Secured-E-Key

Sheldon Johnson, Enjolie Morales, Shawn Gangasingh, and Saint-Surin Paul

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

***Abstract* — Countless number of smart locks exist in the market place today, giving customers the absolute freedom to vote their dollars as to which device they find most favorable. Each smart lock currently available to purchase features a wide range of capabilities that are either similar or entirely different from one another. This paper discusses the design and implementation of Secured-E-Key's smart lock system's capabilities by focusing on the aspect of security without risking home or user safety.**

***Index Terms* — Access Control, Communication System Security, Home Automation, Identity Management Systems, Wireless Communication.**

I. INTRODUCTION

The members of our group wanted to create a Senior Design project that incorporated various hardware and software applications as well as something appealing in today's growing market of technology. Therefore, a home automation security lock system seemed fitting for our desired project. The project of Secured-E-Key provides an innovative way to have a smart lock that functions as a home security system in one unit that can maximize access control and ease of use by using just a smart phone.

The objective of Secured-E-Key is to guarantee the user has a secured keyless entry system to their home through the most direct and simplistic way possible without carrying around or needing to utilize any additional devices as part of the overall home security system. This will be executed by the user communicating with the smart lock device itself by solely using any smart phone the user owns or simply just a finger. The Secured-E-Key home lock system operates by detecting the presence of a person within close proximity to the front door using a passive infrared sensor which then automatically takes a picture from the camera and sends a text message notification to the user's smart phone. The picture taken is then stored in a SD card holder and the user can conveniently access the images and upload them to a computer when they return home. The user is then always aware of whoever is present at his/her home throughout the day through text messaging and verifies the people from the SD card images. This level of security serves as part of the home surveillance feature that Secured-E-Key offers. The other security feature Secured-E-Key offers is identity authentication for the user to access their home. In the way physical keys are utilized in today's homes, Secured-E-Key uses a similar approach of opening the front door, but without the hassle of using a physical key. The user is able to access the home with the option of using Near Field Communication from the smart phone or using the fingerprint scanner via index finger. This access gives the user a higher level of security compared to using a physical key.

II. SPECIFICATIONS

The design specifications for Secured-E-Key are as follows:

1) Door unlocks/locks with NFC within 4cm range
2) Fingerprint scanner scans within 3 seconds
3) PIR sensor detects within 6ft range
4) Camera takes picture within 3 seconds
5) User obtains text message within 10 seconds
6) Unlocked door returns to locked state within 5 seconds
7) Power source lasts up to 3 months

III. OVERALL SYSTEM DESIGN

Secured-E-Key consists of several components that are utilized for this project. The key component is the MCU which carries out all the functionalities to the hardware and software components. The hardware dominant components are the security system aspect of the project and consists of an electronic motorized deadbolt lock, a camera module which connects to a wireless module for transmitting the snapshots to the SD card, the fingerprint scanner for secured user entry, a door motion sensor to automatically lock the door after it's been unlocked, a motion detection sensor to detect people at the front door, and the NFC device for secured user entry using an smart phone with the implementation of NFC sticker tags. The other hardware component of Secured-E-Key is the power supply which will power the entire Secured-E-Key home lock system, and it will also contain a visible LED power indicator to display the power levels of the system. The software dominant components utilized are how Secured-E-Key will communicate with itself and the user's smart phone. The main software dominant components are the MCU and the wireless module which is used to connect and communicate the WiFi to the user's smart phone. Figure 1 shows an overview of the entire system.

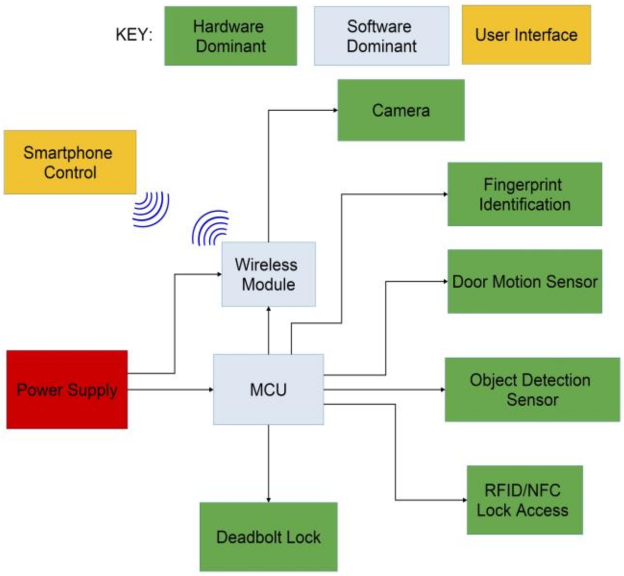

Figure 1. Secured-E-Key Block Diagram

A. Door Layout

The physical door layout of the Secured-E-Key lock system is shown in Figure 2. The camera will be placed on top of the PIR sensor as the highest element on the outside of the front door at the height of roughly 5ft from the ground in order to have the best field of range view for any visitor or intruder. The NFC module will be positioned under the PIR and on top of the fingerprint scanner at a lower level in order to facilitate the operation whenever the user will need to scan either the NFC or his/her fingerprint. The box containing the PCB will be mounted on the inside on top of the lock itself.

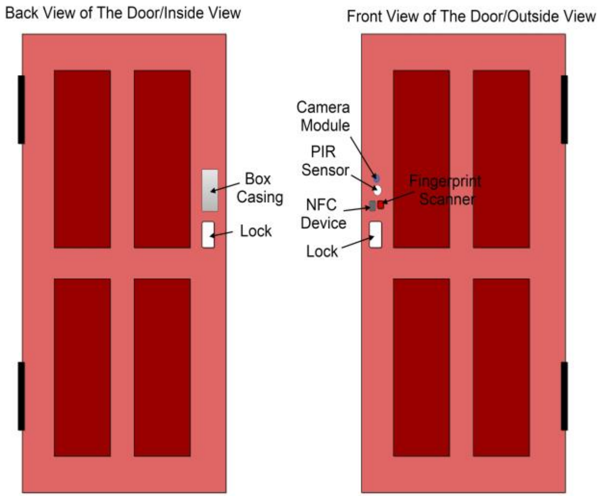

Figure 2. Secured-E-Key Door Layout

B. Device Housing Layout

The housing of Secured-E-Key keeps all external peripherals and PCB boards safe as one single unit. A simple plastic housing will help to avoid from excessive heat being retained internally in comparison to a metal housing, which otherwise would cause all electrical components to over-perform in comparison to their normal operation setting at room temperature. A plastic casing makes assembling the whole project more convenient due to alternations like easily cutting holes into the material and contributes to avoiding the potential problem of wireless signals becoming degraded. The Wi-Fi module used for Secured-E-Key can transmit and receive data while completely covered by the plastic housing, whereas a metal covering would prevent a wireless connection from becoming established. For the most optimum device housing layout to the final assembly of the external peripherals and PCB boards reflect the set-up of Figure 3.

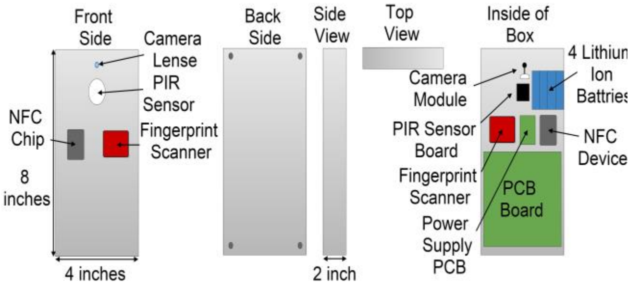

Figure 3. Secured-E-Key Device Housing Layout

C. Deadbolt Lock

The type of deadbolt lock chosen for Secured-E-Key is the motorized electric deadbolt, in particular the Gatehouse Electronic deadbolt. The functionality of the lock uses a motor that is mounted in the lock system and operates by locking and unlocking the door when the motor is powered. The motorized deadbolt lock was mainly chosen because it's the most common lock used in residential buildings, it requires less power to operate, and it's also a highly secured type of lock. The motor operates at only 6 volts and draws a current of 43 mA. The outer size of the lock is 6.75'' H x 3.5'' W x 1.15'' D while its inside size is 8.25'' H x 4.0'' W x 1.4''D. The lock is equipped with one cylinder with backset size that is adjustable. The lock is built to fit a door of thickness in the range from 1-3/8-in to 1-3/4-in and it has a projection of 1.4-in. The bolt type is motorized and it's a graded 2 by the ANSI.

D. Microcontroller

The microcontroller that will be used for Secured-E-Key will be the ATmega2560. This microcontroller was chosen because of the familiarity the members had with C programming language and the IDE. The atmega2560 has 20 Mhz operating frequency and comes equipped with 250 Kbytes of flash. It has 86 I/O Pins and 5 SPI, 1 I2C and 4 UART.

E. Near Field Communication (NFC)

The NFC module chosen for Secured-E-Key is the PN532 NFC/RFID breakout module V1.1 from ElecFreaks. This module was mainly chosen because it has a simple switch to choose between the different protocols of SPI, I2C, and UART which is convenient in case of needing to quickly change protocols; however, the protocol that was chosen to be implemented is I2C. The module also includes a built in tuned 13.56 MHz antenna so an external antenna wouldn't have to be used. The module operates at 5 volts and has a 4cm detection range. The NFC module supports the reader capabilities that will be used to communicate with the smart phone NFC sticker tags that will be placed inside the phone case. The tags chosen were "on metal" NFC sticker tags due to the phone being composed of metal-like components and the sticker tags will be exposed to those components inside the phone case. Overall, the NFC/RFID breakout module V1.1 offers the flexibility of being a simple programmable device and easy implementation that Secured-E-Key needs to achieve its desired functionality.

F. PIR Sensor

The PIR sensor chosen for Secured-E-Key is the PIR Mini Sensor from Parallax. The PIR Mini sensor was mainly chosen because it was the only PIR sensor with an optimal detection angle and distance for a home security system. The PIR Mini sensor has a 100 degree detection angle within a 12ft range and operates at 3.3 volts with a low working current of 28µA. It was also chosen because of its simplistic design of having 3 pins with 1 as ground, 2 as power, and 3 as output voltage. This pin set-up is an easy implementation for the ARMS processor utilized in Secured-E-Key. The PIR Mini sensor also doesn't require much software implementation, a simple Arduino code to turn it on and off makes it an ideal choice as well. Overall, the Parallax PIR Mini sensor provides the best capabilities of easy implementation of hardware and software for Secured-E-Key.

G. Magnetic Reed Switch

The magnetic reed switch chosen for Secured-E-Key is the Zinc Alloy Security Garage Door Rolling Gate Magnetic Alarm Reed Switch to be utilized as the door motion sensor. This magnetic reed switch was mainly chosen because it's already utilized in alarm systems. How this device works is that when the door is closed, the parts of the device are attached and a circuit is running, but when the door opens the circuit is broken and the alarm is triggered. How this is implemented within Secured-E-Key is that the device will be used to automatically control the lock of the door when it's opened and closed.

H. Fingerprint Scanner

The fingerprint scanner chosen for Secured-E-Key is the Adafruit fingerprint sensor. It's an all-in-one optical fingerprint sensor and makes the implementation of identification and verification fairly easy. This device has a high powered DSP chip that does the image rendering, calculation, feature-finding and searching. How the fingerprint scanner works is by connecting it to the microcontroller and it sends the proper commands to take photos and detect prints. The device can store up to 162 fingerprints in onboard flash memory, and it has a red LED in the lens that lights up during the operation to indicate that it's functioning properly. The device operates between 3.6 to 6.0 volts and draws a current of 120 mA. The size of the fingerprint scanner is 56 x 20 x 21.5 mm, which is an adequate size to fit within the Secured-E-Key system.

I. Camera Module

The camera module chosen for Secured-E-Key is the TTL Serial JPEG Camera with NTSC Video from Adafruit. This camera module was mainly chosen because it's built specifically for security systems and in regards to that it can do two main things. One is outputting NTSC monochrome video with the capability of taking snapshots of that video in color, and the other is transmitting that data over the TTL serial link. The NTSC video varies from higher frame rate of about thirty frames per second that would reduce visible flicker to Atomic Color Edit, which is the ability to edit at any four field boundary point without disturbing the color signal. This also leads to less inherent picture noise and almost all pieces of video equipment achieve better signal to noise characteristics in their NTSC form. Other than that, this camera module can snap pre-compressed JPEG pictures at 640x480, 320x240 or 160x120 which literally means it can make them nice, small and easy to store on a SD card. The camera module operates at 5 volts and draws a current of 75 mA. The camera model also has the feature of having manually adjustable focus, auto white balance, auto brightness, auto contrast, and motion detection as well. Overall, the TTL Serial JPEG Camera with NTSC Video provides the best capabilities of a sufficient home surveillance system for Secured-E-Key.

J. Wireless Module

The ESP8266 Wi-Fi module is the wireless communication module chosen for the implementation into Secured-E-Key. The module works compatibly with 802.11 b/g/n Wi-Fi networks and uses a UART connection with the ATmega328 as to send a text message to the user's smart phone through the Twilio API service. Access points (AP) like WPA/WPA2 networks allow the module to achieve and sustain a successful internet connection, but does not work with any WPA Enterprise types. An optimum power performance is attained through a required operational voltage of 3.3 volts and current consumption of 70mA when active, but drops to 5μA during shutdown mode. It remains one of the smallest and inexpensive Wi-Fi modules on the market at 13.2 x 21 mm by containing an imprinted antenna to avoid the necessity of an external one. C programming and AT commands work conjointly with one another as the two programming languages used to control the software.

K. Power

The Secured-E-Key battery unit uses two Li-ion battery packs totaling to 4400 mAh to power all components of the project. As clearly displayed in Figure 4, the final power supply contains a 3.3 volt and 5 volt supply followed by a direct connection of the battery to the electric deadbolt. The 3.3 volt supply comes from the LM3488 regulator to permit a supply current to reach an excessive of 1.5A due to originally expecting to power a micro controller, NFC module, SD card module, and ESP8266 Wi-Fi module. However, the final construction of Secured-E-Key required for the inclusion of similar parts from different manufactures which operate off of 5 volts instead of 3.3 volts. The 5 volt supply from the LM3481 powers majority of all the final hardware and can demand a maximum current consumption of up to 708mA in the case of every 5 volts hardware component running simultaneously. All current values portrayed in Figure 4 for the various loads represent the average current consumption required to actively execute a software designated task. Load 10 features a connection directly to the battery power source since a minimum of 6.5 volt supplied to the electric deadbolt is needed for an acceptable performance without any instances of lag.

The LM3488 input voltage varies from 3 to 45 volts with a shutdown current of 5μA and a minuscule supply current not surpassing 3mA. Similarly, the LM3481 input voltage fluctuates between 0 to 50 volts and features a shutdown current of 5 to 10 μA with a supply current not exceeding 5mA. Both regulators together share the important attributes of having internal short circuit, thermal shutdown, and overvoltage protection, a push-pull 1A peak driver, and best suited for applications such as portable applications, distributive and offline power supplies, and Li-ion battery powered systems. Each regulator has an automatic thermal shutdown temperature point of 165 Celsius (329 F) and output voltages capable of ranging from 5 to 12 volts.

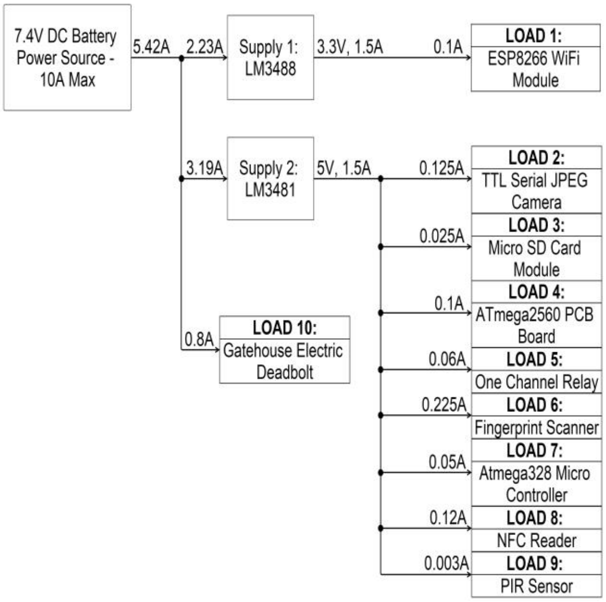
7.4V DC Battery Power Source - 10A Max
5.42A
2.23A
Supply 1: LM3488
3.3V, 1.5A
0.1A
LOAD 1: ESP8266 WiFi Module
3.19A
Supply 2: LM3481
5V, 1.5A
0.125A
LOAD 2: TTL Serial JPEG Camera
0.025A
LOAD 3: Micro SD Card Module
0.1A
LOAD 4: ATmega2560 PCB Board
0.8A
LOAD 10: Gatehouse Electric Deadbolt
0.06A
LOAD 5: One Channel Relay
0.225A
LOAD 6: Fingerprint Scanner
0.05A
LOAD 7: Atmega328 Micro Controller
0.12A
LOAD 8: NFC Reader
0.003A
LOAD 9: PIR Sensor

Figure 4. Power Distribution Model of Secured-E-Key

L. One Channel Songle Relay Module

The Songle relay module uses a high trigger current less than 5 mA to pull or increase the drive capability of a circuit. The device operates off of a simple 5 V logic for home appliance applications to handle voltage and current loads up to 28 VDC at 7 A or 240 VAC at 7A. The module gives Secured-E-Key the ability to put the ATmega2560 micro controller into sleep mode while turning all peripheral devices completely off expect for the PIR sensor. Initially the micro controller successfully used 2N2222 NPN transistors assigned to the control pins of each device in order to switch all peripherals into sleep mode while not executing a task. Due to complications with the software libraries of the PN532 NFC/RFID breakout module, incorporating the code specific to the NFC device prevented the ATmega2560 micro controller from resuming the execution of normal software tasks after awaking from sleep mode. The relay module comes in a size of 46 x 26 x 20 mm, therefore taking up additional space to the Secured-E-Key housing container, but provides the benefit of minimizing current usage to levels even lower than switching all peripheral devices to sleep mode by turning them completely off instead. A simple representation as to how the relay functions corresponds to Figure 5. The PIR sensor connects directly to the power supply since it only demands a measly 28 µA when active as to awaken the micro controller from sleep mode and requires a standby current value of negligible importance during periods of inactivity. The power supply continually remains connected to the relay to power all peripheral devices, while a GPIO pin of the ATmega2560 controls when the peripherals do and do not need powered on by toggling the relay switch

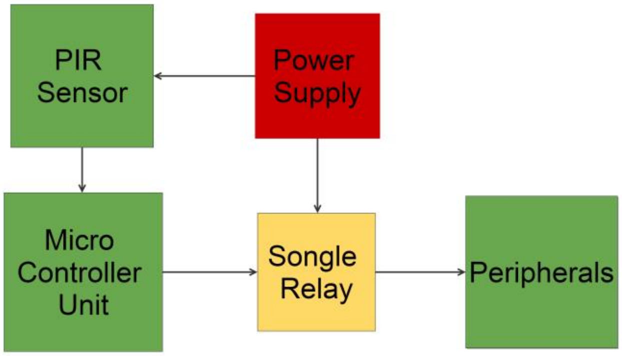

Figure 5. Relay Module Block Diagram

IV. SOFTWARE

The main software dominant components of Secured-E-Key are the MCU and the wireless module. The reason being for less software usage is due to all the members of the group being all electrical engineering majors and having limiting software programming skills. Due to this restraint we are using software that is open sourced and manageable for the members to use. The main software used throughout Secured-E-Key is the Arduino IDE; however, some C level programming is also utilized into some of the component integration as well.

A. Microcontroller Software

To program the ATmega2560 the Arduino IDE will be used. Since Arduino IDE is an open source applications many libraries for the peripheral were incorporated into the overall program. The microcontroller was also programed to optimize power consumptions by implementing power libraries which included timer commands and power states. A flow chart was also created to account for processes that would be used in circumstances. The microcontroller program can be broken down into to 2 states, open and closed. The microcontroller will make the determination if the door is open to keep the door unlocked by determining the value of the reed switch and lock the door if the door is closed. The microcontroller uses the PIR sensor as an interrupt to wake it from power down mode. This will in turn wake up all the peripherals if the door is locked. The presence will have 60 seconds to enter the house or else the microcontroller will go to sleep and lock the door if it is unlocked. The flow chart of Figure 6 gives the explicit details to the overall ATmega2560 program functionality of Secured-E-Key.

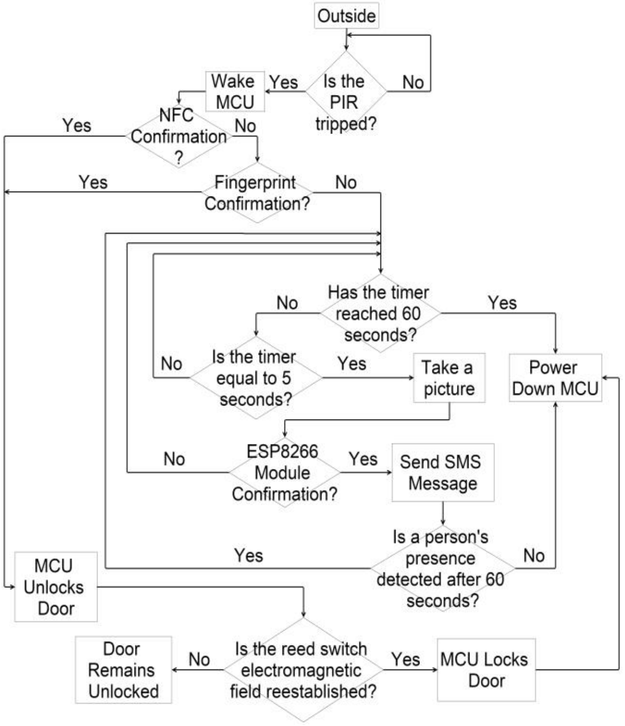
Outside
Is the PIR tripped?
No
Yes
Wake MCU
NFC Confirmation ?
Yes
No
Fingerprint Confirmation?
Yes
No
Has the timer reached 60 seconds?
No
Yes
Is the timer equal to 5 seconds?
No
Yes
Take a picture
Power Down MCU
ESP8266 Module Confirmation?
No
Yes
Send SMS Message
Is a person's presence detected after 60 seconds?
Yes
No
MCU Unlocks Door
Is the reed switch electromagnetic field reestablished?
No
Yes
Door Remains Unlocked
MCU Locks Door

Figure 6. ATmega2560 Controlled Flowchart

B. Communication Protocol Software

The communication protocol that the microcontroller uses is I2C, SPI and UART to communicate with the peripherals. The SD, fingerprint scanner and USB connection uses SPI, the NFC uses I2C and the camera and WIFI uses UART. These devices with its protocol were chosen to allow all of the devices to be implemented on the microcontroller.

C. Wireless Software

AT commands represent the wireless software language needed for Secured-E-Key to fundamentally program the

ESP8266 Wi-Fi module in order to establish wireless communication. The commands work by putting the characters of “AT” before inserting the name of an actual command. The flow chart in Figure 7 shows a generalization to the full context of the software program that Secured-E-Key will execute. Since the user will not receive the image captured as part of the text message notification, the images can be viewed from the micro SD card by removing the card and uploading the images to a computer once the user returns home.

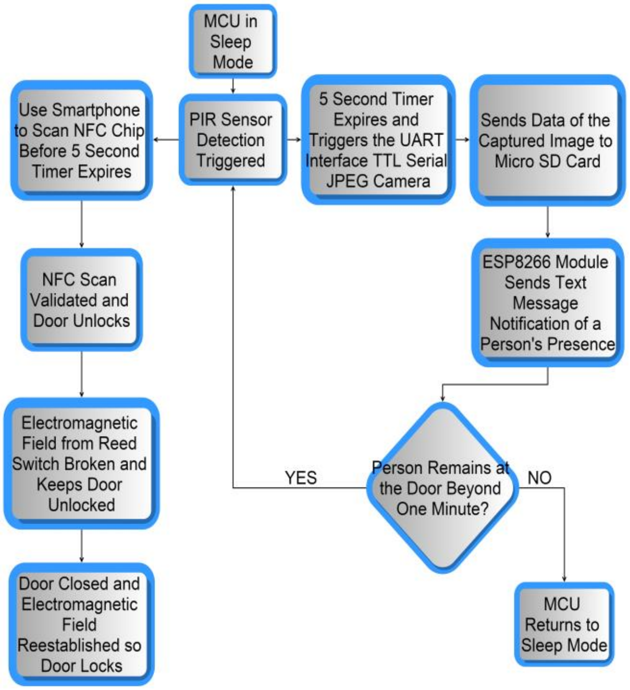
MCU in Sleep Mode
Use Smartphone to Scan NFC Chip Before 5 Second Timer Expires
PIR Sensor Detection Triggered
5 Second Timer Expires and Triggers the UART Interface TTL Serial JPEG Camera
Sends Data of the Captured Image to Micro SD Card
NFC Scan Validated and Door Unlocks
ESP8266 Module Sends Text Message Notification of a Person's Presence
Electromagnetic Field from Reed Switch Broken and Keeps Door Unlocked
YES
Person Remains at the Door Beyond One Minute?
NO
Door Closed and Electromagnetic Field Reestablished so Door Locks
MCU Returns to Sleep Mode

Figure 7. Secured-E-Key ESP8266 Flow Chart

D. JPEG Camera Data Storage and Quality

An interesting feature about the TTL serial JPEG camera is its ability to program the device to capture recognizable images which necessitate the need for only 20 to 30 Kbytes of storage space per image. One clear way of having achieved such a low data size comes from opting for a lower quality camera where the quality will at least remain consistent and reliable. Also, by changing the resolution in the code itself, the camera captures lower quality images. On a number of different camera modules, the image qualities commonly vary from 100 Kbytes to 1 Mbyte size images and do not drop below that size due to being a higher rated camera; even when lowering the resolution quality to the same level as the TTL serial JPEG camera. Captured images requiring low stage space makes Secured-E-Key capable of storing between 100,000 to 666,666 images on a 2 Gbyte micro SD card. Through dramatically lowering the data size of each image, the processing time of capturing and saving each image is reduced down to under 10 seconds, which translates into saving power. Considering the distance of a person when approaching someone’s front door at a distance of around 15 feet, like Figure 8, proves the image quality still provides a sufficient resolution for low byte sized images. Figure 8 equals to a 29 Kbyte size image.

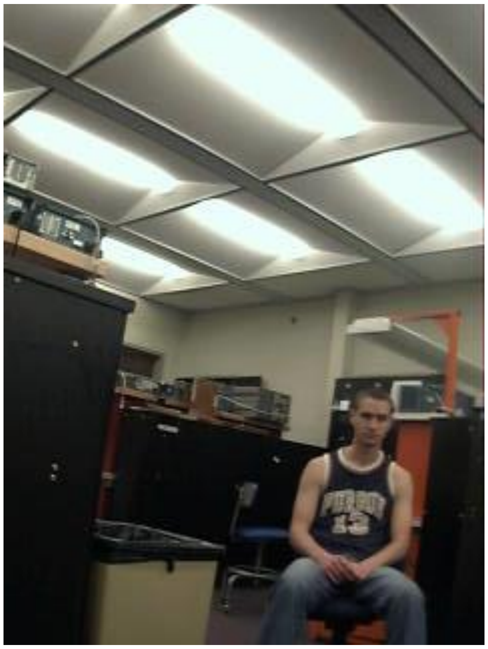

Figure 8. Sample Photo of Low Quality Image at 15 Feet

V. PCB LAYOUT AND DESIGN

The micro controller PCB board featuring the ATmega2560 micro controller and micro SD card socket mounted for storing the pictures taken by the TTL camera, fulfills the role of processing and executing all software related tasks while equaling a total area of 6,921 mm^2 of board space. A second board serving as the power PCB board was solely created to meet the demands of providing power to all of Secured-E-Key’s devices with a total board space of 1,837 mm^2. The Eagle CAD program facilitated with the design and creation of both PCB boards by allowing to develop both boards without a large number of software constraints. The design rules for both boards came from the DRC file located on the OSH Park website for 2-layer boards. The micro controller PCB board cost $62.35 and the power PCB board cost $15.85, although OSH Park automatically sends three copies of any board submitted each time. A computer generated replica of the fabricated micro controller PCB board is shown in Figure 9 whereas the power PCB board is shown in Figure 10. The passive elements primarily used on the boards comprise of resistors, capacitors, and inductors which come in a 0402, 0603, 0805, 1206, or 1210 size footprint.

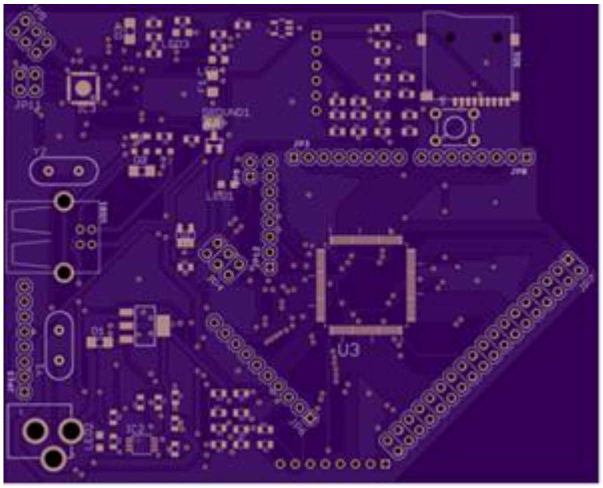

Figure 9. OSH Park Model of Microcontroller PCB Board

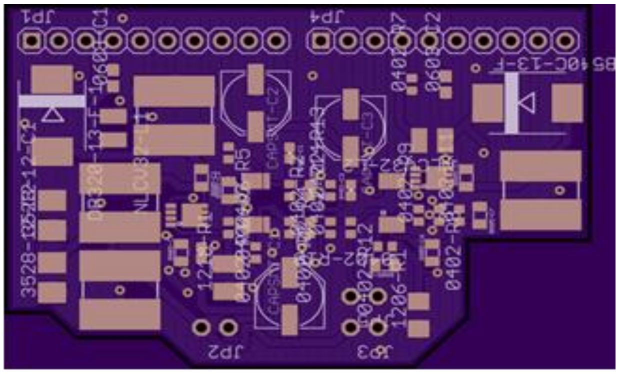

Figure 10. OSH Park Model of Power PCB Board

VI. Conclusion

The group members of Secured-E-Key collaborated very well throughout the project process. Our project allowed each member to gain a set of skills that would be attractive to employers within the engineering workforce. Secured-E-Key involved several different layers of electrical engineering applications such as long range wireless communication, PCB design and development, single source multi-level power design, and software programming into one functioning system. The ability and competency needed to construct Secured-E-Key proved each member's capacity to transition from student to engineer.

Acknowledgement

The group would like to acknowledge and thank the Department of Electrical Engineering and Computer Science at University of Central Florida.

The Members

Sheldon Johnson is currently a senior at the University of Central Florida. He is expected to graduate with his Bachelors of Science in Electrical Engineering on August 8, 2015. Upon graduation he will commission as an officer in the United States Air Force to work in the field of cyberspace operations. He enjoys reading and staying active.

Enjolie Morales is currently a senior at the University of Central Florida. She is expected to graduate with her Bachelors of Science in Electrical Engineering on August 8, 2015. Upon graduation she will commission as an officer in the United States Air Force to work in the field of Cyberspace Operations. She enjoys soccer and cats.

Shawn Gangasingh is currently a senior at the University of Central Florida. He is expected to graduate with his Bachelors of Science in Electrical Engineering on August 8, 2015. Upon graduation he plans to pursue a career in Electrical Engineering. His hobbies include robotics and playing guitar.

Saint-Surin W Paul is currently a senior at the University of Central Florida. He is expected to graduate with his Bachelors of Science in Electrical Engineering on August 8, 2015. Upon graduation he plans to pursue a career in Electrical Engineering as he always wanted. He enjoys watching movies and preaching the good word of God.

REFERENCES

[1] Adafruit Fingerprint Scanner <http://www.adafruit.com/products/751?gclid=Cj0KEQjw27etBRDA3-ux4p3c58EBEiQAkJzTAMDbXq7j6pP1T7vpozMB7-5i8paaFDXsIIzErpHZY0AaAnoW8P8HAQ>

[2] ESP8266 English Specifications, October 2013, July 2015. <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=0CDoQFjADahUKEwih8f-x7OrGAhVCKx4KHehhCo0&url=http%3A%2F%2Fwww.adafruit.com%2Fdatasheets%2FESP8266_Specifications_English.pdf&ei=FoKtVaGOL8LWeOjDqegI&usg=AFQjCNG9qkY0vU9suD7gm74UvB7rqnNnjg&sig2=KHTNFnlfmm6xPQ3Ia1gUUQ&bvm=bv.98197061,d.dmo&cad=rja>

[3] Gatehouse Electronic Motorized Deadbolt <http://www.lowes.com/pd_399128-51800-G2X2D01_0__?productId=3799025>

[4] LM3481 Texas Instruments, November 2014, July 2015. <http://www.ti.com/product/lm3481>

[5] LM3488 Texas Instruments, December 2014, July 2015. <http://www.ti.com/product/lm3488>

[6] PIR Mini Sensor <http://simplytronics.com/products/ST-00082>

[7] PN532 NFC Chip <http://www.nxp.com/documents/short_data_sheet/120112.pdf>

[8] TTL Serial JPEG Camera with NTSC Video <http://www.adafruit.com/product/397>