A1 Security System

Jonathan Chew, Timothy Henry,
and Brandon James

Dept. of Electrical Engineering and Computer Science, University of Central Florida, Orlando, Florida, 32816-2450

Abstract **- A1 Security System is a low-power all-in-1 security system that secures the user's household by automated monitoring, live video feed capabilities, and the removal of a physical key. The security system grants access using successful bluetooth or wifi communication through mobile application, or a valid fingerprint scan. The mobile application that has been developed allows its users to fully control the system with ease. The app features a time log for all interactions with the security system, live video streaming, managing captured videos, and fingerprint scanning configurations.**

Index Terms **- Atmega2560, Bluetooth, Door Lock Solenoid, Fingerprint recognition, Logic Level MOSFET, PIR Sensor, Raspberry Pi 3, and Wifi.**

I. INTRODUCTION

According to the US Department of Justice, there are more than 2.5 million home intrusions that are reported annually. 75% of burglaries occur on residential property. In addition to the total amount of break-ins, 30% of all reported burglaries occur when homeowners leave the front door unlocked/unattended. To put this into perspective, every year more than 750,000 family owned properties are left completely vulnerable to burglars because the owners simply forgot to lock their doors. If families can have the ability to access the lock on their front door by a push of a button anytime and anywhere this will undoubtedly reduce the number of intrusions.

In the world of technology, Smart Home Security Devices are quickly becoming a necessity for the average family household, however, because of high prices for these systems, families have long delayed this expense until their first break in. With all the smart security system devices available to consumers, an affordable and fully equipped security device seems to still be missing from the market.

As society's demand for an all-in-one security device continues to grow, this necessity has inspired us to create a product that will contain all the features a homeowner desires in a security system. The design works parallel with a fingerprint scanner, camera, and mobile application that will provide all the security needs for the users. Our design will guarantee low cost, user friendliness, ease of installation, and most importantly, safety to families and their belongings.

II. OVERVIEW

The group wanted to have an even balance of hardware and software to be incorporated into the design. After weeks of research, the group decided what we wanted to include and achieve for the final product. The peripherals needed to meet our group's expectations for the system include a camera module for video capturing, fingerprint scanner, a motion detector, wifi and bluetooth modules, and a mobile application for easy interactions with the security system.

The group initially intended to power the whole system off a 12VDC 6000 mAH rechargeable battery bank. The low power approach influenced much of the current hardware design and software's algorithm in the final product. Logic level MOSFETs are used for switching peripherals on and off while drawing minimal current. A battery monitoring circuit is implemented for informing users about battery health. The procedure for how the system carefully schedules and executes all the tasks autonomously became critical in order to fully maximize the battery's life.The battery powered approach became unachievable once discovering how long the Raspberry Pi 3 takes to boot up and unfortunately we could not keep the Raspberry Pi on continuously as it would draw near 1 Amp with the camera connected. In order to keep the system running on a battery, the Raspberry Pi required a separate continuous power supply. The group eventually decided to power the entire system with a constant power supply while keeping the overall power consumption to a minimum.

The all-in-one security system is split into 2 sections and each section is to be mounted onto opposite sides of a door. The indoor section will house the main controls for the system, which includes the custom PCB board and Raspberry Pi 3. The reason is for protection from outside environmental forces and from thieves tampering with the electronics. The outside section will house the LCD display, fingerprint scanner, motion sensor, and the camera module.

The mobile application has unique features that allow its users to feel more secure and definitely adds convenience. The mobile app can record all entry/exit activity during any time of day. Live video streaming can be seen right on the mobile app's user friendly interface. The mobile app can manage cloud storage that will contain short videos taken when the sensor detects movement. The mobile app

will allow users to manage the fingerprint scanner's database by adding or removing fingerprints.

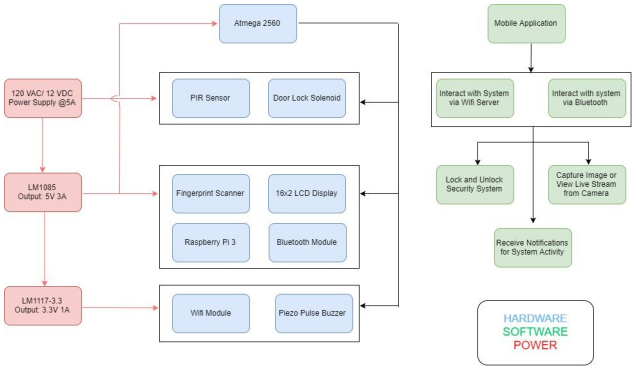

Fig. 1 - Overall System Block Diagram

III. MAIN MICROCONTROLLER

The main microcontroller that is implemented for the security system is the Atmega2560. The Atmega2560 was chosen for its 4 programmable UART serial communication capabilities, 6 low power modes, plenty of GPIO pins (84 pins), and the group's familiarity with the Arduino IDE. The microcontroller uses an 8-bit AVR RISC-based architecture and 8 KB SRAM. At the assembly level the microcontroller has 86 general purpose input/output lines. A RTC (Real Time Counter) comes with its own separate oscillator. The 4 pairs of serial communications are needed because the system will be interfacing between both Bluetooth and Wifi, to the Raspberry Pi 3, and the fingerprint scanner. Power-down Mode will be used in the security system where the external oscillator will cease to run, while the asynchronous modules are kept running. The microcontroller also features 10 bit analog-to-digital converter pins.

Operating Voltage	4.5 V - 5.5 V
Digital Communication Peripherals	4-UART, 1-I2C
Clock Speed	16 MHz
Memory	256 KB ISP Flash
RAM	8 KB SRAM
Pin Count	100
Temperature Range (C)	-40 - 80

Table 1 - Atmega2560 Specifications

IV. IMAGE PROCESSING AND CAPTURING

The A1 Security System will provide clear live video streams and store short clips in the Cloud, allowing for users of the mobile application to see them. In order to achieve these features, the security system will use the Raspberry Pi 3 for its powerful processing ability. The Raspberry Pi 3 has 1.2 GHz ARM Cortex-A53 processor and 1GB of RAM memory. The Raspberry Pi 3 comes with a microSD card for memory storage and has Wifi and Bluetooth built-in.

The device's Wifi module is responsible for the uploading of media straight to a private online cloud storage. The Raspberry Pi 3 supports camera serial interface, which the chosen camera module works well with. The camera that is integrated into the system is Raspberry Pi's NoIR Camera Board v2. This camera module contains a 8 megapixel resolution that is able to capture video up to 1080p resolution at 30 frames per second. This specific camera module does not filter out infrared light, which gives the camera the ability to capture clear and recognizable pictures at night with the addition of an infrared light.

The Raspberry Pi 3 will be communicating to the main microcontroller through one of its four USB ports. To do this, the system will use the CP2102 integrated circuit to convert micro USB to serial communication. The interface behaves in a handshaking manner where the Raspberry Pi 3 will be steadily listening to commands from the main microcontroller. The device's main responsibilities are to capture short videos when the PIR sensor senses movement. The Atmega2560 will send serial command to the Raspberry Pi to record a small clip that will be uploaded into Google's Cloud Storage. The second role is to provide a dependable live stream video to the mobile application for the system user over the internet. This will be achieved with a combination of YouTube's Live Stream abilities and also the Android YouTube APIs.

Fig. 2 - Raspberry Pi 3 Interfaced with NoIR Camera

V. POWER

The security system shall have a continuous power supply that transforms 120 VAC down to 12 VDC when plugged into a wall outlet. The design requires a constant source of power because of the Raspberry Pi and the electronic door lock. The Raspberry Pi 3 behaves similar to a computer with slow boot up times, and its firmware does not include low sleep modes, therefore, the device must be powered on continuously. The power supply chosen is called LEDMO LED power adapter. The product is intended for powering on LED strips, however, it meets the security system's power requirements perfectly. The power supply can output a maximum of 5A, which will be needed for image processing and driving the door lock. The DC voltage levels needed for this design includes 12V, 5V, and 3.3V.

The best option for a low power design is to use step down buck converters. Due to budget limitations, the group has chosen linear voltage regulators because they are inexpensive. The security system shall be using Texas Instrument's LM1085IT-5.0 and LM1117DT-3.3 for voltage regulation. The security system includes a backup battery supply that will turn on instantly once the main power supply has been cut off. The battery supply consists of an 8 double AA battery holder that is connected in series to output 12 VDC. The backup supply is intended for commercial off the shelf lithium ion 1.5 volt AA batteries for convenience to its users. When the security system is running on the battery supply, the design will shutdown the Raspberry Pi to protect it from receiving under voltage levels, and this will increase the battery life duration

VI. BATTERY MONITOR

By removing the requirement for a physical key for access entry, the security system has to be very dependable. A battery monitor feature will be implemented in case there is a power outage that will warn users on battery health. The battery monitor is switched on by the main microcontroller every time it wakes up. The monitoring is switched on/off to prevent current drawn when not needed. The voltage will be read through a 10-bit analog to digital converter (ADC) pin on the Atmega2560. The voltage read will be from the main power source that will be divided down to 3 volts for safe levels for reading. The divided voltage will be converted into an integer between 0-1023. The microcontroller will know when the system is running on the back up battery when reading an ADC value associated with 95% battery health. The security system will then periodically send notifications to user's mobile application as a reminder that the system is running on the backup battery. A LCD display will also show the battery percentage as well incase of power outage.

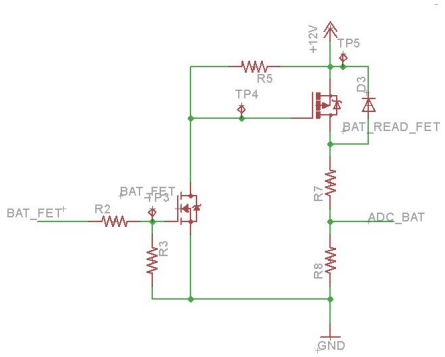

Fig. 3 - Battery Monitoring Schematic

VII. PIR MOTION SENSOR AS EXTERNAL INTERRUPT

The motion detector used in the design is a 3 pin pyroelectric infrared PIR sensor. This sensor operates between 5-20 VDC and outputs 3.3V. The sensor draws 50 microamps in idle mode, and draws up to 65 mA when detecting motion. The sensor is capable for detecting movement up to 7 meters at a maximum of 120 degree angle. The PIR sensor incorporates 2 potentiometers to adjust sensitivity and time delay.

The A1 security system implements a low power architecture that enters sleep mode once left aside with no interaction. In order to wake up from sleep mode, the system will use a PIR motion sensor to send an interrupt signal to the Atmega2560. The sensor's 3.3V output will deliver voltage to the base of an PN2222A transistor that will cut voltage flowing into the interrupt pin. The design creates a low level external interrupt.

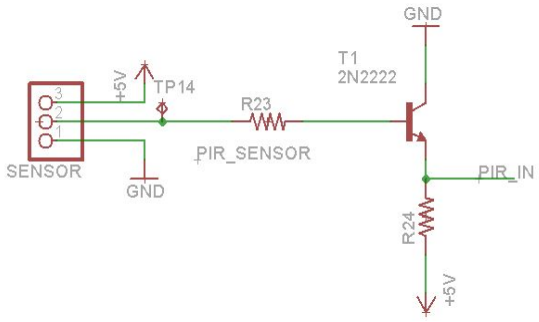

Fig. 4 - PIR Sensor as External Interrupt Schematic

VIII. DOOR LOCKING MECHANISM

There are two technologies that are used with electronic door locks: Fail Safe and Fail Secure. Fail secure is an approach where the door lock will remain locked when

drawing power. Users will gain entry access once the lock loses a power signal. The door lock remains in unlocked position until it draws power from its supply again. The second approach is the fail safe. Fail safe will remain locked at all times until a power signal is received. A flaw to this algorithm is that failsafe creates a possibility for the doorlock to remain in locked position when power is lost during emergency situations. The huge advantage is how little power is consumed compared to fail secure method. For the security system to follow the low power approach, the fail safe method is the best option for the project. A constraint for the system is power must be available at all times for entry/exit.

The door locking mechanism that the security system will use is called the Lock-style solenoid. The door lock fits the requirements for easy installation, affordability, compatibility with most doors, maintain strong locked position, and operate well within our power requirements. The solenoid consists of a copper wire coiled up and attached to an armature (the metal bar). Once the solenoid receives a power signal, the coil pulls the armature into the lock. The lock will remain in open position until power is no longer drawn. The lock has an operating voltage range of 9-12 VDC. This door lock is also not adaptable to different types of door knobs, and is required to be installed in a deadbolt opening. The electronic door lock is mounted where a deadbolt lock would usually fit, therefore, a lock with physical key will become a constraint. The solenoid is easy to integrate with the system because the connected wires can trace back to our main microcontroller with ease as well as screw holes for easy mounting.

The solenoid is able to operate for a few moments by controlling the switching through the Atmega2560 digital pins. A digital HIGH from the MCU will close a switch created by a logic level N-channel MOSFET. The solenoid acts as a inductor and is charged once the switch is closed. A flywheel diode will be placed parallel to the door lock to protect it from back EMF. An exit switch will be used to open the door when exiting without waking up the security system. The exit switch closes a path that allows 5 volts to drive the door lock. Current can flow back into the microcontroller which will cause it to wake up, therefore, a diode will also be placed to the output of the digital pin. A pull down resistor will be used across the gate and source for quick dependable switching.

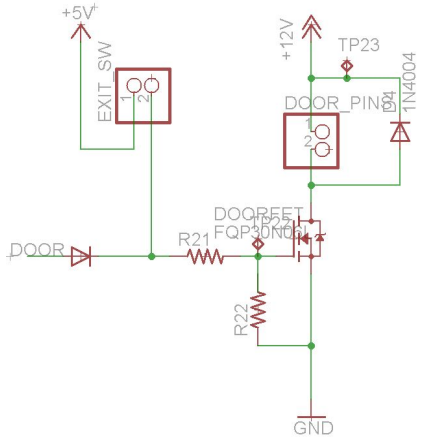

Fig. 5 - Switching Door Lock Solenoid Circuit

IX. BLUETOOTH

The A1 Security System utilizes Bluetooth technology to exchange data back and forth between the system and the complimentary mobile application. As noted beforehand, the system is slated to be secure while also offering flexibility to the user of the security system to lock and unlock the door in a variety of ways. Unlocking the A1 Security System via Bluetooth only takes but a few steps and you are able to walk into your room, home, or business - all of this with the help of the Android Bluetooth API. The steps to get the door unlocked when using Bluetooth are as follows:

1) Log into the mobile application designed to integrate with the A1 Security System and set up to allow unlocking from Bluetooth. This will require a PIN or Fingerprint access.
2) Once bluetooth is turned on, the user can then pull down the notification shade. There, a notification should be present prompting the user to connect and unlock the door with Bluetooth.
3) Before the door unlocks, the user will be prompted to either enter a PIN or use the fingerprint scanner to confirm the option.
4) Once the user's chosen method of authentication has been confirmed the door will then unlock, giving the user access.

This standard technology that has been around since the 1990s and uses short wavelength UHF, Ultra High Frequency, radio waves to transmit or receive data. The frequency band that Bluetooth operates at is between 2.4 and 2.485 GHz.

The module that was utilized for the A1 Security System to conduct its short frequency communications is the HC-05 Bluetooth Module. The compatibility of the HC-05

with Arduino and the Atmega2560 was a selling point for its selection. This serial module, which was a low-cost unit, has a range of communication of up to 10 meters. At the reported range, it's reasonable for the user as he or she may be walking up to the front door.

The module can operate as both a master device or a slave device, which can be configured by the programmer using AT Commands. The Bluetooth board is capable of operating in "command mode" or "data mode". In Command Mode, the HC-05 is able to listen to AT commands. In Data Mode, the board is able to send or receive bits of information from connected environments. This is the mode that the A1 Security System will perform its functions in. The baud rate for communication with the microcontroller has been set at 9600 bps, along with many of the other components.

The Bluetooth module operates natively at a voltage of 3.3 volts across the board. However, it does come packaged with its own level regulator which is 5V-3.3V. Knowing that there is a built-in regulator, sending 5 volts to the VCC was perfectly fine from a power standpoint. Connection and communication between the PCB and HC-05 comprises of four pin connections. VCC, Ground, and a Rx/Tx pairing.

Operating Voltage	3.3V - 5V
Operating Current	25mA
Range	10 meters (30ft)
Communication	UART

Table 2 - HC-05 Bluetooth Module Specifications

X. ESP8266 WIFI MODULE

The ESP8266 is a powerful multifaceted Wi-Fi chip device that is also capable of operating as a development board since it has its own embedded microcontroller. Created by manufacturer Espressif Systems, the role that the ESP8266 chip will play in the A1 Security System is to send notifications to the user wirelessly. Its implementation into the system is significant because it provides Wifi connectivity for the microcontroller with its TCP/IP protocol stack. The TCP/IP protocols that come included in the device gives the system the proper networking tools to send data wirelessly.

With the Wifi module being so cost-effective, it has become a staple for hobbyist, DIYers, and hackers alike to experiment and play with it. That has led to a ESP8266 Wifi community where many others have shared their projects and provided help with the chip. The community support and along with the many heaps of documentation on the board, helped ease the learning curve of getting familiar with the ESP8266 module. Bundled with AT command set firmware comes the Wifi module which have been modeled after the Hayes Command Set. The AT command functionality proved to be a pivotal feature when testing out the module. Getting accustomed to the ESP8266 was much easier seeing that one can simply send "AT" into the serial monitor in the Arduino IDE and sending that to the board to check whether the board is at attention. Using AT commands, programmers can check to see whether the Wifi module is up and running, reset the modem, check or set what mode the ESP8266 is in, join or disconnect from an access point, or list nearby access points and whether they are WPA, WPA2 encrypted, or open. Those were only just some of the bounteous commands available to the programmer.

The Wifi module, which also goes by the name ESP-01, has eight exposed pinouts. The pins are as such:
VCC (3.3V), Rx, Tx, IO16, IO0, Enable (CH_PD), IC2, GND. The ESP8266 module is connected to the A1 Security System via the VCC, EN, Rx, Tx, and GND. When turned high, the enable pin must be connected to a 3.3V source along with the VCC so that is can empower the 3.3V regulator on the ESP8266 board. The board only operates at the 3.3 voltage level including its VCC and GPIO (General Purpose I/O) pins, so anything higher can damage the module.

The are also many libraries to help with developing for the ESP8266. One of the libraries used was the WiFiEsp library, which has useful classes and functions designed specifically for the module prepared.

Processor	Tensilica Xtensa L106
Wireless Type	802.11 b/g/n
Clock Speed	80 MHz
Operating Voltage	3.0V - 3.3V
Memory	1 MB Flash
Communication	UART, SPI, I^2C
Dimensions	25mm x 15mm x 1mm
Weight	1.5 grams

Table 3 - ESP8266 Wifi Module Specifications

XI. MICRO USB-TO-SERIAL ADAPTER

The WINGONEER USB to TTL/UART module converts micro USB to serial by using the integrated circuit CP2102. The primary reason for this adapter is to interface the Atmega2560 microcontroller with the Raspberry Pi 3. The adapter was a cheap and effective way to have the Raspberry Pi handshake with the Atmega2560. The adapter will also be used to program the Atmega2560 once the bootloader has been installed into the microcontroller. This adapter eliminates the use of an FTDI integrated circuit and an extra USB port for the PCB design. The adapter outputs Rx/Tx pins that will be connected to the Tx/Rx pins on the Atmega2560. The programmer is able to connect a micro USB port into the adapter and connect the other end into the PC. The security system's final code is to be uploaded straight to the chip with no other errors.

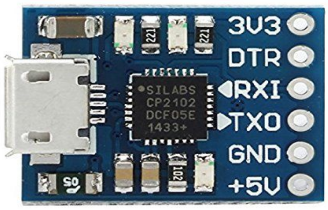

Fig. 6 - Micro USB to Serial Adapter

XII. LCD DISPLAY

A standard 1602 LCD will be mounted onto the outer case for the security system to output important messages for its users. The main microcontroller will present battery percentage on LCD display when backup supply is being used. The LCD display will help guide users for enrolling new fingerprints to the database and displaying a valid or invalid fingerprint scan when attempting to gain entry. The LCD will also show if the door status is opened or closed. The LCD operates at 5 volts and uses I2C communication to reduce the amount of digital pins needed. The LCD display includes a potentiometer for backlight adjusting. The LCD display is turned on through MOSFET switching to reduce the overall power consumption.

XIII. READING DOOR POSITION

The magnetic contact switch will be incorporated into the design to sense the door closed/open status. Being able to sense when the door is open or closed is important for how the locking system algorithm is going to function. The magnetic switch is connected to a digital pin on the Atmega2560 to system ground. The main microcontroller will remain in active mode when receiving an input of 0 from the magnetic switch. This means that the security system will continue to remain active as the door is left in open position. The microcontroller will receive an input of 1 when sensing that the magnetic reeds are in close contact of each other. The microcontroller at this moment knows that the door is in closed position and will enter sleep mode after a few moments. The magnetic contact switch will also incorporate a pulsing 3.3V piezo buzzer. The buzzer is to sound off after the microcontroller senses the door being opened for more than 10 seconds. This sound feature is beneficial to remind users to keep the door closed after entry.

XIV. ANDROID MOBILE APPLICATION

One of the most important aspects of this project is the Android application. This is because the Android app serves as the primary method of interfacing with the A1 Security System. Because it is the primary form of communication for the user, the application must be highly secure. The user will have 3 options for authentication when using the application. These methods include Email and Password, PIN, and fingerprint scanning on the devices that support it.

Email and Password authentication will be done through Google's Firebase SDK - a software suite that provides developers with the tools needed to build an application. PIN authentication will be done through the use of the Android Shared Preferences. This is a persistent storage solution that will allow the PIN to be remembered as long as the Android application is installed and the data has not been cleared from the application. The PIN falls in line with our goals for this form of authentication - something that is stored locally and customizable. Lastly, the third form of authentication, Fingerprint Authentication, will be provided the use of a third party, open-source, Android library named Reprint.

Unfortunately, while Android does have great APIs, connecting all of it together to form a fully functioning Fingerprint Authentication interface can be challenging and time consuming. On top of this, there are Android Manufacturers, such as Samsung, who happen to use their own, specific APIs for the Fingerprint Scanner. Knowing this, it was decided that Reprint should be used so that both the default Android Fingerprint APIs and the Samsung Fingerprint APIs could be used without any compatibility issue. Reprint combines support for both

APIs into one library, which helps greatly in the development process.

Once the user has gained access to the Main summary screen, there is a live feed, which can either be a looping gif of whoever was most recently at the door, or a live video feed. Whether it is a looping gif or a live stream will be specified in the application settings. Below this, the options to activate or deactivate the locks of the A1 Security System are present.

On the following page, user can to see a history of events involving the Security System. These events focus primarily on times when motion was detected at the door. These list of events include timestamps along with a description of the event and an icon that assists the user in recognizing the category of the event. Once one of these events is tapped on, the user is presented with more detailed information on the event and has the ability to see 5 second video of the event that occurred.

The application itself was built using Android Studio, with a minimum API of 19, or Android 4.3 Jelly Bean. This minimum Android version was chosen to strike the perfect balance between the ability to use Bluetooth Low Energy APIs, which were added in API 18, and user adoption rate. With Android 4.3 we are able to hit about 90 percent of Android users worldwide, which means there will be a much greater chance of growth. Furthermore, for VersionControl, GitHub was used, allowing all team members to download and test the software on their own phone and also contribute to the code base.

XV. RASPBERRY PI SOFTWARE

The Raspberry Pi is running Raspbian: an Operating System based on Debian that has been optimized for the hardware of the Raspberry Pi. Debian uses the Linux kernel which allows for the use of many tools and applications that can be used on other Linux OSes, such as Ubuntu. On Raspbian, you are able to take advantage of higher level languages like Python, which was the primary coding language used when programming on the Pi. With Python, it allowed the team to utilize many libraries that were required for our Pi algorithm, such as the PiCamera, Pyrebase, and Serial libraries. With the PiCamera library, we are able to control the proprietary Raspberry Pi NoIR * MegaPixel Camera v2 through simple commands. Pyrebase, perhaps the most important library used, is a third party, open-source Python library , recommended by Google, that handles Firebase Storage, Database, and Authentication operations. Lastly, the Serial library aids in the sending and receiving of data over Serial. The Raspberry Pi listens to data sent over serial from the Atmega2560, which prompts it to record a short video snippet or start a live stream. In the case of the short video snippet, the resulting file is then saved to the Raspberry Pi and uploaded to Firebase Storage. Then a new database entry is created for the media file, along with the url to view the video. This database entry allows the phone to know when it should download the newest media to the live feed. In the case of the live stream, the YouTube API is used to create and start a private live stream on YouTube. Once started the mobile devices will be able to tune into this stream directly from the main Summary screen.

XVI. CONCLUSION

The group has chosen to create an all-in-one security system because of the passion we have towards our homes. We wanted to construct a final product that can possibly be sold in the competitive market today. Our project has an advantage over the market due to its low cost, low power, wifi/bluetooth communication, easy installation, dependability, and user friendly mobile application.

The project consists of two major parts: the entry system and the mobile application. The entry system is built to be powered on in the event of a user approaching the door. To confirm if a user is at the door, a motion sensor is being utilized that is capable of detecting movement up to 7 meters away. After detection, the sensor wakes up the security system and captures a short video of what caused the system to wake up. The sensor and camera used are both effective in all lighting scenarios. The recorded video is then transmitted straight to a cloud storage for temporary use. This step is made possible by integrating the small computer processor, the Raspberry Pi 3. The Raspberry Pi 3 will be a slave device for the security system that will listen for serial commands sent from the Atmega2560. The Raspberry Pi is strictly used for image processing needs for the system and using its onboard wifi ability to upload to cloud storage. The Raspberry Pi 3 will also allow live video streaming for the user.

The user can now use his phone application to open the door using the bluetooth/wifi option, or the user can scan his fingerprint to gain entry. An exit switch is implemented for quick easy access for exiting the house. A backup battery supply is installed for the system to guarantee no power failures until the battery's run out of power. The backup batteries that recommended are 8 lithium ion AA batteries with high mAH ratings to maximize the life duration. The system has the ability to detect when the battery supply is being used by a battery monitoring process. When running on the backup supply,

the system will turn off the Raspberry Pi 3 to conserve power, and keep all other functionality.

The Android application is intended for the user to be able to manage its cloud storage, access live video streams, review time log information, and manage the fingerprint scanner. The Android application will first ask user to enter his login information when using the app for the first time. After a successful login, the user is able to access all the features for the security system. The app has a user friendly interface that divides all options into organized on screen buttons. A large section of the home screen displays a live video stream when opened. Click options on the main menu of the app include activate door lock using bluetooth, activate door lock using wifi, manage fingerprints, and time log viewer. The Bluetooth activation requires the mobile device to pair once, and the phone shall be able to connect to it automatically in the future. The wifi option will unlock the door through our internet server so users can be located at far distances while having full control on the security system. The fingerprint scanner option will allow users to enroll up to 20 fingerprint scans to its database, and delete unauthorized fingerprints. The mobile application will be able to associate a name with each fingerprint saved. The name will be displayed onto the LCD display when gaining entry using the fingerprint scanner.

GROUP MEMBERS

Jonathan Chew is achieving his bachelor's degree in electrical engineering from the University of Central Florida. He is currently an intern at Lockheed Martin Corporation, and will soon be a full time employee at Raytheon after he graduates. Being the only electrical on the team, he has took on the role for power management, designing the overall schematic, and developing custom PCB board. He has created a system that uses a continuous power supply from the grid and steps down the voltages accordingly to power on all the modules needed for full functionality. All hardware components chosen for the custom PCB board and schematic are done with a low power consumption approach. He has also developed majority of the code that A1 security system uses.

Brandon James is a computer engineering student at the University of Central Florida graduating in August 2017. His capacity that he filled in the A1 Security System project was to acquire most hardware and peripheral components test them, and incorporate it into the overall system. Throughout his years at the school he has learned many skills in the academic field and lessons about life while in his attendance. His interests in the computer engineering field are computer hardware computing, hardware testing, and system integration. Brandon plans to one day use his experiences to be a leader of a team at a well represented company. As for his immediate plans after college, Brandon James has already accepted a Solutions Analyst role at Deloitte LLP.

Tim Henry is a Computer Engineering Student finishing up his undergraduate career at the University of Central Florida. He has a passion for mobile development and is currently a Junior Android Developer Intern at SightPlan. Tim was primary responsible for the software aspects of the project and lead the software development of the Android Application, the Raspberry Pi, and the communication for both of these devices through Bluetooth and WiFi. Tim plans to continue work in the Mobile Development field in the short-term future and gain a Masters in Artificial Intelligence and Machine Learning in the long-term future.

ACKNOWLEDGEMENT

The authors wish to acknowledge the guidance and helpful advice received from professor Dr. Lei Wei. He has given thoughtful ideas for the A1 Security System and challenged the team. Thank you to the Project Review Committee for taking the time out your busy schedules to review the A1 Security System.

REFERENCES

[1] Battery Monitoring: http://www.egr.msu.edu/classes/ece480/capstone/fall13/group06/files/everdeen_appnote.pdf
[2] Interrupt Configuration: http://www.gammon.com.au/interrupts
[3] Logic Level MOSFET Switching Techniques http://www.electronics-tutorials.ws/transistor/tran_7.html
[4] Fingerprint Scanner Datasheet https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C1.pdf
[5] Arduino and Raspberry Pi 3 Interface: https://oscarliang.com/connect-raspberry-pi-and-arduino-usb-cable/
[6] Designing Eagle PCB Guide: https://learn.sparkfun.com/tutorials/using-eagle-board-layout
[7] Android Developer Documentation: https://developer.android.com/
[8] Reprint Android Library: https://github.com/ajalt/reprint
[9] Pyrebase Python Library for Firebase: https://github.com/thisbejim/Pyrebase