeowner is authorized to control aspects of HOMES not applicable to other users under the account. The user must register an email username, and password that complies with the password requirement set forth. Once the user has set the password, it is encrypted and stored on our database where it will decrypted and compared to the user's input to verify the password and granting access. If the user enters a password that does not match we will deny the user access to the system and prompt the user to enter the password again. When a user enters an incorrect password three consecutive times, the system will lock the user out for a certain time period, causing a delay between the time the user is denied access and the time the user is allowed to re-enter a password which will protect the system against a brute force approach from unauthorized users. The specified delay will be set to a reasonable value, 30 seconds for example, but will then increment for every third failed attempt e.g. 30sec 60sec 90sec. This algorithm will increment in 30 seconds for up to three lockouts, after the third lock out the delay will jump from 90 seconds to 30 minutes and will increment by 30 minutes thereafter. If the user has forgotten their password to the system there will be a method to safely reset the password.

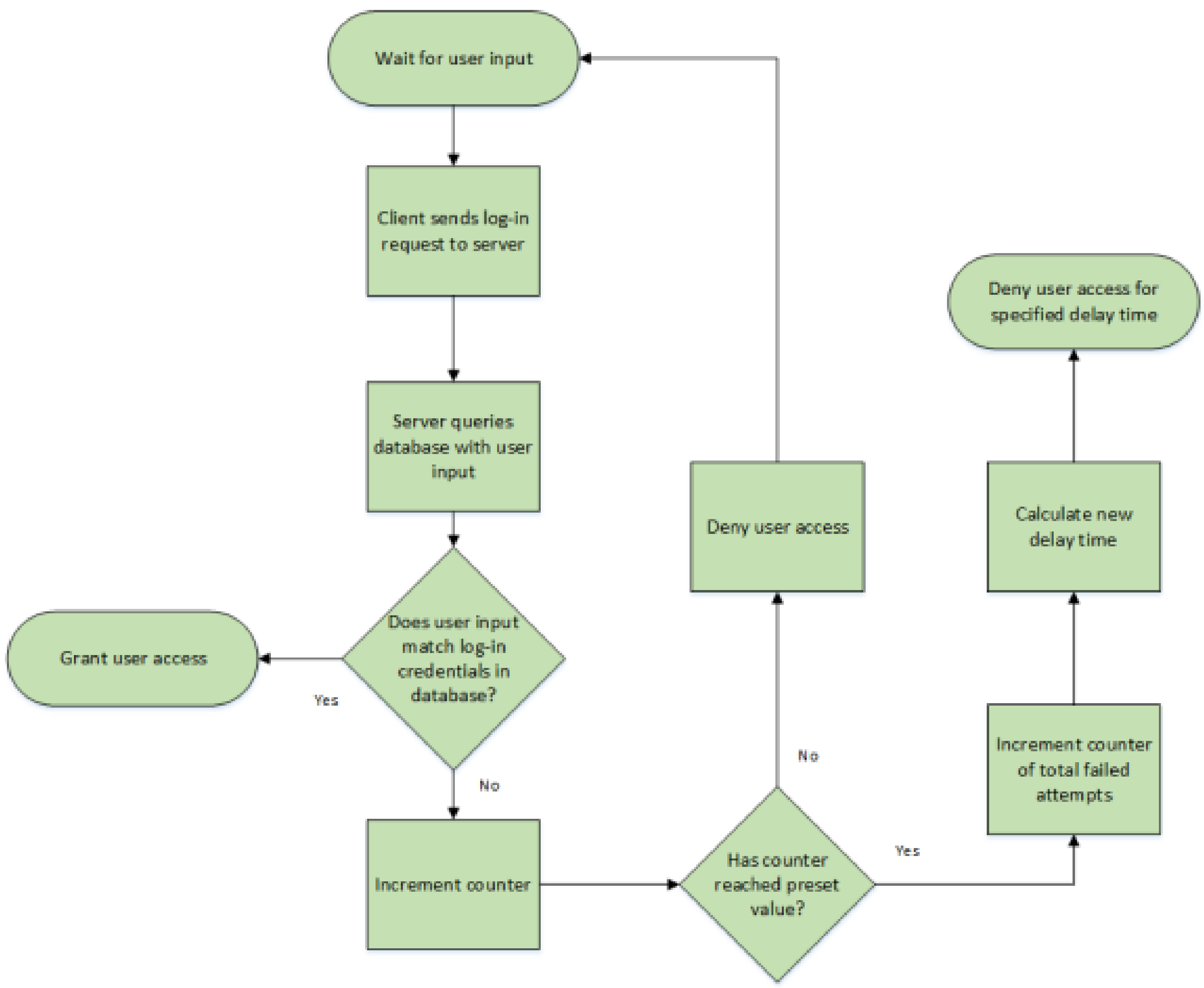


Figure 21 User Login Flow Chart

7.2.3 Facial Recognition

To implement facial recognition we will first have a phone or web application where the user will be asked to register their facial data with perhaps 5-10 pictures. Once a face database is created we will keep and update it as needed as well as create a separate. We will also need to implement a Cascade Classifier which OpenCV's CascadeClassifier() function can handle once we have a XML with the results of training with a database of faces and non-faces. With the Cascade Classifier setup we read each frame of the video as a grayscale image and apply the OpenCV's detectMultiScale() function to detect all the faces present in the image. With the detected face we will now convert it to an compare it to the images in our database using OpenCV FaceRecognizer class and using either Eigenfaces, Fisherfaces, or Local Binary Patterns depending on the accuracy and speed provided by each method which will be determined during our testing.

As with the fingerprint scan there will be two types of users stored in the facial recognition database, guests who have permission to enter and those who do not. If a guest tries to enter the home and they do not have permission then the system will effectively lock them out and not let them try to enter again. However if there was no match found in the database then the guest will be given two more tries. If neither of these tries results in the guest being found in the database then they will not be given a fourth attempt.

7.2.4 LCD User Interface

The main software running on single board computer will be an application written probably in C++ or Python and will be where a user will be able interact with the system. Figure 22 shows this process the entire process. Once the system is on it will be on screen 1 until any input is received. If a user touches the about option the screen will then display screen 2 with all the information about the software and a button to return to screen 1. If a user wants to notify the owner about his presence at door he can ring the doorbell which the displays screen 3 and sends the owner a notification on his phone and the returns the application back to screen 1. If the user touches to video call screen 4 is displayed and the owner receives a notification on the mobile application, if he chooses rejects the call screen 6 is displayed and the user is returned to screen 1, if the call fails the same thing happens with screen 7 displayed, but if the owner chooses to accept the call screen 5 is displayed until the connection has been made and screen 8 is brought up with the video stream, once the call ends the user is returned to screen 1. If the user wants to gain entry via facial recognition screen 9 pops up with the video from the webcam and if the user matches a registered user the door is unlocked for him and screen 10 is displayed otherwise screen 11 is displayed. The last option a user can select is Settings which then leads to screen 12 where the user must provide the access pin in order to view and change the settings, if that is successful screen 13 appears and the user can change the settings he wishes.

Figure 22 User Interface for LCD

Besides these displayed options the system can be depending on which other authentication technologies we implement scanning for pre connected Bluetooth devices as to automatically being able to open the door when the owner is near, or opening the pet door if the Bluetooth device is registered to a pet. It can also be running a RFID/NFC scanner that the user can just scan their card or fob and be granted entry without having to interact with the screen. It can also respond to the use of the fingerprint scanner and verifying if the user is registered and granting entry. All these features don't necessarily need the software to display anything but it can be possible to display something like screen 10 or 11 to confirm if the authentication method was successful or not..

7.2.5 Server

For the backend to our project we will be using an amazon EC2 instance hosting a Node.JS server which will be running our web application, and will have a RESTFUL API in order to be easily accessible to the Android application or the Raspberry Pi. The Pi itself will also be running a Node server so the window modules will be able to communicate directly with the Pi.

7.2.6 Client

For the frontend of our project we will be using AngularJS to run the web application. Angular provides an easy and efficient way of communicating between the logic (the controller) of the client side code and the html (the view). Angular is a well-made extension to html that helps display and organizes logic all on the front end. We will also be using bootstrap as our user interface framework. Bootstrap is easy and intuitive and compliments Angular. Further, Bootstrap is a mobile first frame work which is unique and makes html views much easier to deal with since it is easier to go from a mobile to a computer size page than a computer size to mobile size.

7.2.7 Summary

The flowchart shown in figure 36 illustrates the software flow of HOMES. We will have an android application and a web application that the homeowner can use to view the status of their home and to see who is at their door. They can also use these applications to receive notifications of when a door or window is opened and view logs. Similarly these applications can be used to view a video message a guest left for the homeowner while they were out. Lastly they can use these applications to unlock or lock the front door. For the applications we will have a database on mongoDB that will hold all the information. We will be using node for the web development on the backend and angular with bootstrap for web development on the front end.

The system that handles unlock and lock events has five major ways of entry. Three of these were mentioned in the hardware design section as a wearable, a fingerprint scan and facial recognition. The other two ways are mentioned above as via the mobile and web application. When any of these ways is completed then the Raspberry Pi will send a signal to the unlocking or locking mechanism. The system will also handle the racial recognition and its database as well as the fingerprint scanner and its database. It will also handle signals from the external entry points when one has been opened in order to send a signal to the mobile and web application to alert the homeowner.

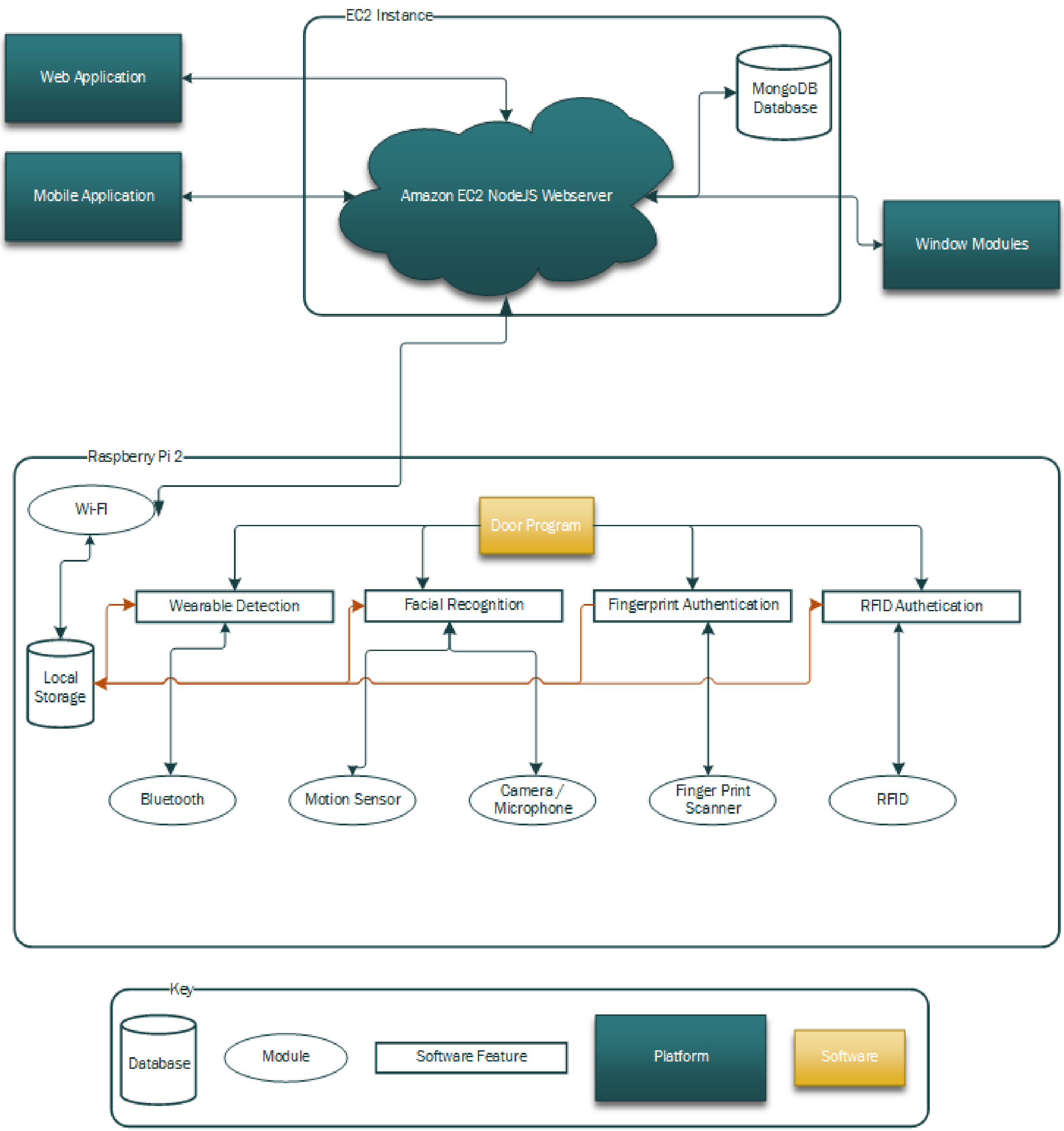


Figure 23 Software Flow Chart

8.0 Project Prototype Construction and Coding

8.1 Parts Acquisition and BOM

The following sections are the bill of materials for the major modules in our project. Each module has a breakdown of the parts needed, the manufacturer, and the price.

8.1.1 Power

This section lists the parts that are needed to build the power supply printed circuit board that will give power to the Raspberry Pi and the electronic strike lock. The Raspberry Pi will then provide power to the camera, LCD screen, fingerprint scanner, and Bluetooth receiver. Table 4 shows the parts needed.

Table 4: Power BOM

Quantity	Description	RefDes	Manufacturer	Unit Price	Total Price
3	DIODE, 1N4001G	D1, D2, D3	ON Semiconductor	0.19	0.57
1	ZENER, 1N4743A	D4	Fair Child	0.19	0.19
1	VOLTAGE_REGULATOR, LM7805CT	U1	Fair Child	0.19	0.19
1	A23 Battery	V2	Energizer	0.19	0.19
				Total:	1.14

8.1.2 Motion Sensor

This bill of materials (table 5) covers the PIR sensor we want to integrate into our system to detect if a guest has entered within three feet of the front door. The motion sensor will be connected to the Pi.

Table 5: Motion Sensor BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	1 PIR (motion) sensor	Adafruit	9.95	9.95
			Total:	9.95

8.1.3 Camera

As was discussed in the hardware design details we choose to use a webcam for the camera because it can be easily taken apart and therefore placed in a small area. Also the webcam that we choose has enough pixels to easily perform facial recognition. Table 6 shows the bill of materials for the camera.

Table 6 Camera BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	Logitech HD Webcam C310	Logitech	32.95	32.95
			Total:	32.95

8.1.4 Single Board Computer

The single board computer is the most important part of HOMES. We choose the Raspberry Pi for our single board computer because it has a lot of processing power and a large amount of memory. The following table (table 7) shows the price of the Pi.

Table 7 Single Board Computer BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	Raspberry pi 2	Raspberry Pi	40	40
			Total:	40

8.1.5 LCD Touch Screen

The LCD touchscreen will be used to display options and status to the guest. The following bill of materials in table 8 show the part we chose.

Table 8 LCD Touchscreen BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	PiTFT 480x320 Touch LCD Screen	Adafruit	45	45
			Total:	45

8.1.6 Light

In this bill of materials (table 9), the parts needed for the porch light are detailed. The light will only turn on if the motion sensor detects motion and it is to dark outside to get a good picture.

Table 9 Light BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	Jelly Jar Outdoor Down Light	Design House	8.46	8.46
1	GE Lighting 41028 60-Watt A19, Soft White	GE Lighting	1.6225	1.6225
			Total:	10.0825

8.1.7 External Entry Point Modules

Table 10 shows the bill of materials for the external entry point printed circuit board. The board as discussed in the design details section will send a message to the webserver when the door or window has been opened by using a reed switch.

Table 10 External Entry Point Module BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	9V Battery	Duracell	2.125	2.125
1	1.43K resistor	Sparkfun	0.15	0.15
1	Reed Switch	Sparkfun	1.95	1.95
1	Neodymium Magnets 1/2 x 1/8 inch Disc N48	Emovendo	0.586	0.586
1	Wi-Fi modules	Sparkfun	29.95	29.95
1	VOLTAGE_REGULATOR, LM7805CT	Fair Child	0.69	0.69
			Total:	35.451

8.1.8 Wearables

We will be using a LightBlue Bean Bluetooth module to handle communication from the wearable, both human and pet. We will also be 3D printing a case for it so it can be semi-weather proof. Table 11 shows the bill of materials for this module.

Table 11 Wearable BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	LightBlue Bean	PunchThrough	30	30
1	3D print housing	n/a	5	5
			Total:	35

8.1.9 Lock and Door

The following bill of materials in table 12 shows the parts we will need for the door and for the locking mechanism. We will be using an electric strike lock as the lock and we will be building a small door replica out of plywood.

Table 12 Lock and Door BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	Seco-Larm SK-990BQ Wood Electric Door Strike	Seco-Larm	27.49	27.49
1	11/32 in. x 4 ft. x 8 ft. Rtd Southern Yellow Pine Plywood Sheathing	Home Depot	15.72	15.72
1	#11-1/2 x 2 in. 6D Bright Steel Smooth Shank Common Nails (1 lb.-Pack)	Home Depot	3.47	3.47
1	12 oz. Gloss Black General Purpose Spray Paint	Home Depot	3.87	3.87
1	Honeywell 8108001 Scroll Entry Door Lever, Polished Brass	Honeywell	14.66	14.66
1	Copper Creek DB2410PB Standard Duty Single Cylinder Deadbolt in PB Finish	Copper Creek	2.7	2.7
			Total:	67.91

8.1.10 Fingerprint Scanner

The fingerprint scanner is yet another way a guest or resident can enter the house through the front door. The bill of materials in table 13 show the exact scanner we choose as well as the manufacturer and price.

Table 13 Fingerprint Scanner BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	Fingerprint Scanner - 5V TTL (GT-511C1R)	Sparkfun	31.95	31.95
			Total:	31.95

8.1.11 RGB LED

The RGB LED will be used to display the status of the system to the guest. It will be used to give quick feedback so they can be sure that the system is doing something. RGB LEDs are fairly cheap as can be seen from the bill of materials in table 14.

Table 14 RGB LED BOM

Quantity	Description	Manufacturer	Unit Price	Total Price
1	LED - RGB Clear Common Cathode	Sparkfun	1.95	1.95
			Total:	1.95

8.2 Printed Circuit Board Vendor and Assembly

For our PCB prototyping needs the best deal we found was OSH Park with its cheap price of 5 dollars per square inch with shipping included per three two layer boards or 10 dollars per square inch with shipping included per three four layer boards. Since we hope to make all our designs compact and efficient we should not be spending more than $10 - $15 on each different custom PCB.

Some other competition from Chinese manufacturers exist but for our low cost, low board count, and tight schedule needs we would are not able to beat the convenience and price plus shipping of OSH Park.

9.0 Project Prototype Testing

9.1 Hardware Testing

9.1.1 Power Supply

Purpose:
To test that the right amount of voltage and current is coming out of the voltage regulator.

Supplies:
- 3 1N4001G diodes
- 1 1N4743A Zener diode
- 1 LM7805CT voltage regulator
- 1 A23 battery

Preparation:
1. Create PCB using schematic in design details section.
2. Plug in AC to DC converter.

Procedure:
1. Verify the expected amount of power is coming from the converter.
2. Measure the voltage and current exiting the regulator and verify it is still 5VDC 2.2A.
3. Disconnect the power from the converter.
4. Measure the voltage and current exiting the regulator and verify it is still 5VDC 2.2A.
5. Reconnect the power from the converter.
6. Disconnect the battery.
7. Measure the voltage and current exiting the regulator and verify it is still 5VDC 2.2A.

Expected Results:
Whether there is a power supply from the AC to DC converter or not there should still be the correct amount of voltage and current exiting the regulator to keep the systems going. The same should be said for whether the battery is connected or not.

9.1.2 Motion Sensor

Purpose:
To test that the motion sensor detects motion detects motion.

Supplies:
- PIR Motion Sensor
- Arduino
- Arduino IDE
- LED
- Jumper Wire

Preparation:
- When the motion detector does not detect any motion, the output is LOW and the Arduino receives no voltage signal. When the sensor detects motion, the output is HIGH and the Arduino receives a voltage signal, which can then trigger another device to turn on, such as an LED we will use for this circuit.
- Pin 1 (Labeled In) is the pin on the PIR which receives the positive DC voltage. The PIR motion sensor needs between 5V-9VDC of power for operation.
- Pin 2 (Labeled Out) is the Output pin of the PIR sensor.
- Pin 3 (Labeled Gnd) is the common or ground pin of the PIR sensor.

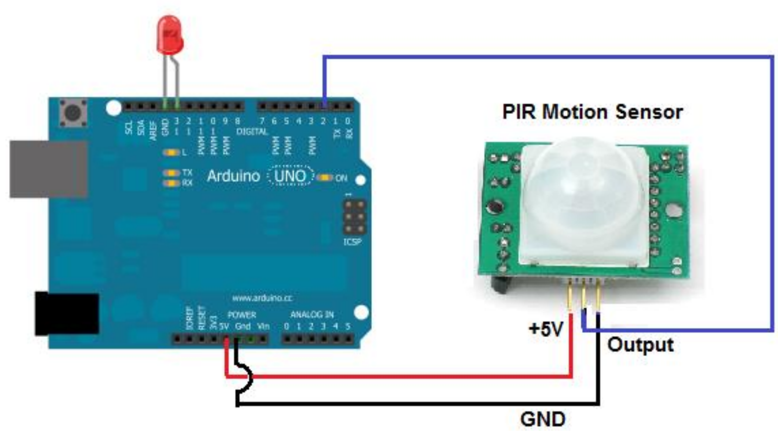


Figure 23 Arduino to PIR Sensor

Besides this sensor, we need an LED, which we will light when motion is detected. The connections needed from the Arduino to the PIR are shown in figure 24 and the pin layout is shown in figure 23.

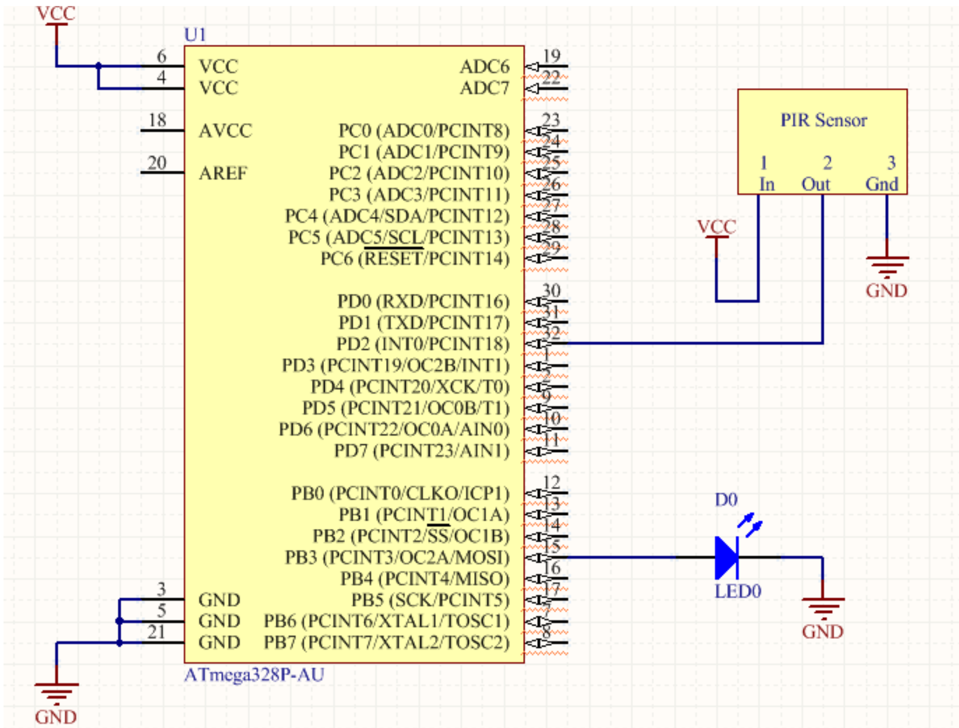


Figure 24 Arduino and PIR Sensor Pins

Procedure:

1. Pin 1 of the motion sensor connects to the 5V DC voltage terminal of the Arduino.
2. Pin 2, the output, connects to the digital pin D3. It is through pin 2 that the Arduino receives output from the motion sensor.
3. Pin 3 connects to the ground (GND) pin of the Arduino.
4. The LED we will light connects pin 13 and ground of the board. The anode (longer lead) connects to pin 13 and the cathode connects to ground. No external resistor is necessary to limit current to the LED, because pin 13 already has built-in resistance to limit current flow.
5. After we connect the USB from the Arduino to the computer, we are ready to write the code that the Arduino board will need uploaded to it so that it knows to light the LED when motion is detected. Figure 25 shows the code.

```
//code for motion sensor circuit
const int ledPin= 13;
const int inputPin= 2;

void setup(){
  pinMode(ledPin, OUTPUT);
  pinMode(inputPin, INPUT);
}

void loop(){
  int value= digitalRead(inputPin);

  if (value == HIGH)
  {
    digitalWrite(ledPin, HIGH);
    delay(60000);
    digitalWrite(ledPin, LOW);
  }
  else
  {
    digitalWrite(ledPin, LOW);
  }
}
```

Figure 25 Motion Sensor Code

6. The first block of code chooses the pin for the LED, which is pin 13 and also chooses the pin for the input pin, which represents the PIR sensor, pin 2.
7. The second block of code declares the LED as output and the input pin as input.
8. The third block of code reads the sensor value of the sensor and assigns it to the integer value.
9. The fourth block of code determines whether the sensor pin is HIGH or LOW. If it is HIGH, then the motion sensor has detected motion. If it is low, the sensor has not detected any motion. If the value is HIGH, it turns the LED on, signaling that motion has, in fact, been detected. The LED stays on for 60000ms, which is equal to 1 minute.
10. This sensor has a sensitivity range up to 20 feet (6 meters) and a 110° x 70° detection range, making it a wide lens detection sensor. This means it can measure 110° vertically (from top to bottom) and 70° horizontally (from left to right). The best way to check its sensitivity is when the circuit is built, try moving around through all of its angles. See at which angles it can detect your movement and at which angles it is not able to detect your movement, meaning you're out of its angle scope.

Expected Results:
When motion is detected by the PIR, its output will go high to 3-5V. When no motion is detected, its output goes low and it gives off practically no voltage. When high you should see it power the LED.

9.1.3 Camera

Purpose:
To test that the camera will take a picture when the motion sensor goes off and when the user chooses to unlock the door via facial recognition and when the user chooses to leave a video message.

Supplies:
- Logitech HD Webcam C310
- Raspberry pi
- Motion sensor
- Power supply

Preparation:
- Make sure the power supply is connected to the power PCB and then to the Raspberry Pi.
- Ensure that the webcam and the motion sensor are both connected properly to the Raspberry Pi.

Procedure:
1. Walk in front of the motion sensor.
2. Verify that the camera took a picture and stored it.
3. Try to unlock the door via facial recognition.
4. Verify that the camera took a picture and stored it.
5. Try and leave a video message.
6. Verify that the camera is recording and stored it.
7. Verify that LCD screen displays a message to user updating them of the status.

Expected Results:
When a guest walks in front of the motion sensor the camera should take a picture and save it to a database to be sent to the homeowner via the app. When a guest tries to open the door via facial recognition the camera should take a picture and save it to the database for comparison. When a guest chooses to leave a video message the camera should record and save to the database to be sent to the homeowner via the app.

9.1.4 Raspberry Pi and LCD

9.1.4.1 Power on Test

Purpose:
To verify if the Raspberry Pi and LCD will turn on.

Supplies:
- Raspberry Pi 2
- PiTFT LCD Resistive touchscreen
- MicroSD with Pi operating system Raspbian
- 5V 2A power source with microUSB head

Preparation:
- Insert MicroSD into the Pi.
- Connect the PiTFT directly to the Pi.

Procedure:
1. With all preparations done, plug the power source into the Raspberry Pi.
2. Wait for boot to start.

Expected Results:
The operating system should begin to boot displaying the sequence on the LCD screen.

9.1.4.2 LCD Screen Touch Test

Purpose:
To verify if the LCD touchscreen can interact with the Pi.

Supplies:
- Raspberry Pi 2
- PiTFT LCD Resistive touchscreen
- MicroSD with Pi operating system Raspbian
- 5V 2A power source with microUSB head

Preparation:
- Pi booted into a UI based operating system.

Procedure:
1. With the system on attempt to open the start menu via touch.
2. Perform gestures such as click and drag selection, or double clicking.

Expected Results:
The system should respond accordingly to the touch input, registering the input at approximately the location it was physically touched, the gestures should also be captured without having to be repeated.

9.1.4.3 Pi Pin Test

Purpose:
To verify if all GPIO pins perform as intended.

Supplies:
- Raspberry Pi 2
- Breadboard
- Wires
- Large LED (so no are resistors necessary)

Preparation:
- Have a program to turn on and off a LED connected to arbitrary GPIO Pins.

Procedure:
1. Wire up the 2 GPIO pins and the LED.
2. Set program to use chosen pins.
3. Repeat for all of the Pi's GPIO pins.
4. Wire the PWR and GND pins to the LED.
5. Repeat for all PWR pins.

Expected Results:
In all cases the Pi should be able to turn the LED on and off using its GPIO pins. Or keep the LED on with its PWR pins.

9.1.6 Light

Purpose:
To test that the light will come on when the motion sensor senses motion.

Supplies:
- Motion sensor
- Photosensor
- Light
- Raspberry pi
- Power supply

Preparation:
- Ensure that the Raspberry Pi is powered and the motion sensor and light are correctly connected.

Procedure:
1. Walk in front of the motion sensor in a dim light setting.
2. Verify the light turns on.
3. Walk in front of the motion sensor in a well-lit setting.
4. Verify the light does not turn on.

Expected Results:
If there is low lighting and the motion sensor goes off then the light should turn on. If there is enough lighting then the light will not turn on whether the motion sensor senses motion or not.

9.1.7 External Entry Point Modules

Purpose:
To test the external entry point modules work correctly and send a signal to the Raspberry Pi when they are opened.

Supplies:
- 9V battery
- 1.43K resistor
- Reed switch
- Neodymium Magnet
- Wi-Fi module
- LM7805CT voltage regulator
- Raspberry pi
- Power supply

Preparation:
- Create the PCB described in the design details section for the module.
- Confirm that the Raspberry Pi is connected to the power supply.

Procedure:
1. Place the PCB with the reed switch on the side of the door or window (the stationary part).
2. Place the magnet on the moving part of the door or window so that when it is opened the magnet will come into close contact with the reed switch.
3. Verify when the magnet is close to the reed switch the voltage regulator outputs 3.3V and 5mA.
4. Verify when the Wi-Fi module is then turned on.
5. Confirm that the Raspberry Pi receives a message.
6. Check that this message is then forwarded to the homeowner via the android application.

Expected Results:
When the magnet is far away from the reed switch (the door or window is closed) the Wi-Fi module is not powered. When the magnet comes into contact with the reed switch (the door or window has been opened) the Wi-Fi module receives power and sends a signal to the Raspberry Pi which then sends a signal to the homeowner’s phone .

9.1.8 Wearables

Purpose:
To test the wearables and the pet collar to make sure they can unlock the front door when the user comes within a certain distance.

Supplies:
- LightBlue Bean
- Fully functional locking mechanism
- Raspberry pi
- Power supply

Preparation:
- Make sure that the LightBlue Bean and the locking mechanism are fully powered.
- Also confirm the Raspberry Pi is powered.

Procedure:
1. Bring the wearable within 3 feet of the door.
2. Door should unlock within 5 seconds.
3. Verify that LCD screen displays a message to user updating them of the status.

Expected Results:
When the wearable comes within three feet of the door it will unlock within 5 seconds.

9.1.9 Lock

9.1.9.1 Lock Control Testing
Purpose:
To verify the ability of the lock to be opened and stay locked.

Supplies:
- Electric Strike.
- Power board with output of 12V DC.

Preparation:
- Wire up the electric strike to the power board.
- Start with power board not connected to outlet.

Procedure:
1. With the strike wired up but not receiving power try to push open the latch.
2. With the strike receiving power try to push open the latch.

Expected Results:
When the strike is not receiving current the latch should not be able to be opened, and when the strike is receiving power the latch should be able to be opened with ease.

9.1.10 Fingerprint Scanner

Purpose:
To test that the fingerprint scanner will recognize a fingerprint that is stored in the database and will unlock the door for a guest that is allowed inside.

Supplies:
- Fingerprint scanner
- Raspberry pi
- Power supply

Preparation:
- Make sure the Raspberry Pi is connected to the power supply PCB and the fingerprint scanner.
- Have a database with approved fingerprints ready for comparison.

Procedure:
1. Place finger on scanner.
2. Verify that it is scanning properly.
3. Verify that it unlocks the door if the fingerprint is in database.
4. Verify that LCD screen displays a message to user updating them of the status of the scan.

Expected Results:
The scanner will photograph the finger and compare it to fingerprints in the database. If there is a match then it will unlock the door. If not then the door will remain locked.

9.1.11 RGB LED
Objective:
To test the functionality of RGB LED.

Supplies:
- Arduino
- Arduino IDE
- RGB Led
- Breadboard
- 270Ω Resistors (3) (red, purple, brown)
- Jumper Wire

Preparation:

- The RGB LED has four leads, the common negative connection of the LED package is the second lead from the flat side of the LED package. It is also the longest of the four leads. This lead will be connected to ground.
- The red lead is the first lead from the flat side of the LED package and is also the singular lead on the side of the common lead.
- The green lead is the third lead from the flat side of the LED package and is also the longer lead on the other side of the common and
- The blue lead is the fourth lead from the flat side of the LED package and is also the shorter lead on the other side of the common.
- Each LED inside the package requires its own 270Ω resistor to prevent too much current flowing through it. The three positive leads of the LEDs (one red, one green and one blue) are connected to Arduino output pins using these resistors. These connections are shown in figure 26 and the pin diagram shown in figure 27.

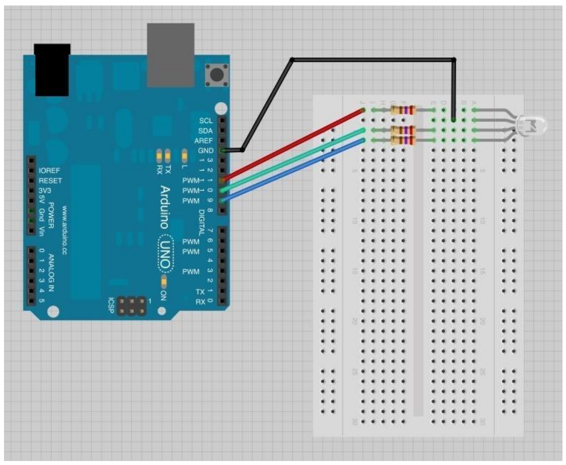


Figure 26 Arduino to RGB LED Circuit Connections

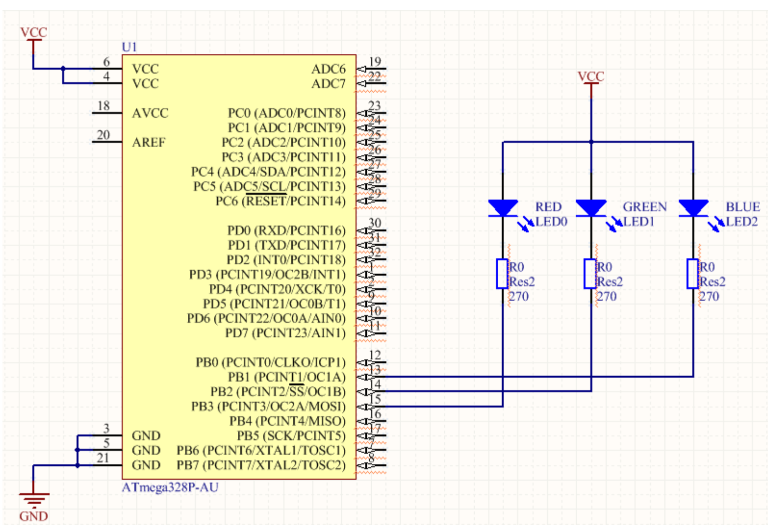


Figure 27 Arduino and RGB LED Pins

Procedure:

1. Connect the common lead to ground on the Arduino and connect the 3 other leads to 3 PWM pins (9, 10, 11) on your Arduino with a resistor between (the value depends on the led).
2. After we connect the USB from the Arduino to the computer, we are ready to write the code that the Arduino board will need uploaded to it so that it knows to light the LED (figure 28 and 29)

```
//Code for rgb led circuit

int redPin = 11;
int greenPin = 10;
int bluePin = 9;

void setup()
{
  pinMode(redPin, OUTPUT);
  pinMode(greenPin, OUTPUT);
  pinMode(bluePin, OUTPUT);
}

void loop()
{
  setColor(255, 0, 0);  // red
  delay(1000);
  setColor(0, 255, 0);  // green
  delay(1000);
  setColor(0, 0, 255);  // blue
  delay(1000);
  setColor(255, 255, 0);  // yellow
  delay(1000);
  setColor(80, 0, 80);  // purple
  delay(1000);
  setColor(0, 255, 255);  // aqua
  delay(1000);
}
```

Figure 28 RGB LED Code

```
//Function
void setColor(int red, int green, int blue)
{
  #ifdef COMMON_ANODE
    red = 255 - red;
    green = 255 - green;
    blue = 255 - blue;
  #endif
  analogWrite(redPin, red);
  analogWrite(greenPin, green);
  analogWrite(bluePin, blue);
}
```

Figure 29 Set Color Function

3. In the first block the, sketch starts by specifying which pins are going to be used for each of the colors.
4. In the second block, the sketch defines the three pins we are using as being outputs.
5. In the fourth block, the "setColor" function takes three arguments, one for the brightness of the red, green and blue LEDs. In each case the number will be in the range 0 to 255, where 0 means off and 255 means maximum brightness. The function then calls "analogWrite" to set the brightness of each LED.

6. The third function is setting the amount of red, green and blue light that we want to display and then pausing for a second before moving on to the next color, the function “delay” takes in microseconds.

Results:
The following test sketch will cycle through the colors red, green, blue, yellow, purple, and aqua. If the red lead is brighter than the other two, then use a higher ohm resister or adjust the code to make your colors more balanced, for example: analogWrite(RED_PIN, redIntensity); to analogWrite(RED_PIN, redIntensity/3);

9.1.12 Photo Cell

Purpose:
To test functionality.

Supplies:
- Arduino
- Arduino IDE
- Photocell
- Breadboard
- 10kΩ Resistor
- Jumper Wires

Preparation:
- The LDR / Photo-resistor is basically a very simple light sensor that changes its resistance with light, lowering with more light. The LDR isn't very precise but it is good enough to tell the difference between light and shadow, or know if the light in your room is on/off. The connections are shown in figure 30 and the pins are shown in figure 31.

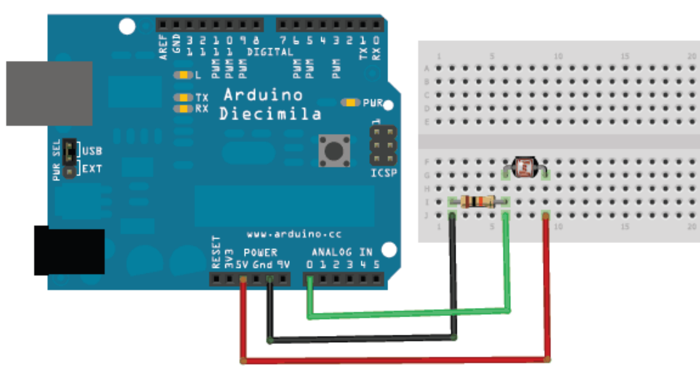


Figure 30 Arduino to Photo-resistor Connections

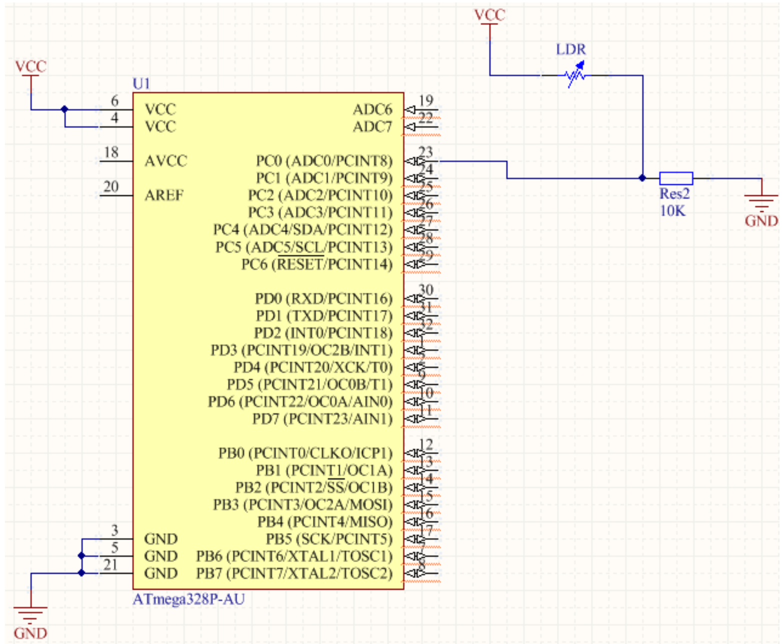


Figure 31 Arduino to Photo-resistor Pins

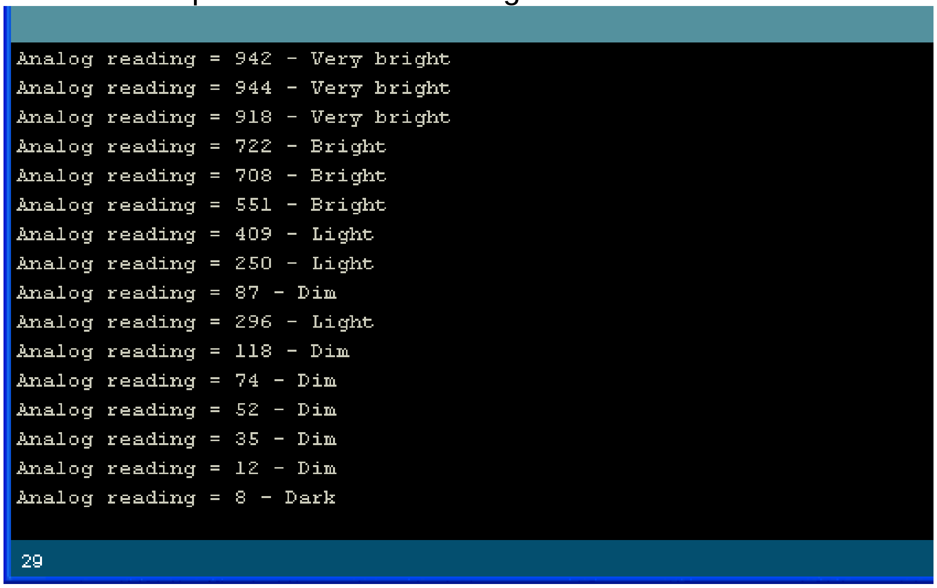
Procedure:

1. Connect one end of the photocell to 5V, the other end to Analog 0.
2. Then connect one end of a 10K resistor from Analog 0 to ground.
3. After we connect the USB from the Arduino to the computer, we are ready to write the code that the Arduino board will need uploaded so we can see the readings (figure 32).

```
// Photocell simple testing sketch.

int photocellPin = 0;     // the cell and 10K pulldown are connected to a0
int photocellReading;     // the analog reading from the analog resistor divider

void setup(void) {
  Serial.begin(9600);
}

void loop(void) {
  photocellReading = analogRead(photocellPin);
  Serial.print("Analog reading = ");
  Serial.print(photocellReading);     // the raw analog reading

  if (photocellReading < 10) {
    Serial.println(" - Dark");
  } else if (photocellReading < 200) {
    Serial.println(" - Dim");
  } else if (photocellReading < 500) {
    Serial.println(" - Light");
  } else if (photocellReading < 800) {
    Serial.println(" - Bright");
  } else {
    Serial.println(" - Very bright");
  }
  delay(1000);
}
```

Figure 32 Photo-cell Testing Code

Expected Results:
The results that are expected are shown in figure 33.



```
Analog reading = 942 - Very bright
Analog reading = 944 - Very bright
Analog reading = 918 - Very bright
Analog reading = 722 - Bright
Analog reading = 708 - Bright
Analog reading = 551 - Bright
Analog reading = 409 - Light
Analog reading = 250 - Light
Analog reading = 87 - Dim
Analog reading = 296 - Light
Analog reading = 118 - Dim
Analog reading = 74 - Dim
Analog reading = 52 - Dim
Analog reading = 35 - Dim
Analog reading = 12 - Dim
Analog reading = 8 - Dark

29
```

Figure 33 Photo-cell Results

9.1.13 RFID Module

9.1.13.1RFID Scan and Response Test

Purpose:
The purpose of this test is to see if the RFID module can properly scan a RFID card.

Supplies:
- ID-3LA RFID reader
- RFID card
- Raspberry Pi 2

Preparation:
- Properly connect the Pi and the RFID module with appropriate power and data cables.
- LED or Beeper connected to pin 10 of RFID reader.

Procedure:
1. With everything set up move RFID card towards the sensor.

Expected Results:
When the card is about an inch away from the sensor the LED or Beeper should activate and the Pi should see the card information via TTL.

9.1.13.2 RFID Case Range Test

Purpose:
The purpose of this test is to see if the RFID module can properly scan a RFID card while inside a 3D printed case.

Supplies:

- ID-3LA RFID reader
- RFID card
- Raspberry Pi 2

Preparation:

- Properly connect the Pi and the RFID module with appropriate power cables.
- Sensor placed inside 3D printed case, or behind 0.5” thick 3D printed sheet.
- LED and/or Beeper connected to pin 10 of RFID reader.

Procedure:

1. With everything set up move RFID card towards the sensor.

Expected Results:
When the card is in close proximity to the sensor it should still be readable, although perhaps at a smaller range than if it were not separated by the material.

9.1.14 Pet Door

Purpose:
To verify that the pet door unlocks when only the pet wearable (collar) comes within two feet and that the door locks after thirty seconds.

Supplies:

- Pet door
- Raspberry pi
- Power supply
- Pet door locking/unlocking mechanism
- Pet wearable

Preparation:

- Make sure the Raspberry Pi is powered correctly.
- Make sure the locking mechanism is powered correctly.

Procedure:

1. Send a test signal from the Raspberry Pi to the locking mechanism.
2. Verify the mechanism received the message.
3. Tell the mechanism to unlock the door.
4. Verify the door is unlocked.
5. Verify that the door automatically locks thirty seconds later.
6. Bring the pet wearable within two feet of the door.

7. Verify that the Raspberry Pi sends a message to the mechanism.
8. Confirm the mechanism received the message.
9. Verify that the door is unlocked.
10. Make sure the door locks thirty seconds later.
11. Make sure that the pet door will not unlock if any wearable approaches, only if the pet wearable.
12. Ensure that the pet wearable does not unlock the main front door.

Expected Results:
When the pet only comes into close proximity with the door, only the pet door will unlock. Then the pet door will lock after a thirty second period.

9.2 Software Testing

9.2.1 Facial Recognition

9.2.1.1 Positive Facial Recognition Test
Purpose:
To verify if the system can detect a known person and act on it.

Supplies:
- Raspberry Pi 2
- Camera
- LCD Screen.
- Wires
- LED

Preparation:
- Have the program on the Pi in facial recognition mode outputting to the LCD screen or via HDMI.
- Have the database of known faces for the system to compare to set up.
- Have the LED wired to the Pi.

Procedure:
1. As a known face walk with in rage of the camera.

Expected Results:
The camera should detect and identify the face displaying an identified square over the face to the LCD. While the camera detects a known face the LED should be kept on. Otherwise it should keep the LED off and not react.

9.2.1.2 Negative Facial Recognition Test
Purpose:
To verify if the system can react to an Unknown face.

Supplies:

- Raspberry Pi 2
- Camera
- LCD Screen.
- Wires
- LED

Preparation:

- Have the program on the Pi in facial recognition mode outputting to the LCD screen or via HDMI.
- Have the database of known faces for the system to compare to set up.
- Have the LED wired to the Pi.

Procedure:

1. As an unknown face walk with in rage of the camera as it is in detect mode.

Expected Results:

The camera should detect the face displaying a square over the face but listing it as unknown to the LCD. While the camera detects an unknown face the LED should be kept on. Otherwise it should keep the LED off and not react. After 30 seconds and no face is recognized the system should exit facial recognition mode.

9.2.2 Android Development & Web Development

9.2.2.1 Unlock Door

Purpose:

To verify the ability of the HOMES APP signal the Raspberry Pi to open the door.

Supplies:

- Android Phone or web browser
- Raspberry Pi
- Electric Strike

Preparation:

- Have the HOMES application installed.
- Have a connection to the Internet.
- Have an registered HOMES Account
- Have the Pi and HOMES system set up.
- Be logged in to the HOMES APP.

Procedure:

1. On the HOMES app main page click the Unlock Door button.

Expected Results:

The door should now be unlocked for a preset amount of time (30 seconds default).

9.2.2.2 View Door

Purpose:

To verify the ability of the HOMES APP signal the Raspberry Pi to view the door camera.

Supplies:

- Android Phone or web browser
- Raspberry Pi
- Webcam

Preparation:

- Have the HOMES application installed.
- Have a connection to the Internet.
- Have an registered HOMES Account
- Have the Pi and HOMES system set up.
- Be logged in to the HOMES APP.

Procedure:

1. On the HOMES app main page click the View Door button.

Expected Results:

The Raspberry Pi should then turn on the webcam and send the stream to the HOMES application. If the camera is unavailable it should display an error message and return to the HOMES app.

9.2.2.3 View House Status

Purpose:

To test the functionality of the front door status and the external entry point module status.

Supplies:

- Raspberry Pi
- Power supply
- External entry point modules
- Front door status sensor
- Android phone or web app

Preparation:

- Ensure that all systems are properly powered

- Verify that all doors and windows with a entry point module is closed (the Wi-Fi module should not be powered)
- Verify the front door is closed

Procedure:

1. Check that all sensors are currently reading that everything is shut
2. Open the front door
3. Ensure that the house status will change to reflect that the front door has been opened.
4. Close the front door.
5. Ensure that the house status reflects that the front door has been shut
6. Repeat step 2 through 6 with a door or window with an external entry point module.

Expected Results:
The house status should reflect which doors or windows are currently open or shut to give the user an idea of their external entry points.

9.2.2.4 Call Door
Purpose:

To verify the ability of the HOMES APP signal the Raspberry Pi to start a video call with the camera.

Supplies:

- Android Phone
- Raspberry Pi
- Webcam

Preparation:

- Have the HOMES application installed.
- Have a connection to the Internet.
- Have an registered HOMES Account
- Have the Pi and HOMES system set up.
- Be logged in to the HOMES APP.

Procedure:

1. On the HOMES app main page click the Call Door button.

Expected Results:

The Raspberry Pi should then start a video call using the webcam. It should transmit both audio and video both ways with enough quality to be understood.

9.2.2.5 History
Purpose:
To verify the login functionality of the HOMES APP.

Supplies:
- Android Phone or Web browser

Preparation:
- Have a connection to the Internet.
- Have an registered HOMES Account
- Have the Pi and HOMES system set up.
- Be logged in to the HOMES APP/WEBAPP.

Procedure:
1. On the main page click the view history button.

Expected Results:

The application should look in the database for all recorded events in the last 15 days (more if the use wishes). Then it should display these results in chronological order with the ability to look at any media (video or photo) stored with said event.

9.2.2.6 Login

Purpose:

To verify the login functionality of the HOMES APP.

Supplies:
- Android Phone

Preparation:
- Have the HOMES application installed.
- Have a connection to the Internet.
- Have an registered HOMES Account

Procedure:
2. Open the application.
3. Enter correct email and password.
4. Click Log-in Button

Expected Results:

The application should verify the submitted credentials and if they are valid the My HOMES screen should come up and you should be able to control your HOMES. If the credentials were invalid it should display a notification of error and ask the user to try again.

9.2.2.7 Create Account

Purpose:

To verify the create account functionality of the HOMES APP.

Supplies:

- Android Phone

Preparation:

- Have the HOMES application installed.
- Be logged out of the application.
- Have a connection to the Internet.

Procedure:

1. Open the HOMES app.
2. Click the create account button on the login screen.
3. Fill out the required information on the create account form.
4. Submit.
5. (To test the form from any bugs this can be automated to fill in random or malignant data in the form to test its response)

Expected Results:

If the user entered proper data with an email not already registered a new account should be create for him and then he should then be able to login. Any other data entered should either be escaped or discarded, and the user should be asked to submit the correct information.

9.2.2.8 Recover Account

Purpose:

To verify the recover account functionality of the HOMES APP.

Supplies:

- Android Phone

Preparation:

- Have the HOMES application installed.
- Be logged out of the application.
- Have a connection to the Internet.

Procedure:

1. Open the HOMES app.
2. Click the recover account button on the login screen.
3. Enter your email.
4. Submit.

Expected Results:

The user will receive a email with a link to renew their password.

10.0 Administrative Content

10.1 Milestones

To keep the project on schedule and going smoothly we set up approximate milestones of what we should have completed by certain periods in time. These are but loose guidelines that should be stringent enough to not allow us to fall too behind but also flexible enough to handle all the unpredictable things that always happen with projects of this magnitude. We started by making a Gantt chart that will be used to keep us on schedule throughout both semesters. Then we made a day and date breakdown to help analyze how much time we are really spending on each process.

10.1.1 Gantt Chart

As can be seen on Figure 34 our milestone plan distributes the allocation of days per each step relatively evenly giving favor to research and testing which are crucial to the success of our project. A Gantt chart helps plot processes on a timeline and can be used to easily visualize the spread of work over time.

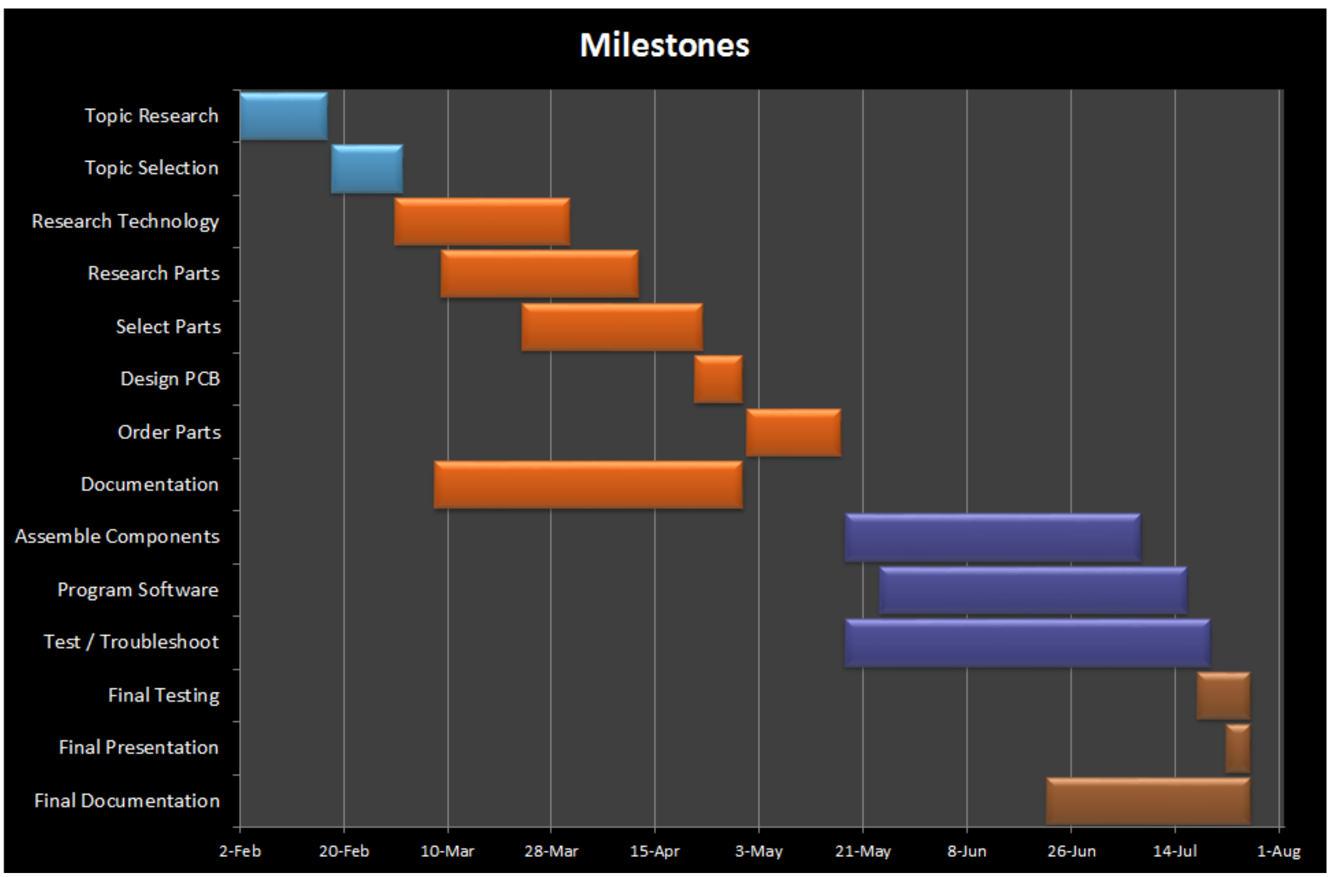


Figure 34 Milestone Chart From February to August

The vertical axis of the Gantt chart represent the major processes we identified in our senior design project. These processes are topic research and selection, research of technology and parts, printed circuit board and part selection and ordering, documentation, assemble hardware and software components, test, and then final presentation and documentation. We used this layout to help us see the times that we should be working on a process. At the beginning of the semester we did not follow the chart and thus fell behind. Then we needed to work harder and subtract time from the part selection and documentation phases.

This hurt us because we may not have made the best design decisions since we were shorter on time than we expected. For next semester we will make sure to strictly stick to the predetermined schedule in order to stay on time and ensure that all the process get the correct amount of time dedicated to them.

10.1.2 Day Breakdown

Figure 35 shows the days per major development step and accounts for the total number of days from both semesters that we are in senior design. This seems to be indicative of how projects function out in the field with a lot of time being dedicated to researching before any designing or prototyping ever gets started. This analysis chart was made to help us keep a strict schedule and only spend a certain number of days on each development step.

Figure 35 Days Per Development Step

10.1.3 Date Breakdown

Table 15 is a task breakdown of the major parts of HOMES. It describes the start and end dates that each section was worked on. This table was made to help us stay on schedule throughout the project.

Table 15: Task Breakdown

Task	Start	End
Project Start		
Topic Research	2/2/2015	2/17/2015
Topic Selection	2/18/2015	3/2/2015
Research and Design		
Research Technology	3/1/2015	3/31/2015
Research Parts	3/9/2015	4/12/2015
Select Parts	3/23/2015	4/23/2015
Design PCB	4/22/2015	4/30/2015
Order Parts	5/1/2015	5/17/2015
Documentation	3/8/2015	4/30/2015
Prototyping/Testing		
Assemble Components	5/18/2015	7/8/2015
Program Software	5/24/2015	7/16/2015
Test / Troubleshoot	5/18/2015	7/20/2015
Finalize Project		
Final Testing	7/18/2015	7/27/2015
Final Presentation	7/23/2015	7/27/2015
Final Documentation	6/22/2015	7/27/2015

10.2 Budget and Finance

With the exception of the Raspberry Pi related items the cost of all the other items shall be split evenly between the three group members, with a portion of the cost being generously covered by Boeing up to the amount of $334.53. These parts will likely be sourced from Adafruit, SparkFun, Amazon, or Texas Instruments, and will be ordered at the start of May.

Since we will not be using any software that doesn't require a free license they shall not be included as part of the budget. Our budget is shown in table 16. More descriptive budget can be found in the bill of materials section where each module is split up and each part accounted for.

Table 15 Budget

Part	Unit Cost	Quantity	Total Cost
Raspberry Pi 2	$40.00	1	$40.00
PiTFT 480x320 Touch LCD Screen	$45.00	1	$45.00
USB Wi-Fi Module	$10.00	1	$10.00
USB Bluetooth module	$10.00	1	$10.00
Logitech C310 Webcam	$30.00	1	$30.00
Power Supply Raspberry Pi 2	$10.00	1	$10.00
RFID Reader ID-3LA (125 kHz)	$26.00	1	$26.00
RFID Breakout	$2.00	1	$2.00
Fingerprint Scanner	$33.50	1	$33.50
Bluefruit LE	$20.00	1	$20.00
Motion Sensor	$15.00	1	$15.00
Electronic Strike	$40.00	1	$40.00
Window Modules	$40.00	1	$40.00
3D Printing	$35.00	1	$35.00
Demo Door Materials	$35.00	1	$35.00
Circuit Materials (Resistors, Breadboards, Wires, etc.)	$25.00	1	$25.00
PCB Prototyping	$15.00	2	$30.00
Total			$446.50

10.3 Personal

The following table 17 outlines the three group members working on HOMES and the content they worked on. Each member had a major module to be in charge of and paper content such as administrative content, the executive summary, constraints, etc. The table below describes what each member was responsible for.

Table 16 Team Members

Member	Email	Content
Colleen Caffey	colleencaffey@gmail.com	• Power supply • Camera • Light • External Entry Point Modules • Wearables • Fingerprint Scanner • Pet door • Constraints • Executive Summary • Similar Projects
Bruno Calabria	brunocalabria92@gmail.com	• Single Board Computers • LCD Screen • Lock • Facial Recognition • Administrative content • Mockups & Design • RFID • Bluetooth • Wi-Fi
Ricardo Georges	ggrick1130@gmail.com	• Motion Sensor • RGB LED • Android development • Web development • Testing Motion Sensor

10.4 Project Summary and Conclusions

We choose HOMES as our senior design project because we wanted to add technology to a previously fairly ancient process of entering ones home. We wanted to come up with a comprehensive and easily manageable system that makes smart home entry for the average American a snap. We were very eager to apply our knowledge from school to a real world project and to learn new things. We hope that HOMES becomes a completely realizable, affordable, and user-friendly household entry monitoring system.

HOMES will consist of a module attached to the front door. This module will have a LCD screen, a camera, a fingerprint scanner, and a motion sensor. When a guest comes within three feet of the front door the motion sensor will activate the camera to take a picture and forward it to the homeowner via a mobile application. Then the guest can look at the LCD screen and see several options for entering the home. The methods the guest has for entering the house are via fingerprint, facial recognition, or wearable. If none of these options are available to the guest they can wait for the homeowner to unlock the door via the mobile application. They also have the option of leaving a video message for the homeowner.

The fingerprint scanner and the facial recognition will both have a database stored on the Raspberry Pi. Each user in the database will be assigned a status of either ok or not ok to let into the home. If a user tries to unlock the door and is an ok user then the door will unlock for them. If the user tries to unlock the door and is a not ok user then the system will lock them out and not let them try again. If the user tries to unlock the door and no match is found in the database then the system will give him or her two more tries before it locks him or her out as well.

There will be a mobile and a web application that the homeowner can use to unlock the door, view the house status, and several other functionalities. The mobile app will be on the Android platform via the android SDK. The web app will use node and mongoDB on the backend and AngularJS with bootstrap on the front end. The basic functionalities of these two applications will be very similar however we want to offer both so a homeowner who doesn't have a smart phone or who prefers a web browser can still access all the information HOMES will provide.

In conclusion we hope that HOMES will be able to teach us a lot about engineering. We want to be able to take the knowledge we gained in the classroom and apply it to any engineering problem we are faced with. We also want to gain experience in designing and building a project from scratch and all the skills that go along with it. Further, we want to perfect the HOMES system into a useable, secure, and easily manageable system that could one day be on the market.

References

Constraints:

- http://faculty.cua.edu/kellyw/teachstandard/Standards%20and%20Design%20Constraints-slides.pdf

Home alarm:

- http://www.statisticbrain.com/home-security-alarm-system-statistics/

Alarm industry:

- http://clients1.ibisworld.com.ezproxy.net.ucf.edu/reports/us/industry/keystatistics.aspx?entid=1491#ID

KEES:

- http://www.eecs.ucf.edu/seniordesign/fa2013sp2014/g17/index.html

Close To Home:

- http://www.eecs.ucf.edu/seniordesign/fa2013sp2014/g23/

August:

- http://august.com/

Kwikset:

- http://www.kwikset.com/
- http://www.kwikset.com/kevo/default.aspx#.VT_pyiHBzGc

Power:

- Texas Instruments LM78xx 3-Terminal Positive Regulators PDF
- http://www.energy.gov/science-innovation/energy-sources/renewable-energy/solar
- Device Electronics for Integrated Circuits by Richard S. Muller and Theodore I. Kamins
- http://www.jameco.com/Jameco/Products/ProdDS/227993.pdf
- http://elinux.org/Beagleboard:BeagleBoneBlack
- http://www.atmel.com/Images/doc8161.pdf
- http://www.arduino.cc/en/Main/ArduinoBoardUno
- https://www.raspberrypi.org/products/raspberry-pi-2-model-b/

Software Applications:

- *Open Source Technology: Concepts, Methodologies, Tools, and Applications* by Information Resources Management Association (Author, Editor) Publisher: IGI Global
- *Legacy Application Modernization: High-Impact Strategies - What You Need to Know: Definitions, Adoptions, Impact, Benefits, Maturity, Vendors*

by Kevin Roebuck Publisher: Emereo Publishing
- *IOS - Unabridged Guide*
  by Stephanie Jennifer Publisher: Emereo Publishing

Fingerprint scanner
- http://www.takeoffprojects.com/embd-con-finger-print-based.php
- http://computer.howstuffworks.com/fingerprint-scanner3.htm
- https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C1R_datasheet_V1%205_20140312.pdf

Camera:
- http://www.logitech.com/en-us/product/hd-webcam-c310
- https://www.raspberrypi.org/products/camera-module/
- http://www.adafruit.com/products/1567

Light:
- https://www.sparkfun.com/products/531
- http://energy.ltgovernors.com/led-lighting-explained-questions-and-answers.html
- http://www.designrecycleinc.com/led%20comp%20chart.html

Wearables:
- http://www.wearabledevices.com/what-is-a-wearable-device/

Microphone:
- http://hyperphysics.phy-astr.gsu.edu/hbase/audio/mic.html

External Entry points:
- http://www.eleinmec.com/article.asp?23
- http://www.infineon.com/cms/en/product/sensor-ics/magnetic-sensors/channel.html?channel=ff80808112ab681d0112ab68f47200a6
- http://www.dimensionengineering.com/info/accelerometers
- http://www.lionprecision.com/capacitive-sensors/index.html#apps
- http://www.chicagosensor.com/HowFloatSwitchesWork.html

Communication:
- ZigBee
  - http://www.eetimes.com/document.asp?doc_id=1278172&page_number=2
  - http://www.zigbee.org/
- RFID
  - http://cdn.sparkfun.com/datasheets/Sensors/ID/ID-3LA.pdf
- Wi-Fi
  - http://www.ti.com/product/cc3200
  - https://electricimp.com/

- http://www.espruino.com/ESP8266

Face Detection:

- http://docs.opencv.org/modules/contrib/doc/facerec/facerec_tutorial.html
- http://opencv.org/
- https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-IJCV-01.pdf

Single Board Computer:

- https://www.raspberrypi.org/products/raspberry-pi-2-model-b/
- http://beagleboard.org/BLACK

Lock:

- http://www.locksmithledger.com/article/10238119/electric-strikes-everything-you-should-know

Permissions

Figure: Capacitive vs optical fingerprint scanner
Status: Pending

permission to reprint

Colleen Caffey <colleencaffey@gmail.com> Apr 6
to takeoffstudent.

Hello,

I am a electrical engineering student at University of Central Florida doing my senior design project on a smart home entry device. I would like to include the pictures of the capacitance and the optical fingerprint scanner from the biometric fingerprint reader article in my senior design paper.

Thank you for your time,
Colleen Caffey

Figure: Open versus shut reed sensor
Status: Accepted

Ralph DelZenero <Ralph@chicagosensor.com>
to me

Hi Colleen,

Thanks for writing, you can use the image you have requested. If possible, I would welcome the opportunity to read your paper, particularly if it deals with float switches and uses in industry. Just send a copy to this e-mail address. Good luck.

Regards,
Ralph

Ralph Delzenero
Chicago Sensor, Inc.
Phone:(773) 252-9660
Fax: (773) 751-4443

Manufacturing & Warehouse:
7617 State Route 31
Richmond, IL 60071

http://www.chicagosensor.com/
follow us on twitter: http://twitter.com/chicagosensor
Chicago Sensor - Supporting Your Innovation

On Mon, 27 Apr 2015 23:00:31 -0400, colleencaffey wrote
> email: colleencaffey@gmail.com
> realname:
> comments: Hello, I am a senior design student at UCF and I have been
> asked by my instructor to request permission for any images I wish
> to use in my senior design paper. I would like to use the image on
> the page titled 'How Magnetic Reed Liquid Level Sensors Work' Thank
> you for your time, Colleen Caffey name: Colleen Caffey submit: Submit
>
> ==================================

Figure: Two vs three reed switch
Status: Accepted

Figure: ZigBee data transfer and latency
Status: Pending

reprint permission

Colleen Caffey <colleencaffey@gmail.com> 4:49 PM (0 minutes ago)
to termsofservice

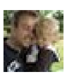
Hello,

I am a senior design student at UCF and I have been asked by my instructor to request permission for any images I wish to use in my senior design paper. I would like to use figure 4.1 and 4.3 on the page titled "ZigBee applications - Part 1: Sending and receiving data"

Thank you for your time,

Colleen Caffey

Figure: BeagleBone pins
Statue: Accepted



Frits Lyneborg <fritslyneborg@gmail.com>
to brunocalabria

Hi there, sure, thanks :)

Frits

On Wed, Apr 29, 2015 at 4:05 AM, <brunocalabria@knights.ucf.edu> wrote:

> Bruno Calabria sent a message using the contact form at
> http://letsmakerobots.com/contact.
>
> Hello I'm a student at the University of Central Florida working a senior
> design project and wish to use a image found in the post mentioned below.
> Would it be possible to display this image in my report?
>
> post: http://letsmakerobots.com/node/37063
> file:
> http://letsmakerobots.com/files/userpics/u19048/600x700xB_3PinOut3.png.pagespeed.ic.PwIAPM8prs.png
>
> Thank you,
> Bruno

Figure: Raspberry Pi Pins
Status: Pending

Regards,
Your Newark element14 Team

Submit a Question Form

*Required field

*Name:
Bruno Calabria

*Email:
brunocalabria92@gmail.com

Phone Number:
9548032028

Reason for Inquiry:
Other Questions / Comments

Order Number:
Please enter your order number

*How can we help you?:

Hello, I'm a student at the university of Central Florida and for my senior design project I was wondering if I could use the following image I found on you site in my documentation.
http://www.element14.com/community/servlet/JiveServlet/showImage/38-16317-199592/GPIO.png

Thank you,
Bruno

Submit form

Figure: Electric Imp
Status: Approved

Permission to use image — Inbox x — brunocalabria@knights.ucf.edu x

Bruno Calabria <brunocalabria@knights.ucf.edu> — 8:44 PM (1 hour ago)
to info

Hello,

I am a Computer Engineer at the University of Central Florida,
My group and I will be using an imp in our Senior Design project and would like to use some pictures of the 001 and 002 modules in the documentation, but to do so we need permission first.
Would it be possible for us to use those images?

Thank you,
Bruno Calabria

Matt Haines <matt@electricimp.com> — 8:51 PM (1 hour ago)
to Bruno, info

Hi Bruno,

No problem - you have permission to use the images.

Figure: LCD Display anatomy
Status: Accepted

Cut through an TFT display.

View author information

Public Domain
File: Color TFT-LCD Layout.png
Uploaded by Lozère
Uploaded: December 4, 2005

About Media Viewer | Discuss this feature | Help