**Intelligent Door System**

**Group #33 3333 33**

Team Members:

Gregory Escobar

Stephen Benavides

Shawn Carnevale

Geomar A. Reyes

Advisor:

Dr. Sosnowski

Area of Study:

Computer Engineering

Electrical Engineering

Submission date:

4/7/2019

**Abstract:**

The name of this project is intelligent door system. Our team members are Gregory Escobar, Stephen Benavides, Shawn Carnevale and Geomar A. Reyes. The name of our advisor is Marek Sosnowski. The ideal behind our project is to create an intelligent door lock that can be lock and unlock through a cellphone app. Also this intelligent door lock has to be able to unlock and lock the door lock through a keypad just in case a person loses the phone.

**Table of content:**

**Abstract …………………………………………………….2**

1. **Introduction…………………………………………..4**
2. **Project accomplishment ……………………………..5**
3. **Budget ………………………………………………...10**
4. **Acknowledgment……………………………………..11**
5. **Reference……………………………………………...11**
6. **Appendices……………………………………………..12**
7. **Introduction**

The ongoing evolution of the network of computing devices embedded in everyday objects to transmit and receive data better known as the Internet of Things (IoT) has enabled devices to become smart objects. For our senior project we wanted to do something that could be practical, have multiple uses, and would be marketable to the public. Everyone likes the feeling of their house being secure. For this reason, we decided to do a security system. Our previous proposal we were interested in designing an Intelligent Door System. Unfortunately, due to time constraints and our project getting more complex the scope of the project changed from being marketed to the industry and residential homes to being strictly marketed to residential homes.

When we were in the design phase of the project we were influenced by the *Ring Door Bell* and the *Nest Padlock*. What we liked about the *Ring Door Bell* is the built-in camera. When someone comes into the vicinity of the doorbell the camera turns on and your phone will get a notification and you can see through your phone who is at your door step. This concept alone made us interested implementing a camera because previously we only had our project lock and unlock a door so we wanted to make our project more interesting. Another item that influenced our project is the *Nest Padlock.* How this worked is you download an application on your phone. Once downloaded you can lock or unlock your door through your phone. It also has a keypad on it so instead of giving someone a key you can give them a passcode. What aspects of the *Nest Padlock* influenced our project is the application on your phone, being able to lock or unlock your door through your phone, and that the user doesn’t need a key. This also replaces deadbolt doors and someone would not have to deal with losing keys.

Our original intention for our project was we wanted the user to able to lock and unlock the door. If somebody entered the wrong passcode the user would get a notification on their phone and the camera would turn on and the user could see who was at the door*.* Unfortunately, due to time constraints and shipping issues we were not able to add the camera module to our project. Since it would be too expensive and complex to implement it onto a door we instead have 3D printed enclosure with a moveable part. What will happen is when the user wants to unlock the door the user will open an application on their phone and enter a username and password. When the user enters the correct information, the application will go to a new page and the user can tap an open icon on their phone. Once the user presses the open icon a solenoidal lock will get energized and the movable part will be unlocked. At this point the user has the option to lock the door by pressing the close icon on the phone application or the solenoid will get un-energized in thirty seconds. In the case of a power outage there is a keypad where if you enter the correct passcode you unlock the door. If somebody enters the wrong passcode you will get a notification on your phone telling you somebody entered the wrong passcode.

**Project Objectives**

For our project our objective was to design a residential security system. When considering how we would design it we put took some stuff into consideration. The first consideration was to make it affordable because of limited funds. Another thing we took into consideration is making it simple enough to build. Since we have a time constraint we wanted to make sure we were able to complete our project and make it as interesting as possible.

**Project Significance**

What makes our project significant is the application of the security of homes. Everybody likes to feel safe when they are in their home and want to make sure that when they are not home their home is secure. This reason alone makes our project significant. Parks Associates in 2018 estimate that by 2021 27% of Americans will have security systems installed in their homes proving that more people in the America are getting interested in equipment that helps make their home more secure. It allows the user to integrate the regular key that is usually used to a smartphone and make it more practical.

**Project Novelty**

When looking at what the market has to offer for residential security systems we noticed we have aspects that make our project unique. The main reasons why our project is different is than what is offered on the market is our software.

**2. Project accomplishments**

2.1 Technical details

**Hardware**

**Power and Battery:** It consists of the following three components

* 100 - 240V 50/60Hz AC Adapter (5V 1A).
* Panasonic NCR18650B lithium battery 3.7V
* Wemos 18650 Battery Shield v3

The power system was designed to behave as an uninterruptable power supply by allowing the user to power the electronic using an AC-DC convert adapter (5V 1A) and in case of a power outage condition it will be powered by a high capacity lithium battery. It provides the system with a 3.3V line for the microcontroller and12V line for the solenoid. The battery shield consists of a 1A Standalone Linear Li-Ion Battery Charger with Thermal Regulation (TP4056), three low voltage dropout CMOS voltage regulators (LDO 3.3V) and a LM2577 step up voltage regulator (3.3V to 8V). A block has been attached to the appendix of this paper.

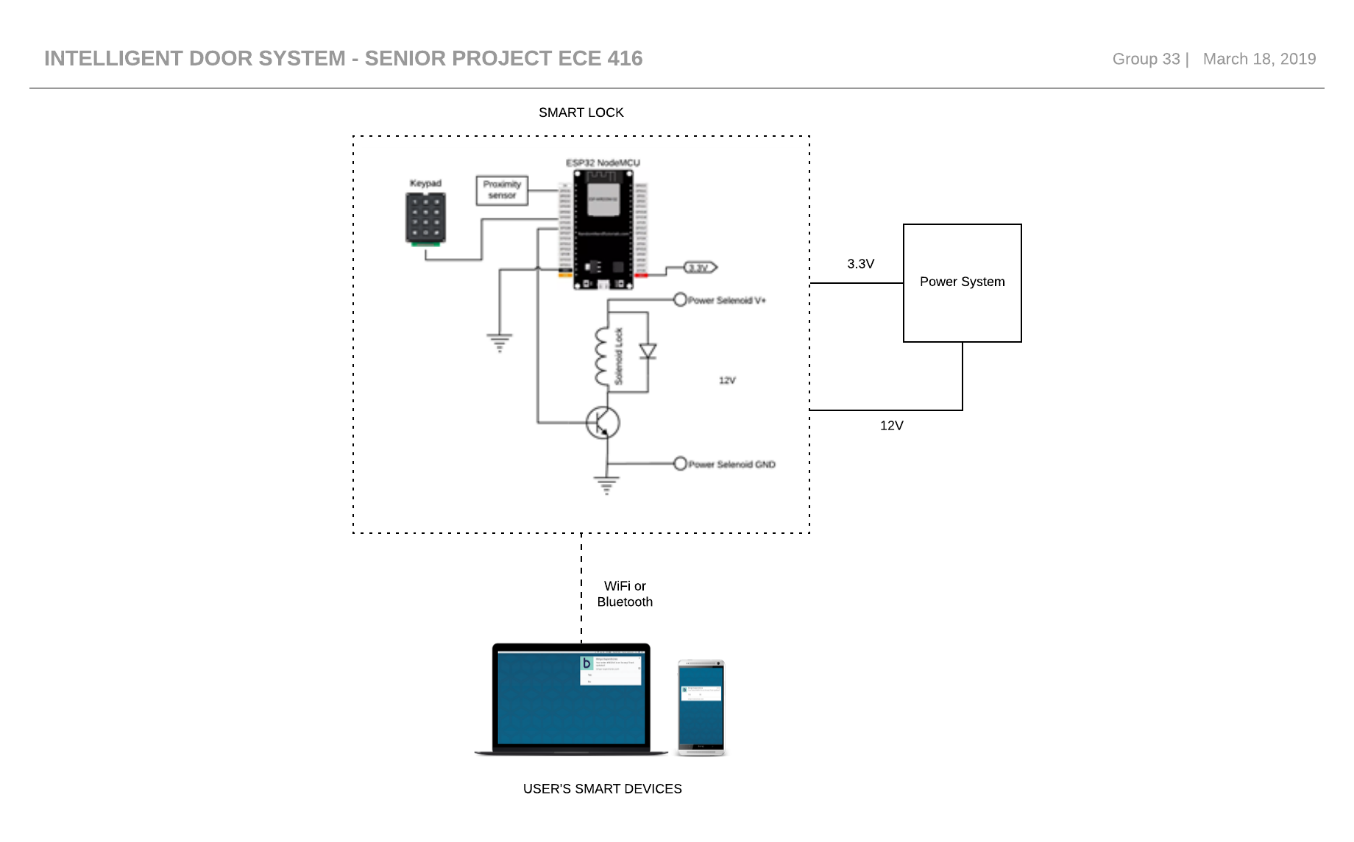
**Microcontroller:**

* ESP32S Node MCU

The ESP32S is a single chip microcontroller with 2.4 GHz Wi-Fi-and-Bluetooth capabilities that targets a wide variety of applications that required low power consumption and good RF performance. It uses two adjustable clock frequency (80-240MHz) 32-bit Xtensa LX6 processors that use the Tensilica ISA. ESP32S integrates a rich set of peripherals, ranging from capacitive touch sensors, Hall sensors, low noise sense amplifiers, SD card interface, Ethernet, high speed SDIO/SPI, UART, I2S and I2C. This microcontroller supports data rates up 150Mbps and 20dBm output power at the antenna. The ESP32S was designed using the TSMC ultra-low-power 40 nm technology.

**Lock-Style Solenoid:**

* 12VDC (you can use 9-12 DC volts, but lower voltage results in weaker/slower operation)
* Draws 650mA at 12V, 500 mA at 9V when activated
* Designed for 1-10 seconds long activation time
* Max Dimensions: 41.85mm / 1.64" x 53.57mm / 2.1" x 27.59mm / 1.08"
* Dimensions: 23.57mm / 0.92" x 67.47mm / 2.65" x 27.59mm / 1.08"
* Wire length: 222.25mm / 8.75"
* Weight: 147.71g



**Engineering Standards:**

**FCC title 47 CRF part 15**: The smart lock complies with the FCC title 47 CRF part 15 regulates everything from [spurious emissions](https://en.wikipedia.org/wiki/Spurious_emission) to unlicensed [low-power broadcasting](https://en.wikipedia.org/wiki/Low-power_broadcasting).

**IEEE 802.11b Standard:** It has a maximum raw data rate of 11 Mbit/s, and uses the same media access method defined in the original standard. 802.11b products appeared on the market in early 2000, since 802.11b is a direct extension of the modulation technique defined in the original standard.

**IEEE 802.11g Standard:** This works in the 2.4 GHz band (like 802.11b), but uses the same [OFDM](https://en.wikipedia.org/wiki/Orthogonal_frequency-division_multiplexing) based transmission scheme as 802.11a. It operates at a maximum physical layer bit rate of 54 Mbit/s exclusive of forward error correction codes, or about 22 Mbit/s average throughput.

**IEEE 802.11n Standard:** It is an amendment that improves upon the previous 802.11 standards by adding [multiple-input multiple-output](https://en.wikipedia.org/wiki/Multiple-input_multiple-output) antennas (MIMO). 802.11n operates on both the 2.4 GHz and the 5 GHz bands.

**IEEE 802.15.1 WPAN/Bluetooth Standard:** It defines physical layer (PHY) and [Media Access Control](https://en.wikipedia.org/wiki/Media_Access_Control) (MAC) specification for wireless connectivity with fixed, portable and moving devices within or entering personal operating space.

2.2 Testing and Performance Measures

The system was tested to estimate operation time and the power consumption in case of a power outage condition. The ESP32S Node MCU + electronics (LEDs and keypad) was estimated to consume 38mA when the CPU is operating at 80MHz clock frequency. Since this microcontroller operates at 3.3V the power consumption is about ~125.4mW. The solenoid consumes 400mA at 9V meaning that the power consumption is about ~3.6W. The time that the solenoid consumes such power is limited by the software implementation. The capacity of the battery that is used on the system is 3500mAh. Therefore, the lock can operate for at least 8 hours in case of a power outage.

2.3 Future Potential

The project could be enhanced by implementing different method of authentication like biometric or face recognition.

2.4 Learning Experience

The project allowed us to learn about PCB design, soldering skills, power electronics and network design.

**Software:**

The ESP 32 software has been successfully implemented into the hardware. The team was able to test the Wi-Fi connection by using a cellphone with hotspot included as a router to transmit a signal between the ESP32 and the APP by using the mobile network provided by AT&T. The test was successful, so we were able to send the right signal from the APP to the lock to open or close it at will. Our next goal was to check if the app was able to communicate across networks that are intended to be used by outside guests such as the ones that you get at a coffee shop, they are usually open for everyone and unsafe. For this test, we used NJITguest with a student credential to access. Unfortunately, the NJIT network asks for a specific set of permissions and confirmations when accessing their network; therefore, the test for direct connection with the NJIT network was unsuccessful. Then we decided to use a “router” to redirect the signal from the NJIT into the ESP 32. We were able to do so by sharing hotspot with the cellphone to the esp32, but instead of using the mobile connection we shared the NJIT Wi-Fi through the phone. Thus, proving that we can connect our device on any network that has a router to redirect the signal.

Application

• Our goal was to add a background for the app, we made it look more professional and user friendly • We tested the communication between the hardware and the app through the ESP 32 • A link was successfully created between the app and the ESP32 • The user interface can store the username and password by using a TinyDB to store that information in the app’s cache • The user interface sends error messages when the username or password is incorrect

Network Framework

• Connection has been made successfully between the lock, the esp32 and the application. • The ESP 32 can now build a web server to send and receive requests from the exterior. • A protocol has been implemented into the esp32 to change the way in which we access into the server. We no longer have to put an IP address into the search bar of any device connected in LAN, now we can use an specific name to make it easier to access i.e. from http://192.168.43.57 we changed it to http://smartlock.local • The code that requests signals from the ESP 32 has been modified using an encrypted password, and the only way to decrypted is by using the app.

Future Upgrades

• Implement a method to send messages to the user when initializing the smart lock for the first time • Implement a method to send messages to the user every time the door has been access • The messages will be sent to the costumer via text messages and email to make it safer. The user will have control over everything that happens around the lock on real time

• Create a dedicated web server http://smartlock.local where the user is going to be able to know the status of the lock. i.e. How long the door has been active for as well as the temperature of the internal mechanisms.

**3. Budget**

|  |  |  |
| --- | --- | --- |
| Name | Quantity | Price |
| 12V Electronics Lock Assembly Solenoid Low Power Consumption | 1 | $17.61 |
| ESP32S | 1 | $11 |
| 1N4004 Diode | 1 | $0.05 |
| TIP102 Transistor | 1 | $1.60 |
| Wemos 18650 Battery Shield v3 | 1 | $3.0 |
| DC-DC boost converter | 1 | $8.00 |
| Single Pole Double Throw Switch | 1 | $1.62 |
| RGB LED WP154A4SUREQBFZGC | 1 | $1.88 |
| Pushbutton | 2 | $0.42 |
| Female Headers | 2 | $2.00 |
|  | Total | $47 |

**4. Acknowledgements**

We thank Diego Ramos, EE student, for helping us designing the PCB for the project.

**5. References**

“IEEE 802.11.” *Wikipedia*, Wikimedia Foundation, 6 Apr. 2019, en.wikipedia.org/wiki/IEEE\_802.11#802.11b.

“IEEE 802.15.” *Wikipedia*, Wikimedia Foundation, 26 Mar. 2019, en.wikipedia.org/wiki/IEEE\_802.15#Task\_group\_1\_(WPAN/Bluetooth).

Pluvinage, Lucas. “The Xtensa Architecture.” *MirageOS on ESP32 - a Tale of Cross-Compilation*, 28 Mar. 2018, www.lortex.org/posts/esp32/2018/03/28/the-xtensa-architecture.html.

*ESP32 Overview | Espressif Systems*, www.espressif.com/en/products/hardware/esp32/overview.

**Appendices**

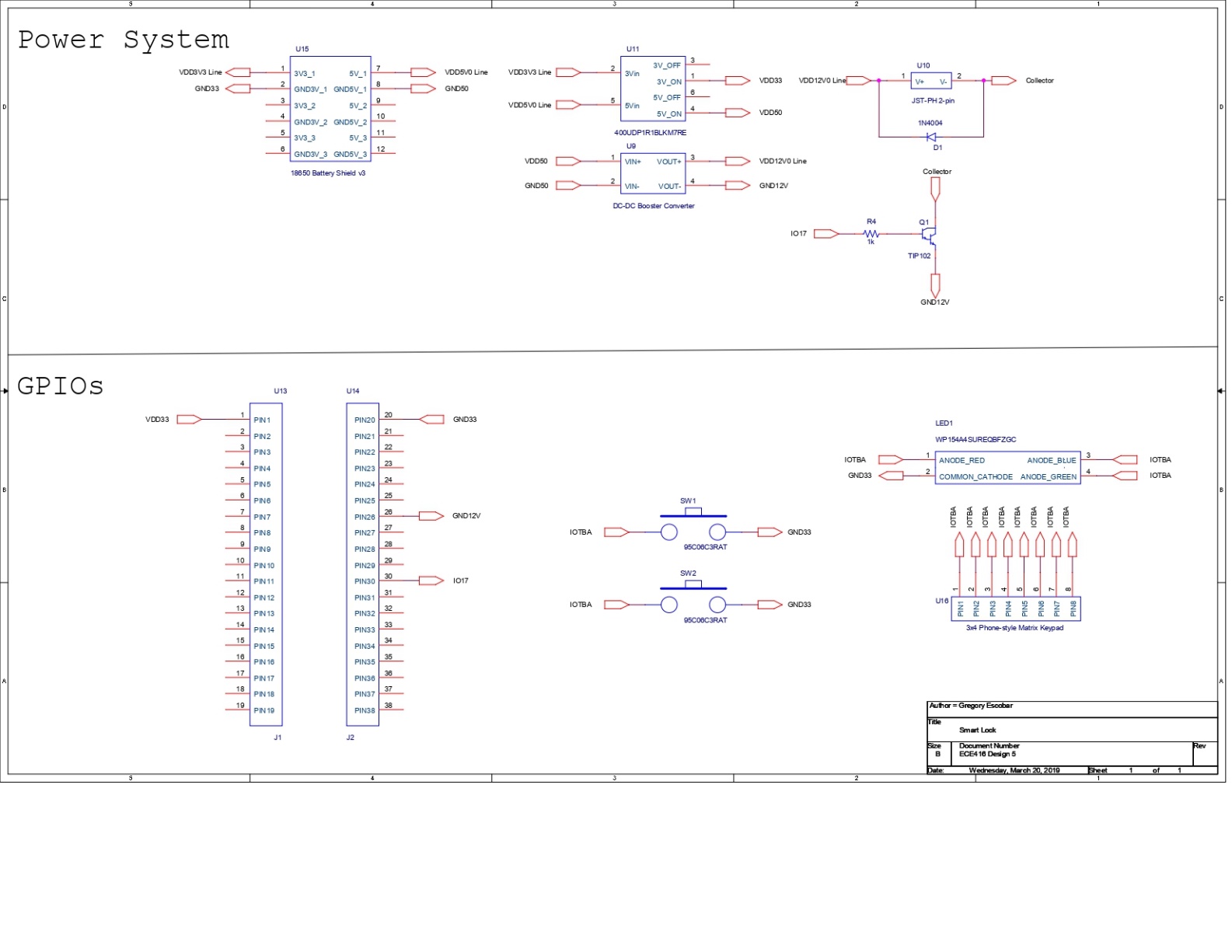
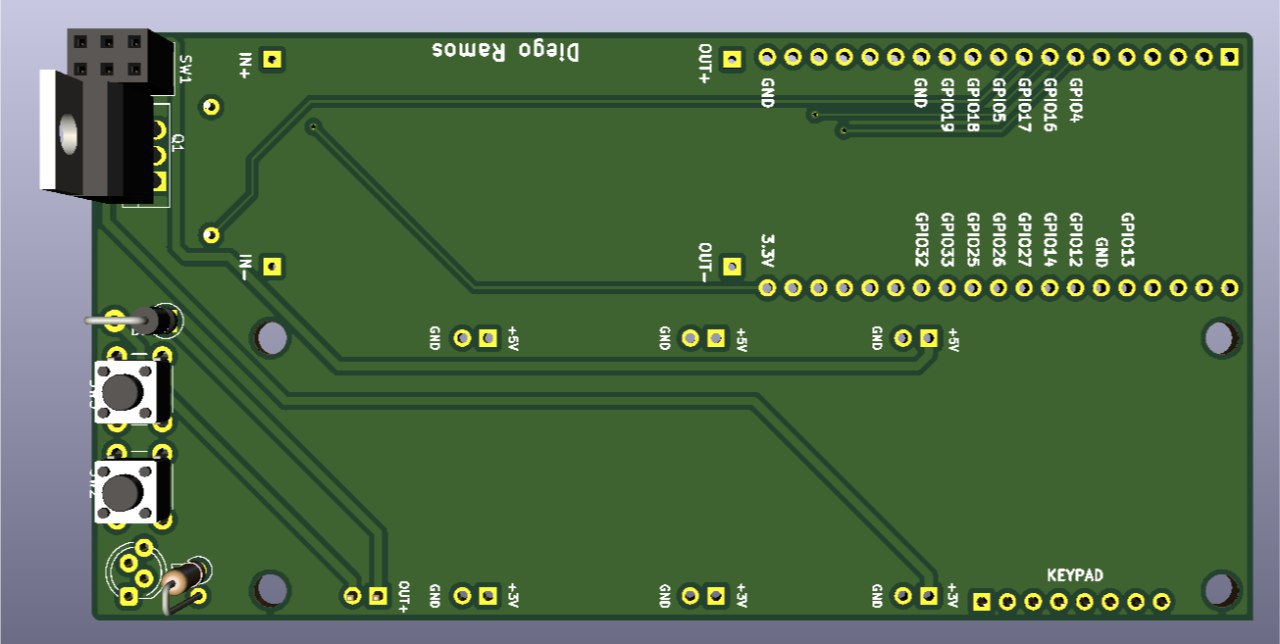
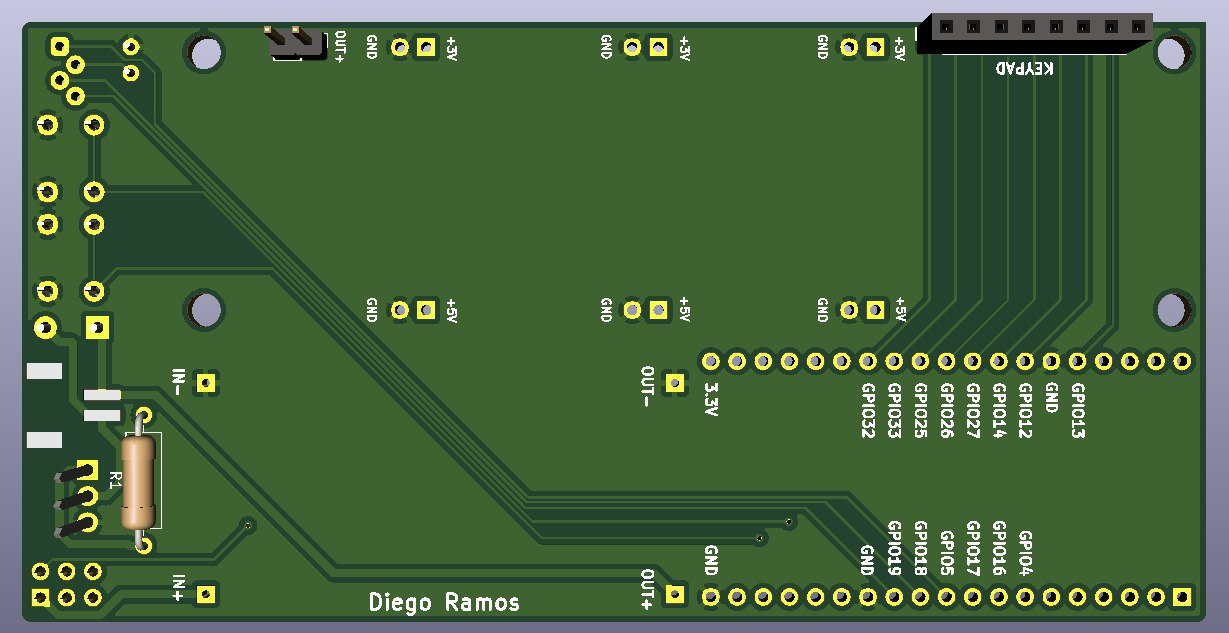


Figure 1 Smart Lock Schematic





App code:

