Section 1 - Summary (150 words)

Our project is a smart locking door that is designed to unlock a door when receiving instructions from an authorized device using RFID cards/tags or using a keypad. Instead of the traditional way which is using a door key, our smart locking door provides the users convenient ways while they have the same level of security as traditional locks. When the user tapped the authorized cards or inputted the correct password, our system would open up the door and close the door for the user immediately once they entered the apartment. In case there is no one passing through, it still closes the door automatically. When the access way is unauthorized, the system will capture a photo for further investigation and send an email/SMS if there are too many attempts. All the access records are uploaded to the server eventually for the user to check. We also provided a mobile application to modify the permission of the RFID cards/tags.

Section 2 – Introduction (300 words)

Burglary is a serious case for a criminal getting inside others' areas without their assent. The purpose of the behavior of burglary is to try to steal others' property and take it into their own, to hurt others or even ruin. According to the Hong Kong Police (2021), the cases of burglary from 2011 keep staying at least one thousand and five hundred. Calculated from 2018, the cases of burglary in the first half of the year remain the same (Hong Kong Police, 2021). The statistic shows that there is still a lack of crisis awareness among people, or it needs some more technical protection. The main purpose of this project is to increase safety insurances for users, also to decrease the case of burglary in Hong Kong.

The smart locking door is designed for enhancing security to users. In this project, it is expected to replace the usage of a traditional format. The smart locking door is supposed to use a unique card, the same as an identity card, to detect whether the users have permission to get inside. It is also hoped to add an alert system to remind the users as error attempts are high enough and get the proof for someone who fails to access. The system is also designed to allow the owners to review the record anytime.

Compared with a traditional door, if the flat owner loses his/her key, s/he may worry about someone picking it up and getting into the owner's flat someday. The smart locking door system solved the problem. When the owner loses the RFID card/tag, s/he can access the system and cancel the access permission of the tag/card, which is an interesting innovation function highlighted inside the system.

Section 3 – Objectives (in point form)

- Enhance security for accessing (an entrances).
- Replace the traditional method of using a key.
- Provide a convenient way of accessing.
- Prove the problem and consequence of losing an identity tag/card.
- Able to check a record of access at all times.

Section 4 – Function Specification (in point form)

- Identify authorized RFID cards. The door will be opened when the tapped RFID card/tag has permission to do so.
- Password input on the keypad. The door will be opened when the input password matches the recorded one.
- Measure the distance when the door is opened. When the user gets inside their home, the door will be closed automatically. If no one is entering, the door will still be closed after 6 seconds.
- LED indicates the status of door open attempts and reminds the user of the count-down period.
- No matter if the attempt is successful or not, the date, time, status and access way will be uploaded to the web spreadsheet.
- OLED can show the user the error attempts, successful messages and count down for distance measurement.
- Camera module captures photos and saves them in the SD card every unsuccessful attempt.
- When 5 unsuccessful attempts are reached in a row, a warning SMS/email will be sent to the user.
- Mobile app: it can modify the permission of RFID cards/tag and view the log remotely

Section 5 – Technical Background (800 words)

In our project, the system provides a different access method,RFID card and a keypad. RFID(Radio Frequency Identification) is a wireless communication technology that can identify specific targets, read and write related data through radio signals without requiring mechanical or optical contact between the identification system and specific target. Each RFID card has a different uid number. We can get the uid number through the RFID sensor. We only need to compare the uid in the RFID card with the database to know whether the card has permission. Also, this technology has another feature that can be applied to various objects, including car keys, cards, toys, etc. This feature can be applied to different occasions.

Another access way is the password input on the keypad. We used a 4x4 keypad module in our project because it is a common module in the parts market. A 4x4 keypad has 16 buttons, arranged in a telephone-line 4x4 grid. The keys are connected into a matrix, so we only need 8 microcontroller pins (4-columns and 4-rows) to scan through the pad. In order to test whether any key is pressed down, we have to connect power to rows, so they are High level. Then set all the rows R1-R4 as Low and then detect the status of the columns. If it is pressed, a column will become low, and this key is among the 4 keys of that column. And then we just set the rows as Low one by one and keep others be High until any row is unveiled accordingly. Now we found the row and column, thus we will know the key that intersects with the row and column is the exact key the user is pressing.

In our project, the system can indicate the users' different kinds of information by using an OLED display and LED light bulb. To show the user error counts and successful messages, we used a SSD1306 module in our project. SSD1306 module is an OLED display, a mono color, 0.96-inch display with 128×64 pixels. The OLED display has no backlight and they make their own light. That's why the OLED display is a very low power device. In the project, we put the error times and corresponding messages when the users try to open the door. But in fact, an OLED display is able to show scrolling words, draw the shape and even draw the animation by editing the pixels one by one.

The other display module is RGB LED. RGB LED is a simple and versatile module. It has 3 pins. Each pin represents a different color, which are red, green, and blue. The three primary colors can be different according to the value we input, and the RGB LED displays a variety of different colors. We use different colors to represent different situations.

In addition, in order to measure whether the user enters the room, ultrasonic technology is also used. The ultrasonic sensor module has the function of transmitting and receiving ultrasonic. When the emitted ultrasonic wave touches the object, the object will bounce the ultrasonic wave. At this time, the ultrasonic sensor can estimate the distance between the sensor and the object based on the received ultrasonic data. When these data are collected, we can act accordingly.

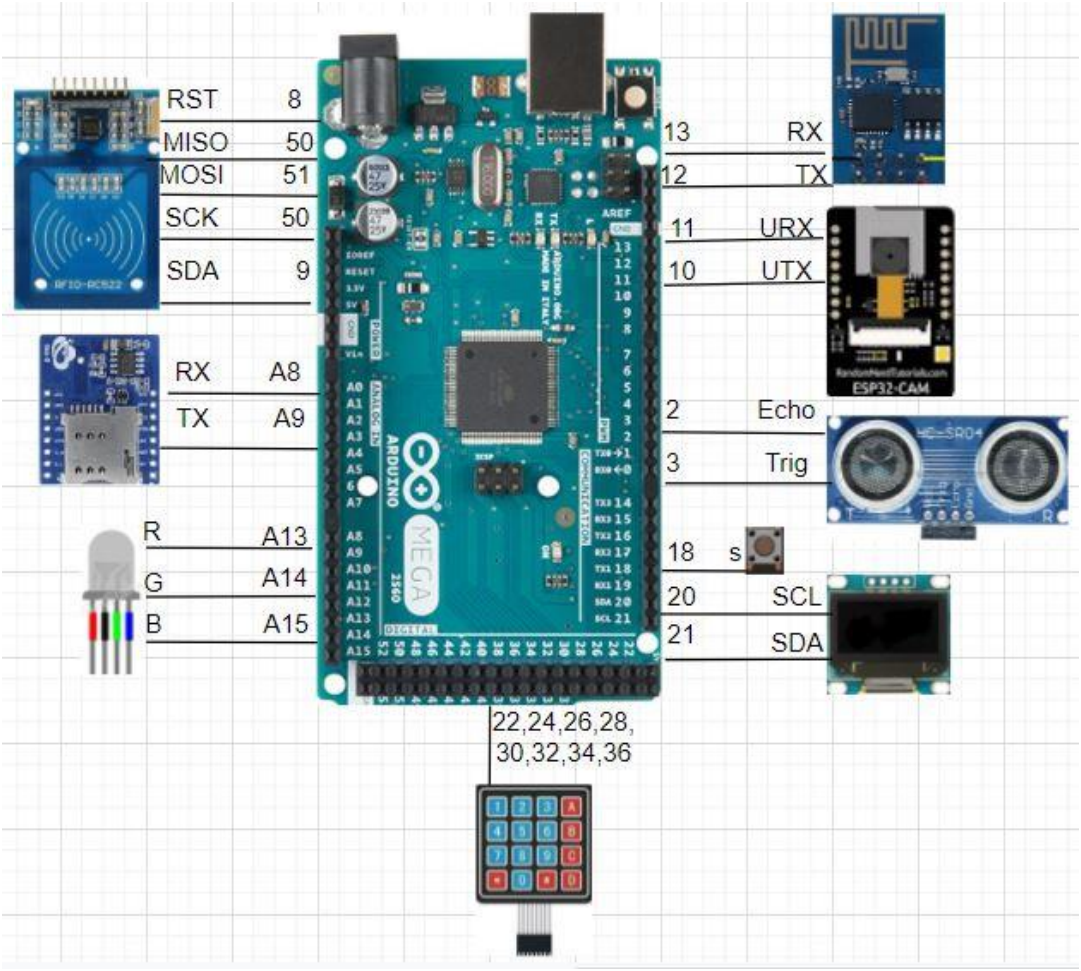
There are cases when the user fails to access. We used an ESP32 camera instead of the OV7670 cam sensor for a photo capture as the OV7670 board required more pins, which caused space wastage. ESP32 is one of the serial boards that can be communicated with the main monitor. ESP32 bluetooth board can be used as a board that can run uniquely; once the user does the wrong actions, including detecting the wrong RFID card/id and pressing the password incorrectly, the ESP32 will receive the instructions and take the pictures automatically. As for saving the captured photo and browsing by USB, it is required to insert the micro SD card inside the ESP32 camera; the photo captured may not be very clear because the ESP32 supports only up to 4 GB micro SD cards.

Besides, the system will count the error attempts (the number of error attempts will show on the OLED board as mentioned above). When the error attempt is high enough, the GA6 MINI gsm module starts to communicate with nearby cell sites, or mobile phone masts to send out message sending requests. The mobile phone mast will help to send out the specified message to the targeted users. The GA6 MINI gsm module is also required to insert a SIM card; the users can buy a prepaid SIM card outside.

In addition to the use of multiple modules in the system, in order for users to check the usage of the system anytime and anywhere, we used the Google form service and created a mobile application. Once the user tags the RFID card or input the password, all the log data will be uploaded to the Google spreadsheet. Google spreadsheet is an online spreadsheet which can save the data at any time no matter it is at midnight. For this reason, it is used with our smart locking door which is also a always standby device. Also, In order to build a mobile application, we used the android studio. Android Studio is an integrated development environment for developing programs for the Android platform. It has a variety of different tools to achieve a variety of complex and diverse functions. By using different tools in the android to build graphical user interfaces, forms, etc., we hope that to make users more convenient.

Section 6 – Hardware and Software Architecture (1500 words)

Hardware Architecture



Hardware Architecture Overview(do not including VCC,GND)

The following session will introduce the hardware architecture; it means the connections between all kinds of the modules and the main board, mega 2560.

In order to keep the consistency and avoid the garbled happens, we set the baud rate of all the modules we used in the project as 115220.

As the module ESP8266, it required only five pins as it contains eight pins, such as transmit pins, receive pins, and the pins for supplying electricity uses. (They are: 3.3V, 5V and ground respectively). The usage of the module ESP8266 is to send up a log record to the client, and to be reviewed by the users. The connections between ESP8266 and Mega 2560 are: from RX to D13, TX to D12, 3.3V to 3.3V, 5V to 5V, and GND to GND respectively.

In the 4x4 keypad part, we connected R1 to R4 to pin 40, 38, 36 and 34. And then we connected C1 to C4 to pin 32,30,28 and 26 respectively. Interrupt button pin 18. Its function is to provide more choice to users in case the users want to use a password to access instead of using RFID.

For the module ESP32, although the module ESP32 has lots of pins, it only needs 4 pins to connect to Mega 2560, as same as the module ESP8266; they are transmit pins, receive pins, and the pins for supplying electricity uses. The module of the ESP32 is used to take a photo once the users detect the RFID card and the password incorrectly. The connections between ESP32 and Mega 2560 are: from RX to 11, TX to 10, 5V to 5V, and GND to GND respectively.

Ultrasonic sensor module can detect the distance between the users and the module. In this system, it only works when the users press the password and have their RFID card correctly. The sensor contains only four pins. The connections between Ultrasonic sensor and Mega 2560 are: From 5V to 5V, GND to GND, Enho to D2 and Trig to D3 respectively. The pins of the Echo and Trig have the same definition as the SCL and SDA.

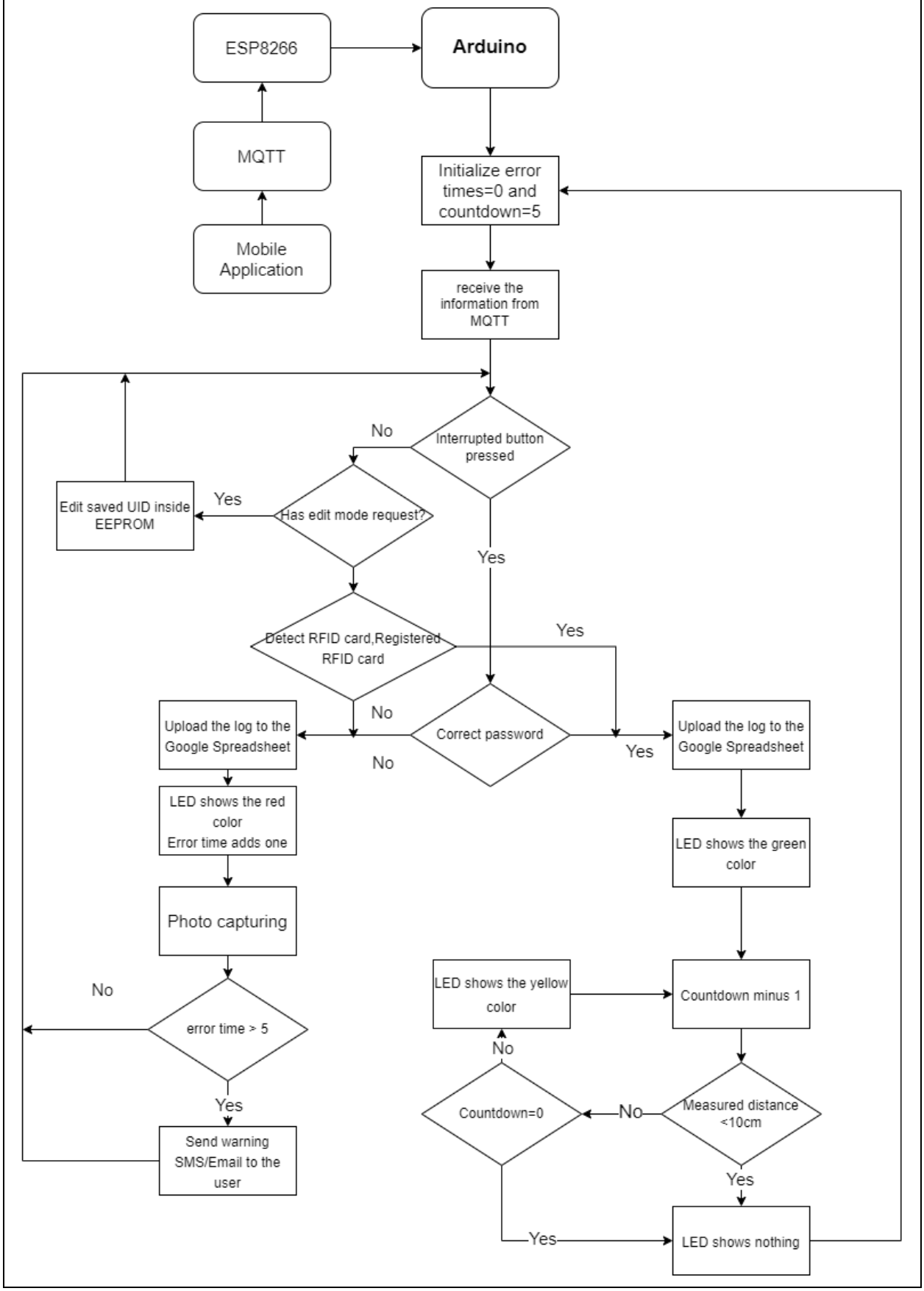
In addition, the OLED board shows some displays about the status of the system. For instance, when the users choose to use the 4x4 keypad to enter the password instead of using the RFID tag/card the OLED board shows the “Enter password: “ words on the OLED board. The number of pins of the OLED board is the same as the Ultrasonic sensor. The connections between the OLED board and Mega 2560 are: SCL to D20, SDA to D21, 5V to 5V and GND to GND respectively.

Besides, the RFID modules are divided by two parts: the RFID unit, which looks like a white board, has the responsibility to scan the RFID tags or cards and read its ID. Another part is a RFID card and tags. They can be defined as an identity card. In other words, they contain a unique ID and will be read by the RFID units. The RFID module contains eight pins but only seven pins are needed. The connections between the RFID board and Mega 2560 are: From Reset to D8, MISO to D50, MOSI to D51, SCK to D50, 5V to 5V and GND to GND respectively.

Moreover, the GA6 gsm module contains lots of pins but needs four pins, which is the same as the ESP8266 and ESP32 mentioned above. The connections between the GA6 gsm module are: From RX to A8, TX to A9, 5V to 5V and GND to GND respectively. The function of the GA6 gsm is to communicate with nearby mobile phone masts and send messages to targeted phones.

Apart from the modules mentioned, there is a button with only two pins; it is designed to switch the input mode when the users want to press the password instead of using RFID tag/card. It only needs to connect from S to D18 and GND to GND between the button and Mega 2560 respectively. On the other hand, The RGB led is a function showing a light with different colors. When the users succeed to access, the green light will be on, otherwise showing a red light. The connection between the RGB led and the Mega 2560 is from R to A13, G to A14 and B to A15 respectively.

Software Architecture



System Overview

In our design, we hope that the system can make users feel convenient, user-friendly, and more secure. At the same time, it is also necessary for users to know the information of the system clearly. Of course, one of the features of smart home automation. It is also one of the manifestations of our plan. In addition to the use of the system itself, we also provide more additional functions, so that users can clearly know the status of the system anytime and anywhere.In order to achieve these features, we will introduce our design and methods below,one by one.

Different Access Method

In order to make users feel convenient, we provide two different access methods. To realize the different access methods of the door to replace the traditional methods, we used a 4x4 keypad and RFID sensor (MFRC522). Users can use a 4x4 keypad to enter the password. In addition, RFID cards can also be used. Different RFID cards have different UIDs. If the RFID sensor senses the authenticated RFID card, the door will be opening. If the user forgets one of the access methods, they can use the other access method.

For the different access methods, the main difference is whether the interrupt button is pressed or not. If the user does not press the interrupt button, the RFID sensor will continue to check whether there is an RFID card.If the user tags an RFID card, the sensor will compare the UID of the RFID card with the UID stored in the EEPROM. lt is a registered RFID card or not, there will be corresponding different actions.

A 4x4 keypad is another access way for the user to open the door. No matter the user input a correct or incorrect password, it will show the corresponding message on the OLED display. The user has to press the interrupt button in order to enter the keypad mode. Since the system is using a polling method and keeps checking whether an RFID tag/card is tapped, it has no way to exit the checking process and switch to the keypad mode. For this reason, we attached an interrupt function to the interrupt button which will call the ISR function when the user pressed the button (signal falling). In the ISR function, I set a boolean variable to true and exit the ISR function. Once the system in the main loop detects it becomes true, it will enter the keypad mode until the user pressed * to submit the password.

Display function

As mentioned above, entering the correct RFID card/password or not will have different actions. One of the actions is the display function. To implement the display function, we will be using an OLED(SSD1306) and RGB LED display panel. The OLED(SSD1306) display panel can write text, draw shapes, and display bitmap images. By using this module, it can indicate which button the user is pressing. And then, it can directly show whether the password/RFID is correct or not. And another display panel is RGB LED. By mixing three different colors (Red, Green, Blue), it can show different colors. We will use different colors to show the status of the door. For instance, When the RGB LED is showing green color, it means the password/RFID is correct and the door is open. When the RGB LED is showing red color, it means the password/RFID is incorrect and the door will not have any action.In addition to displaying this information, other things will also be displayed, and now I will introduce. If the system is not in use, the LED display will use text to remind the user to tap the RFID card or enter the password. It will also indicate the number of errors. After entering the correct password or RFID card, the LED display will show a countdown to remind the user of when the door will close

automatically. In addition to the LED display, the RGB LED will also flash yellow to remind users of when the countdown is close to zero.

Door automation and humanization

In terms of the door automation and humanization, we used an ultrasonic sensor. The ultrasonic sensor will continuously send ultrasonic waves. When the sensor senses that the user has entered the room (distance between sensor and user less than 10 cm), the door will automatically close. Of course, we have also made some humanized designs. When the door is opened and the ultrasonic sensor does not detect the user entering the room for more than 6 seconds, it will also automatically close the door. Even if the user has an emergency, the door is opened but the user does not enter the room, and the door is automatically closed, which can also enhance the security of the home.

Log and warning SMS/Email function

To increase the security of our system, it uploads all the Log data to the Google spreadsheet at any time. Firstly, we set up a software serial connecting the arduino board and ESP8266 module so that they can communicate with each other. At the same time, we created a Google script which handles the HTTP POST request and inserts the log to the Google spreadsheet. Our way is to send a command from the arduino main program to the ESP8266 wifi module. For instance, when the user tries to open the door, it sends an integer (48, 49, 50, 51, which means incorrect RFID card, correct RFID card, correct password and incorrect password) to the ESP8266 as a command. And the program in ESP8266 takes that integer as the parameter of the HTTP POST request and sends it to the Google script. Once the Google script on the server receives the request, it parses the payload and gets the command. Depending on the command it gets, it inserts different Log into the spreadsheet. For example, if the parameter is 48, it inserts the date, time, status (which is incorrect) and access way (which is RFID cards).

In addition, our system can send SMS/email when the user opens the door unsuccessfully 5 times in a row. At the very beginning, we initialize an integer variable called errorTimes. Every time the user opens the door unsuccessfully, errorTimes will be added by 1. It will also be resetted once the user opens the door successfully. When the number reaches 5, it sends a command to the Google script just like what we did in sending Log data, and the script will send an email to the user via Gmail. For the SMS part, we set up another software serial for the communication between the Arduino board and GSM module. We firstly send a “AT+CMGF=1” command to the GSM module to indicate that we picked the SMS text mode only. And then we send a “AT+CMGS=\+852XXXXXXXX\<CR>” to tell the GSM module the number it has to send to. And finally, we send the message "Warning. 5 times attempt reached \x1A" and a <CTRL-Z> to send it out to the destination.

Mobile Application

To implement editing RFID permission and viewing the log data. We built a mobile application. About editing RFID permissions, we used ESP8266, MQTT, a mobile phone application. ESP8266 is a low-cost Wifi microchip, with a full TCP/IP stack and microcontroller capability. It will be used to connect to the household’s own WIFI network. When the mobile phone application sends a RFID edit permission request to MQTT. Then, MQTT will forward the request to the ESP8266. Finally, ESP8266 will notify Arduino, and the Arduino will change the RFID UID in EEPROM. For viewing the log data, we set up the form on the mobile app and imported the data from the database to the form.

Section 7 – Project Schedule

In week 6, we were trying to test and combine all the features on hand since we have already done some features of our project. For example, the OLED display, the basic function of our mobile application, the ultrasonic sensor.

In week 7 and week 8, we were trying to implement communication between the Arduino board and the spreadsheet on the Internet. In addition, we integrate the parts that two teammates are responsible for. Unfortunately, we encountered some problems.For example, the keypad and the RFID sensor could not work at the same time.

In week 9, We used the method of adding an interrupt button so that the keypad and the RFID sensor can run at the same time. Also,the entire program has been optimized, and some errors have been corrected.

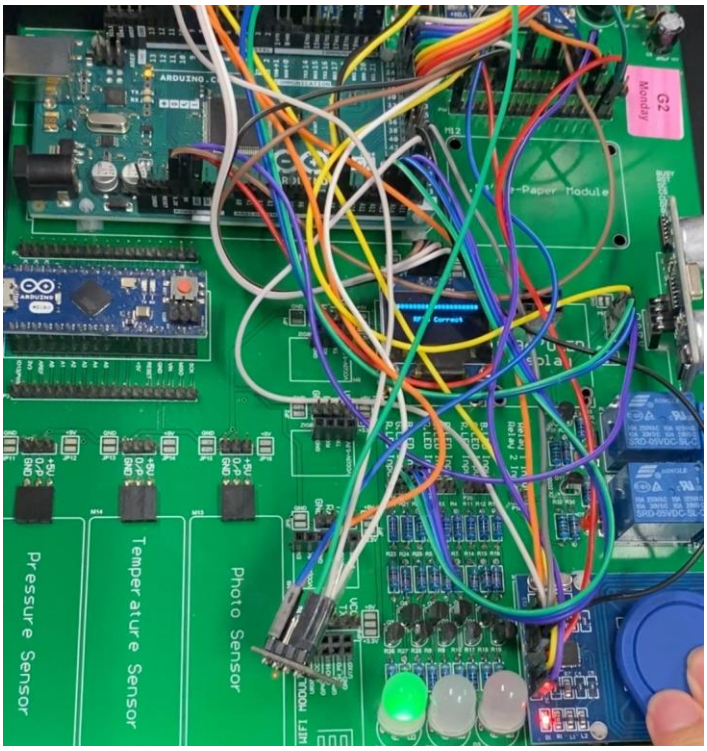
In week 10, we integrated the program with the part that the other teammate is responsible for. At this time, we found that the function of sending SMS is not working properly. After a lot of testing, we found that there is no error in the code, but due to the limitations of the module, it needs to be in a place where the mobile phone signal is well received to work properly.

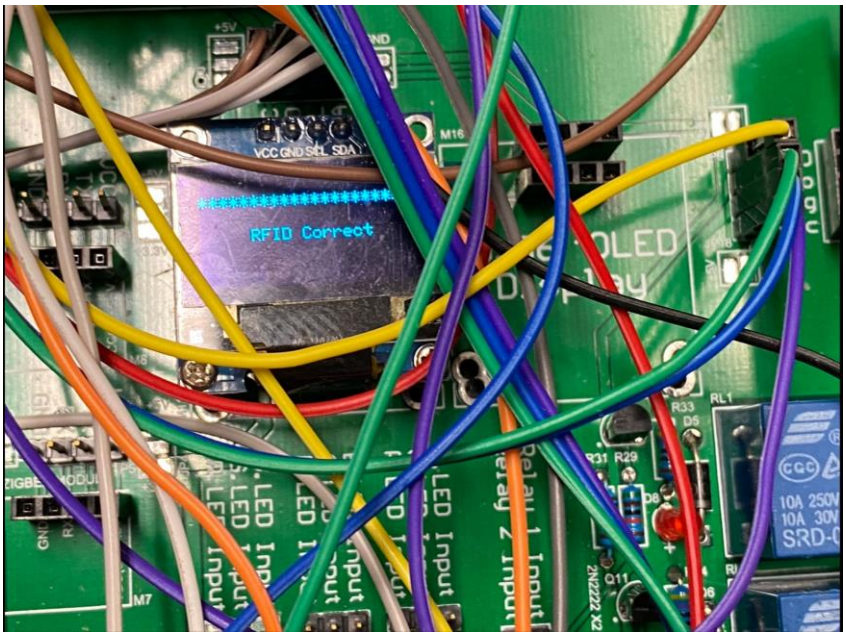
In week 11, we think about how we can make the system better.After some discussion, we believe that adding a picture capturing function can increase security. Of course, we have carried out a series of checks and made sure that all functions are working properly.

Section 8 – Testing, Results and Discussion

- RFID Access Test
- Keypad Access Test
- Distance Detection Test
- RFID Permission Addition And Deletion Test
- Capture Photo Test
- View Log Test
- Sending SMS/Email Test
- Mobile App Viewing Log And Modifying Permission Test

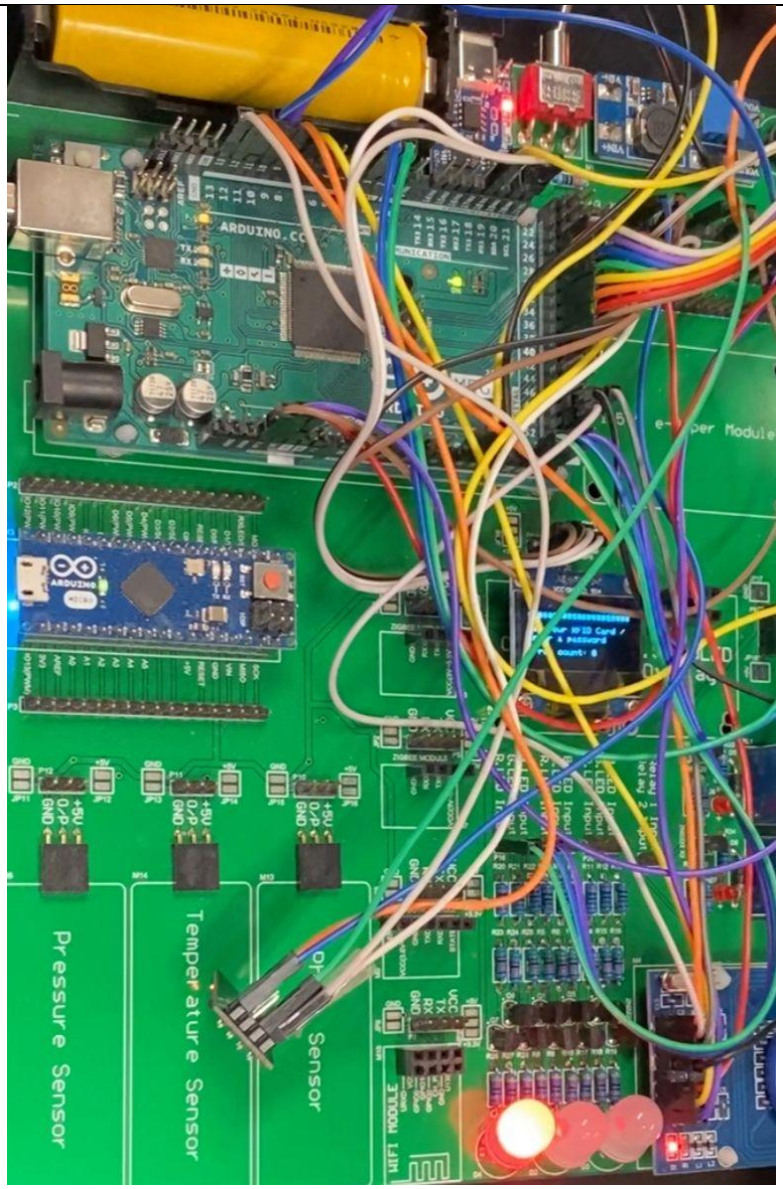
RFID Access Test





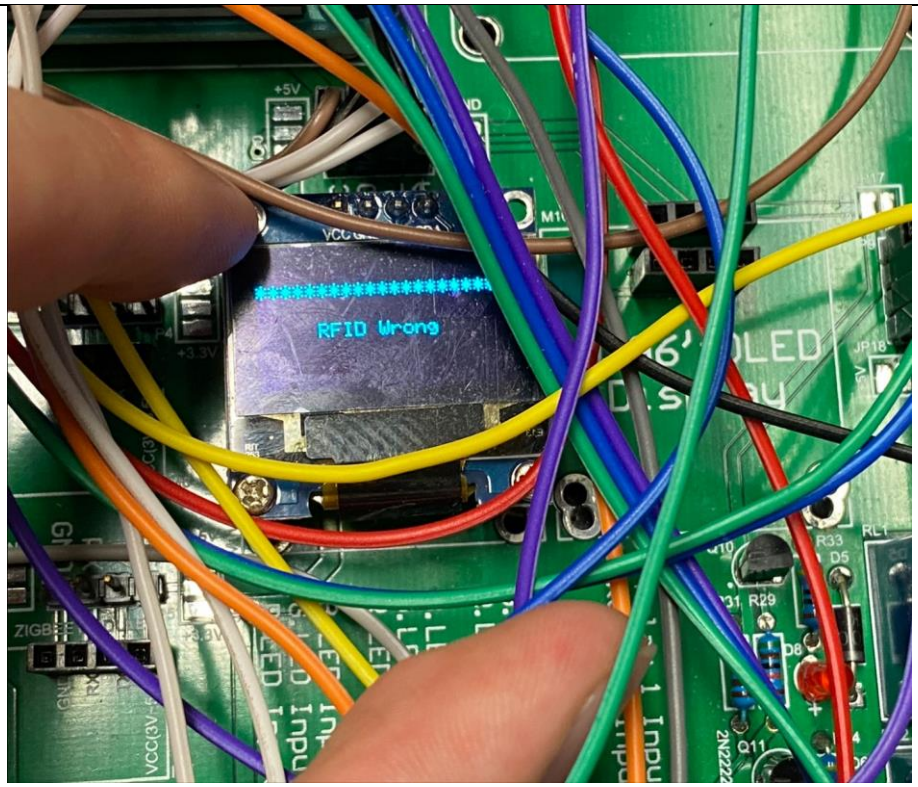
These two figures show a format for a case if the user gets the RFID card/tags or the password correct. According to these figures, the RGB LED is currently lighting with a green color and the OLED

board is showing “RFID correct“. Likewise, if the user gets the password correct, the OLED board will show the “password correct”, also with a green color.



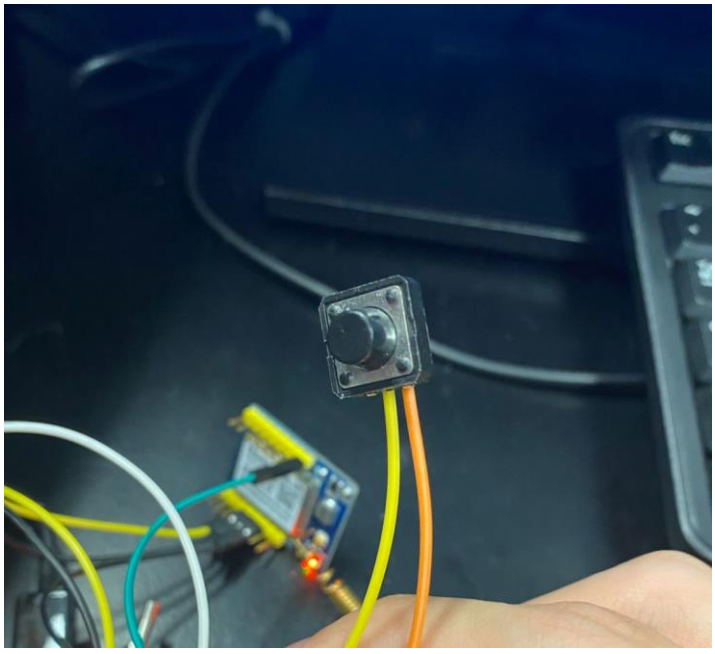
COM16

```
Plhe door! Press * after entering
Pressed: hardware serial!
size of RFIDTag:6
size of tag:24
RFID reader is ready!
Please enter password to open the door! Press * after entering
Pressed: 123456
Wrong password!
Error times now: 1
```



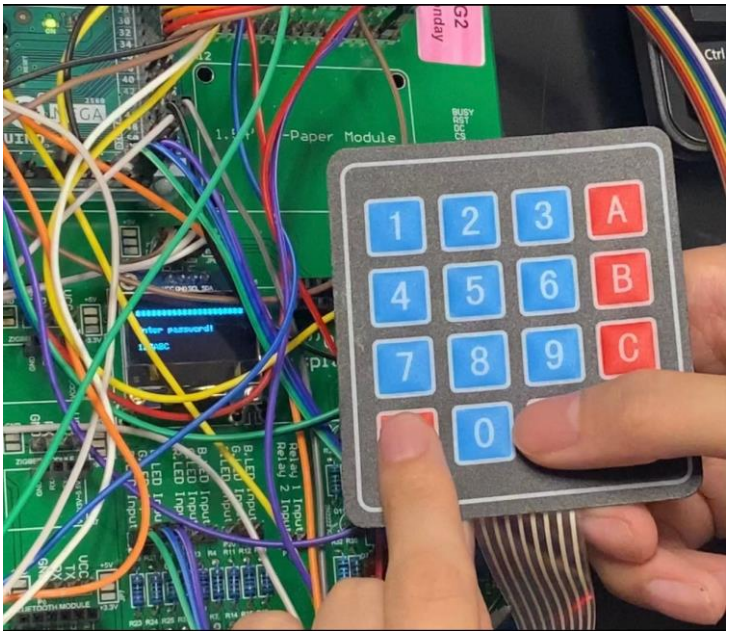
These figures are showing an opposite case as mentioned above. It is a case when the user gets the RFID card or the password incorrectly. According to these figures, the RGB LED is currently lighting with a red color and the OLED board is showing “RFID wrong“. Likewise, if the user gets the password incorrect, the OLED board will show the “password wrong”, also with a red color.

Keypad Access Test

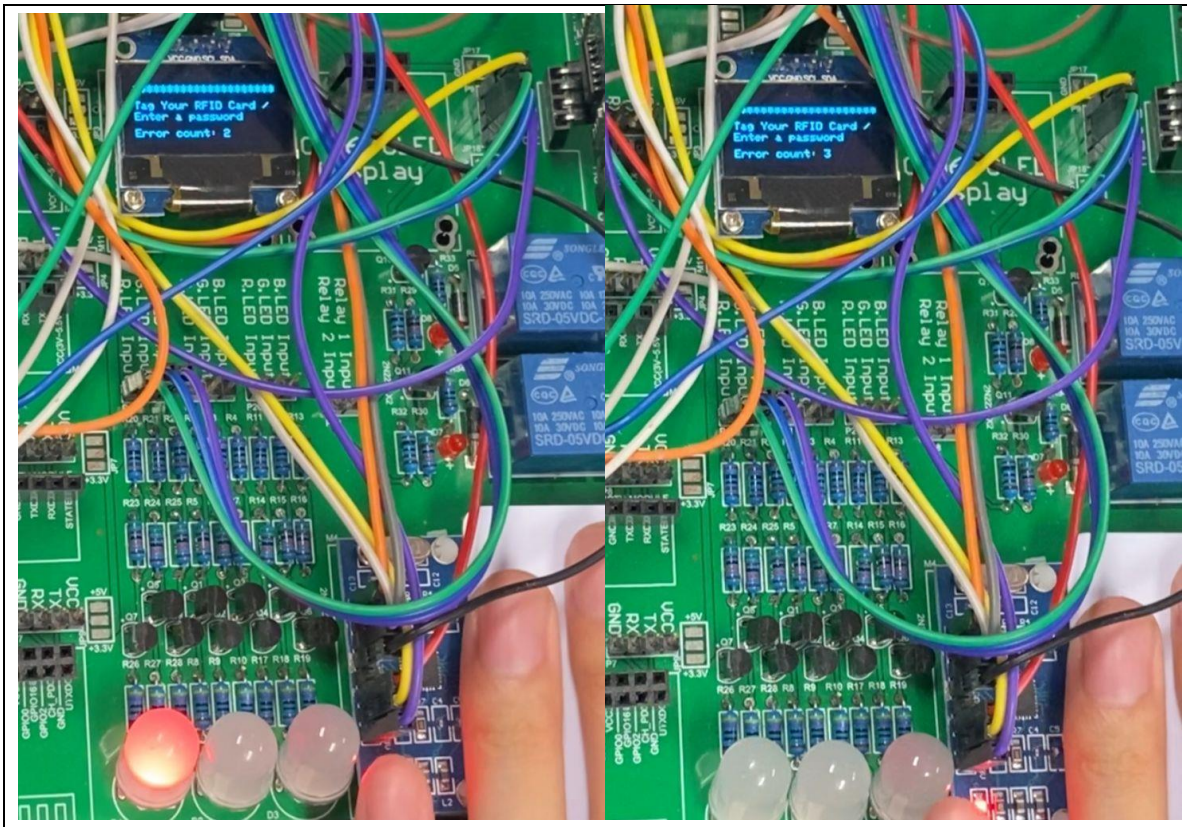


```
COM16

hardware serial!
size of RFIDTag:6
size of tag:24
RFID reader is ready!
Please enter password to open the door! Press * after entering
Pressed: 123ABC
Correct password!
```

By pressing the interrupt button, the system enters the keymode mode and allows the user to input a password on the keypad. As you can see in these 2 photos, the performance is completely good since it immediately shows the messages after the users ends the password with *. In the real implementation, we stuck at doing this function because we took time to find out the solution of the polling problem in the main loop. At the end, our solution is to add an interrupted button to exit the main loop polling which may cause some inconvenience to the users. I think that we can use the most right column on the keypad as the interrupted button and only allow the users input the password on the 4x3 keypad, so that we can remove the extra button from the arduino board. The second figure shows a serial monitor for a case that uses a password. According to the serial monitor, the “Pressed: 123ABC” means the users choose to use the password format, and the result shows a correct case.

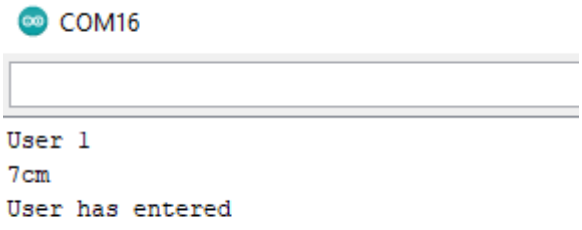


This figure shows an OLED board and the 4x4 keypad, it is password pressing format reacting as the serial monitor mentioned above. According to the figure, the OLED shows “Enter password, 123ABC”, which means the user presses the keypad for “123ABC”.

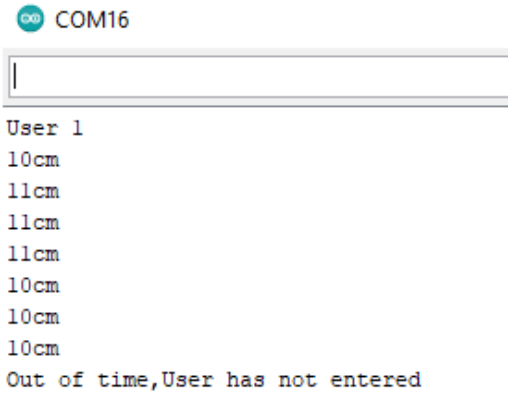


The figures are showing examples of the OLED displays. As the left figure, the error attempt is currently two. After the wrong RFID card detection, the error attempt is increased by one to three (As shown from right figure).

Distance Detection Test

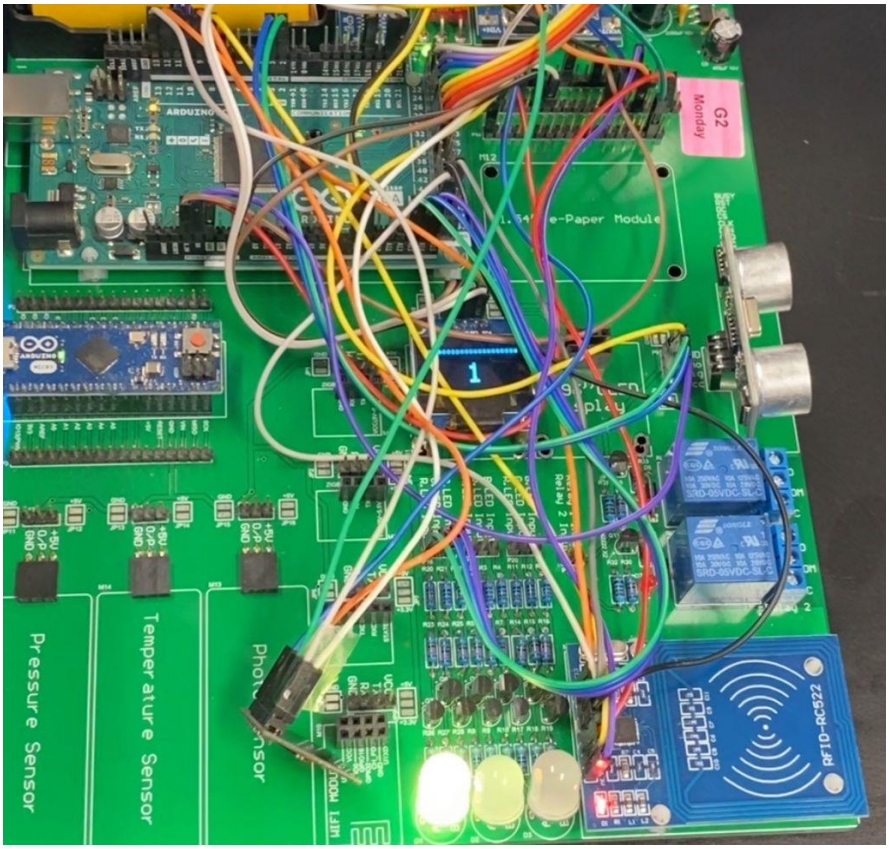


(User entered correct password and enter the Room less than at time limit.)



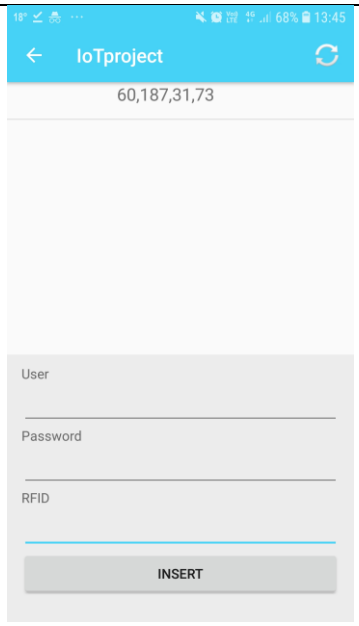
(User entered correct password but do not enter to room and it is over 6 second)

These pictures show measuring the distance when the user has entered password/RFID correctly. The performance is fine. It can show the distance between user and sensor. If the user enters the room, it will stop measuring the distance immediately (the condition is the distance less than 10cm) and close the door automatically. Otherwise, If the time is over 6 seconds, it will also close the door. It is because the door cannot keep opening for security reasons.



The system not only measures the distance when the user has entered password/RFID correctly. Also, it will show the timer is counting down. The RGB LED shows a light with a yellow color whilst the system is counting down, shown on the OLED board, the action is to remain the user to get inside as soon as possible.

RFID Permission Addition and Deletion Test



(Mobile Application editing permission function Graphical user interface)

Users can use this function to add or delete the uid inside the EEPROM of Arduino. If the user wants to add the RFID permission, just need input uid at “RFID”, then click the synchronize icon. It will synchronize with Arduino via MQTT.

```
Please Enter ID
48
ok
0, 0, 0, 0
0, 0, 0, 0
0, 0, 0, 0
0, 0, 0, 0
out
```

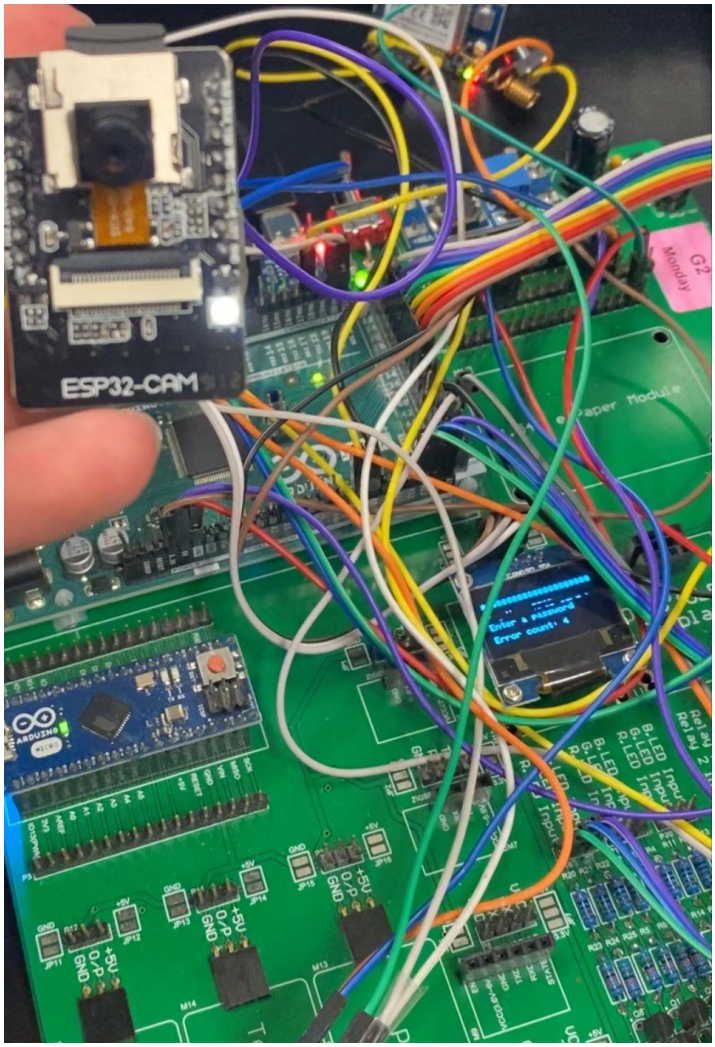
(Deleting the RFID permission)

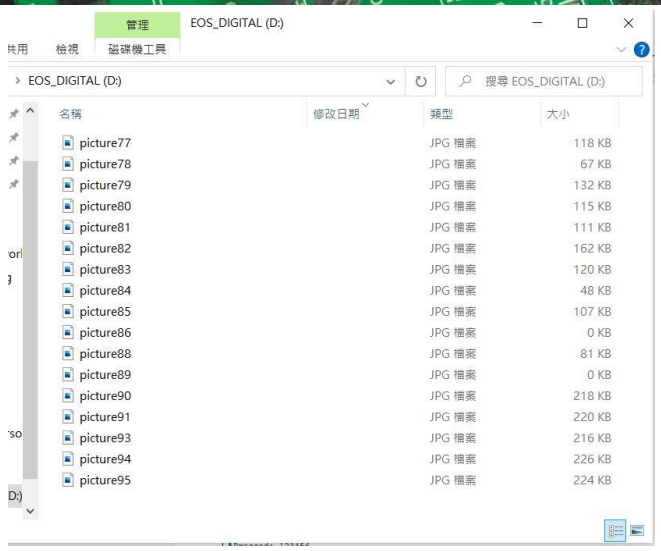
```
Please Enter ID
48
ok
60, 187, 31, 73
0, 0, 0, 0
0, 0, 0, 0
0, 0, 0, 0
out
```

(Adding the RFID permission)

When the ESP8266 receives the request from MQTT, it will forward to the arduino. If it is a deletion request, the uid inside EEPROM will change to 0,0,0,0. we can see the function is working normally. If it is a adding request, it will change to corrsending uid. For example, we can see the picture of the mobile app above. We add “60,187,31,73” and synchronization, then we can see the serial monitor.We can find that the arduino received the uid and modified successfully.But sometimes, the received UID data will be wrong. This is due to the performance limitation of the module.

Photo Capturing With Camera Test

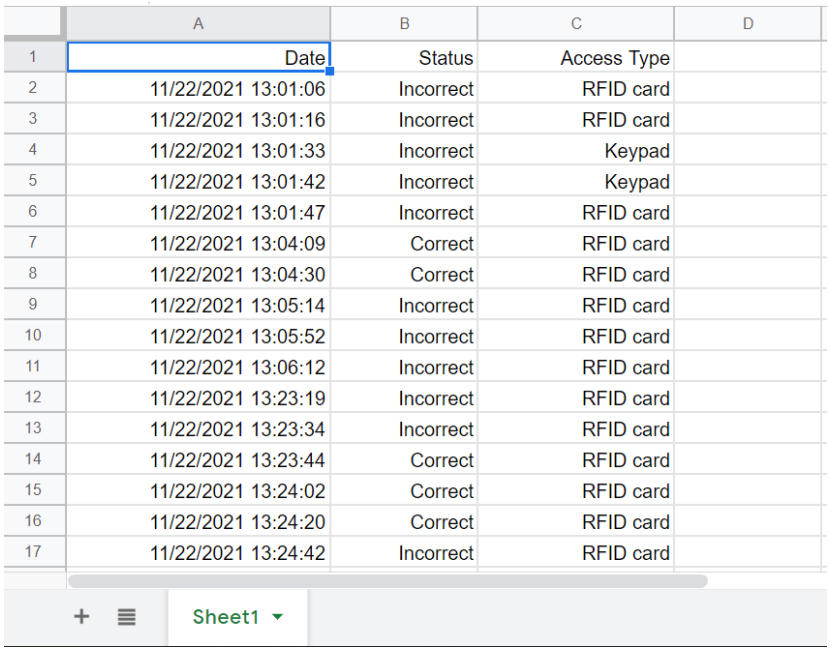




It is an ESP32 cam for taking photo use once the users get the wrong password or RFID tags. When the ESP32 is flushing with a white light (as te white light point, given from photo), it means the ESP32 cam takes a photo. The ESP32 module saves a photo to the SD card (The photo inside the SD card can

be read by USB), once it does a photo capture action. The difficulty of implementation of ESP32 is that it has no reactions even if the users get the wrong RFID cards or a password. Once the whole system resets, the ESP32 automatically takes a photo (the number of times taken is based on how many error attempts). The solution is to add some delay to ESP32. Once the ESP32 takes a photo, it needs a cool down for running the uploading to SD card session. In other words, if the ESP32 is not endowed for a delay session., it will not run the whole process and save it to os.

View Log Test



	A	B	C	D
1	Date	Status	Access Type	
2	11/22/2021 13:01:06	Incorrect	RFID card	
3	11/22/2021 13:01:16	Incorrect	RFID card	
4	11/22/2021 13:01:33	Incorrect	Keypad	
5	11/22/2021 13:01:42	Incorrect	Keypad	
6	11/22/2021 13:01:47	Incorrect	RFID card	
7	11/22/2021 13:04:09	Correct	RFID card	
8	11/22/2021 13:04:30	Correct	RFID card	
9	11/22/2021 13:05:14	Incorrect	RFID card	
10	11/22/2021 13:05:52	Incorrect	RFID card	
11	11/22/2021 13:06:12	Incorrect	RFID card	
12	11/22/2021 13:23:19	Incorrect	RFID card	
13	11/22/2021 13:23:34	Incorrect	RFID card	
14	11/22/2021 13:23:44	Correct	RFID card	
15	11/22/2021 13:24:02	Correct	RFID card	
16	11/22/2021 13:24:20	Correct	RFID card	
17	11/22/2021 13:24:42	Incorrect	RFID card	

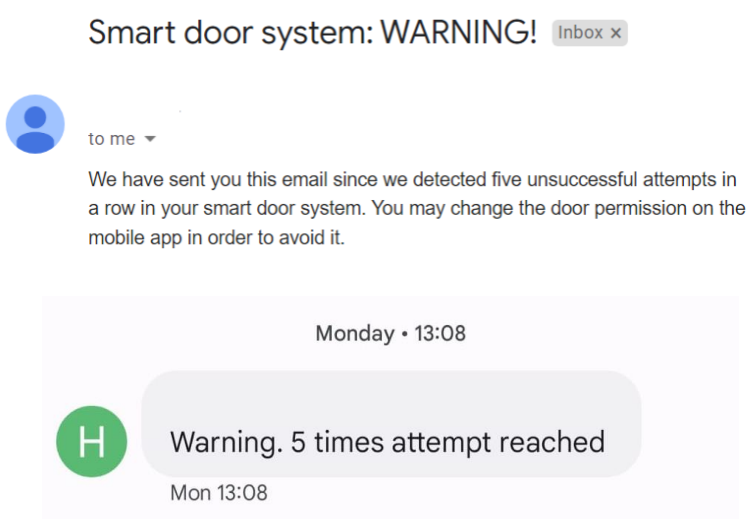
Sheet1

The online Log spreadsheet

All the Log data from the system is uploaded to the online log spreadsheet which contains the data, time, status and access type. All the transmission is immediately and available in 7x24.

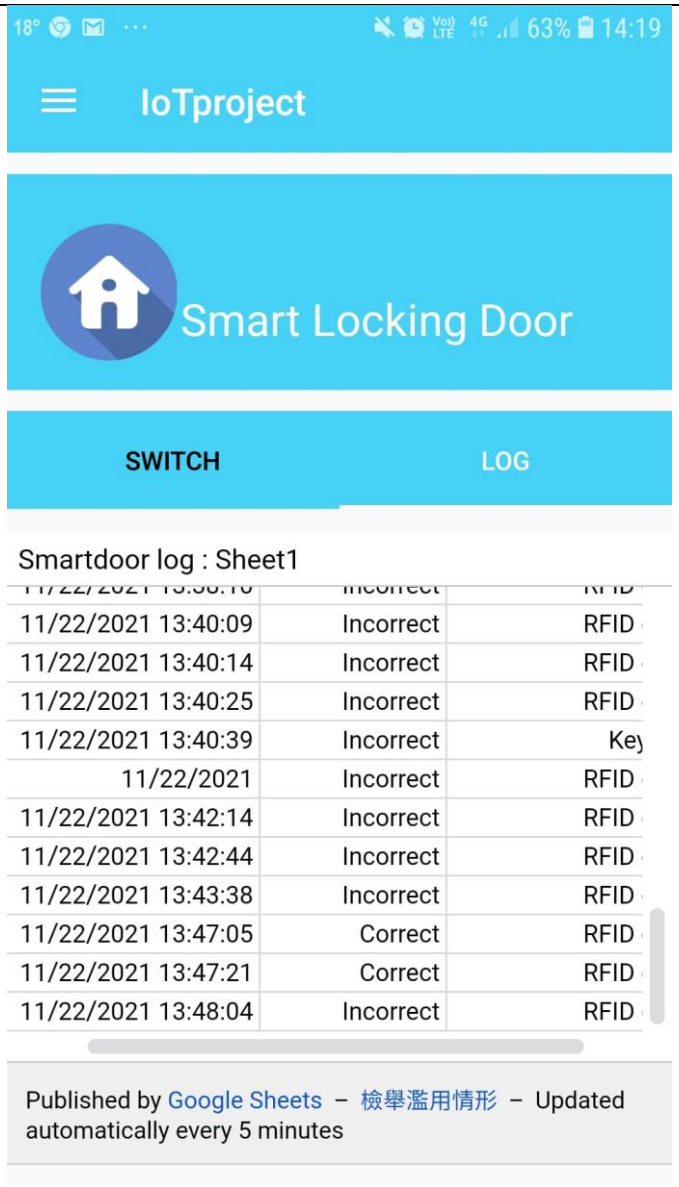
Sending SMS/email Test

```
hardware serial!
size of RFIDTag:6
size of tag:24
RFID reader is ready!
Wrong card!
Error times now: 1
Wrong card!
Error times now: 2
Wrong card!
Error times now: 3
Wrong card!
Error times now: 4
Wrong card!
Error times now: 5
Sending Message

Set SMS Number


SMS has been sent to the user since five errors were detected
```



The example is talking about a case when the users get the password and RFID card wrong and also have the error attempted five times. When the RFID card detects the wrong ID and the wrong password is pressed, the system remembers the incorrect record and increments the error attempt by one. If the same step repeats five times, in other words, error attempts are currently five times, the system starts to communicate with nearby cell towers for sending message requests. The cell tower will send the particular message to the target users (the system owner). On the other hand, the email will also be sent to the email client owned by the users.

Mobile App Viewing Log And Modifying Permission Test



The other features of the mobile application is viewing the log. Users can check when the user used the system, what methods had been used and the access is correct or Incorrect.

Section 9 – Conclusion and Suggested Improvement

The smart locking door runs on the whole process successfully and contains no errors and bugs. The system only remembers the fixed RFID tags id, same as identity card, and rejects the invalid card id until the modification by the system owner. The system can also remember the records on access time, in both success and failure cases, and leave evidence on who makes an error attempt.

The smart locking door also provides more access choices. Apart from using the tags, users can also choose to use passwords in case they forgot the tag/cards. The smart locking door enhanced the problem using the traditional method perfectly as for the users who are still using the key, they need to worry about losing the key and having it picked up by somebody. The system may run quite slowly and require some patients as the size of the system is large and need to send the record to the client. Yet, it doesn't cost and influence anything to run the process.

For further development, in order to add more access methods (For example, Fingerprint, Face recognition), we can use better performance modules since the modules we are using in our project encountered some problems. Although there is no error in the code, some unacceptable results occurred due to the performance limitations of the module. For instance, when the ESP8266 is receiving the uid from the MQTT server, sometimes the received uid will be wrong. Those uids are very sensitive and we cannot accept any bit of error. The reason is due to the limited performance of the module. If we want to improve this situation, we can only replace the module with better performance.

To conclude, the system provides a different trend for improving security. Despite the fact that the new system of the smart locking door may lead to a higher cost of the door installation, it is designed to decrease the case of burglary in Hong Kong. The smart locking door shows its ability for blocking the criminals outside the door.

Section 10 – References

Arduino Keypad Library (2021). *Arduino*. https://playground.arduino.cc/Code/Keypad/

HTTPSRedirect (2021). https://github.com/electronicsguy/HTTPSRedirect

Jason Chu (2020). *[Arduino 範例] RFID RC522 辨識系統入門，讀取 UID 和比對*. https://blog.jmaker.com.tw/arduino-rfid/

Password Library (2021). *Arduino*. https://playground.arduino.cc/Code/Password/

Software Serial Library(2021). *Arduino*. https://www.arduino.cc/en/Reference/softwareSerial

Understanding AT commands (n.d.). https://sites.google.com/site/vmacgpsgsm/understanding-at-commands/

Appendix: Submit your code to CANVAS