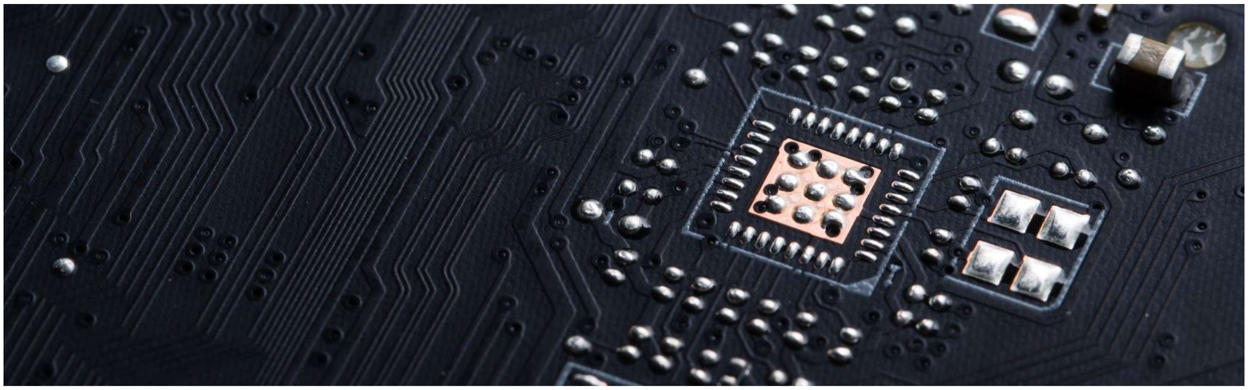
ELECTRICAL & COMPUTER ENGINEERING
UNIVERSITY of WASHINGTON



Password Based Door Lock Report

Hao Lam
Gang Ouyang
Jun Fang
Quan Vo
Osman Torres-Alfaro

University of Washington
Department of Electrical and Computer Engineering
Seattle, WA 98195 USA

Submission Date: March 13th, 2023

Table of Contents

Teams, Roles, and Responsibilities

For this project, we decided to split the whole project into three big components, where each component is taken care by one team. The first portion is the embedded part which will be completed by Hao and Gang. They are responsible for programming the RPI to process and communicate among elements in the system. The elements include the camera, Gmail, phone notification, facial recognition, keypad, and LCD. The second portion is the mechanical part, Osman and Quan will work together to program the STM32 to control the servo based on the state of the lock. The last portion is the hardware portion. In this part, Jun will generate the 3D model for the whole project by using fusion 360 which is a CAD platform for 3D modeling and printing. This team is also responsible for power consistency of the system.
In addition, Hao also serves as the project manager, responsible for managing the overall project schedule and holding meetings.

Product Requirements Document

Our project consisted of making a door lock security system. Our door lock security system would be able to provide an extra layer of security to the consumers through a password-based system. This would solve an issue of security both at households and businesses. Our system would be installed on doors where the user would have to go up to the door and input a password to open the door. The user would setup a four-digit password that would open the lock from the outside. The user would have three attempts to enter the correct passcode, after every failed attempt, the main user will receive a notification on their phone stating someone has entered the incorrect password. After a third consecutive incorrect password, the camera controlled by the Raspberry Pi will capture a picture of the person inputting the passwords and send an e-mail to the main user reporting the suspicious activity. Additionally, after the three consecutive incorrect password input, the main user would also get an e-mail with a new, randomized password that would unlock their door. The old password will no longer work after the suspicious activity. Furthermore, our project also includes two buttons. One button acted as a button that would be inside the household or building, and the second button was outside. The button on the inside would be able to close and open the lock whenever the button was pressed. However, the outside button can only close the lock, if the lock is already closed pressing the outside does nothing. Optionally, there is a face recognition feature, which acted as a second layer of security if the user prefer.

Realistic Constraints and Engineering Standards

The Realistic Constraints are described in the System Requirements Document section. The following is the Engineering Standards section.

1. Safety standards (rigid)

Our door lock product needs to meet certain safety standards to ensure that it operate properly and do not pose any risk to users or their property. Here are the safety standards:

- UL 1034: This is a standard for burglar-resistant electric locking mechanisms. UL 1034 evaluates the safety and effectiveness of electronic locks to ensure that they provide the necessary level of protection against forced entry.
- ANSI/BHMA A156.25: This standard specifies the requirements for electronic access control systems. ANSI/BHMA A156.25 evaluates the safety and durability of electronic locking systems to ensure that they meet the necessary standards for functionality and safety.
- FCC Part 15: This is a standard for electromagnetic interference (EMI) emissions. FCC Part 15 ensures that electronic devices do not emit harmful levels of EMI that could interfere with other electronic devices or cause safety hazards.
- RoHS: The Restriction of Hazardous Substances (RoHS) directive is a set of standards that restrict the use of certain hazardous materials in electronic devices. RoHS compliance ensures that smart door locks do not contain harmful substances that could pose a risk to users or the environment.
- IP Rating: The Ingress Protection (IP) rating is a standard that indicates how well a device is protected against dust and water intrusion. If our door lock product installed outside, then it should have an IP rating that protects the device from weather conditions, such as rain, snow, and extreme temperatures.

2. Encryption standards (rigid)

Our system uses Secure Hash Algorithm 2 (SHA-2) published by the National Institute of Standards and Technology (NIST) to encrypt the passwords, following the U.S federal standard.

3. Communication and interface standards (negotiable)

- Raspberry Pi GPIO: The Raspberry Pi has General Purpose Input/Output (GPIO) pins that can be used to interface with hardware components such as sensors, motors, and switches. It can be used to communicate between the Raspberry Pi and STM32 microcontroller.

- SMTP: SMTP is a standard protocol used for sending email messages. The door lock system could use SMTP to send email notifications to designated email addresses when a wrong password is entered.
- WIFI: Wi-Fi is a wireless communication standard that can be used to connect the Raspberry Pi to a local network or the internet. It can be used for remote monitoring and control of the door lock system.
- Gotify API: Gotify API uses the HTTP protocol to send and receive push notifications. The door lock system could use Gotify API to send push notifications to the Gotify server, which would then forward the notifications to designated clients.

4. Software development standards (negotiable)

We use the following standard to manage the development process. This can improve the modularity and maintainability of the software system.

- ISO/IEC/IEEE 12207:2017 ISO/IEC/IEEE International standard – Systems and software engineering – Software life cycle processes

System Requirements Document

1. Functional Requirements

1. The system must stay locked from the outside until the correct password is entered.
2. The system reset must be done by authorized employees only.
3. The system must detect possible break-ins and notify owner with sufficient information within a reasonable amount of time.
4. The system must unlock and lock within seconds after a user open or closes the system.

2. Mechanical Requirements

1. The system must not break under force applied by a typical adult human.

3. Size, Weight, and Cost Requirements

1. The system is approximately the size of a typical double lock (6” x 4”), weighs less than 2 lb, and cost less than $250.

4. User Interface Requirements

1. The system must notify owners through owner’s mobile cellular devices.
2. The system must provide users instructions and feedback in an intuitive manner using neutral, inoffensive language.

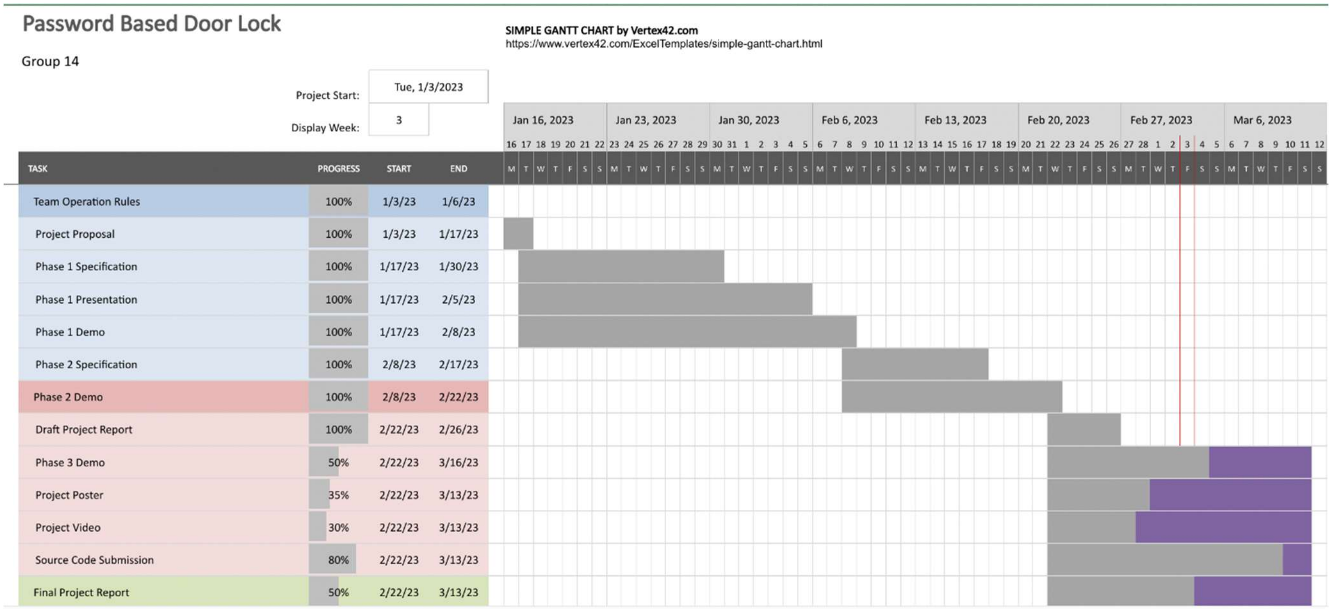
5. Data Storage, Format, Security Requirements

1. The system must store all passwords in hashed and salted form.
2. The must system must store all user identifiable information in a secure manner.

6. Precision and Accuracy Requirements

1. With face recognition as an optional feature, we know that there is no way to guarantee 100% accuracy, but for facial recognition to be usable, we must guarantee at least 80% accuracy. That is, facial recognition was successful in 4 out of 5 attempts.
2. Facial recognition is based on confidence. Find a suitable level of confidence, so that facial recognition is relatively reliable and has more than 80% accuracy.

Project Schedule



Project Resources

1. Human Resources:

R&D Team members: Hao Lam, Gang Ouyang, Jun Fang, Quan Vo, Osman Torres-Alfaro

2. Funding:

Financial budget: $50 per person. Total is $250.

3. Hardware Resources:

- RPI camera Module V1
- MG996 Servo
- 4x4 Membrane Matrix Keypad
- 16x2 LCD
- STM32
- RPI
- Lock
- Box
- Power bank
- AA Batteries Holder
- Dupont Wire and other wires
- Double sided PE Foam Tape

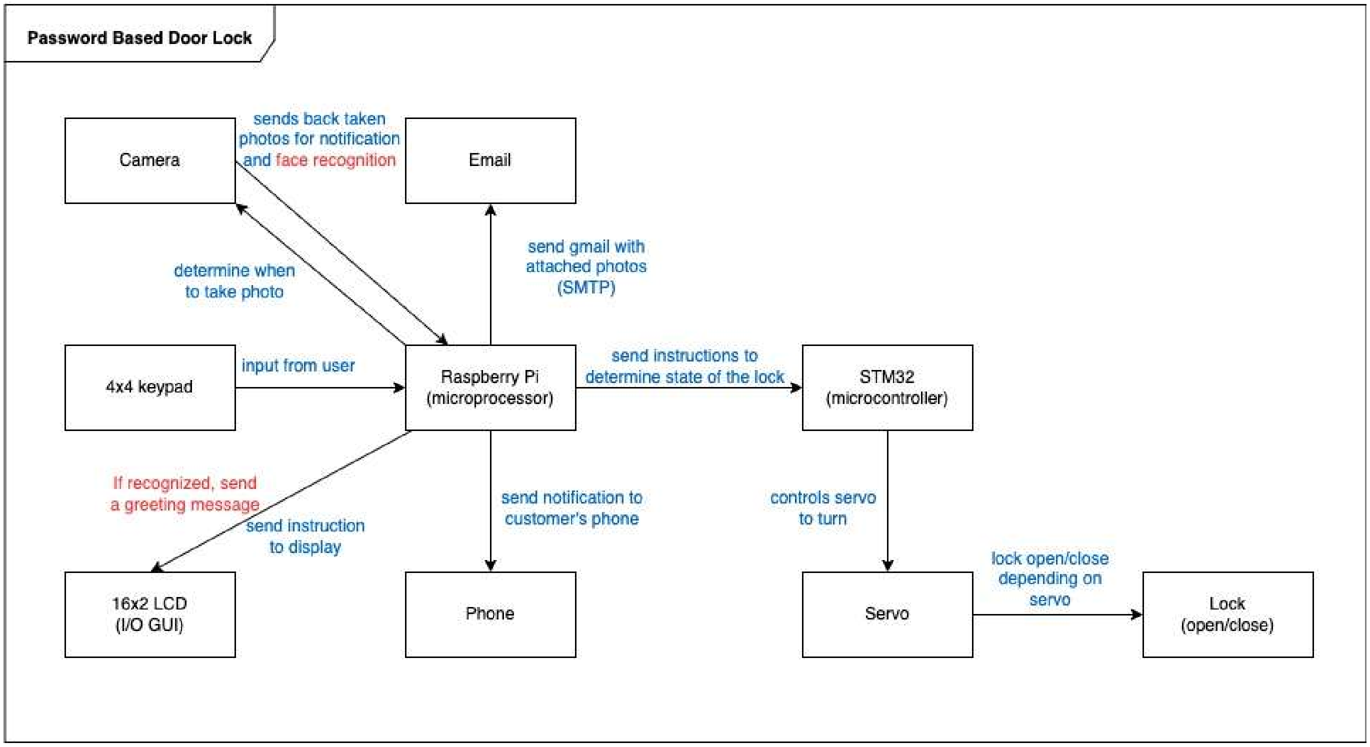
Outline of Experiments

First, we prioritized finishing the overall design and listing all the required hardware parts of the project. Next, we ordered the parts, and each team started working on their responsible tasks. The hardware team started with paper then CAD design for the product prototype. The mechanical team worked on setting up the STM32 and controlling the servo. The embedded team worked on implementing the modules to communicate among each element. Next, when the parts arrived, we put them together and start testing. Once everything works, we start to assemble the box and wirings based on the CAD design. Finally, we added face recognition feature and optimize for the system to run faster.

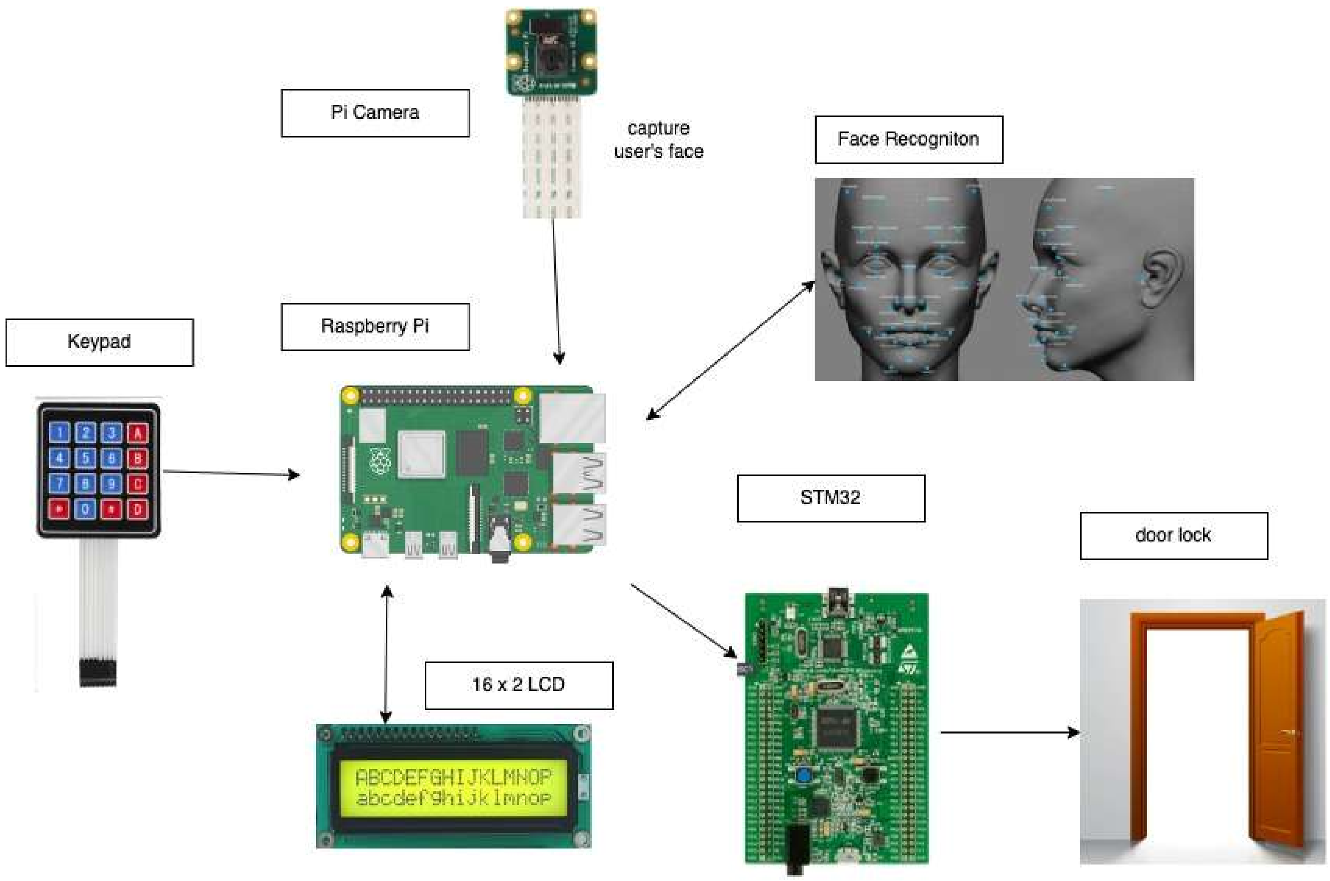
Trial Designs

The following is our relevant experimental design drawing for the door lock project, including block diagram, hardware schematic diagram, bill of materials, assembly drawing, UML workflow diagram, and an explanation of how it works.

1. Door lock system design block diagram:



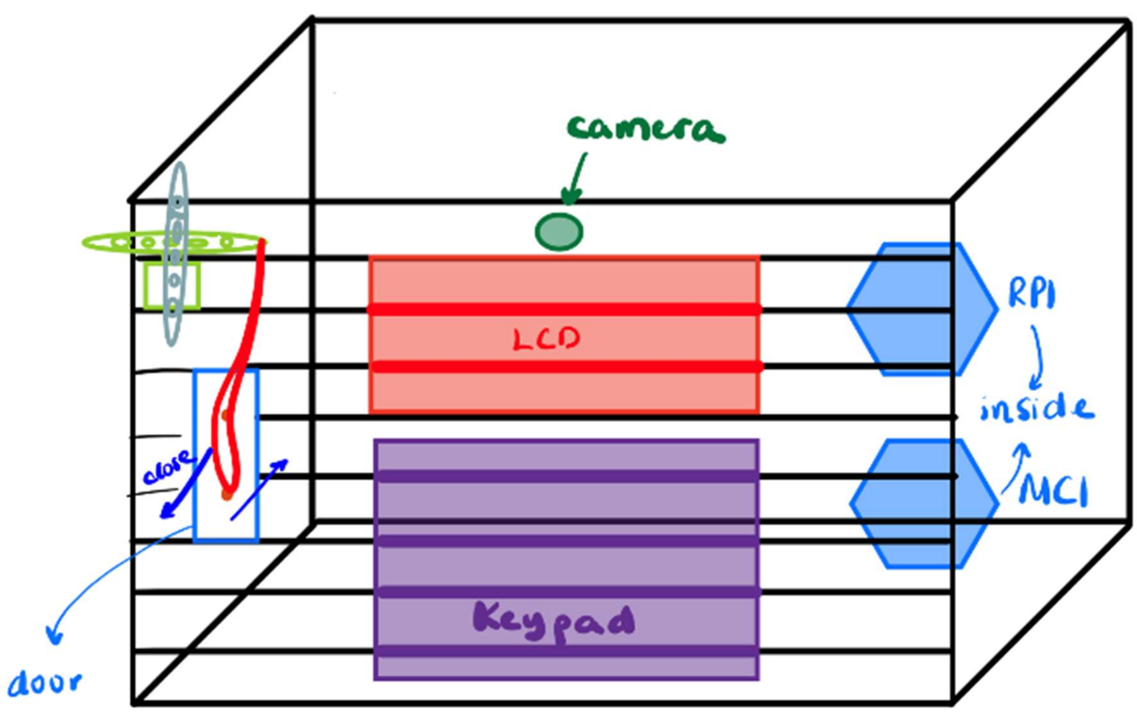
2. Hardware schematic diagram

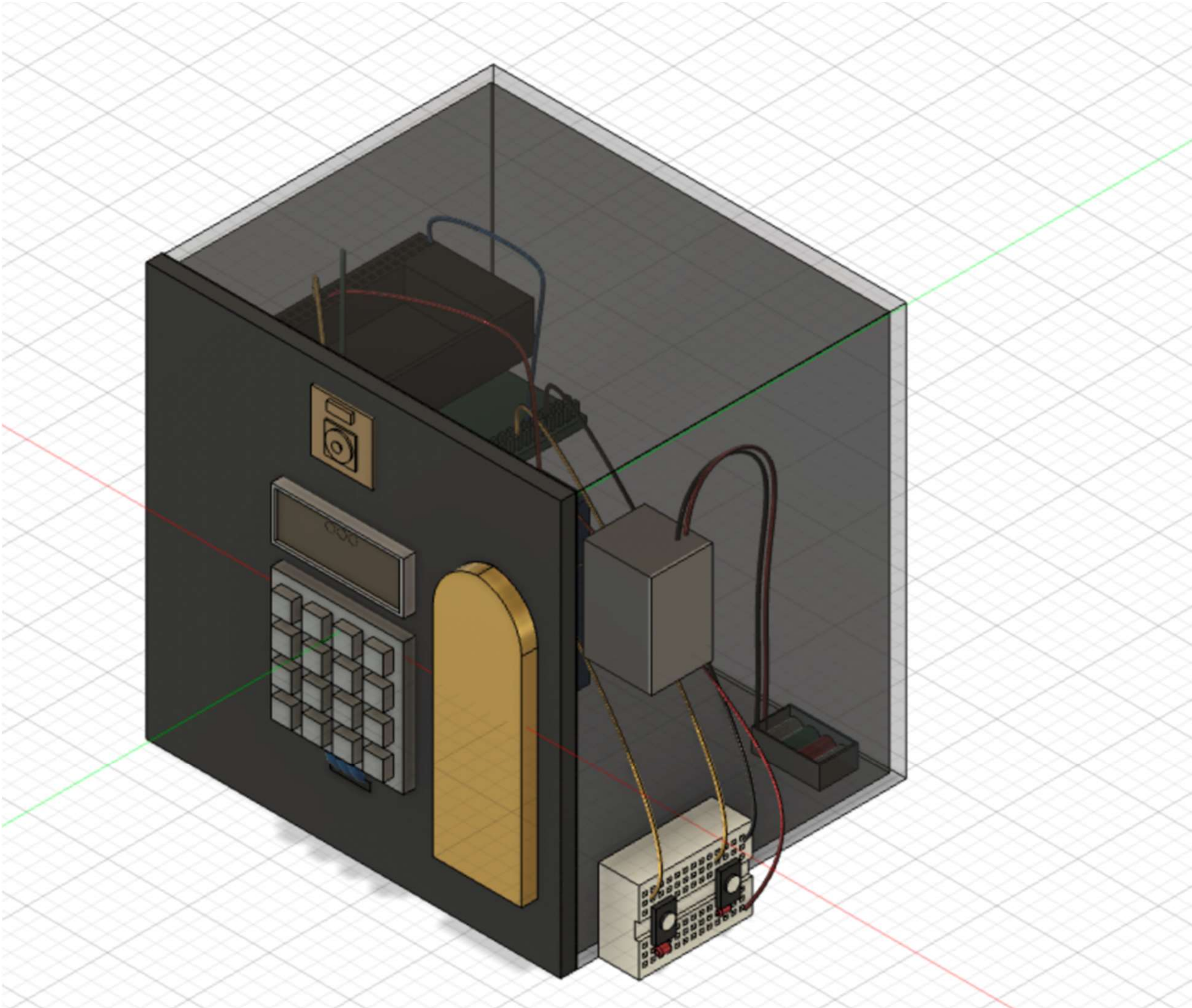


3. Bill of materials

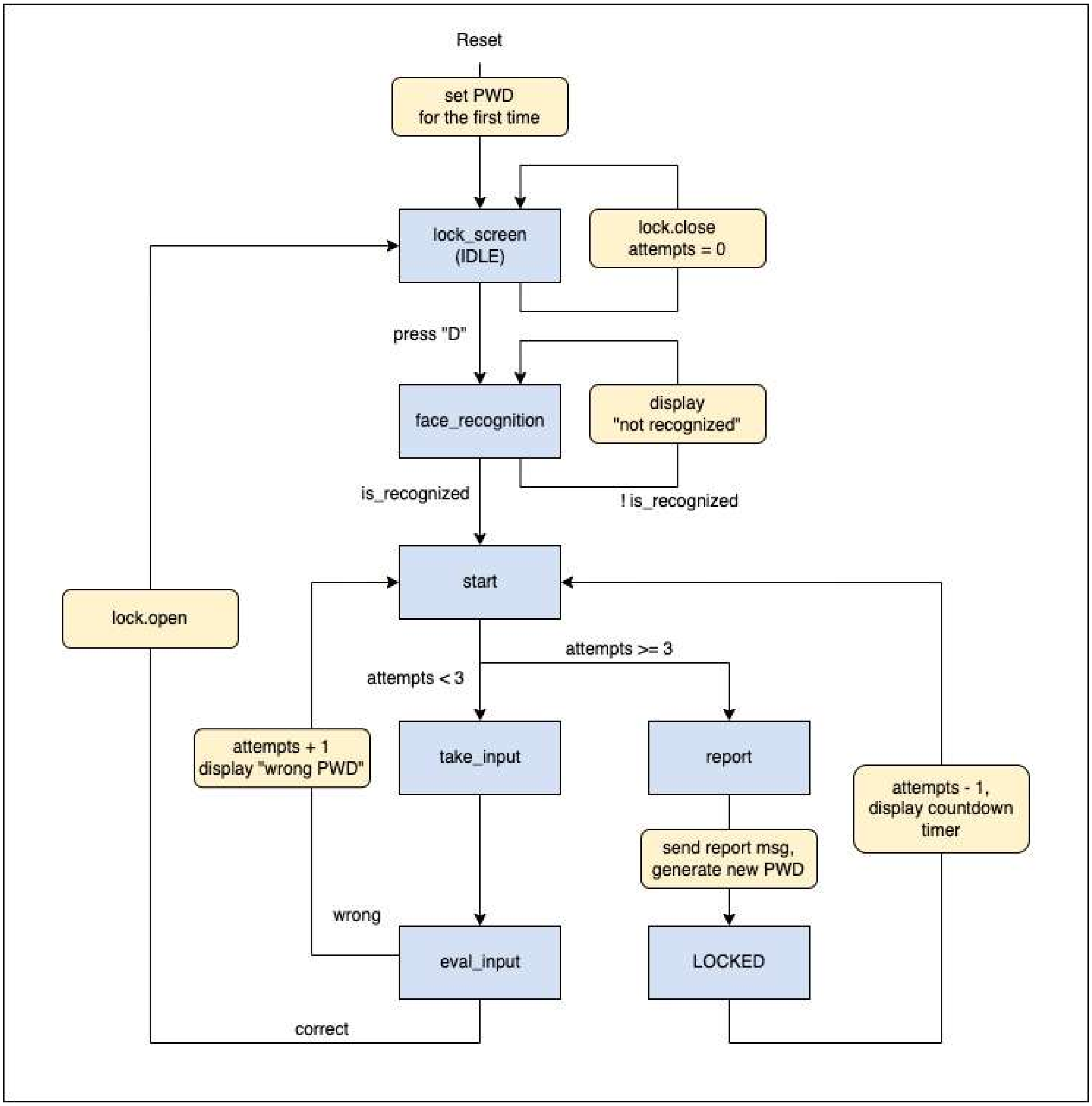
BILL OF MATERIALS VERSION 2				
No	Item	Quantity	Approx. cost per item ($)	Total
1	ATC2816	0	12.99	0
2	Raspberry Pi Camera Module V1	1	25	25
3	MG996 Servo	1	8.76	8.76
4	EEPROM programmer (optional)	0	0	0
5	4x4 Membrane Matrix Keypad	1	6.99	6.99
6	16x2 LCD (count:2)	1	10.39	10.39
7	STM32 (given)	1	0	0
8	Raspberry Pi (given)	1	0	0
9	Lock	0	15.99	0
10	Box	1	5	5
11	AA Batteries	0	7.29	0
12	Baseus Power Bank 65W	0	47.99	0
13	LAMPVPATH AA Batteries Holder	1	7.99	7.99
14	Light Intensity Detection	0	9.99	0
15	Dupont Wire	1	6.98	6.98
16	Double Sided PE Foam Tape	1	9.99	9.99
				81.1

4. Assembly drawing





5. Workflow Chart



6. Working principle

Raspberry PI is the processor, which takes the information it receives and process it and sends instructions to other components. First, Raspberry PI drives PI camera to capture user's face for face recognition. If user's face is in the database and Raspberry PI evaluates the face data is match, Raspberry PI will send instructions to LCD component to greet the user and prompt user to enter password, else it will continue to lock the door. Second, the 4x4 keypad accepts the user's input and sends it back to Raspberry PI. Raspberry PI evaluates the user input. If it matches the correct password, Raspberry PI will drive the Servo through STM32 to unlock the door. If it doesn't match, PI will prompt user to enter password again. If the password does not match for over 3 times, PI will drive PI camera to capture user's face, and regenerate the password. At the meantime, PI will send a warning notification to the administrator's email by Gmail SMTP, and the administrator's phone by Gotify.

Experimental Outcomes

The parts arrived on time, and we met each phase specification by its deadline. However, it was time consuming during the assembling phase. The biggest problem we faced was when constructing the door, the box is not durable enough to keep it in place. After trials and errors, we figured out the correct position to place the door and the servo(so that the servo can turn to open/close the door). On the other hand, adding face recognition feature is also challenging because the algorithm was not recognized the trained faces correctly. We ended up figure out that it was because the number of photos was not enough. After increasing the number of photos for training, the result is much better.

Impact and Consequences

Our project is intended to provide a secure digital lock to our customers and has a large and direct impact on both the physical safety and information security of the users. The lock is a barrier between an assailant and the home of the users, so we have a duty to make the project physically robust and durable. Since the lock is a digital lock, the lock can also compromise the user's digital safety because the lock stores the users' personal information. For example, the facial recognition feature stores photos of the users to train and the password used for the lock may be used for other applications by the users. We must prevent leaks of these types of information to keep the users safe.

Conclusions and Recommendations

The initial purpose that our team had for developing this project is that we wanted to construct a password-based lock which could provide users a very effective method for entry. Based on our effort, we have developed a type of lock that is relative secure and cost-efficient which can give our product some competitive advantage in the market. However, some unexpected outcomes have shown up when we tried to conduct the tests for the prototype. There are several potential vulnerabilities that our products encounter during the test process which need additional measures to be implemented for ensuring the security. In this way, further evaluation and development of our product is needed to address these potential risks. After discussion, our team decide to implement additional features such as facial recognition to enhance the security of our password-based lock.

Based on the conclusions above, we come up the following recommendations:

1. Additional research and development work will be needed to address the potential vulnerabilities of our password-based door lock model. In the meantime, it will be better if we can construct more features to enhance the security of our prototype.

2. The cost and performance of our product needs to be evaluated. In this way, we can identify the tradeoffs in market, consumer needs, cost and performance. Based on this, we can establish a useful business model which can be very helpful when it comes to build a successful business plan for the new product.

References, Acknowledgements, and Intellectual Property

1. Reference

"Raspberry pi quick start guide," *CanaKit*. [Online]. Available: https://www.canakit.com/Media/CanaKit-Raspberry-Pi-Quick-Start-Guide-4.0.pdf.

"Raspberry Pi 4 Model B Datasheet". [Online]. Available: https://datasheets.raspberrypi.com/rpi4/raspberry-pi-4-datasheet.pdf.

"STM32F4 Datasheet". [Online]. Available: https://www.st.com/resource/en/datasheet/dm00037051.pdf.

"Pi camera 2 manual". [Online]. Available: https://datasheets.raspberrypi.com/camera/picamera2-manual.pdf.

"Gotify". [Online]. Available: https://gotify.net/.

M. J. R. B. (M. Rovai), "Real-time face recognition: An end-to-end project," *Hackster.io*, 11-Jul-2018. [Online]. Available: http://www.hackster.io/mjrobot/real-time-face-recognition-an-end-to-end-project-a10826.

"Simple Gantt Chart". [Online]. Available: https://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html?utm_source=ms&utm_medium=file&utm_campaign=office&utm_content=url.

2. Acknowledgement

Sincerely appreciate Prof. Rania Hussein for her guidance and support throughout this project. Thanks to TAs, Marcos Inonan and Brody Mahoney for advising and helping us figure out the problem with camera not working.

3. Intellectual Property

Our door lock design is self-developed, and reference to some open-source code.
No part of the intellectual property of the design will be protected by patents, Copyrights, trademarks, or trade secrets.