

**A SMART DOOR ACCESS SYSTEM WITH DUAL SECURITY AND
IOT APPLICATION**

LEE KAR TIEN

**A project report submitted in partial fulfilment of the
requirements for the award of the degree of
Bachelor of Engineering (Honours) Electronic Engineering**

**Faculty of Engineering and Green Technology
Universiti Tunku Abdul Rahman**

May 2023

DECLARATION

I hereby declare that this project report is based on my original work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature :



Name : Lee Kar Tien

ID No. : 18 AGB 03713

Date : 12/05/2023

APPROVAL FOR SUBMISSION

I certify that this project report entitled “**A SMART DOOR ACCESS SYSTEM WITH DUAL SECURITY AND IOT APPLICATION**” was prepared by **LEE KAR TIEN** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Engineering (Honours) Electronic Engineering at Universiti Tunku Abdul Rahman.

Approved by,

Signature :

Supervisor: Dr. Lee Yu Jen

Date : _____

The copyright of this report belongs to the author under the terms of the copyright Act 1987 as qualified by Intellectual Property Policy of Universiti Tunku Abdul Rahman. Due acknowledgement shall always be made of the use of any material contained in, or derived from, this report.

© 2023, Lee Kar Tien. All right reserved.

ACKNOWLEDGEMENTS

I would like to express my special thanks to my project supervisor Dr. Lee Yu Jen for his time and efforts he provided throughout the year. Your helpful advice and suggestions were really helpful to me during the project's completion. In this aspect, I am eternally grateful to you.

In addition, I'd like to express my appreciation to the lab officer, Mr. Thong Marn Foo for helping and guiding me on the printed circuit board fabrication. Besides, I would also like to express my gratitude to Mr. Choon Chee Ming and Puan Nur Hafiza Binti Harith Wekchit for helping me when I used the equipment and components in the lab.

A SMART DOOR ACCESS SYSTEM WITH DUAL SECURITY AND IOT APPLICATION

ABSTRACT

Due to the advancement of technology, the traditional way to open a lock or enter a building has been replaced by a smart door access system. The smart door access system is a digital technology that allows users to replace their troublesome key with some credentials, for example, RFID cards, smart tags, mobile applications, face, fingerprint or voice. The system provides the user a faster, safer, and more convenient way to access the lock. This project has created a smart door access system with hardware and software. The access system of this project contains one central control unit, a reader unit, a camera unit, an internal switch, a door sensor, and a solenoid lock with a driver. The Blynk IoT platform works as the software for the system. The system supports three access methods, which are the double-factor authentication method (scan a RFID card and key in password), Blynk mobile application method (press unlock button), and the internal switch method (press the limit switch). If the wrong card ID or wrong password is provided to the system twice, a notification is received on the Blynk mobile application, and the camera unit is activated to capture an image. The image will be stored as evidence in the receiver's email after receiving it. In order to let the user control the system over a long distance, the Blynk application has been used as a mobile application in the smartphone. This mobile application can download directly from Google Play Store or Apple Store. The internet is a connection between the application and the system. An overall system analysis has been performed to determine the system's functionality and reliability. The system analysis is divided into five parts, and the accuracy for each is calculated. Project cost analysis has also been done to determine the spending amount for the whole system. The total cost to build the whole project

is RM257.67, but the actual cost for the system is only RM170.47. The weakness of the project is pointed out in the last chapter, and the ways to improve the weakness are recommended in the same chapter.

TABLE OF CONTENTS

DECLARATION	ii
APPROVAL FOR SUBMISSION	iii
ACKNOWLEDGEMENTS	v
ABSTRACT	vi
TABLE OF CONTENTS	viii
LIST OF TABLES	xii
LIST OF FIGURES	xiv
LIST OF CODE LISTING	xviii
LIST OF SYMBOLS / ABBREVIATIONS	xix
LIST OF APPENDICES	xxii

CHAPTER

1	INTRODUCTION	1
	1.1 Background Study of Door Access System	1
	1.2 Problem Statements	6
	1.3 Objectives	6
	1.4 Scope	7
	1.5 Outline	8
	1.6 Summary	9
2	LITERATURE REVIEW	10
	2.1 Introduction	10
	2.2 Product Review About Student's Projects	10

2.2.1	RFID and Password Based Door Lock by Prajwalnsn	10
2.2.2	RFID and Keypad Door Lock and Alert System Using Arduino by Aqib	11
2.2.3	Door Access System - Arduino Based by Shuhada Natasha Bint Mohd Zainor	12
2.3	Product Review About Commercial Projects	13
2.3.1	Vanma Company	14
2.3.1.1	Product Description for Smart Padlock	14
2.3.2	MAG Company	16
2.3.2.1	Product Description of Touchless Door Access System with FR300 Reader	17
2.4	Microcontroller Review	18
2.4.1	Introduction to Arduino	18
2.4.1.1	Types of Boards for Arduino	19
2.4.2	Introduction to Raspberry Pi	20
2.4.2.1	Types of Boards for Raspberry Pi	21
2.4.3	Introduction to Esp8266 and Esp32	22
2.4.3.1	Comparison Between Esp8266 and Esp32	22
2.5	IoT Application for Microcontroller	23
2.5.1	Introduction to Arduino IoT Cloud	24
2.5.1.1	Hardware Compatible and Internet Connection	25
2.5.2	Introduction to Blynk	27
2.5.2.1	Hardware Compatibility and Internet Connection	27
2.6	Introduction to Fingerprint Recognition	28
2.6.1	Different Types of Scanner for Fingerprint Recognition	30
2.7	Introduction to RFID	32
2.7.1	Working Principle for RFID System	33
2.7.2	Operating Frequency for RFID System	34

2.8	Summary	35
3	METHODOLOGY	37
3.1	Introduction	37
3.2	System Block Diagram	37
3.3	System Flowchart	38
3.4	Microcontroller and Language Selection	41
3.4.1	Microcontroller	42
3.4.2	Language	44
3.5	IoT Application	44
3.5.1	Esp01s Module	45
3.5.2	Blynk Application	46
3.6	Credential Input Mechanism	49
3.6.1	Double Factor Authentication	50
3.6.2	Mobile Application	53
3.6.3	Internal Button	54
3.7	Lock Mechanism	55
3.7.1	Solenoid Lock	55
3.7.2	Lock Driver	56
3.8	Door Sensor	58
3.9	Image Capturing Mechanism	59
3.10	Pin Allocation of Arduino Mega 2560	61
3.11	Printed Circuit Board	63
3.12	3D Design	63
3.13	Project Management	65
3.14	Summary	68
4	RESULTS AND DISCUSSION	69
4.1	Introduction	69
4.2	Preliminary Work	69
4.3	Project Model	71
4.3.1	Model Overview	71
4.3.2	Hardware Overview	73

4.4	Project Software	76
4.4.1	Programming Language and Program Tools	76
4.4.2	Mobile Application	77
4.5	Sensor Mechanism	82
4.5.1	Door Sensor	84
4.5.2	Intruder Sensor	85
4.6	Overall System Analysis	86
4.6.1	Access Signal Analysis	87
4.6.2	Lock Analysis	88
4.6.3	Fault Tolerance Analysis	90
4.6.4	System Halting Analysis	92
4.6.5	Sensor Analysis	94
4.7	Project Cost Analysis	96
4.8	Summary	99
5	CONCLUSION AND RECOMMENDATIONS	101
5.1	Introduction	101
5.2	Conclusion	101
5.3	Limitations of Project	102
5.4	Recommendations for Project	104
5.4.1	Biometric Technology	104
5.4.2	Energy Saving Mode	104
5.4.3	Human Detection Function	105
5.4.4	Full Custom Build Printed Circuit Board	105
	REFERENCES	107
	APPENDICES	112

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Types of Authentication Use by Access Control Systems	3
2.1	Common Features in Arduino IoT Cloud	24
2.2	Aspect to Determine Suitability of Fingerprint Recognition	29
3.1	The Technical Specifications for UNO and Mega 2560	43
3.2	Pin Connection Between Esp01s Modules Adaptor and Arduino Mega	46
3.3	Pin Connection Between RC522 Scanner and Arduino Mega	51
3.4	Pin Connection Between Matrix Keypad and Arduino Mega	52
3.5	Connection Between L293D Chip, Arduino Mega, Power Supply, and Solenoid Lock	57
3.6	Connection Between Esp32 Cam Module and Arduino Mega 2560	61
3.7	Pin Connection Between Arduino Mega2560 and Other Devices or Components	62
3.8	Gantt Chart for Final Year Project 1 (June 2022 Trimester)	66
3.9	Gantt Chart for Extra Semester (October 2022 Trimester)	67
3.10	Gantt Chart for Final Year Project 2 (January 2023 Trimester)	67

4.1	Accuracy of Three Different Access Signal	88
4.2	Accuracy of Solenoid Lock and Current Usage	89
4.3	Status of Entering Wrong Password Twice and Scanning Wrong Card Twice	91
4.4	Accuracy of Fault Tolerance Analysis	92
4.5	Status of Solenoid Lock During Temporary Termination Period	93
4.6	Accuracy of Halt Feature Analysis	94
4.7	Status of Blynk Notification for Intruder Sensor and Door Sensor	95
4.8	Accuracy of Sensor Analysis	96
4.9	Cost for Every Item Use to Build Smart Door Access System	97
4.10	Difference Between Total Cost and Actual Cost for Smart Door Access System	99

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Example of a Door Access System (Catie, 2020)	2
2.1	Smart Padlock from Vanmalock Company (VANMA, 2022)	15
2.2	Total Price for One Smart Padlock and One Electronic Key (Including Bluetooth & Fingerprint) (VANMA, 2022)	15
2.3	Full Connection of Touchless Door Access System with FR300 Face Recognition Reader (MAG, 2022)	17
2.4	Classification for Original Arduino Board (Joseph, 2022)	19
2.5	Appearance Comparison for Raspberry Pi B, Pi Compute and Pi Zero (Wu, 2020)	21
2.6	Two Most Popular Board for Esp32 Chips and Esp8288 Chips, Esp32 DevKit V1-Doit (Left side) and Esp8266 Esp-12E NodeMcu Kit (Right side) (Santos, 2021)	23
2.7	Example Appearance of Dashboard from Arduino IoT Cloud (Mohahan, 2022)	25
2.8	Selection Between Arduino Board or Third-party Board in Arduino Web Editor	26
2.9	Many Types of Microcontroller Boards from Third Parties are Compatible with Arduino IoT Cloud	26
2.10	Selection of Microcontroller Board and Internet Connection in Blynk IoT Platform (Blynk, 2022)	28

2.11	Scanning Procedure of Optical Sensor (Triggs, 2022)	30
2.12	Scanning Procedure of Capacitive Sensor (Triggs, 2022)	31
2.13	Scanning Procedures of Ultrasonic Sensor (Rascagneres, 2020)	32
2.14	Block Diagram of RFID System with Four Major Devices (kynix, 2018)	33
2.15	Working Schematic of RFID System (kynix, 2018)	34
3.1	Block Diagram of Whole System	38
3.2	Flow Chart of Whole System	40
3.3	Classification of Flow Chart of Whole System	41
3.4	Connection Between Esp01s Module and Module Adaptor	45
3.5	Log In Page or Sign Up Page for Blynk Account	47
3.6	Interface of Creating a New Template in Blynk Website	47
3.7	A Switch Used to Create an User Interface at Blynk Web Dashboard	48
3.8	Interface of Creating New Virtual Pin Datastream in Blynk Website	48
3.9	Interface of Creating New Event in Blynk Website	49
3.10	RFID Scanner with Model of RC522 at Left and Mifare Card at Right	50
3.11	Comparison Between 4x4 Matrix Keypad and 4x4 Membrane Keypad (Amazon, n.d.)	51
3.12	Internal Connection for 4x4 Matrix Keypad (Rathnayake, 2021)	52
3.13	User Interface of Blynk Application for Smart Door Access System Created by Button from Widget Box	53

3.14	Datastream Integer V0 is Link to Button in Blynk Application for Smart Door Access System	54
3.15	Limit Switch with Common Terminal at Left, Normally Open Terminal at Middle and Normally Close Terminal at Right	55
3.16	Solenoid Lock with Two Philip-Head Screws on Top	56
3.17	H-Bridge Motor Driver with Eight Pins at Each Side (Proto Supplies, 2023)	56
3.18	Pin Out of L293D H Bridge Motor Driver (Last Minute ENGINEERS, 2022)	57
3.19	Working Mechanism of Magnetic Sensor Switch (RANDOM NERD TUTORIALS, 2019)	58
3.20	Magnetic Switch Sensor on Door Model	59
3.21	Main Parts of Esp32 Cam Module OV2640 Camera at Left, Development Board at Middle, and Programme Unit at Right	60
3.22	Full Connection of Esp32 Cam Module for Programming	60
3.23	Pinout of Arduino Mega 2560 (The Engineering Knowledge, 2023)	61
3.24	3D Model Case for Reader Unit in TinkerCad	63
3.25	3D Model Case Slice in Ultimaker Cura	64
3.26	3D Model Design for Solenoid Lock and Camera Unit in TinkerCad	64
3.27	3D Model Design for Solenoid Lock and Camera Unit Slice in Ultimaker Cura	65
4.1	Graphic Diagram of Smart Door Access System Without IoT Part and Image Capturing Part	70
4.2	Schematic Diagram of Smart Door Access System Without IoT Part and Image Capturing Part	71
4.3	Front View of Door Model	72
4.4	Back View of Door Model	72

4.5	Appearance of Credential Reader Unit	73
4.6	Appearance of Solenoid Lock and Lock Driver	74
4.7	Front Appearance of Camera Unit	74
4.8	Development Board of Esp32 Cam is Solder with Three Wire and Connect to External Antenna	75
4.9	Appearance of Central Control Unit Build by Printed Circuit Board and Arduino Mega 2560	75
4.10	Main Menu for Arduino IDE with Version 1.8.19	76
4.11	Selection of Board at Arduino IDE with Version 1.8.19	77
4.12	Login Interface of Blynk Mobile Application on Android Handphone	78
4.13	Devices Link to Blynk Mobile Application	78
4.14	User Interface of Blynk Application for Smart Door Access System	79
4.15	Datastream and Button Mode for Unlock Button and Halt Button	80
4.16	Effect of Pressing Unlock Button and Halt Button	80
4.17	Information of Notification in Timeline Feature of Blynk Mobile Application	81
4.18	Status of Device in Timeline Feature of Blynk Mobile Application	82
4.19	Notification of Door Sensor from Blynk Mobile Application	85
4.20	Notification of Intruder Sensor from Blynk Mobile Application	86
4.21	Blue LED Light Up during Temporary Termination	93
5.1	Digital Camera Door Lock from Tuya Company (tuya, n.d.)	106

LIST OF CODE LISTING

CODE LISTING	TITLE	PAGE
4.1	Fragmented Code of Door Sensor for Pressing Internal Switch	83
4.2	Fragmented Code of Intruder Sensor for Pressing Internal Switch	84

LIST OF SYMBOLS / ABBREVIATIONS

2D	2 dimensions
3D	3 dimensions
AADR	Automatic adaptive detection reading
ADC	Analog to digital converter
AT	ATtention
CAN	Controller area network
CMOS	Complementary metal-oxide semiconductor
COM	Common
CPU	Central processing unit
DAC	Digital to analog converter
DC	Direct current
DIP	Dual in line package
EEPROM	Electrically erasable programmable read only memory
FYP	Final year project
GND	Ground
GPIO	General purpose input/output
GSM	Global system for mobile communication
GUI	Graphic user interface
HF	High frequency
HW	Hardware
I/O	Input/output
I2C	Inter integrated circuit
IC	Integrated circuit
ID	Identity document
IDE	Integrated development environment
IoT	Internet of things
IP	Internet protocol

IRQ	Interrupt
LED	Light emitting diode
LF	Low frequency
LNA	Low noise amplifier
MISO	Master in slave out
MOSI	Master out slave in
NC	Normally close
NO	Normally open
OS	Operating system
PCB	Printed circuit board
PIN	Personal identification number
PWM	Pulse width modulation
RAM	Random access memory
RFID	Radio frequency identification
RGB	Red green blue
RST	Reset
Rx	Receiver
SCK	Serial clock
SD	Secure digital
SDA	Serial data line
SMD	Surface mount device
SMS	Short message service
SoC	System on a chip
SPI	Seri peripheral interface
SPIFF	Still picture interchange file format
SRAM	Static random-access memory
STL	Standard triangle language
SW	Software
TCP	Transmission control protocol
Tx	Transmitter
UART	Universal asynchronous receiver/transmitter
UHF	Ultra high frequency
UNIX	Uniplexed information computing system
USB	Universal serial bus

WiFi

Wireless fidelity

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Code of Smart Door Access System	112
B	Code of Camera Unit	123
C	Printed Circuit Board of Central Control Unit	134
D	Printed Circuit Board of Lock Driver	135

CHAPTER 1

INTRODUCTION

1.1 Background Study of Door Access System

Humans try to manage their door carefully to control who enters it when a straw hut was thatched together millennia ago. Initially, efforts to control flow of traffic had all been focused on preventing wild animals and elements from entering the house. Over time, the main focus was shifted to blocking random people and ill-intentioned individuals from gaining access to their personal belongings, their whole family unit as well as their private store. Most of the time, humans are successful in preventing wild animals like grizzly bears from entering their foyer, but simple blocking can no longer meet human needs for the doors. Humans expect it to perform more complicated tasks. With the advancement of technology and society, most of the traditional lock and key methods had been replaced with card access solutions especially in business areas. This access solution has revolutionized ways of handling people who has access to the building and when they have access (EPS Security, 2020). By referring to the picture in Figure 1.1, it has shown one of the famous access controls, which uses a biometric scanner and keypad as the credential input signal for the access system. Besides, the system can also record all user access records.



Figure 1.1: Example of a Door Access System (Catie, 2020)

Due to the advancement of technologies because of the industrial revolution, the lock and keys design had been replaced by the basic pin and bolt design. In 1778, the level tumbler lock was invented by Robert Barron. This design did away with pins entirely, instead having the key lift a lever to release the locking bolt. Linus Yale Sr. brought the ancient Egyptian pin lock idea into the modern age by creating a common Yale lock in 1848. The Industrial Revolution, with its unprecedented ability to mass-produce and standardize products, brought affordable door security to the masses. The high mass popularization of locks has increased interest in lockpicking from thieves; while the ability and convenience to copy physical keys provide better chances for some unauthorized people to steal the key for invasion purposes. Security vulnerabilities and the inability to differentiate visitors are the main security problems for traditional locked doors. This problem wasn't overcome until the invention of the access control system.

Access control systems overcome the restriction of traditional lock and keys by using computers. The system uses several types of credentials for replacing physical keys, providing access to any people depending on the credentials provided by humans. Doors will unlock within a set time and record the access action immediately when access has been granted. The door will stay locked if access is rejected by the computer, but there will still be a recording action for safety purposes. Not only that, the door and alarm will be monitored by the system to prevent the door from getting forced open by some people or to warn that the door is not closed properly after unlocking. Normally, at least one reader will be present in the access control system, as it is used to detect, scan or read credentials provided by the user. When the reader detects any types of credentials, the information will get transferred

to a control panel (basically a reliable processor) for comparing purposes. The credential's information is compared with the access control data in order to grant access or deny access for the door, and every access record is recorded into a database. The control panel will instruct the relay to unlock the lock if the credentials match the access control list. The reader also provides feedback to notify the user about the access status, for example blinking a green Light Emitting Diode (LED) for success status or blinking a red LED for denied status (Newman, 2010).

The single-factor authentication access system has one dangerous weakness, which is that the credential of the system can get stolen by others. Those people can use it to gain access without notice by the access system. For example, Christine has access to a server room, but John doesn't. There is a possibility Christine gave her credentials to John or he stole the credentials from Christine in order to enter the server room. This situation causes the access control system to lose its functionality (Newman, 2010). To solve this problem double factor authentication can be used for the access control system. Under this condition, the user needs to provide more than one credential for access to be granted. Nowadays in the market, authentication factors are classified into three main types, three of them has been shown in Table 1.1. Furthermore, somebody the user knows is considered as the fourth factor of authentication. Other users may provide their authentication to the user for accessing purposes. However, this scenario must be set within the access system first. For example, if user A loses the card but still has the password, then other users from the same system can provide their cards or tags to combine with the password from user A to access the system. Therefore, the combination of credential input from the different users is also allowed for access purposes.

Table 1.1: Types of Authentication Use by Access Control Systems

Types	Example
End User (Know It)	Password, Pin, Passing phrase
End User (Own It)	Key, Smart card, Tag
End User (Own It Naturally)	Voice, Fingerprint, Face
End User (Recognize It)	Designated peoples

Many benefits have been brought to humans by replacing the traditional lock system with the access control system. An access control system provides convenient ways of access, allowing the user to access different zones with full control. As long as authorization is provided, workers, employees or users can access their desired working area by using smart card, Personal Identification Number (PIN), or password. The access control system also provides easy ways for tracking purposes. As mentioned above, the system will keep every access record into the database whether access is granted or denied. With this action, the system will be able to keep track of who is entering the building and when does he/she enter. Thus, information collected from the system will help to check personnel attendance or tracking the staff when any problem or illegal act is reported. Besides, an access control system also helps to reduce financial burden. Companies no longer require a security guard, since the system has better verification and higher accuracy to identify people. Integrating the access control system with other systems also helps save costs by adding lighting control into the system to automatically turn the light in the office on and off by detecting if there are any people present. Besides, minimizing the risk of stealing is one of the main benefits of using the access control system. An access control system can protect personal belonging, assets, and equipment since it allows users to set their restrictions. Thus, only authorized individuals are allowed to enter the area or building. As the arrival and departure status of employees are tracked by the system, it also helps to deter theft and minimize criminal rates (cie, n.d.).

With the passage of time and the emergence of more and more complex requirements, a simple access control system can no longer meet these requirements. Thus, many new and advanced technology have been used to replace outdated technology from the access control system. The following paragraph will discuss about the evolution of the access control system. First the PIN access control device was invented in 1967, which is a great technical advancement for locking mechanism. This device contains a keypad, which is used by the user to key in their password. Even though the PIN access device is able to prevent an unauthorized person from entering, but it also has some serious drawback. Sharing of PIN became the major problem for the PIN access device, as a physical key could not be shared by many people but sharing a 4-digit password among a few people can be done easily. The more the people who know about the password, the higher the risk of crimes to

happen. If users forgot about their PIN, it would be very difficult to regain access and retrieve back the PIN since the internet was not yet invented. In 1970, magnetic strip technology had been used by the hotel industry to replace the cumbersome and expensive keys. The advantage of this technology is that the “Magstripe” cards can be activated or deactivated easily. It is easier to be replaced and has a lower price. However, this technology also brings some negative impact, like the card becoming less magnetic over time. Hackers can manipulate the card reader after knowing how the magstripe cards are configured.

The invention of Radio Frequency Identification (RFID) and the internet in 1990 has advanced the access control system. Server based networking and databasing has become possible. The invention of RFID is used to solve the demagnetizing problem of magstripe card. RFID technology uses a unique identifying data method to program the card, and information on the card will be shared out through electromagnetic waves when it is near to the card reader. Identification data will be sent to the access control database for comparing and checking. The card will unlock the door in a fraction of a second if the data is matching. Even with the most advanced RFID technology, users still needed to carry an extra keycard, as there is a possibility of forgetting or losing the keycard causing the user to be unable to access into the building. One way to solve this problem is to let the user become the key of the entrance. Fingerprint, voice or the face can be used to access the control system. This forms the concept for biometry technology. Biometric technology is able to achieve “keyless entry”, since it does not require any card, tag or even a password. Even though biometric technology is more convenient than RFID technology, most will act as extra protection for high-security settings. The biometric technology will work together with RFID or PIN technology in the access system because the biometric technology is less reliable than RFID technology or PIN technology. Although biometric technology is not that reliable compared to PIN or RFID control system but with the advancement of technology in finger scanning, voice recognition, and facial recognition, biometric technologies are very likely to dominate access control systems in the coming decades (Current Technologies, 2021). The following subsection will discuss the problems statements for the system.

1.2 Problem Statements

With the development of modern society, the pace of people's lives has become faster than before, which also includes the speed at which they deal with affairs. Especially in big cities, this phenomenon is simply the norm. The traditional way to access a building door would require a physical key to unlock it. However, it would be troublesome and time-consuming since it is not convenient to bring a bunch of keys, and it requires time to search for that key to open a lock. Thus, a smart access control system can solve this kind of problem. The system does not require a physical key to unlock the door; the user will use a password, smart card, tags, fingerprint, or voice to gain access. Due to the advancement of technology, more and more systems have started to integrate with the Internet of Things (IoT), including access control systems. The applications send a signal to the smart access control system for accessing purposes. It is more convenient to download an application into a smartphone instead of bringing a key around. A smart access control system is used to provide convenient ways to access a door and increase safety for people. The system should be able to provide any warning signal to people if any dangerous input signal is detected. When any crime occurs, sufficient evidence is crucial in convicting the perpetrator. However, a regular access control system only can be used to stop unauthorized people from entering. Thus, a surveillance system can be combined with a smart access control system to increase safety and provide evidence if any criminal cases happen. The following subsection will mention the main objectives for the system.

1.3 Objectives

The objectives of the project are shown as follow:

- i) Design and create a modern door access system which has multiple access methods, such as manual mode (using keypad), wireless mode (using proximity readers), or internet mode (using applications).

- ii) Increase the rate of safety for this access system by sending notifications to warn the end user. Notifications will be sent in message form or picture form if the door access system is aware of any danger, for example, an invalid password entered more than N times, or any motion detected by the sensor at night time.
- iii) Long-range remote-control function and internet mode (using application) are accessible for the user who is already registered under the door access system.

Additional objectives are added in Final Year Project 2, after achieving the main objectives of the thesis. The following subsection will discuss the scope for the system.

- iv) Design a halt function to temporarily terminate the system. The system turns into temporary termination within a certain period through a mobile application.
- v) Design an intruder detection function. The system can notify user of the system through message notification if an intruder tries to enter the building.

1.4 Scope

This project is the study of a smart door access system. The operation process of the door access system will be analysed and serve as a foundation knowledge to design and implement a smart door access system. A smart door access system mainly requires central control units and input and output devices. The main control panel (a microcontroller) used in this smart door access system is selected from an existing microcontroller at the market rather than a custom design. Multiple inputs will be implemented in the smart door access system, including manual input and wireless input. A simple electric lock will be used as an output device for this smart access system since the project's main focus is on the operation of the smart door access

system. Thus, this project will not consider the reliability and robustness of the simple electric lock. The following subsection will discuss the outline for the thesis.

1.5 Outline

Chapter 1 of the thesis is about the introduction of the whole project. The background study, problem statement, and objectives are included. The description, history, and trend of the evolution of access control systems are mentioned in the background study. A few problems are mentioned and discussed in the problem statement. The objectives of the project have been stated in order to solve the problems. The Chapter 2 is about the literature review. Commercial-based products and student/personal-based products will be reviewed in this chapter. Reviewing design methods, explanations, theories for technology, and suitable devices will also be included in this chapter.

Chapter 3 discusses the methodology for the system. The solution and procedures to design the smart door access system will be discussed in the chapter. This chapter also covers the selection of hardware and software necessary for the door access system. Furthermore, the progression of the whole project will be shown using the Gantt chart at the end of this chapter. Next, the Chapter 4 is about the result and discussion of the project. Preliminary work for the system will be shown in this chapter. The prototype model for the system and software needed is also discussed and shown in Chapter 4. This chapter has the analysis of the system's reliability through some hardware testing, and the overall cost is listed in this chapter also. Lastly, Chapter 5 is about the conclusion of the whole project. This chapter will summarise all the chapters covered from chapters one to four. The chapter also will discuss the limitations of the system and list recommendations for the improvement of the system.

1.6 Summary

In this chapter, a background study for smart door access systems has been reviewed. The background study includes the working principle of an access control system and the trend of the evolution of access control systems. Besides, the advantage of using smart access control to replace traditional locks is also discussed within the background study of smart door access systems. Furthermore, different types of credential input devices are also discussed in the background study section. The devices include wired, wireless, and biometric devices. A few problem statements have been discussed in this chapter. Three main objectives and two extra objectives have been listed to solve the problems stated in this chapter. The next chapter will review a few projects related to or similar to the smart door access system. Besides, some necessary devices and theories will also be reviewed in Chapter 2.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter has a review of five different projects. Among five projects, three are commercial-based, while another two are student-based. Three famous microcontroller boards will be discussed and compared in this chapter. The chapter also includes a review and comparison between two IoT application platforms. A biometric technology suitable for the door access system is also discussed in the chapter. The last section of the chapter will discuss about wireless communication technology.

2.2 Product Review About Student's Projects

This section will discuss and analyse the smart door access systems done by students, and three projects will be discussed in the following subsections.

2.2.1 RFID and Password Based Door Lock by Prajwaln

This project used Arduino UNO as the main control unit to design a door lock system. In this project, two different types of input signals are used to access the system, both

of them working independently. The system will be accessed if any input signal provides the correct credential. This system has two modes: mode A (using a keypad) and mode B (using an RFID scanner). Mode selection can be made by using a 4x4 keypad. Users need to press A or B from the keypad before providing any credentials for accessing. The user can access the system by keying in the correct password via a 4x4 keypad or scanning the correct tags or RFID cards on top of the RFID scanner. Red Green Blue RGB LED, and a buzzer are used to indicate the access status. The red LED indicates access denied, while the green LED indicates access granted. Furthermore, the password-changing function is also included in this project. Users can replace old passwords after successfully keying in the current password before changing it (prajwalsn, 2022).

The advantage of this system is high flexibility since the two input signal works independently. The user is not required to provide two credentials to access the system if the user forgets to bring or loses the card. They can still enter the building by keying in the correct password. Besides, the user can change the current password without relying on the admin or the door lock system company. This option is very convenient for any user who likes to change the password frequently. The disadvantage of this project is that the safety level is low because the system only depends on a single authentication factor. The system can be accessed if the password is valid or a valid card is scanned. There is a possibility of an RFID card getting stolen by other people. They may use this card to access the building without the system noticing.

2.2.2 RFID and Keypad Door Lock and Alert System Using Arduino by Aqib

This project uses Arduino UNO to design a door lock and alert system. There are two types of credentials used to access this system. A 4x4 keypad is used to key in a 4-digit password, while an RFID scanner is used to scan a tag or an RFID card. The system implements double-factor authentication, meaning the user must provide two correct credentials for access. The user needs to scan an RFID card first before being allowed to key in a password after successfully scanning. The lock will only unlock

if the user provides both credentials correctly. An alert function is included in this project; a Short Message Service (SMS) notification will be sent to the user during each access action. The user will receive an alert message if the wrong card is scanned or wrong password is keyed in, while a confirmation message will be received after access is granted. Besides, this system also contains a halt function. The user can temporarily terminate the system when a “close” word is sent into the system. Under this condition, the system will not receive any input signal, although it is a correct signal. The system returns to normal operation if the user sends an “open” word. SIM900 module is used to send or receive an SMS message from the user. This module is very important in carrying out the alert and halt functions (Aqib, 2018).

The advantage of this project is having a higher safety level because it executes double-factor authentication. Users must provide two different credentials for the system to gain access, so it can prevent unauthorized people from stealing the card or tags or using a lost card to access the building. Secondly, the system has higher alertness compared to the system in subsection 2.2.1. The system will notify the user via SMS for each access action. Thus, users can know and monitor the system, even though they are far from the building. The system in subsection 2.2.1 only provides light and sound alert. This feature will lose effectiveness if the user is away from the system. The disadvantage of this project is the imperfect halt function. This project only allows one user to use this function. There is a possibility the user might forget to return the door lock system to normal, causing other users to not be able to access the system. Under the halt condition, the system will not scan any cards or tags and stop receiving the password from the keypad. This problem seriously impacts financial loss or endangers life in case any emergency happens.

2.2.3 Door Access System - Arduino Based by Shuhada Natasha Bint Mohd Zainor

Arduino Uno was used as a main control unit to design a door access system. This project has implemented double-factor authentication, which means the user needs to

provide two different types of credentials to access the system. Users need to provide the correct password via a 4x4 matrix keypad, then only be allowed to scan their fingerprint on the fingerprint sensor. As long as one of them is wrong, the system will reject access. The system also includes an alert system; every user has three chances to key in or scan their credentials. If it exceeds this range, a siren will be activated for warning purposes. This project also includes an intruder alarm system. The wrong credential does not activate this system, but no credential activates it. For example, any unauthorized people who try to push the door without entering the correct password and scanning fingerprints will turn on the alarm system to warn people (Natasha, 2012).

The advantage of this project is it “frees the users’ hands” because the end user of this system does not need to bring any physical keys, cards or tags to access the system. As long as users remember their password and scan with the correct finger, they can pass through. This design is convenient for the user who always needs to carry many things. They do not need to spend much time finding keys or cards for the system. The weakness of this project is the alert system is too fragile; it only uses a siren circuit to warn people if it detects an intruder or enters the wrong credential more than 3 times. Such a design is only workable for a short distance. If the user is far from the system, this warning will lose effectiveness because a simple siren circuit will not notify them. The following subsection will review the commercial-based project.

2.3 Product Review About Commercial Projects

This section will discuss and analyse the smart door access system manufactured by different companies for commercial use. A total of two products will be discussed in the following subsections.

2.3.1 Vanma Company

Vanmalock is a key-centric access control system with three major elements: intelligent electronic keys, electronic-based locks, and powerful management software. The appearance of the electronic lock of Vanma looks similar to a mechanical lock, but it has a big difference based on the function. The Vanma electronic lock can store information during operation. The electronic key from Vanma is unique; it is impossible to duplicate and re-programme. By using the management software, employers can determine their employees' particular unlocking period and unlocking list. Unlocking authority is only workable within the specified period, so employees cannot unlock at other times. There will be an unlock record after each system access. The record is uploaded into the software for tracing purposes. Management can use this record to view the unlock process and trace it back to individual employees (Vanma, 2022).

Vanmalock provides multiple access for a single electronic key. One electronic key can be programmed to unlock multiple locks. Thus, it can replace bulky bunches of keys. The Vanma management system can generate access records. The system can provide access to all activities done by the relevant personnel, as well as an audit report in its entirety. Besides, Vanmalock also provides Blacklist management to the user. In case of any loss or theft of smart electronic keys, the keys can be disabled by software to prevent crime. Vanmalock has a more flexible access control option. Using a management system, the access period, including dates or times, can be set, as well as the location of the electronic lock. In addition, AES256 encryption technology has been used in this lock system to provide better security. Installation of the Vanma lock is convenient and easy since the electronic lock does not require power or wiring.

2.3.1.1 Product Description for Smart Padlock

Vanmalock system contains three major elements: smart electronic lock, electronic keys and a management software. Several types of locks have been provided by the

Vanmalock system, including Padlocks, Cam locks, Cabinet locks, etc. Vanma lock has provided three versions of smart electronic keys: smart-based, Bluetooth-based, and fingerprint-based. All types of electronic locks and electronic keys are managed under the same management software. Users can customize their access system by combining smart locks and electronic keys. The smart padlock will be selected as the representative of Vanmalock to understand the access system better.



Figure 2.1: Smart Padlock from Vanmalock Company (VANMA, 2022)



	Vanma Electronic Padlock IP65 Waterproof Padlock 35mm + Smart Key TIME-LIMITED SAMPLE PROMOTION (-\$43.00)	\$215.00 \$172.00
	Vanma Electronic Padlock IP65 Waterproof Bluetooth Fingerprint Key TIME-LIMITED SAMPLE PROMOTION (-\$30.00)	\$150.00 \$120.00
Subtotal		\$292.00
Shipping		Free
Total		USD \$292.00

Figure 2.2: Total Price for One Smart Padlock and One Electronic Key (Including Bluetooth & Fingerprint) (VANMA, 2022)

The Vanma padlock shown in Figure 2.1 is similar to a mechanical lock, but it is a high-security lock with data task management capabilities. The smart padlock requires “smart keys” to unlock, and the keys will provide power to the padlock when it is unlocking. With the implementation of rigorous encryption technology and

wireless communication function, the padlock cannot be unlocked technically. Installation of a smart padlock is very easy since the process does not require wiring and an extra power supply. The system software will uniformly set the authority for unlocking specific door locks for each smart electronic key. The electronic key should perform unlocking within its effective times. This system software has realized multiple unlocking of a single key with highly efficient and systematic management. According to the price shown in Figure 2.2, a single set of smart padlocks will cost USD292, and there are no extra shipping charges.

2.3.2 MAG Company

MAGNET Security & Automation Sdn. Bhd. (MAG) was founded in 1980 under the strong leadership of two generations of leaders. As a leading provider of safety and automation solutions in Southeast Asia, MAG is one of the pioneers in the industry, with over 40 years of extensive technical experience and knowledge. Building on the success of its own MAG Auto Gate, MAG has expanded its service and product offerings to include comprehensive security and automation solutions such as barriers, pedestrian gates, access control and video surveillance.

The touchless access system from MAG provides a hands-free experience for the end-user. There is a possibility of forgetting to bring cards, tags, or keys. However, users will always remember to bring their faces; they can access the system with smiling faces. The reader of the touchless access system requires “faces” for entrance purposes. Besides, the touchless access system saves extra costs for the end-user. The system can store up to 50k face capacity in the recognition reader; with this massive amount of storage, the end-user does not require extra access cards. Implementation of Automatic Adaptive Detection Reading (AADR) technology in the touchless access system can reduce recognition time for each user. This technology will automatically adjust the detection area to have accurate face recognition for end-users from far. The touchless access system can operate continuously within the shortest time under this feature. Furthermore, face recognition will provide the highest security level. The access card can be cloned, but

the human face is tough to be cloned. The touchless system also includes dual lens technology, which helps to reject any photo from a smartphone or hardcopy (MAG, 2022).

2.3.2.1 Product Description of Touchless Door Access System with FR300 Reader

MAG company provides many touchless access systems for different kinds of entrance, including pedestrian, lift and door. Thus, the touchless door access system shown in Figure 2.3 is selected to be described. The access system requires three main devices: a face reader, the MagEtegra access software and a touchless button. The access software provides simple enrolment for tenants' and visitors' profiles through the face. Enter and exit events can be monitored easily using the MagEtegra software. Using the TB01 touchless button, the user is not required to physically touch the button for exit purposes. This touchless button can be mounted on the wall also. The FR300 face recognition reader has been used as an input sensor for this touchless door access system. The MAG FR300 reader has been built with a modern face-tracking algorithm. The algorithm allows the reader to perform faster and more accurate dynamic detection for facial recognition (MAG, 2021). Well designed sizes allow the FR300 reader to easily fit into commercial premises. The reader is suitable for door access for offices, hospitals, airports, factories, etc. The following subsection will review and compare the microcontroller boards.

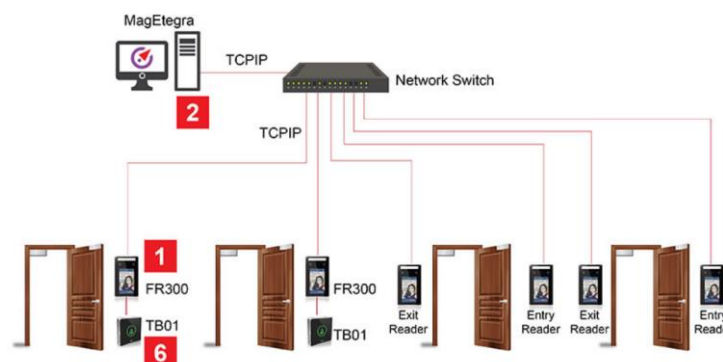


Figure 2.3: Full Connection of Touchless Door Access System with FR300 Face Recognition Reader (MAG, 2022)

2.4 Microcontroller Review

This section will discuss three types of microcontroller boards from Arduino, Raspberry Pi, and Espressif systems.

2.4.1 Introduction to Arduino

Arduino microcontroller board is an open-source platform with low difficulty in using hardware and software. The microcontroller board can read input signals, for example, sensor value due to the intensity of light, button pressing, or even detect a message from Twitter. An Arduino board will process the input signal and turn it into an output signal to control other devices, like turning ON or OFF a Direct Current (DC) motor. Users can set their desired instructions into the Arduino board to perform some operations. The user would need Arduino programming language and an integrated development environment to set their instructions into the Arduino microcontroller board (Arduino, n.d.).

Over the years, Arduino has served as the brain of thousands of projects, ranging from simple household objects to complex scientific equipment. An international society of creators, educators, hobbyists, artists, software developers, and experts has assembled around this open-source platform. Their contributions have added up to an enormous amount of accessible knowledge that can significantly assist novices and experts.

In comparison to other microcontroller platforms, Arduino boards are relatively inexpensive. One can create the cheapest Arduino module, or even pre-obtain pre-assembled Arduino modules under RM220. Furthermore, the integrated development environment of Arduino can run on different operating systems like Windows, Linus, OSX, or Mac. In comparison, most of the microcontroller Integrated Development Environment (IDE) software from other brands is only compatible with the Windows operating system. The IDE software of Arduino has great flexibility between beginners and experts. Beginners can quickly master IDE

usage, while experts can use it to do more advanced usage. In addition, the Arduino board require less power to program itself. Even a battery can power up the Arduino board. Low power consumption can prolong the service life of the power source. The Arduino board can run on a minimum of 286mW (Chris, 2021).

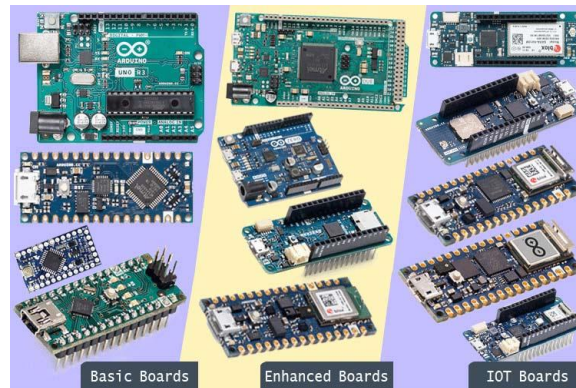


Figure 2.4: Classification for Original Arduino Board (Joseph, 2022)

2.4.1.1 Types of Boards for Arduino

The Arduino board shown in Figure 2.4 can be classified as basic, enhanced or IoT boards. For enhanced board and IoT board, both of them can perform more complicated tasks like wireless communication, internet connection, etc. A basic board is a preferable choice to start with. Most of the basic boards are powered by 8-bit microcontrollers, contains lower clock speed, or have a limited number of General Purpose Input/Output (GPIO) pins. Besides, many modules and external shields are available on the market, and all these modules can be added to the basic board to increase their functionality. Arduino Uno, Arduino Mega2560, and Arduino Nano are people's most popular basic boards. Multiple kinds of Arduino UNO boards are obtainable on the global market, but a large percentage of these boards are clones or copies of the original UNO board (Joseph, 2022).

2.4.2 Introduction to Raspberry Pi

It is a compact single-board computer, and it can act as a small personal computer by adding peripherals like a monitor, mouse, and keypad to the Raspberry Pi. The main application of Raspberry Pi is used for the Internet of Things, video editing, processing real-time images or advanced robotic applications. Even though Raspberry Pi behaves like a computer, but its operation speed is still lower than a laptop or PC. A Raspberry Pi board needs an operating system; Raspbian is the official Operating System (OS) for Raspberry Pi. The Raspbian OS is well-suited for use with the Raspberry Pi. It contains a Graphical User Interface (GUI) that includes tools for surfing the web, Python programming, office, games, and so on. The Raspberry Pi's capacity is not sufficient to install the OS. Thus, a Secure Digital (SD) card with at least 8GB is needed to add to the board for OS storage. Raspberry Pi is much more than a computer because it provides access to on-chip hardware, like GPIOs, for developing applications. We can connect and control equipment like LEDs, actuators, and cameras by using GPIO (ElectronicWings, 2019).

Among most microcontroller boards, Raspberry Pi is considered quite expensive. The lowest priced Pi board start from RM120; the price and specifications are strongly correlated. Pi board with the more advanced specifications will be more costly. For example, the price of a Pi 4B+ with 8GB Random Access Memory (RAM) version is RM422 while the price of Pi 4B with 2GB RAM versions is RM229. For the Raspberry Pi, there is a significant overhead in simply reading sensor signals; the user must install some libraries and software packages before connecting all those sensors and components. Since Raspberry Pi operates under a certain OS, it must be properly shut down before removing the power supply. It will help to prevent software corruption and damage to the Raspberry Pi board.

In comparison, another microcontroller board can easily turn on or off at any time, including accidentally powering off. Raspberry Pi is a powerful hardware device that requires continuous 5V power, which is difficult to run on battery cells. In contrast, other microcontrollers like Arduino require less power and can easily be driven by a battery pack. Like a computer, the Raspberry Pi can perform various tasks at the same time. If the user wants to create a complex project, like an advanced

robot, or the user needs to manage things from a web page over the internet, the Raspberry Pi is the best option. The Raspberry Pi can be converted into a web server, virtual private network, network storage, database, or management system (Jayant, 2016).

2.4.2.1 Types of Boards for Raspberry Pi

On the market, many Raspberry Pi boards are available. Even though most of them provide a similar function but their specifications differ greatly. The boards will have different operating speeds, sizes, memory capacities and costs. Some of the popular Pi boards shown in Figure 2.5 will be introduced in this section. Raspberry Pi model A is suitable for a low-cost project which requires a complete computer without networking capabilities and limited Input/Output (I/O) support. The Raspberry Pi B+ is considered as an enhanced version compared to the Pi A model, and it is suitable for a project in which cost is not an issue and the most powerful Pi is required. This model also comes with simple I/O, which makes it ideal for first-time Pi projects. The model B or B+ board supports networking capabilities without adding an extra sensor or shield. For Raspberry Pi Compute model, it is ideal for commercial applications that require a large number of I/O lines. This model also preserves strong Central Processing Unit (CPU) abilities. The last board is the Raspberry Pi Zero model. It is great for a low-cost, tiny project that requires a completely operational computer and would gain from wireless access (Maker.io., 2018).

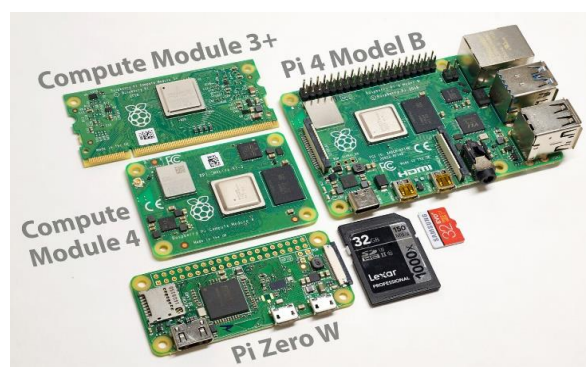


Figure 2.5: Appearance Comparison for Raspberry Pi B, Pi Compute and Pi Zero (Wu, 2020)

2.4.3 Introduction to Esp8266 and Esp32

The Esp8266 is a comprehensive System on a Chip (SoC) circuit that contains a Wireless Fidelity (WiFi) module with Internet Protocol/Transmission Control Protocol (IP/TCP) protocol stack. The board allows the user to connect to any microcontroller via WiFi. The Esp8266 has a function to organize any application or to unload any WiFi functions. It is strong and can operate robustly in terrible industrial environments. This is entirely due to its wide range of operating temperatures. It also includes a power-saving architecture built with a 32-bit processor from Tensilica company (Ashwak, 2021).

Espressif Systems' Esp32 is a budget SoC microcontroller. The Esp8266 board is the predecessor for the Esp32 board. The Esp32 microcontroller is manufactured in single or double-core versions with a 32-bit Xtensa LX6 model microprocessor. The Esp32 microcontroller, just like the Esp8266, has embedded radio frequency components like a Power amplifier, Low Noise Amplifier (LNA), antenna, and a Radiofrequency Balun. Another important aspect of the Esp32 microcontroller is that it is built with super low power 40nm technology from TSMC company. So, using Esp32 to design battery-powered applications such as wearables, audio devices, children's monitors, or timepieces should be a simple task (Teja, 2021).

2.4.3.1 Comparison Between Esp8266 and Esp32

Both microcontroller boards contain 32 bits of microprocessors; the Esp32 boards have two cores and operate with a CPU speed range from 160MHz to 240MHz. The Esp8266 only have one core processor with a CPU speed operating at 80MHz (Santos, 2021). Both of them are considered low-budget WiFi modules, which are suitable for any IoT project or automation. However, only Esp32 supports Bluetooth connection since there is a built-in Bluetooth inside. Furthermore, the GPIO pins of Esp32 is more than Esp8266, and different kinds of pins are included in GPIO pins, for example, Analog to Digital Converter (ADC) pins, Digital to Analog Converter (DAC) pins, and serial communication pins. Esp8266 does not have ADC pins, but

Esp32 has two 8 bits DAC pins. The Esp8266 only contains one ADC pin, while the amount of ADC of ESp32 is 18 times more than Esp8266. Both boards support most serial communication like Serial Peripheral Interface (SPI), Inter-Integrated Circuit (I2C), and Universal Asynchronous Receiver-Transmitter (UART), but Controller Area Network (CAN) serial communication is unavailable on the Esp8266 board. Even though Esp8266 and Esp32 are sold at low prices, the price for Esp32 is higher than Esp8266. Since Esp8266 was developed earlier, some libraries and features are considered better for Esp8266, and more resources are available. Some development boards under Esp32 and Esp8266 have been shown in Figure 2.6. The following subsection will review and compare IoT application platforms.

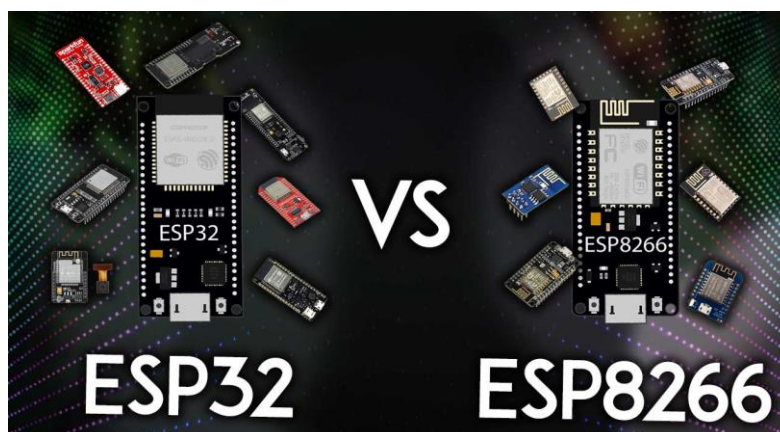


Figure 2.6: Two Most Popular Board for Esp32 Chips and Esp8288 Chips, Esp32 DevKit V1-Doit (Left side) and Esp8266 Esp-12E NodeMcu Kit (Right side) (Santos, 2021)

2.5 IoT Application for Microcontroller

This section will discuss and analyse a suitable IoT application for the Arduino Mega2560. Two IoT platforms will be discussed in the following sub-section.

2.5.1 Introduction to Arduino IoT Cloud

Arduino IoT cloud is an application that provides a faster, easier, and safer way for the designer to build up their connected object. The Arduino IoT cloud allows multiple devices to exchange real-time data with each other. The connection between Arduino IoT cloud with the devices is established securely. Thus, every transmission of data is protected. Besides, the designer can create a simple user interface to monitor their devices anywhere and anytime. Designers can produce a unique dashboard by using widgets, which will be linked to coding and uploaded to devices via the browser (Mohahan, 2022).

The designer can create or edit a new template code in the Arduino IoT cloud. The code can be uploaded to the microcontroller board using a web editor created by the Arduino company (Project Hub, n.d.). Arduino IoT cloud provides many features to the designer. Some standard features that most designers use in their IoT projects have been shown in Table 2.1, and one example of a user interface created by Arduino Web Editor has been shown in Figure 2.7.

Table 2.1: Common Features in Arduino IoT Cloud

Features	Description
Monitor Data	All the data from the designer's project can be easily monitored through a dashboard. The dashboard refers to a User Interface created by the designer on the Arduino Web Editor.
Sharable Dashboard	Many people can view the data via dashboard sharing.
Synchronize Variable	Variable sets in the Arduino Web editor can be synchronised across devices and use minimal codes to enable communication between devices.
Scheduler	The task or job of the IoT project can be turned ON/ OFF by using the scheduler feature at a specific time. Schedulers allow designers to set a specific time in seconds, minutes, and hours.

Over the Air (OTA)	The designer can upload new or edited codes into the microcontroller via the internet without a solid wire connection.
Webhooks	Integration of project with other services.
Amazon Alexa	Support integration with Amazon Alexa to get a voice-controlled function in the project.



Figure 2.7: Example Appearance of Dashboard from Arduino IoT Cloud (Mohahan, 2022)

2.5.1.1 Hardware Compatible and Internet Connection

Even though the Arduino IoT cloud is designed by Arduino company, it still supports internet connection to a third-party microcontroller like the Espressif system (Esp8266 or Esp32). Board selection can be easily found in the Arduino Web editor, which is shown in Figure 2.8 and Figure 2.9. The Arduino IoT cloud supports three internet connections: WiFi, LoRaWAN and mobile networks. WiFi connection is easier during project set-up; all credentials from the user can be entered safely in this way. This connection method will be suitable for low-range projects. For low-power projects, the LoRaWAN connection is recommended to be used in urban and remote areas if other famous connectivity

types are not accessible. In comparison, the mobile network connection is suitable for remote areas since WiFi services are not vital. A mobile project like cargo tracking is also suitable for using a mobile network connection (Soderby, 2022).

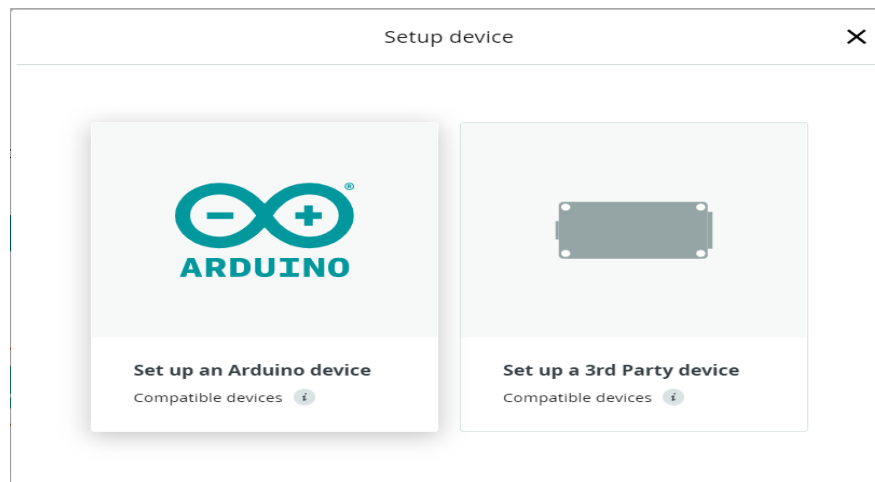


Figure 2.8: Selection Between Arduino Board or Third-party Board in Arduino Web Editor

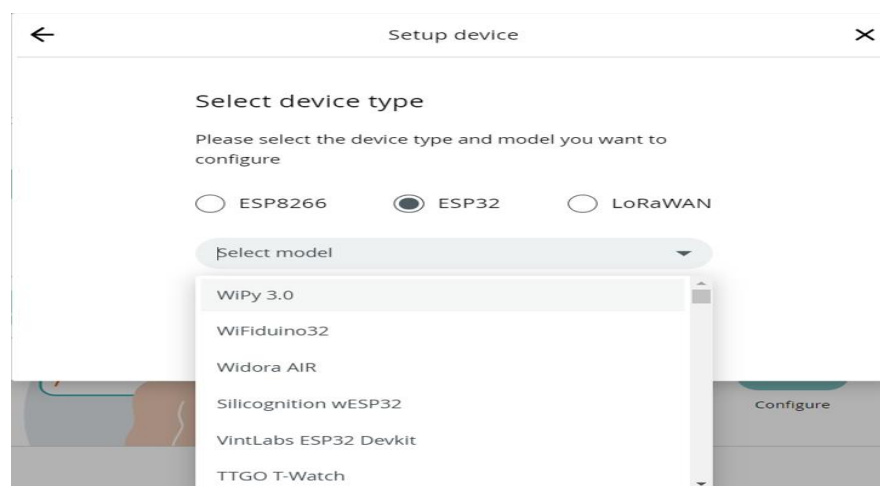


Figure 2.9: Many Types of Microcontroller Boards from Third Parties are Compatible with Arduino IoT Cloud

2.5.2 Introduction to Blynk

Blynk is a comprehensive software package for developing, testing, deploying, and remotely managing connected electronic devices at any scale; it ranges from personal projects to millions of commercially connected products. The designer can connect their electronic hardware to the Blynk cloud and generate an application without coding. The application is compatible with iOS and Android. Analysing real-time data, reviewing history, controlling, getting notifications, and remotng devices can be done from anywhere in the world through this application. Besides, Blynk also supports a multi-tenant solution. The designer can set up some roles and configure permission to allow other users to access the data in the Blynk application. Anyone like a family member, employee or customer who purchased the product from a designer can download the Blynk application and start using it since it is ready to be used by end-users.

Furthermore, Blynk has provided Business Plan for the designer. They can add in their company logo, design a new app icon, design a new theme and publish a new app to App Store or Google Play. The new app will work independently for that designer's devices and products (Blynk, 2022).

2.5.2.1 Hardware Compatibility and Internet Connection

Blynk IoT platform can support more than ten microcontroller boards, including Arduino, BBC Microbit, Espressif system, Plantronics Fox, etc. The selection of a microcontroller can be made when creating a new template, as shown in Figure 2.10. In addition, the Blynk IoT platform also supports up to four different types of internet connections, which include Ethernet, WiFi, Universal Serial Bus (USB), and Global System for Mobile Communication (GSM). The following subsection will discuss fingerprint recognition technology.

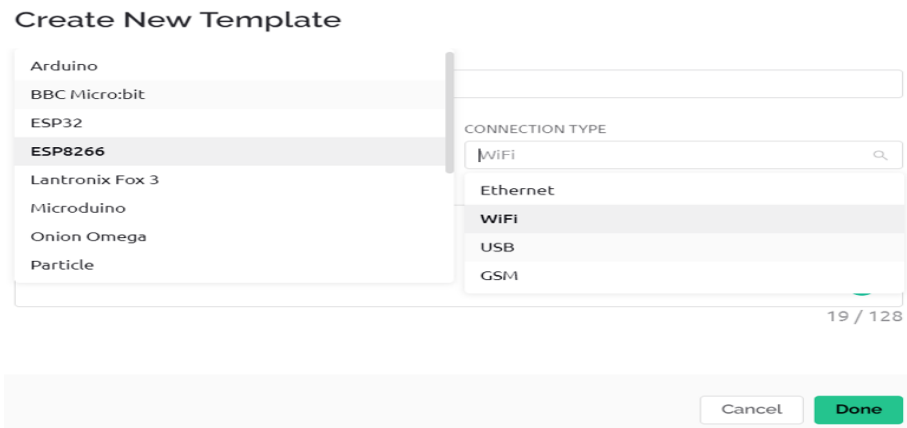


Figure 2.10: Selection of Microcontroller Board and Internet Connection in Blynk IoT Platform (Blynk, 2022)

2.6 Introduction to Fingerprint Recognition

Fingerprint recognition is an automated method to identify the characteristics of an individual based on differentiating two different fingerprints. The fingerprint recognition is a famous biometric technology and is the most popular biometric solution used on computerized systems for authentication purposes. Compared to other biometrics, the convenience of acquisition, established use, and acceptance of fingerprint identification are the factors for its popularity.

Fingerprint recognition is famous as a biometric solution and has many applications. This recognition can be applied to logical access control. Many digital devices, such as personal computers, have fingerprint reader devices and software for logical access control. Besides, some smart locks on the market also contains fingerprint readers, so physical access control is also one of the applications for fingerprint recognition. Some companies have implemented fingerprint recognition for their attendance system, and the punch card system would be replaced by fingerprint recognition for collecting employee attendance (Biometric Solutions, 2021). Since fingerprint recognition is famous and has many applications, let us consider the suitability of fingerprint recognition as a biometric solution. Five aspects will be considered on the suitability and listed below:

Table 2.2: Aspect to Determine Suitability of Fingerprint Recognition

Aspect	Description
Universality	Fewer people will have incorrect matching for their ten fingers since most fingerprint readers allow an individual user to enter multiple fingerprints to prevent denied access after getting injured.
Uniqueness	Most fingerprints are unique for every person, but two different people may have the same fingerprint. This problem is due to the low resolution of the fingerprint image. Thus FAR strongly relies on the fingerprint reader's quality.
Permanence	Fingerprints stay the same due to ageing but losing collagen may cause reading fingerprints to become challenging. This can result in a significant increase in false rejections among the elderly. In addition, severe damage, like a fire wound, can lead to fingerprint damage. If multiple fingers are registered, the possibility of an authorized individual getting rejected by recognition will be reduced.
Acceptability	Fingerprints are readily accepted once people recognize that they leave their fingerprints everywhere and that fingerprints could even reveal sensitive information such as medical conditions.
Collectability	The fingerprint is easily collected, and the digital camera is available as the cheapest fingerprint reader. Some advanced fingerprint reader like Complementary Metal-Oxide Semiconductor (CMOS) reader is not easy to get fooled, and it is affordable. In some situations, such as when people cannot clean their hands, more expensive methods may be needed to get a utilizable fingerprint image.

2.6.1 Different Types of Scanner for Fingerprint Recognition

The optical scanner uses the oldest method to capture and compare fingerprints. The scanner relies on an optical image like a photograph for detection. It will use an algorithm to differentiate unique patterns on the image, for example, ridges or marks, via analysing the intensity of the image. The optical scanner is highly dependent on the resolution, greater pixel density, and the finer details about your finger that the sensor can discern, raising the level of safety. Usually, an optical scanner contains a massive amount of diode per inch to capture sharper details on the fingerprint. When the finger is placed over the scanner, it is incredibly dark. As a result, scanners integrate arrays of LEDs or your phone's display as a flash to illuminate the image when scanning. The process of scanning can be viewed in Figure 2.11. Too easy to be fooled is the major weakness of an optical scanner since it only captures a 2 Dimensions (2D) image for comparison. Any high-quality prosthetics or picture can easily fool the optical scanner, so this scanner is not safe enough to protect sensitive details. As a result, the industry has shifted toward more protected hybrid solutions (Triggs, 2022).

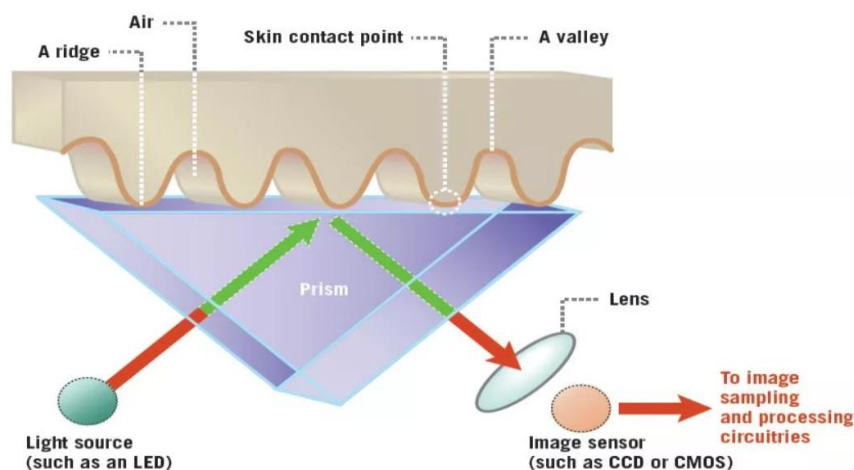


Figure 2.11: Scanning Procedure of Optical Sensor (Triggs, 2022)

Due to additional security advantages, capacitive scanners have become prominent on the market. By referring to the name of this scanner, we know that the main component will be a capacitor. The capacitive scanner uses a group of delicate capacitor circuits to collect fingerprint data. Since the characteristic of the capacitor

is storing electric charge, connecting them to a conductive plate to the surface of the scanner allows them to track the outfit of the fingerprint. When the finger's ridge is placed on the scanner, the store charge of a capacitor will be changed slightly, but the store charge remains unchanged if an air gap is detected. An op-amp integrator circuit tracks all the changes in electric charges, and then an ADC converter will record the signal. After finishing capture, the digital data is analysed to search for distinguishing and unique fingerprint aspects. They will then be saved for future comparison. The process of scanning has been shown in Figure 2.12. The capacitive scanner is more challenging to fool compared to an optical scanner. The simple image will not work on the capacitive scanner. Furthermore, prosthetic do not fool the scanner since different materials will cause different changes on the capacitor if compared to actual fingerprints. Software and hardware hacking will be a security risk for the capacitive scanner.

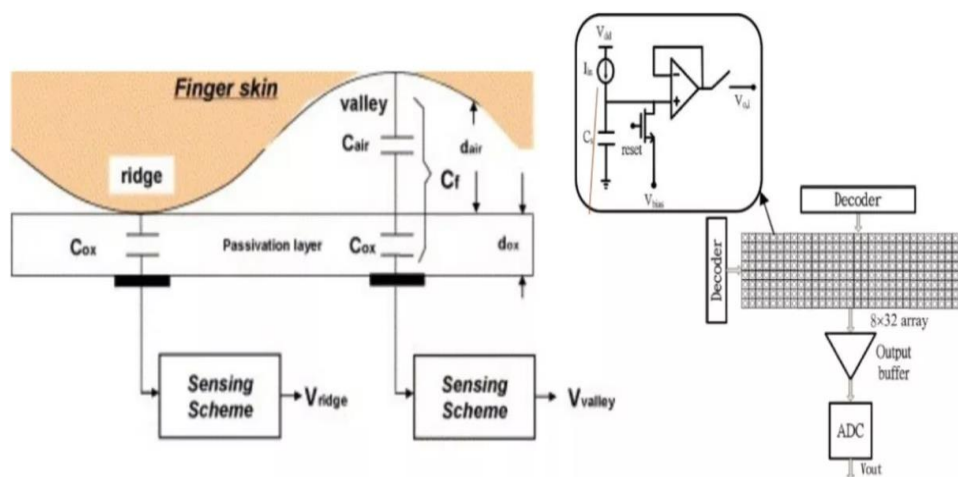


Figure 2.12: Scanning Procedure of Capacitive Sensor (Triggs, 2022)

The ultrasonic sensor was announced in 2016 and is implemented on the Le Max Pro smartphone. By referring to the ultrasonic sensor shown in Figure 2.13, the scanner consists of an ultrasonic transmitter and receiver. The ultrasonic pulse will be transmitted against the finger when it is placed on the scanner. Some pulse is absorbed, while others bounce back to the ultrasonic receiver. The reflection of the pulse depends on pores, ridges and other details unique to every fingerprint. There is no microphone listening out on the bounce-back signal. Alternatively, a sensor will be used to detect mechanical press to calculate the intensity of returning the bounce-

back pulse at different scanner points. Scanning for a more extended period allows for the collection of more in-depth data. This produces a detailed 3 Dimensions (3D) replica of the scanned fingerprint. Due to its 3D nature, the capture technology is a more secure alternative to capacitive scanners. The ultrasonic scanner is not that snappy compared to other scanners. Furthermore, the scanner does not function well with some screen protectors, significantly thicker ones. The ability of the ultrasonic scanner will decrease due to all these factors, which causes the scanner not to recognize the fingerprint correctly. The following subsection will discuss radiofrequency identification technology.

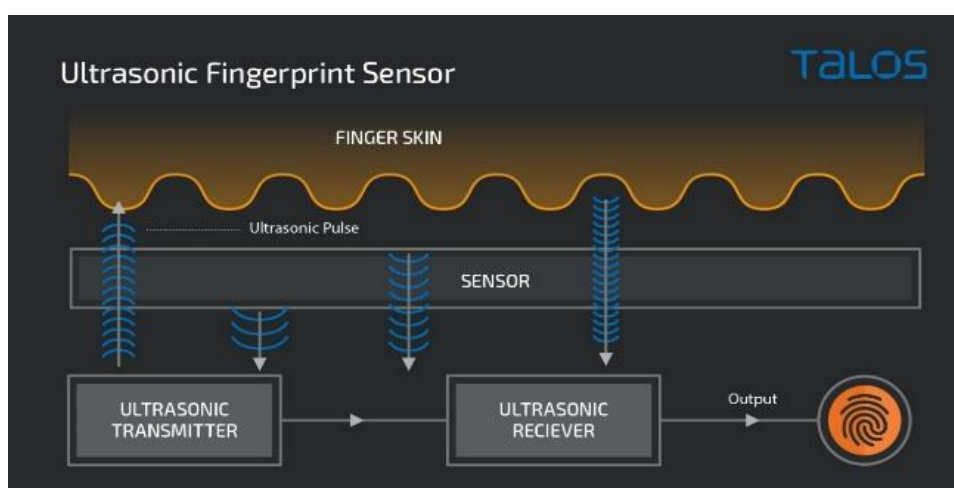


Figure 2.13: Scanning Procedures of Ultrasonic Sensor (Rascagneres, 2020)

2.7 Introduction to RFID

RFID is classified as a communication technology that utilizes radio frequency to search specific targets and read or write related data. Identification of mechanical or optical contact is not required for the system. The RFID technology can perform fast reading, writing, recognition (non-visual, mobile, multi-targets), locating, and tracking management. The RFID system's recognition process is not affected by the poor environment. The RFID technology can perform fast reading and secure scanning and is reliable. As a result, RFID technology offers a wide range of application possibilities.

Furthermore, RFID is also considered as an automatic contactless identification technology. The RFID technology can identify targeted objects automatically and get essential data via radio frequency. The devices contained inside the RFID system are interrogators and transponders. The antenna will perform wireless communication between the transponder and the interrogator. The RFID system consists of four primary devices: reader, tags/cards, software, and antenna. The figure below shows the RFID system's primary commutation path for four significant devices (kynix, 2018).

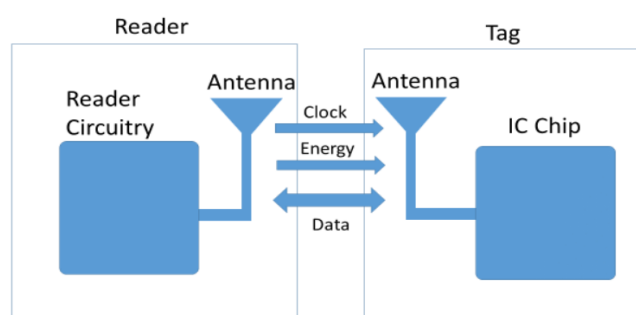


Figure 2.14: Block Diagram of RFID System with Four Major Devices (kynix, 2018)

2.7.1 Working Principle for RFID System

By referring to the picture shown in Figure 2.15, the reader will send energy out at a specific frequency. This energy is used to drive the transponder in order to get the internal data for it. At the same time, the reader can collect the data and interpret it. After interpretation, the data will be sent to specific applications for further processing. Usually, a half-duplex communication mode is implemented to exchange information between the reader and the transponder. The reader will provide timing, energy, and other relevant data through coupling to the transponder. The transponders are the primary information carrier for RFID systems, most of them made by coupling components like coils and antennae. The reader can control and process the information according to the structure and technology of RFID system information. It comprises a transceiver module, a combining module, an interface unit, and a control circuit.

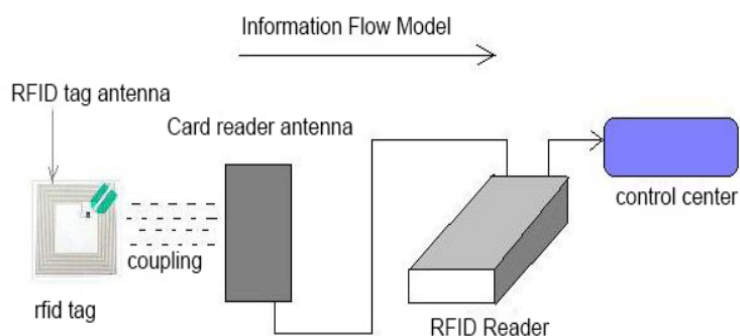


Figure 2.15: Working Schematic of RFID System (kynix, 2018)

2.7.2 Operating Frequency for RFID System

Low operating frequencies range from 30kHz to 300kHz. The RFID systems with Low Frequency (LF) will mainly operate at 125kHz, but some low-frequency RFID systems will also operate at 134kHz. Under the low-frequency system, a short range of 10cm and a low reading speed are provided. However, the sensitivity of the LF RFID system towards radio wave interference will be much lower compared to a high-frequency RFID system (IMPINJ, n.d.). Aside from some metal-related effects, the overall low system can penetrate most of the material without narrowing its maximum possible reading range. There is no licensing restriction for RFID readers, which operate under low operating frequency.

High operating frequency ranges from 3MHz to 30MHz. Generally, the RFID with High Frequency (HF) will operate at 13.56MHz. The high-frequency system has a read range of up to 1m. The sensitivity of the HF RFID system is higher than the low-frequency RFID system. Wavelengths under high frequency can transmit over most materials, but it shortens the reading distance. Sensors typically require a distance from the metal. The HF RFID system has better anti-collision properties and can scan multiple tags simultaneously (kynix, 2018).

Ultra High Frequency (UHF) bands enclose the range from 300MHz to 3GHz, and its reading range is up to 12m. The RFID system with ultra-high frequency can

transfer data faster than LF and HF RFID systems, but it has the highest sensitivity to radio wave interference. Many application materials, particularly water, dust, and other substances, will block radio waves in the ultra-high frequency band from passing through. However, the manufacturer has found a solution for the RFID system to keep performing well even in terrible environments. The UHF RFID system has the highest transmission rate and can scan many electronic tags.

2.8 Summary

In this chapter, a literature review has been done for the devices, products, design ideas and theories. There are a total of three student projects, and two commercial projects that have been reviewed. The first student project is done by Prajwal, and his project implements single-factor authentication. The user is required to provide one type of credential for access. Aqib does the second student project, and his project implements double-factor authentication. The user must provide two correct credentials in order to access the lock. Shuhada Natasha Bint Mohd Zainor does the third student project, and her project also implements double-factor authentication. Two credentials must be provided to the system for access purposes. The fourth and fifth project belongs to the commercial projects, by Vanma and MAG company. The access control system from Vanma company includes three main elements: smart lock, electronic key, and management software. Three of them work dependently in order to build an access control system. The touchless access system from MAG company requires the user's face for access, allowing the user to free their hand.

Three different microcontroller boards from Arduino, Raspberry Pi, and the Espressif system company are reviewed in this chapter. The specification, difficulty of usage, pricing, and software needed are also discussed within this chapter. Arduino board has low difficulty for any beginner, and the integrated development environment is compatible with many operating systems. Raspbian OS is the official operating system to be installed for the Raspberry Pi board, and it requires at least an external 8GB SD card to store it on the board. The Espressif system board includes the Esp8266 board and Esp32 board. Both of them are considered system on chip

boards. Two IoT application platforms have been discussed in the chapter: the Arduino IoT platform and the Blynk platform. The Arduino IoT platform is built by Arduino company, which also supports connecting to third-party microcontroller boards. Blynk has supported more than ten types of microcontrollers and four types of internet connections.

The biometric technology covered in this chapter is fingerprint recognition. This technology is used to differentiate fingerprint scans on the scanner. Five critical aspects need to be considered for the suitability of fingerprint recognition: universality, uniqueness, performance, acceptability, and collectability. RFID is the wireless communication technology used to detect, read or write data. Two fundamental devices for the RFID system are the interrogator and transponder. Both of them communicate wirelessly by using an antenna. The operating frequency for RFID systems can be classified into three groups, which are LF, HF, and UHF. The next chapter will discuss the methodology for building the smart door access system. The selection of hardware and software will be included in the next chapter. Furthermore, the design process and design idea will also be discussed in Chapter 3.

CHAPTER 3

METHODOLOGY

3.1 Introduction

This chapter discusses the system design idea. The operation flow of the whole system is also discussed in this chapter to provide a clear picture of the system. This chapter also includes the selection of the necessary hardware and software. The hardware includes a microcontroller, sensors, components, and modules, while the software includes an IDE and mobile application. Furthermore, the Gantt chart at the end of this chapter shows the progress of the whole project.

3.2 System Block Diagram

Figure 3.1 shows the Arduino Mega as the central control unit for the whole system. The keypad, RFID scanner, mobile application, and switch are the inputs to trigger the system for access purposes. One magnetic switch sensor is used to guide the door of the system. The output devices like solenoid lock, mobile notification, LED, buzzer, and Esp32 camera provide a visual or auditory signal for users. The following subsection will discuss the operating flow of the system.

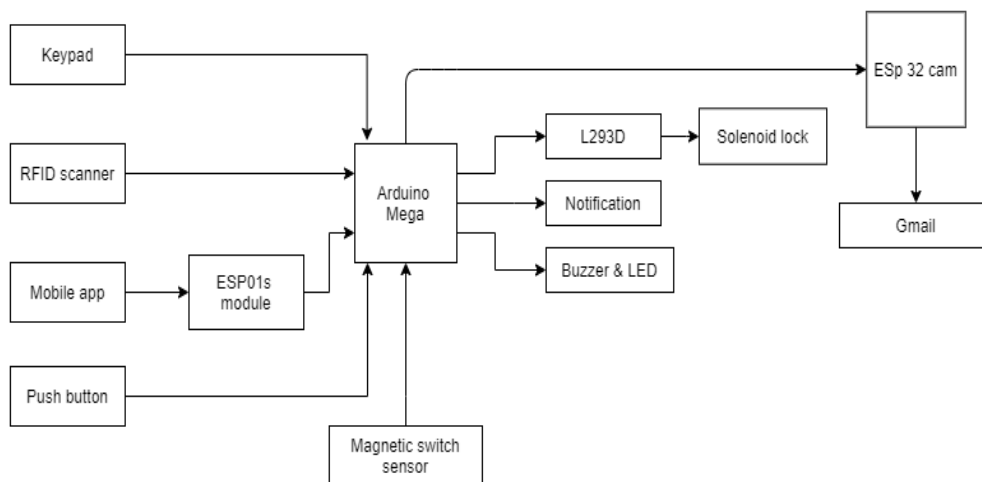


Figure 3.1: Block Diagram of Whole System

3.3 System Flowchart

Figure 3.2 shows that the smart door access system has three different ways of accessing: pressing an internal switch, pressing the Blynk mobile application and scanning the RFID card. The system has implemented double-factor authentication, so any user who used the RFID card would need to provide a set of passwords after scanning with the correct RFID card. When the card Identity Document (ID) and password match the credential list of the system, the solenoid lock unlocks for three seconds and allows the user to enter. The magnetic sensor is activated and starts counting as long as the lock is unlocked. The user will receive a mobile notification if the door does not close appropriately after five seconds. The red LED and buzzer are also turned on if the door is not closed correctly after five seconds. When the door is closed properly, it will stop the warning signal and stop sending notifications to mobile phones.

The system can detect and differentiate credentials from the user. There is a limit set within this system for providing wrong credentials. Every user has two chances when providing the wrong card ID or password to the system. The system will only show a warning signal, like turning on a buzzer and a red LED for the first wrong scan. If the user still provides the wrong card ID for the second round, the

warning signal is shown, and a mobile notification will be received by the user registered under this system. Not only that, the Esp32 camera is activated to capture the user's photo and the image is sent to a registered email under this system. The image acts as evidence if there is any crime happening in the surrounding system. The detection process is the same for any user who has provided the wrong password. The system will show a warning signal, send a mobile notification, and activate the Esp32 camera to capture an image as long as the user provides the wrong password two times continuously.

The second way to access the system is by pressing the unlock icon in the Blynk mobile application. The users do not need to provide any single credential before pressing the icon, but it only allows the users registered under this smart door access system to use it. A limiting switch works as the internal switch for the system. It is placed within buildings or houses. The internal switch can access the system after pressing it without providing any credentials. Usually, the internal switch is used to exit from the building or house.

An intruder feature is implemented in the system. The magnetic sensor switch is the main sensor for this feature. When the magnet detaches from the sensor without providing credentials, the system detects that an intruder has broken the door. Thus, the buzzer is turned on, and the registered user will receive a mobile notification every second. Furthermore, the halt feature has also been implemented in the system. The registered user can halt the smart door access system by pressing the halt icon from the Blynk application. The system is temporarily terminated and does not accept any credentials, whether correct or wrong. There is a terminating period for the halt function for the system, and it returns to normal after the terminating period is over. Figure 3.3 has classified all the functions and features for the system flow chart. The following subsection will discuss a selection of the microcontroller and language for the system.

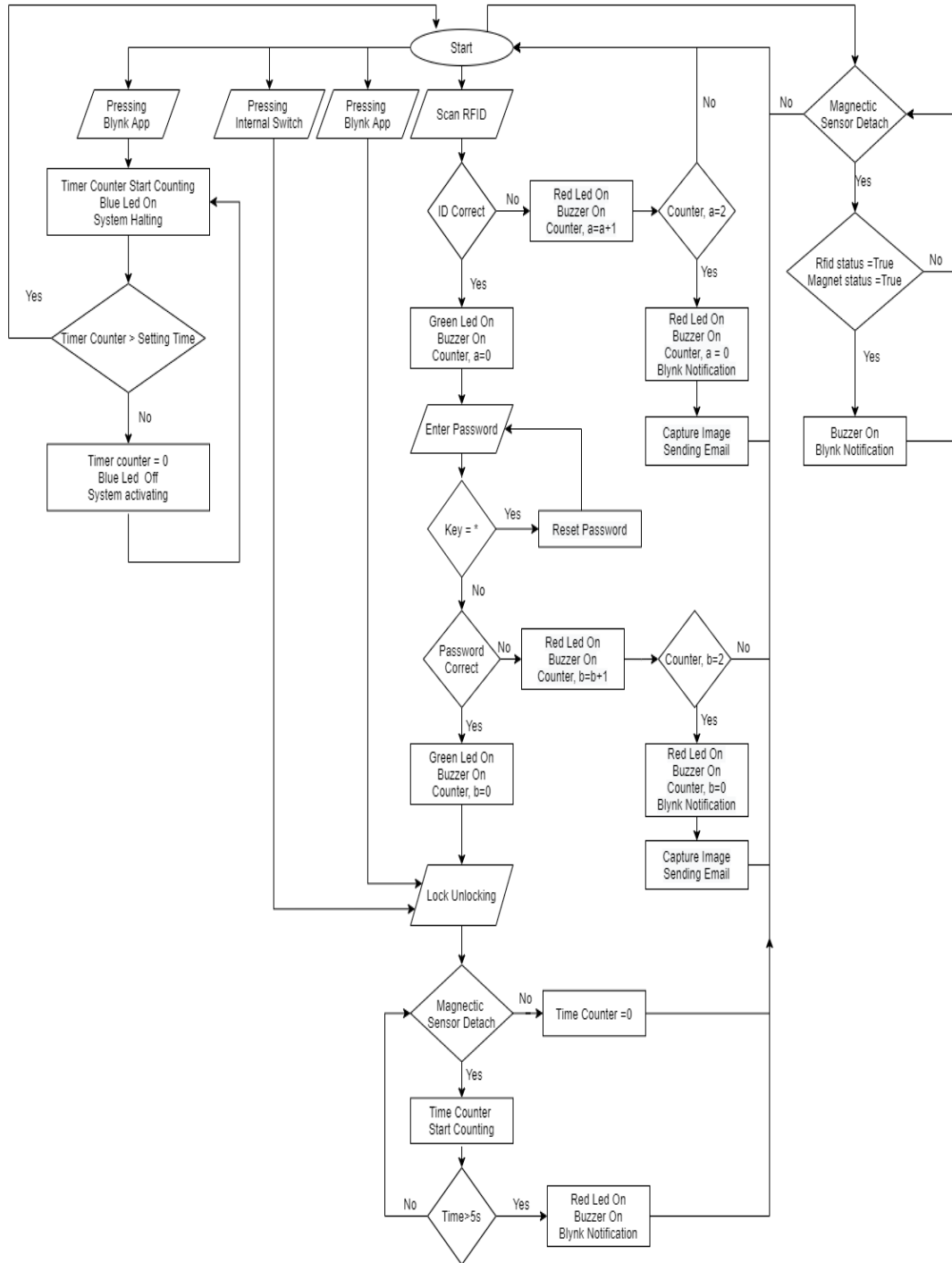


Figure 3.2: Flow Chart of Whole System

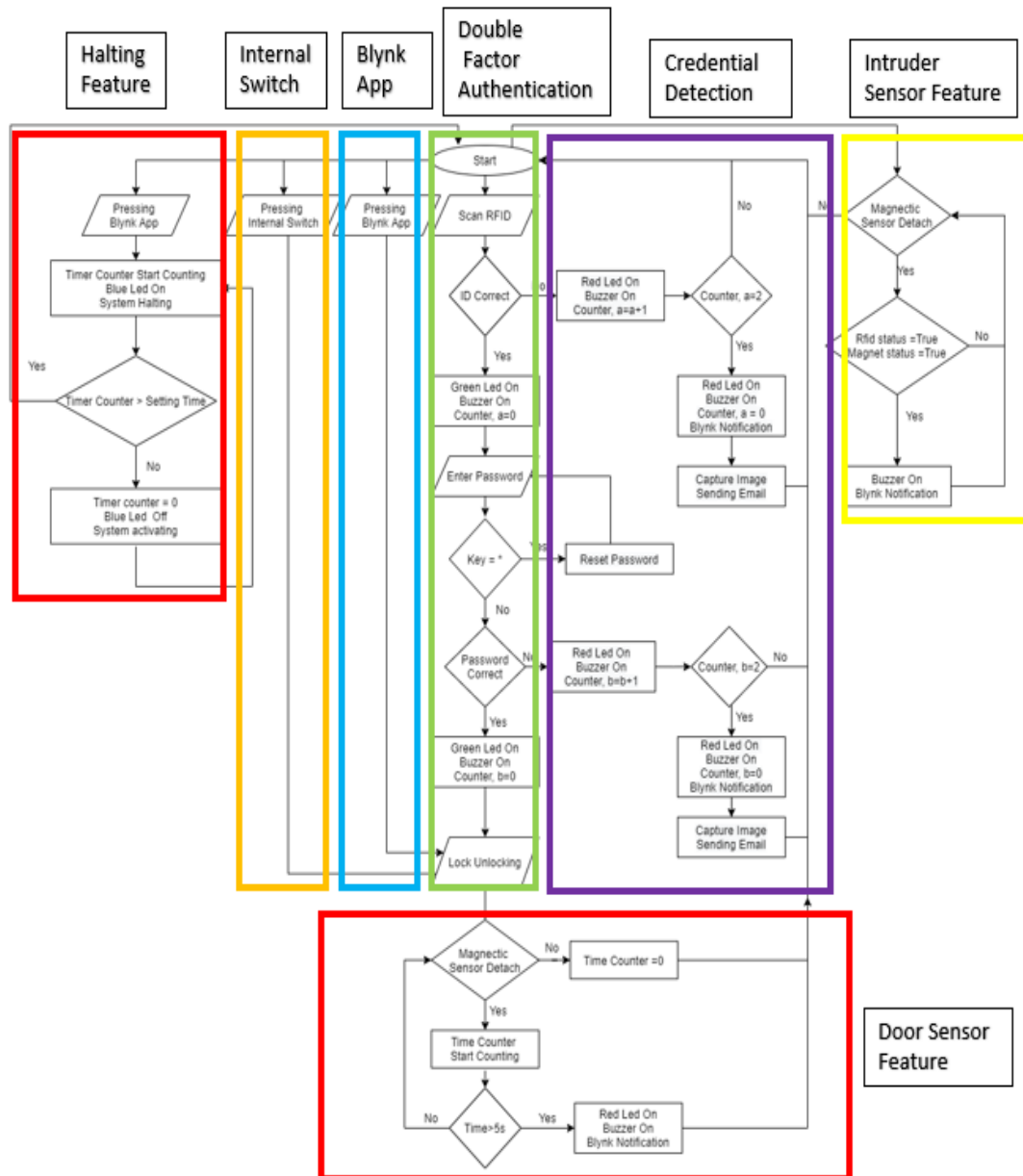


Figure 3.3: Classification of Flow Chart of Whole System

3.4 Microcontroller and Language Selection

The microcontroller is used as the central control unit for the system and the language is used to program the whole system.

3.4.1 Microcontroller

The Arduino microcontroller board is selected as the central control unit for this smart door access system due to four main reasons, robustness, pricing, power consumption, and powerfulness. There is a high possibility of damaging some microcontroller board if it is not shut down properly due to OS. So, the Arduino board will not get damaged if it shuts down suddenly since it does not require an OS. Besides, the Arduino board is a low-budget microcontroller, and the price will be at most RM100 for the basic board. Power consumption for Arduino boards among the three of them (Raspberry, Arduino, Espressif system) is considered much lower. The minimum power consumption requires 250mA++. Even though Arduino boards only have a single core, it would be sufficient to handle an advanced task like designing an access control system.

Arduino Uno is the most popular board from Arduino company, and it is made with Atmega328P chips from Atmel company. There are 20 I/O pins on the board, including 14 digital pins (6 pins are able to produce a PWM signal) and six analogue input pins, which contain a 16MHz ceramic resonator and support direct USB connection (Arduino store, 2022). However, Uno's total pins are not sufficient for this project. Thus, Arduino Mega2560 is chosen as a replacement for the UNO. It is a microcontroller based on Atmega2560 chips from Atmel company, and most of the functionality is similar to UNO. Nevertheless, the I/O pins are several times more than UNO. 70 I/O pins can be used, including 54 digital pins (15 pins are able to produce a PWM signal) and 16 analogue input pins. Both boards support similar serial communication protocols like UART, SPI, and I2C, but Mega2560 has more UART ports than UNO. A more detailed comparison of Mega2560 and UNO has been shown in the table below.

Table 3.1: The Technical Specifications for UNO and Mega 2560

Board		UNO R3	Mega 2560
Processor	Main Processor	Atmega 328P	Atmega2560
	Serial to USB Converter	ATmega16U2, CH340G	ATmega16U2, CH340G
	Clock Speed	16M Hz	16M Hz
Power	Input Voltage(V)	7-12	7-12
	I/O Voltage per Pin(V)	5	5
	I/O Current per Pin(mA)	20	20
	Source Connector	Standard A/B	Standard A/B
	Output Voltage(V)	3.3 or 5	3.3 or 5
Memory	SRAM	2KB	8KB
	FLASH	32KB	256KB
	EEPROM	1KB	4KB
I/O pin	Digital	14	54
	Analog	6	16
	PWM	6	15
	Built in LED	13	13
Communication	SPI	1	1
	I2C	1	1
	UART	1	4
	CAN	-	-
Dimension	Weight	25g	37g
	Size (Width x Length)	53x69 mm ²	53x 102 mm ²
Shield Compatibility		Yes	Yes
Wireless	Ethernet	-	-
	WiFi	-	-
	Bluetooth	-	-
	GSM	-	-

3.4.2 Language

The programming language used for Arduino Mega 2560 is C language. Dennis M. Ritchie created it at Bell Laboratories to assist the OS Uniplexed Information Computing System (UNIX). In 1972, C was used for the first time on the DEC PDP-11 PC (Vatsal, 2021). Besides, C language is a general-purpose language, middle-level language (supports low and high functionalities), and procedural language (instructions get executed step by step) (Programiz, n.d.). The C code is almost as fast as assembly language code, which was implemented as a system development language. Some examples of C language use are UNIX OS, test editors, language compilers, networks driver, and print spoolers.

Arduino IDE supports many languages, while C language is one of the languages compatible with IDE. The C language is highly portable because it is based on ASCII characters and functions well on different platforms, including Mac OS X, Windows, Android, and iOS. As a result, the C program can be run anywhere. In addition, C language executes quicker than other programming languages such as Java, Ruby, and PHP because it uses the least instructions. Lastly, C languages have high compilation speed, and the C compiler generates the machine code quickly. A thousand lines of codes can be assembled in a matter of seconds. The C Compiler enhances the code for faster execution. The following subsection will discuss about hardware and mobile application of internet of things for the system.

3.5 IoT Application

The smart door access system would implement the IoT. An internet connection module and IoT platform will be used within this system.

3.5.1 Esp01s Module

The Arduino Mega is selected as the central control unit for this system, but it cannot connect to any internet like WiFi or mobile hotspot. Thus, the Esp01s module is selected as the WiFi module for Arduino Mega for internet connection. The Esp01s is one of the microcontroller boards under Esp8266. It is a system on chip board with the integration of a Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack. So, the Esp01s allow any microcontroller to access the internet connection. Most Esp01s modules have come with ATtention (AT) command firmware, allowing users to hook up easily with an Arduino board and conveniently connect to WiFi.

The Esp01s modules are connected to Arduino Mega, and both communicate via UART communication. A modules adapter is added to the Esp01s module to make the connection easy. The adapter can reduce wire connections and provide constant voltage and current to the Esp01s modules. The Esp01s module shown in Figure 3.4 is stacked on top of the adaptor, and then the output pin of the adaptor will be connected to the serial port of Arduino Mega.



Figure 3.4: Connection Between Esp01s Module and Module Adaptor

Since the serial port 0 of Arduino Mega will be busy when the serial monitor is open in the Arduino IDE, so serial port 1 is selected as the communication port between Arduino Mega and Esp01s module. The pin connection between both of them is shown in Table 3.2.

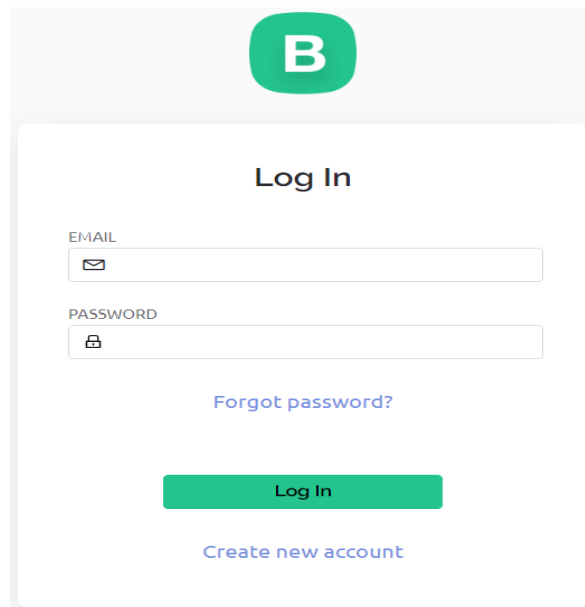
Table 3.2: Pin Connection Between Esp01s Modules Adaptor and Arduino Mega

Esp01s Modules Adaptor	Arduino Mega
Pin Name	Pin Name
Vcc	5V
Gnd	Gnd
Tx	Rx1(pin 19)
Rx	Tx1(pin 18)

3.5.2 Blynk Application

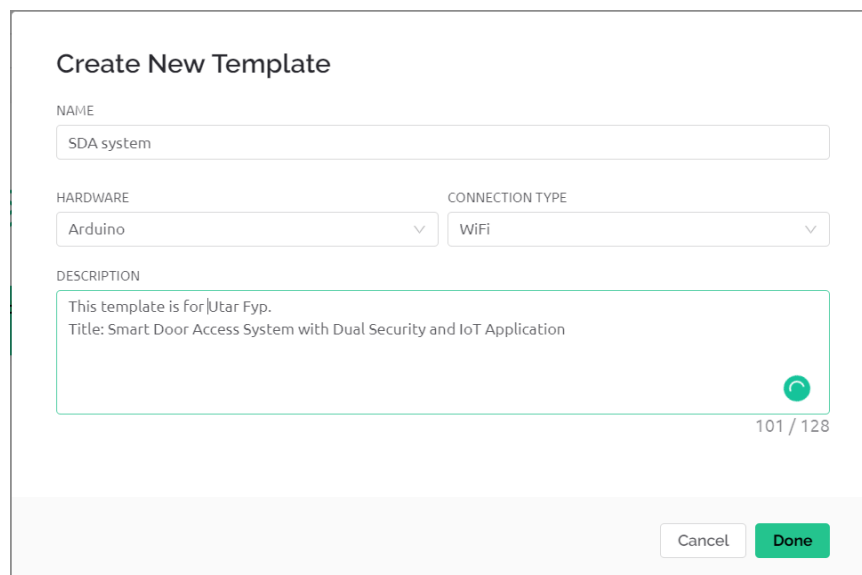
Blynk is selected as the IoT application for the smart door access system. It is an IoT platform that controls microcontroller boards like Arduino boards, Espressif system boards or Raspberry Pi boards through iOS or Android smartphones. The Blynk platform is chosen due to its pricing and powerful function. The Blynk platform has come out with some advanced plans for users, but it also provides free plans. Under the free plan, users can create their user interface with up to 10 widgets and control two devices within one account. A mobile notification function and multiple user functions have also been provided in the free plan.

Before using the Blynk platform, an account must be signed up at Blynk's official websites, as shown in Figure 3.5. Then, the user is allowed to create a template, as shown in Figure 3.6. The user must provide a template name before generating a template. Since this project uses Arduino Mega as the central control unit, the hardware selection from the template must be Arduino board, and the connection type should be WiFi. Furthermore, the user can choose whether to write a description or not.



The image shows the Blynk login page. At the top center is a green circular logo with a white letter 'B'. Below the logo is the heading 'Log In'. There are two input fields: 'EMAIL' with an envelope icon and 'PASSWORD' with a lock icon. Below the password field is a blue link 'Forgot password?'. At the bottom, there is a green 'Log In' button and a blue link 'Create new account'.

Figure 3.5: Log In Page or Sign Up Page for Blynk Account



The image shows the 'Create New Template' interface. It has a title 'Create New Template'. Below it is a 'NAME' field with the text 'SDA system'. There are two dropdown menus: 'HARDWARE' set to 'Arduino' and 'CONNECTION TYPE' set to 'WiFi'. Below these is a 'DESCRIPTION' field with the text 'This template is for Utar Fyp. Title: Smart Door Access System with Dual Security and IoT Application'. A character count '101 / 128' is shown at the bottom right of the description field. At the bottom of the form are 'Cancel' and 'Done' buttons.

Figure 3.6: Interface of Creating a New Template in Blynk Website

After that, users can create their desired user interface using a widget from the widget box. There are two user interfaces in the Blynk platform: the web dashboard and the mobile dashboard. The web dashboard can be designed using the Blynk website but will not be synchronous with a mobile dashboard. Thus, users need to create their mobile dashboard again by using the Blynk mobile app. The Blynk mobile can be downloaded at Google Playstore or Apple Store. Figure 3.7

shows that a button has been placed in the web dashboard and will function as one of the input credentials for the smart door access system. Furthermore, the button must link to a datastream before it starts working.

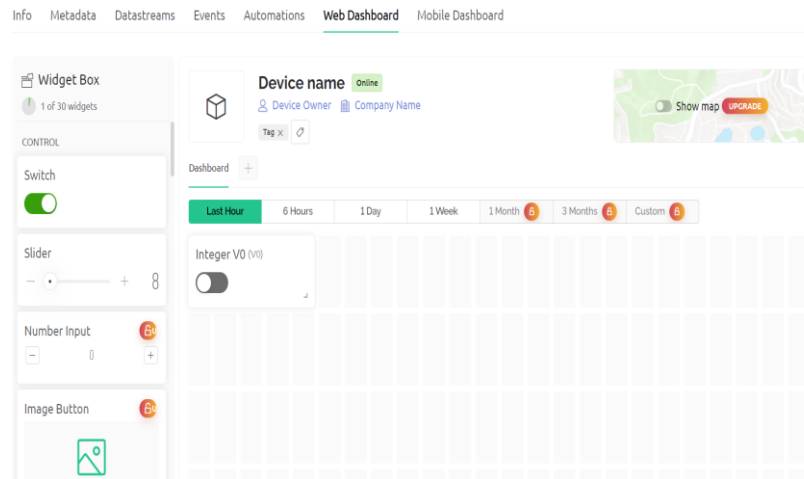


Figure 3.7: A Switch Used to Create an User Interface at Blynk Web Dashboard

Five different datastreams are available in the Blynk platform: digital, analogue, virtual pin, enumerable and location. From Figure 3.8, the virtual pin datastream is selected for the button in the web dashboard. The integer data type is selected, and no units are provided for the virtual pin datastream because the button in the web dashboard acts as the input signal to access the system. This virtual pin is named Integer V0 and will provide maximum output at one.

 The image shows the 'Virtual Pin Datastream' configuration form. It includes the following fields:

- NAME:** Integer V0
- ALIAS:** Integer V0
- PIN:** V0
- DATA TYPE:** Integer
- UNITS:** None
- MIN:** 0
- MAX:** 1
- DEFAULT VALUE:** Default Value

 There is an 'ADVANCED SETTINGS' section that is currently collapsed. At the bottom right, there are 'Cancel' and 'Save' buttons.

Figure 3.8: Interface of Creating New Virtual Pin Datastream in Blynk Website

As mentioned in this paragraph, the Blynk platform supports a notification function. In order to let users receive the notification on their smartphone or tablet, events need to be created. The event shown in Figure 3.9 is named a keypad, and the event code is key. The event code must not be repeated because it will be used in the coding to trigger each particular event. The event is selected as a warning type, and it is recorded into the timeline for every trigger. The user will receive notifications every second as long as one event has been triggered. The frequency of receiving notifications can be adjusted in the highlighted red box in Figure 3.9. The following subsection will discuss different types of credential input mechanisms for the system.

Figure 3.9: Interface of Creating New Event in Blynk Website

3.6 Credential Input Mechanism

The smart door access system supports multiple access for the user who wants to enter the building and single access for the user who wants to exit the building.

3.6.1 Double Factor Authentication

RC522 scanner and 4x4 matrix keypad work together to provide double-factor authentication input for the system. A valid card needs to be scanned on the scanner, before being allowed to key in the password through the matrix keypad. The RC522 scanner is classified under the HF RFID module. The reason for choosing RC522 is that it has a wider reading range, and the scanner can support reading and writing capabilities. Besides, the RC522 scanner has a 5V pin tolerance, which means the pin can accept a 5V input signal without extra Integrated Circuit (IC) to step down to 3.3V. The 5V pin tolerant is very useful for connecting Arduino boards since most of the digital pins from Arduino Mega will generate a voltage of up to 5V.

The RC522 scanner shown in Figure 3.10 scans the Mifare card at the side. The scanner acts as an interrogator, while the card acts as the transponder. The transponder will be energized by the interrogator and sends out internal data. Then, it will be collected and sent to Arduino Mega for comparison. The RC522 scanner is directly connected to the Arduino Mega and communicates through Serial Peripheral Interface communication. All the pin connection between the scanner and Arduino Mega is shown in Table 3.3.



Figure 3.10: RFID Scanner with Model of RC522 at Left and Mifare Card at Right

Table 3.3: Pin Connection Between RC522 Scanner and Arduino Mega

RC522 Scanner	Arduino Mega
Pin Name	Pin Name
SDA	Pin 53
SCK	Pin 52
MOSI	Pin 51
MISO	Pin 50
IRQ	-
GND	Gnd
RST	Pin 2
3.3V	3.3V

The 4x4 matrix keypad is used to key in the password for the system. The reason for choosing this keypad is that it is durable and more compact. Figure 3.11 shows the comparison between the membrane keypad and the matrix keypad. Both have 16 different characters, but the dimension of the matrix keypad is smaller than the membrane keypad. Since the membrane is built only by a thin layer of plastic, it is not that durable compared to a matrix keypad.



Figure 3.11: Comparison Between 4x4 Matrix Keypad and 4x4 Membrane Keypad (Amazon, n.d.)

The internal connection of the matrix keypad is shown in Figure 3.12. Four columns and four rows are present in the 4x4 matrix keypad. The button that gets pressed will be determined by recognizing which column and row are connected. All

rows are connected to the input pin, and all columns are connected to the output pins. The input pins are set to high by enabling the internal pull-up resistor. The Arduino Mega will set the column pins low sequentially and check the status of all row pins. If the row pin is detected as low, the button for that row is pressed. After the button gets released, the Arduino Mega will check with the keymap array and search for the character corresponding to that button (Last Minute ENGINEERS, 2022). The connection between the keypad and Arduino Mega is much more straightforward. It can connect to any digital pin of the microcontroller board. Table 3.4 shows all the connections for both of them.

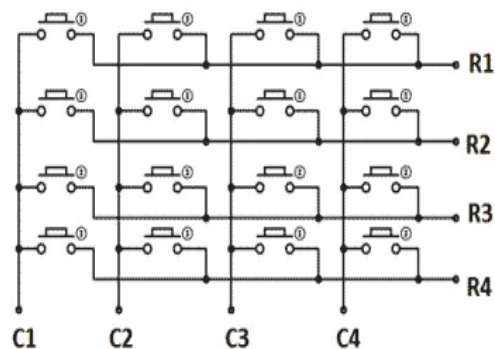


Figure 3.12: Internal Connection for 4x4 Matrix Keypad (Rathnayake, 2021)

Table 3.4: Pin Connection Between Matrix Keypad and Arduino Mega

4x4 Matrix Keypad	Arduino Mega
Pin Name	Pin Name
C1	Pin 33
C2	Pin 35
C3	Pin 37
C4	Pin 39
R1	Pin 41
R2	Pin 43
R3	Pin 45
R4	Pin 47

3.6.2 Mobile Application

The Blynk platform has launched a Blynk application on the Google Play store. After downloading the application, it would require an email to log in. The email is the same as the mail used to sign up for a Blynk account on the website. The Blynk application will contain a mobile dashboard and allow the design of any user interface using the widget. Figure 3.13 shows a button that makes the Blynk application user interface from the widget box. The button must link to a datastream to function, allowing it to choose an existing datastream or create one directly in the Blynk application. The button is chosen to link with the existing datastream created previously at the Blynk website, as shown in Figure 3.14.

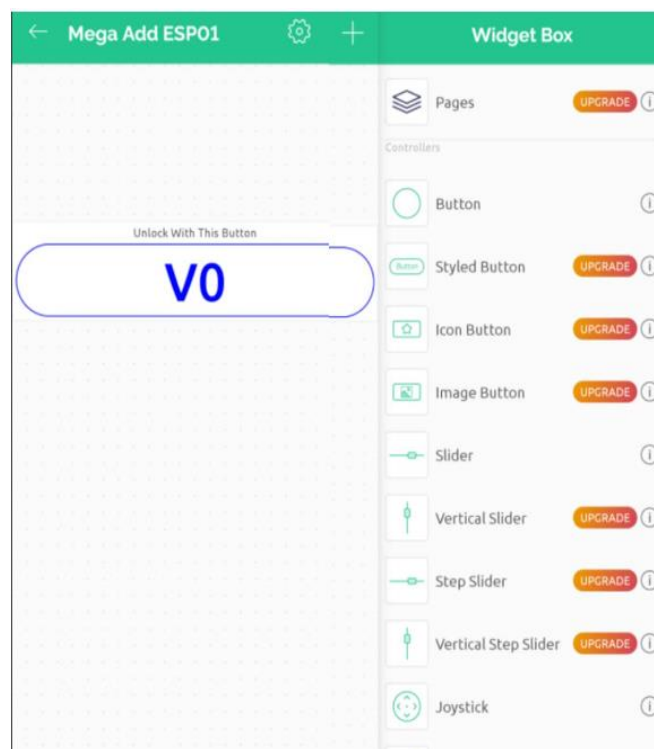


Figure 3.13: User Interface of Blynk Application for Smart Door Access System Created by Button from Widget Box

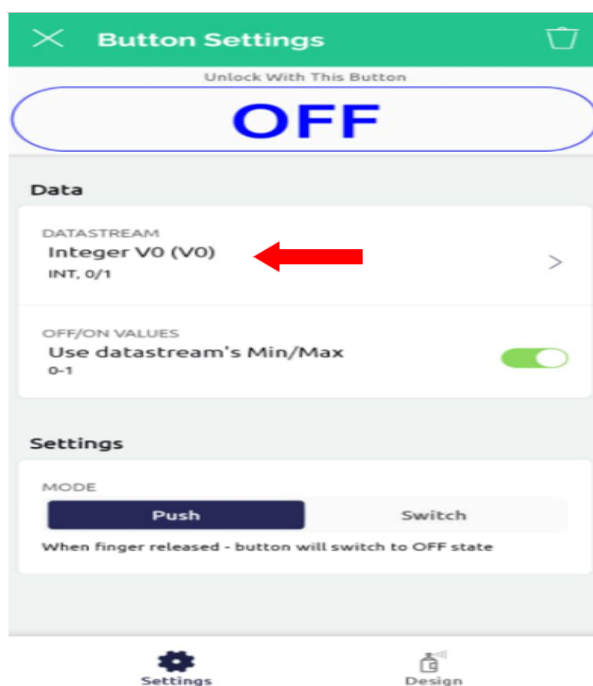


Figure 3.14: Datastream Integer V0 is Link to Button in Blynk Application for Smart Door Access System

3.6.3 Internal Button

The limit switch shown in Figure 3.15 is used as the internal switch for the smart door access system. It is placed in the building and unlocks the door after people press it. The pin with white wire is a Common (COM) terminal, the pin with black wire is Normally Closed (NC) terminal, and the pin with orange wire is Normally Open (NO) terminal. If the switch is pressed, the NO terminal and COM terminal link together, but the NC terminal will disconnect from the COM terminal. The NC and COM terminals will link together while the switch is not pressed. The NO terminal of the limit switch is connected directly to pin 25 of Arduino Mega, and the COM terminal will link to the ground. The following subsection will discuss the lock mechanism of the system.



Figure 3.15: Limit Switch with Common Terminal at Left, Normally Open Terminal at Middle and Normally Close Terminal at Right

3.7 Lock Mechanism

An electric lock is used as the output device for the smart door access system. It is controlled by L293D integrating circuit.

3.7.1 Solenoid Lock

The solenoid lock shown in Figure 3.16 is the output device for the system. It is formed by a big coil of copper wire and an armature placed in the middle. The reason for selecting this lock is due to simple wiring and the flexibility of changing the armature. The lock can be energized through two simple wires with a minimum of 11V. Besides, the direction of the armature can rotate by 90, 180 or 270 degrees after taking out the screws on top of the lock. This modification is very convenient to match with any door. The solenoid lock would need at least 0.6A and 11V for energized. When the voltage is applied to the lock, the armature gets pulled in for unlocking. The armature will return to normal when the voltage supply is removed.



Figure 3.16: Solenoid Lock with Two Philip-Head Screws on Top

3.7.2 Lock Driver

The IC in Figure 3.17 is an L293D dual channel H bridge motor driver chip. It can control two motors at the same time in any direction (Last Minute ENGINEERS, 2022). Even though it is stated as a motor driver, it can also be used to drive other devices like solenoid locks. This is because the IC can produce an output voltage of up to 36V and a current of up to 0.6A. Therefore, replacing a relay for controlling the solenoid lock is suitable.



Figure 3.17: H-Bridge Motor Driver with Eight Pins at Each Side (Proto Supplies, 2023)

The L293D chip contains two sets to control devices, as shown in Figure 3.18. Since only one solenoid lock is used for the system, one channel is enough to control the lock. Pin 1 must always be high in order to enable the left channel. Pin 8 is the supply voltage for output pins 3 and 6. The output voltage is determined by the amount of voltage supply at pin 8. There will be some voltage drop across the IC, so a minimum of 12V must be supplied on pin 8 because the solenoid lock requires at

least 11V. Pin 2 and 7 are the input pins for the left channel, as long as any of the pin gets high. The output pins 3 and 6 will produce a specific voltage. No voltage is produced at the output pin if both input pins get low or high. Pin 16 must always be connected to 5V to drive the internal logic circuit of L293D. All the pin connection of the L293D is listed in Table 3.5. The following subsection will discuss the door sensor for the system.

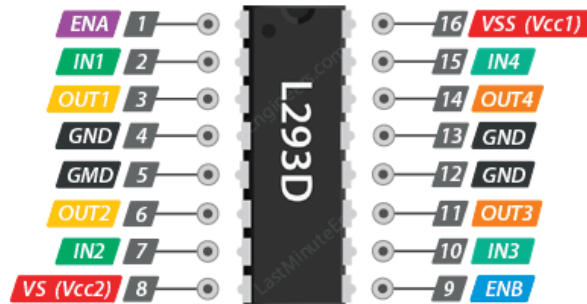


Figure 3.18: Pin Out of L293D H Bridge Motor Driver (Last Minute ENGINEERS, 2022)

Table 3.5: Connection Between L293D Chip, Arduino Mega, Power Supply, and Solenoid Lock

L293D	Arduino Mega	External Power Supply	Solenoid Lock
Pin Name	Pin Name	Pin Name	Pin Name
Pin 1, Ena	5V		
Pin 2, In1	Pin 31		
Pin 3, Out1			Red wire
Pin 4, Gnd	Gnd		
Pin 5, Gnd	Gnd		
Pin 6, Out2			Black wire
Pin 7, In2	Gnd		
Pin 8, Vcc2		13V	
Pin 9 to Pin 15	-	-	-
Pin 16, Vcc1	5V		

3.8 Door Sensor

The magnetic contact switch is being used in the smart door access system. The switch contains two parts, a wire sensor and a magnet. The magnet is used to trigger the internal circuit within the wire sensor. The wire sensor will form a complete circuit if the magnet is close to it, but the circuit will break if the magnet is far away. Figure 3.19 shows how the magnet affects the internal circuit of the wire sensor.

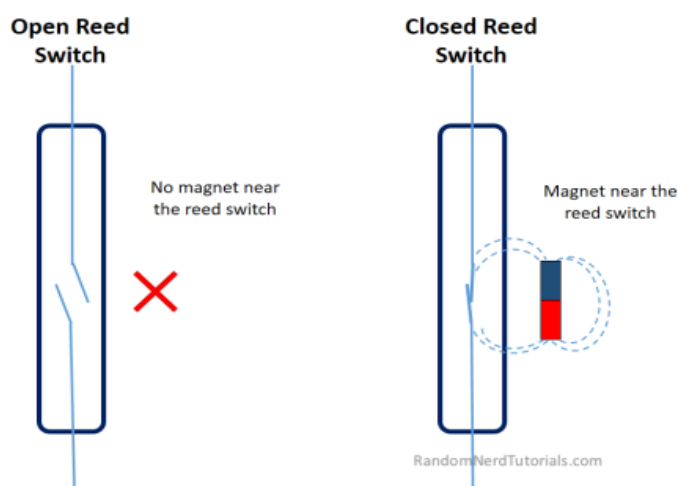


Figure 3.19: Working Mechanism of Magnetic Sensor Switch (RANDOM NERD TUTORIALS, 2019)

The wire sensor has two wires; one is connected to pin 30 of the Arduino Mega, while another is connected to the ground. Pin 30 is set to high internally in Arduino Mega. If the magnet is far from the sensor, pin 30 will go high, indicating the door is not closed correctly. If the magnet is near the sensor, pin 30 shorts to the ground, indicating the door is closed correctly. The magnetic sensor is placed side by side on the door model shown in Figure 3.20. If the door is open, the magnet will break the internal circuit of the sensor and cause pin 30 to go high. Then, the Arduino Mega will detect that the door is not closed correctly. The following subsection will discuss the image capture mechanism for the system.

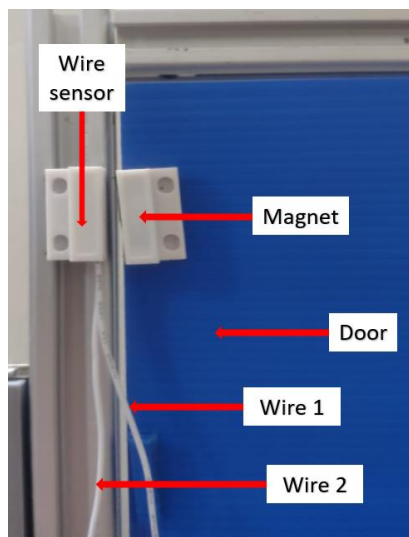


Figure 3.20: Magnetic Switch Sensor on Door Model

3.9 Image Capturing Mechanism

Esp32 cam works as the camera of the smart door access system. It is a compact size and low energy consumption camera module. The Esp32 cam has a wide application for image upload, or video monitoring (RANDOM NERD TUTORIALS, 2020). Figure 3.21 shows that the Esp32 cam contains three parts: the OV2640 camera, development board and programmer unit. The camera needs to install on the connector of the development board in order to capture an image. Before programming the Esp32 cam development board, the programmer unit must stack at the back of the development board and upload code via micro USB from the programmer unit, as shown in Figure 3.22.

The reason for choosing Esp32 cam as the camera module is because it has a built-in WiFi module. The Esp32 cam can capture and send images online without adding an extra WiFi module. Besides, the size of the Esp32 cam is compact. The dimension of the camera module is 2.7cm x 4.05cm x 0.45cm. Thus, it is not bulky and only occupies a little space. The Esp32 cam is flexible on the programming software. The main microcontroller chips for the Esp32 cam are built by the Espressif system company, but the Esp32 cam can also support program software from other companies. The IDE from Arduino company can reprogramme the Esp32

cam after installing the Esp32 board library. Since the central control unit for the system is Arduino Mega, Arduino IDE is the main program software for the whole system. Therefore, choosing Esp32 cam as the camera module for the smart door access system helps to reduce the complexity of the program because it unites the IDE for two different microcontrollers.



Figure 3.21: Main Parts of Esp32 Cam Module OV2640 Camera at Left, Development Board at Middle, and Programme Unit at Right

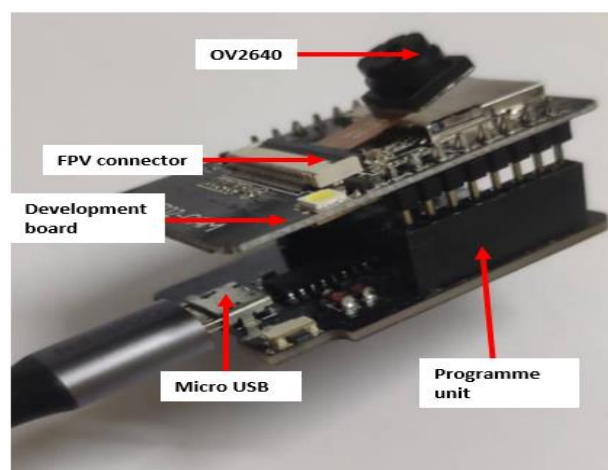


Figure 3.22: Full Connection of Esp32 Cam Module for Programming

The Esp32 cam is activated and captures an image after pin 12 of the development board is triggered by Arduino Mega. The digital pin 28 of Arduino Mega will provide a high signal to pin 12, and then the Esp32 cam will start to capture the image. After done with the capturing action, the image is sent to the

receiver's email and stored as evidence. The connection between the Esp32 cam and Arduino Mega is shown in the table below. The following subsection will discuss all pin allocations for the system.

Table 3.6: Connection Between Esp32 Cam Module and Arduino Mega 2560

Esp32 Cam	Arduino Mega
Pin Name	Pin Name
5V	5V
Gnd	Gnd
Pin 12	Pin 25

3.10 Pin Allocation of Arduino Mega 2560

The Arduino Mega 2560 shown in Figure 3.23 has 70 I/O pins that can be programmed. All used I/O pins are listed in Table 3.7, while the pins not listed in the table below indicate it is not linked to any devices or components. Among all the usage pins, some function as input pins to receive a signal from devices, while others work as output pins to generate a signal to devices. The following subsection will discuss the printed circuit board of the system.



Figure 3.23: Pinout of Arduino Mega 2560 (The Engineering Knowledge, 2023)

Table 3.7: Pin Connection Between Arduino Mega2560 and Other Devices or Components

Pin	Connection	Status	Type
4	Anode of RGB LED (Blue)	Output	Digital
5	Anode of buzzer	Output	
6	Anode of RGB LED (Red)	Output	
7	Anode of RGB LED (Green)	Output	
18	Rx pin of Esp01s adaptor	Output	UART
19	Tx pin of Esp01s adaptor	Output	
23	Wire of magnetic switch sensor	Input	Digital
25	NO pin of limiting switch	Input	Digital
28	Pin 12 of Esp32 cam module	Output	Digital
33	Pin 1 of matrix keypad	Input	Digital
35	Pin 2 of matrix keypad	Input	
37	Pin 3 of matrix keypad	Input	
39	Pin 4 of matrix keypad	Input	
41	Pin 5 of matrix keypad	Input	
43	Pin 6 of matrix keypad	Input	
45	Pin 7 of matrix keypad	Input	
47	Pin 8 of matrix keypad	Input	
49	Pin 7 of RFID scanner	Input	Digital
50	Pin 4 of RFID scanner	Input	SPI
51	Pin 3 of RFID scanner	Input	
52	Pin 2 of RFID scanner	Input	
53	Pin 1 of RFID scanner	Input	
Gnd	Pin 6 of RFID scanner	Output	Power supply
3.3V	Pin 8 of RFID scanner	Output	
Gnd	Gnd pin of Esp01s adaptor	Output	Power supply
5V	5V pin of Esp01s adaptor	Output	
Gnd	Gnd pin of Esp32 cam module	Output	Power supply
5V	5V pin of Esp32 cam module	Output	

3.11 Printed Circuit Board

The Printed Circuit Board (PCB) of the smart door access system has been designed and printed at the PCB lab of UTAR. There are two printed circuit boards; one is used for the central control unit, and another is for the lock driver circuit. The following subsection will discuss the 3D modelling of the project for the system.

3.12 3D Design

TinkerCad is an online 3D modelling software used to design the external casing for the system. 3D objects can be designed in this software and generate Standard Triangle Language (STL) files for the slicer tool. The external casing shown in Figure 3.24 is designed in the TinkerCad and generates an STL file for slicing. The STL file is imported into a slicer software called Ultimaker Cura in order to generate G-code before starting printing. A slicer is a software that converts a 3D model into a 3D printing instruction for any 3D printer. Some helpful details can be found in the slicer software: the size of the printing object, time usage for printing, and filament usage. Figure 3.25 shows that the 3D object in Figure 3.24 requires 7 hours and 39 minutes for printing. The filament usage for the 3D model is 48 grams with a length of 16 meters.

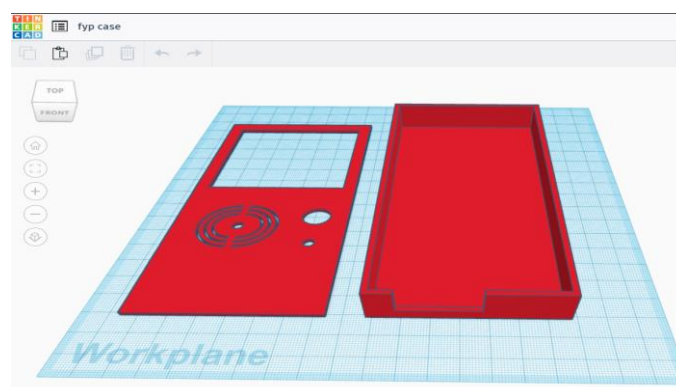


Figure 3.24: 3D Model Case for Reader Unit in TinkerCad

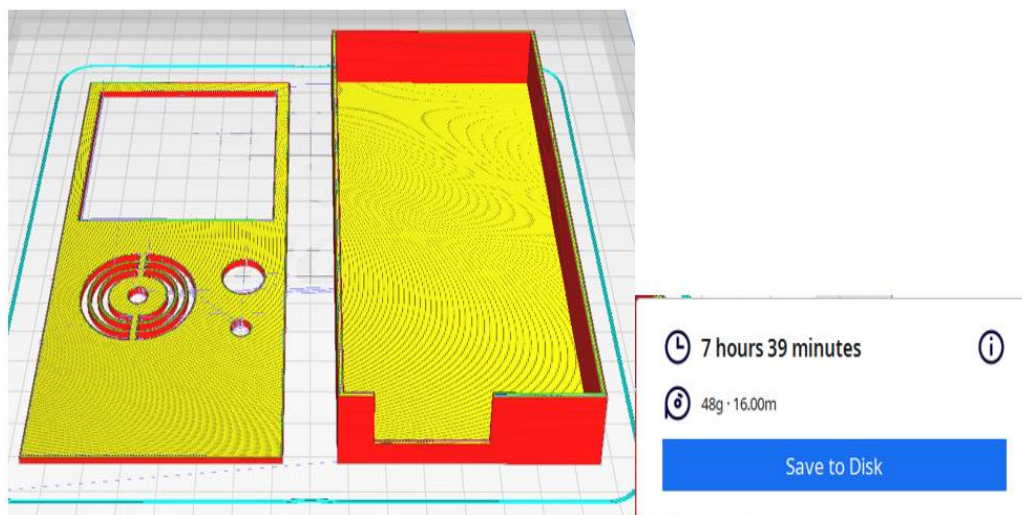


Figure 3.25: 3D Model Case Slice in Ultimaker Cura

Figure 3.26 shows the board to lock the solenoid lock on the left, the stand for the camera unit in the middle, and the antenna holder for the camera unit on the right as designed in the TinkerCad. The slicing detail in Figure 3.27 shows the 3D model in Figure 3.26 requires 1 hour and 14 minutes for printing. The total filament used to print the 3D model is 7 grams, with a length of 2.2 meters. The following subsection will discuss the progress of the project for the system.

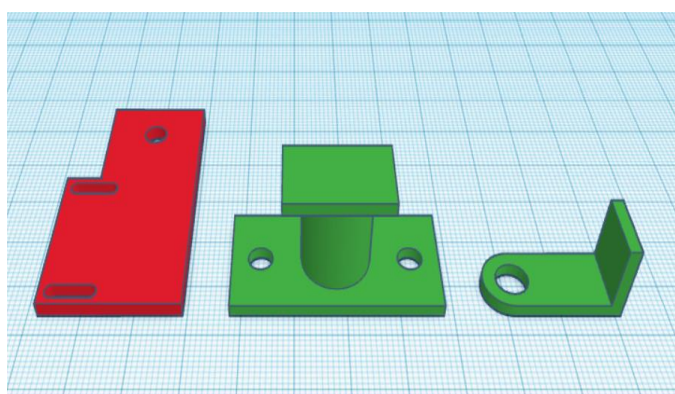


Figure 3.26: 3D Model Design for Solenoid Lock and Camera Unit in TinkerCad

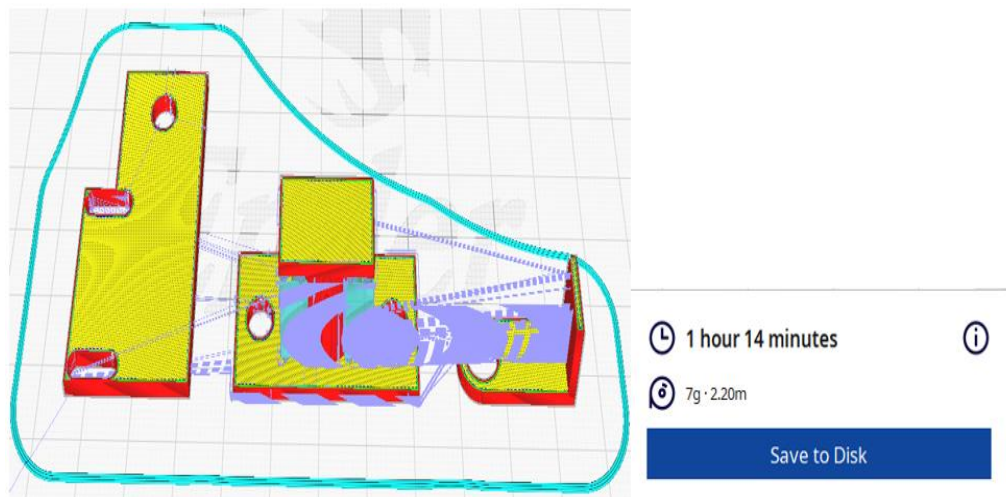


Figure 3.27: 3D Model Design for Solenoid Lock and Camera Unit Slice in Ultimaker Cura

3.13 Project Management

The Gantt chart in Table 3.8 shows all the task schedules for Final Year Project (FYP)

1. The project title is submitted to supervisor Dr. Lee Yu Jen, followed by some detailed discussion with the supervisor after the project title gets approved. From week two onwards, all the necessary research will be done, which includes theory, methodology, product research, and devices research. Hardware and software design starts in the middle of the semester. A simple prototype smart door access system will be built out. At the same time, the prototype will undergo testing to make sure it functions well. There is an FYP presentation at the end of week 13. Thus, PowerPoint slide preparation starts in week 12. Week 15 until week 17 is the final exam week, thus most of the task is suspended at week 14.

By referring to the Gantt chart in Table 3.9, the task for report writing continues until the end of the October semester. Hardware and software design will continue in this semester, but it is more focused on the internet. The prototype from the previous semester will be upgraded and able to support internet applications. Prototype testing is performed in parallel with its design process. The outer casing for the prototype will be designed and printed within three weeks, from week 12 to

week 14. Since the prototype still needs to be completed, the printed circuit board will be designed and not printed out in this semester in case of changes. Due to the final exam, all the tasks will be paused until week 10.

Table 3.10 shows all the tasks needed in FYP 2, and the prototype building will be completed before week 11. Besides, the PCB design will be finalized and printed out in this semester. After finishing all the testing, the prototype circuit on the breadboard will be soldered to the PCB. The whole circuit will be put into the outer casing printed previously in the October semester. Project presentation and poster presentation starts from weeks 13 onwards, so in week 11, preparation for both of them will start. Lastly, the FYP final report will be completed in this semester and the hardcopy will be submitted in week 16.

Table 3.8: Gantt Chart for Final Year Project 1 (June 2022 Trimester)

Activities	Weeks																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Title Proposes	■																			
Title Discussion	■																			
Research		■	■	■	■	■	■	■	■	■	■	■	■	■						
Report Writing				■	■	■	■	■	■	■	■	■	■	■						
HS&SW Design (Partial Only)							■	■	■	■	■	■	■	■						
HS&SW Testing							■	■	■	■	■	■	■	■						
Presentation Preparation												■	■	■						

Table 3.9: Gantt Chart for Extra Semester (October 2022 Trimester)

Activities	Weeks													
	1	2	3	4	5	6	7		1	1	1	1		
									1	2	3	4		
Report Writing								EXAM WEEKS						
HS&SW Design (Focus on IoT)														
HS&SW Testing														
3D Printing (Design and Print)														
PCB Design														

Table 3.10: Gantt Chart for Final Year Project 2 (January 2023 Trimester)

Activities	Weeks																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
Report Writing																	EXAM WEEKS
HW&SW Design (Full)																	
HW&SW Testing																	
Integration of HW and case																	
PCB Printing and Testing																	
Presentation Preparation																	
Poster Presentation																	
Final Report Submission																	

3.14 Summary

In this chapter design idea and operating flow of the smart door access system have been discussed through a block diagram and system flowchart. The Arduino Mega 2560 is selected as the central control unit for the system and will be programmed in C language. An extra WiFi module is added to the Arduino Mega for an internet connection. The Blynk application is used as the mobile application to control the system and receive a notification from the system. The smart door access system supports two credential ways to access the system: double-factor authentication and mobile application. The internal switch allows the user to exit the building or house without providing any credentials. The solenoid lock act as the output device for the system, it will unlock as long as the credentials match the list of the system. For the lock driver, it would be L293D IC. After receiving a signal from the central control unit, the chip will provide an 11V signal to the solenoid lock unit.

The magnetic switch sensor is used to guide the door of the system. If the magnet is away from the switch sensor, the internal circuit will break and generate a signal to the central control unit. The main control unit will process the signal and perform further action. The Esp32 cam module is chosen for the system's camera module. After receiving a trigger signal from the central control unit, it captures an image and is stored in a registered email as evidence. Two printed circuit boards are designed and printed for the system. Lastly, the progress of the whole project for three semesters is shown in Gantt charts. The next chapter is the results and discussion of the smart door access system. The chapter includes simulation work and discusses the project model and system software. Some analysis will also be done in the next chapter.

CHAPTER 4

RESULTS AND DISCUSSION

4.1 Introduction

This chapter discusses the results before building out a prototype model. The system prototype model is also shown and discussed part by part in this chapter. Furthermore, this chapter also shows and discusses the software used for the smart door access system. It includes the main usage language and mobile application. A few system analyses are tested on the prototype, and the result are tabulated and discussed in the chapter. The testing process has covered input devices, output devices, and central control units. The total cost for building this project is mentioned at the end of the chapter.

4.2 Preliminary Work

The simulation was done before purchasing any components, and the circuit for the smart door access system was built. A simulation software called Fritzing is used to perform the simulation. The Fritzing is selected because it is a free simulation software that can generate schematics and show graphics for the microcontroller, module, sensor, and components. Besides, the Fritzing also has a much more complete component list than other freeware, such as TinkerCad. According to subsection 3.3, the system supports multiple access modes and can capture an image.

However, due to the limitation of Fritzing, the IoT parts and image-capturing parts cannot be simulated in the software.

Figure 4.1 shows the graphic schematic for the system. The Arduino Mega 2560 is the central control unit for the whole system. The matrix keypad and RFID scanner form a double-factor authentication method. The reed switch is selected to replace the magnetic switch sensor because they have the same working principle. The connection of the internal circuit for the reed switch is affected easily by a magnet, so it can also be considered a magnetic switch sensor. The 9V battery act as the external power supply for the L293D driver. Since Fritzing does not have a solenoid lock and an Esp32 camera, two red LEDs replace both devices. As long as the red LED turns on, it indicates that the lock or camera gets triggered. The RGB LED and buzzer are used to provide an access signal or denied signal during simulation. The button acts as the internal switch for the system. The schematic diagram for Figure 4.1 is generated and shown in Figure 4.2. The following subsection will discuss about the project hardware model for the system.

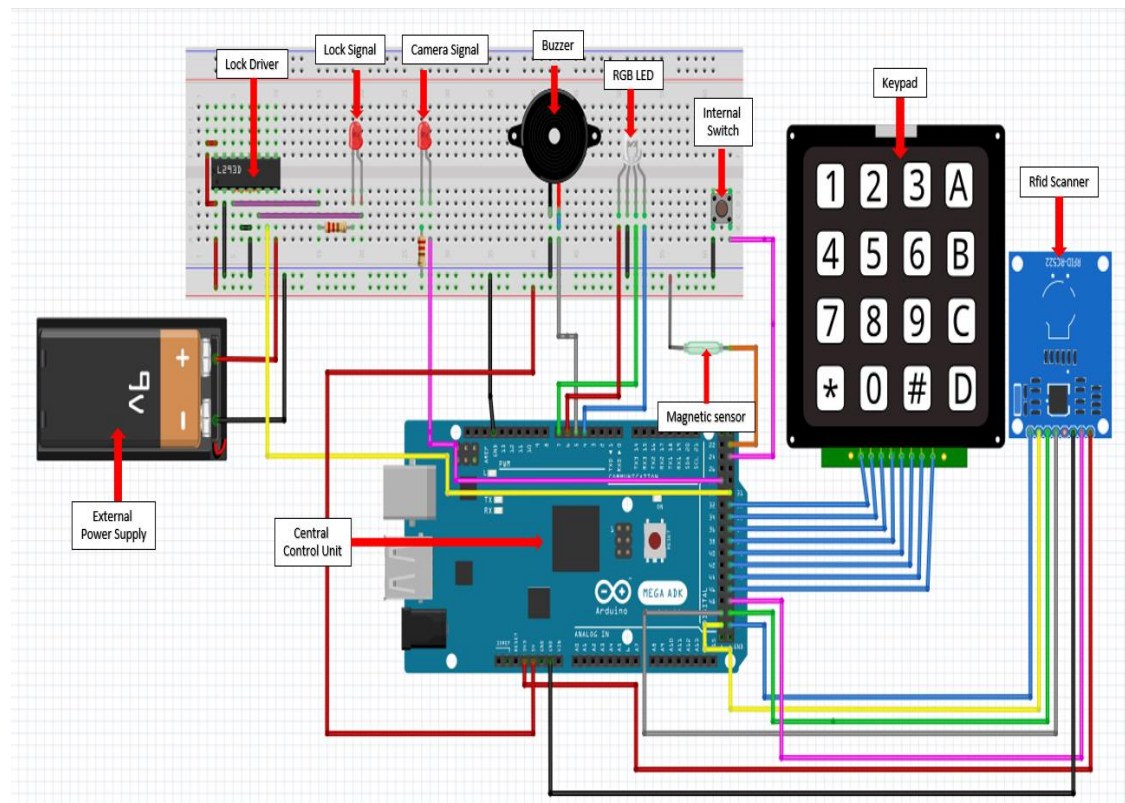


Figure 4.1: Graphic Diagram of Smart Door Access System Without IoT Part and Image Capturing Part

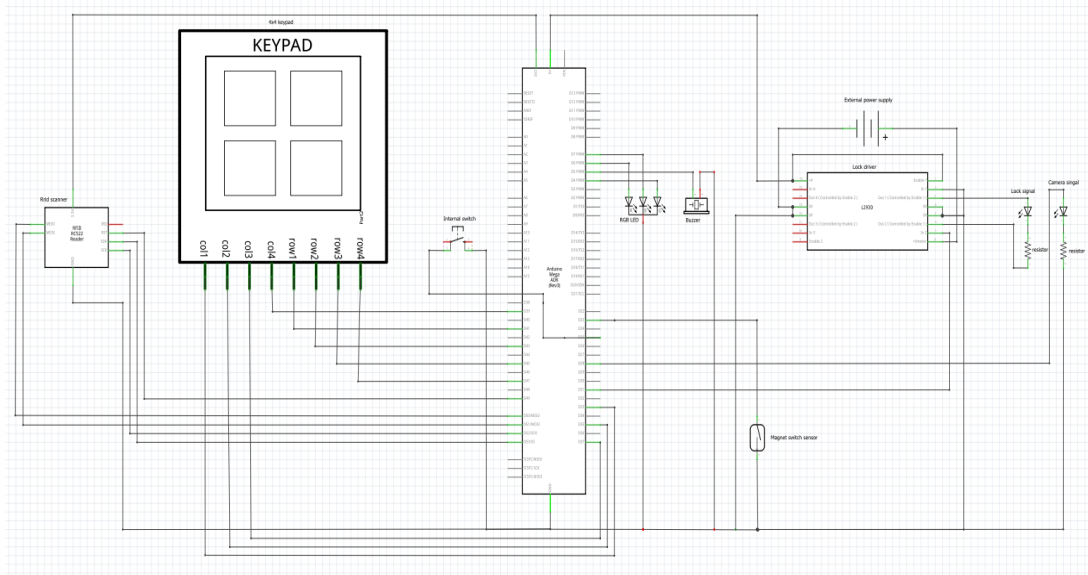


Figure 4.2: Schematic Diagram of Smart Door Access System Without IoT Part and Image Capturing Part

4.3 Project Model

A prototype door model has been built using an aluminium profile and corrugated plastic sheet. The door model is installed with one central control unit, one camera unit, one solenoid lock with a driver, one sensor, and one credential reader unit.

4.3.1 Model Overview

Figure 4.3 shows the front view of the smart door access system. A credential reader unit is placed on the right-hand side of the door, and the camera unit is placed on the top right of the door. According to the back view of the door model shown in Figure 4.4, the magnetic sensor is placed on the left-hand side. The solenoid lock is screwed at the top of the magnetic switch sensor and connected to a solenoid lock driver. The central control unit is placed behind the door model to indicate it is in the building or house.

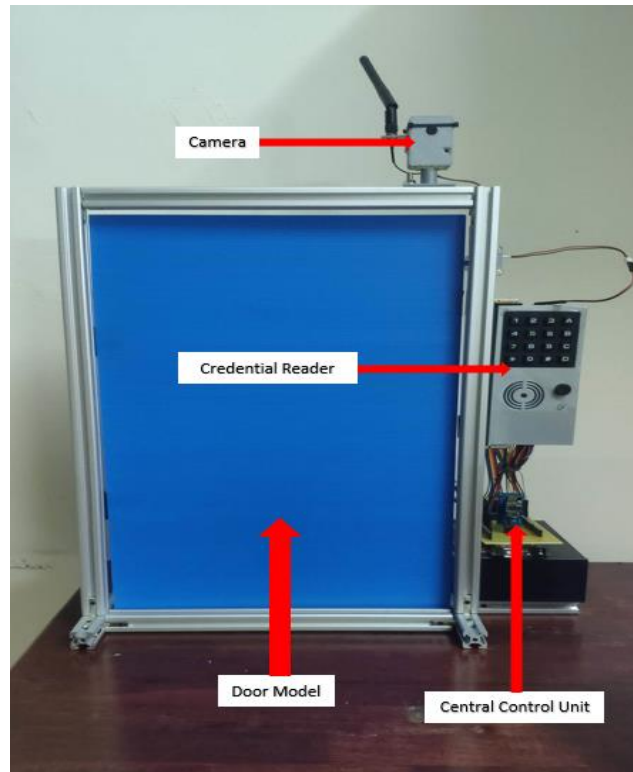


Figure 4.3: Front View of Door Model

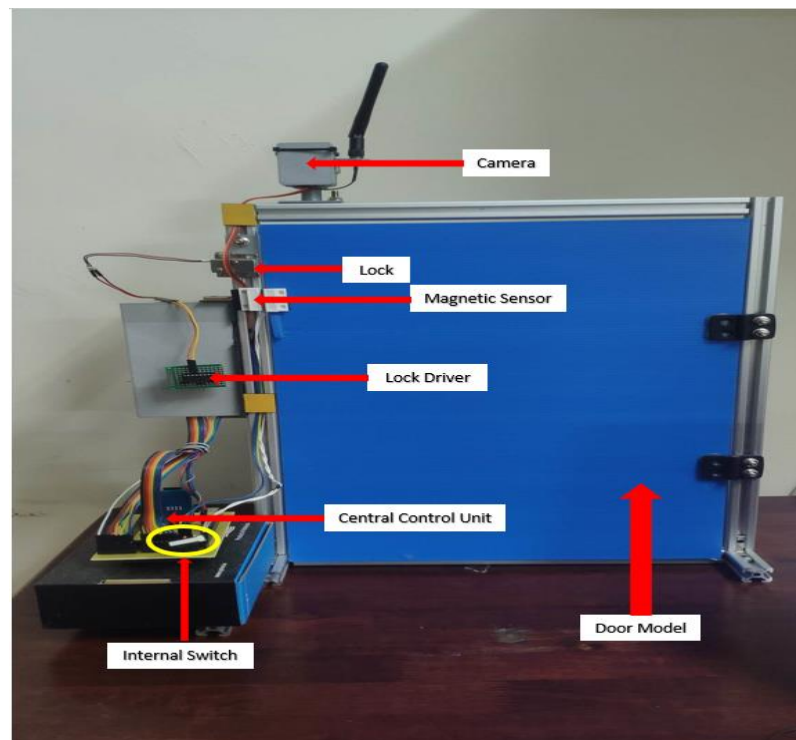


Figure 4.4: Back View of Door Model

4.3.2 Hardware Overview

The smart door access system only has one hardware input device, the reader unit shown in Figure 4.5. The reader contains a 4x4 keypad, RFID reader, RGB LED, and a buzzer. The external case of the reader is designed by TinkerCad software and printed out using the Ender3v2 printer. The reader's wire connection is concentrated at the bottom of the case.

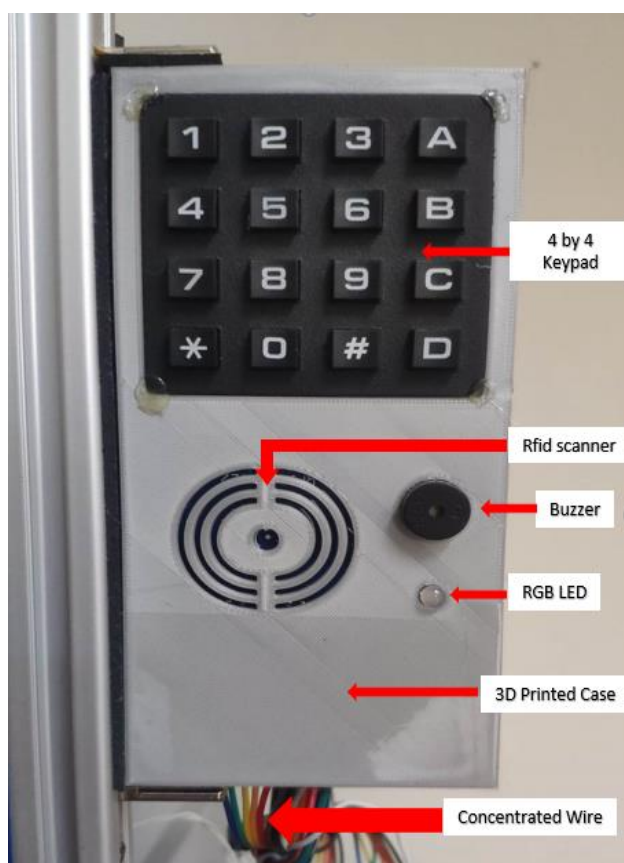


Figure 4.5: Appearance of Credential Reader Unit

The output device for the door system is a solenoid lock, as shown in Figure 4.6. The lock is screwed on a 3D printed board because the screw hole of the lock itself is not matched with the groove of the aluminium profile. Two M3 screw are used to lock the solenoid on the 3D-printed board, and one M5 screw is used to lock the board on the aluminium profile.

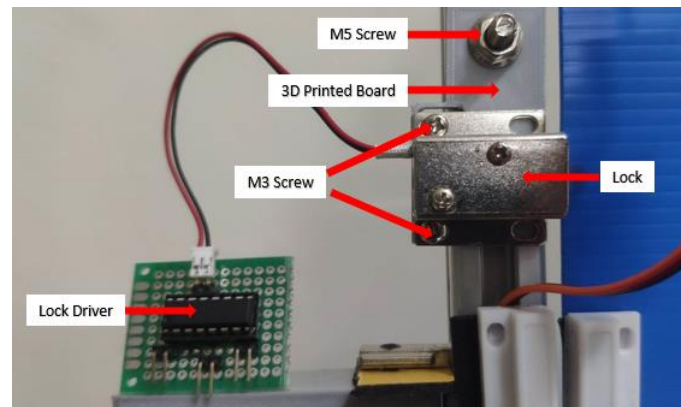


Figure 4.6: Appearance of Solenoid Lock and Lock Driver

Figure 4.7 shows the camera unit built by the Esp32 cam. The camera unit is covered with a 3D-printed case. It is placed at the top of the door model and locked using an M5 screw. As discussed in subsection 3.9, the Esp32 cam contains three main parts: a development board, a program unit and an OV2640 camera. However, the Esp32 cam used to build the camera unit only uses OV2640, a development board and added an external antenna. The external antenna can make the WiFi connection more stable. Figure 4.8 shows the development board of the Esp32 cam is soldered with three wires. The red wire is the supply voltage for the camera unit, while the black wire is the ground of the camera unit. The orange wire sends a trigger signal from the central control unit.

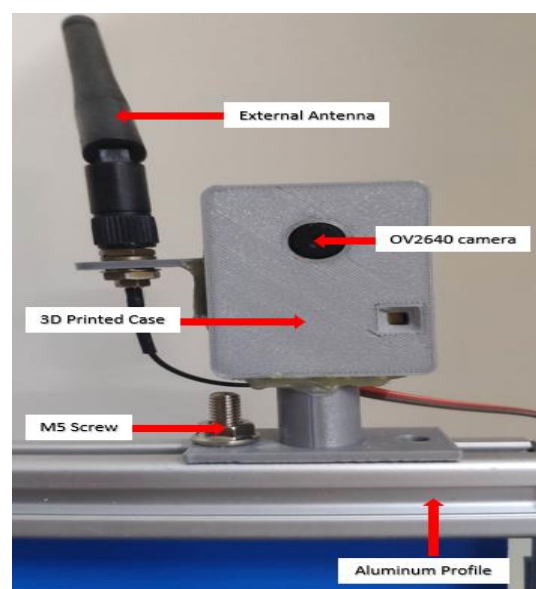


Figure 4.7: Front Appearance of Camera Unit



Figure 4.8: Development Board of Esp32 Cam is Solder with Three Wire and Connect to External Antenna

Figure 4.9 shows the central control unit for the whole system. The central control unit is built with an Arduino Mega and printed circuit board. All devices, sensors, and modules are connected directly to the female port on the PCB of the central control unit. The unit will receive an input signal from a credential reader, mobile apps or internal switch. All the signals will be processed by Arduino Mega 2560 before generating an output signal to trigger any devices. The following subsection will discuss about the project software for the system.

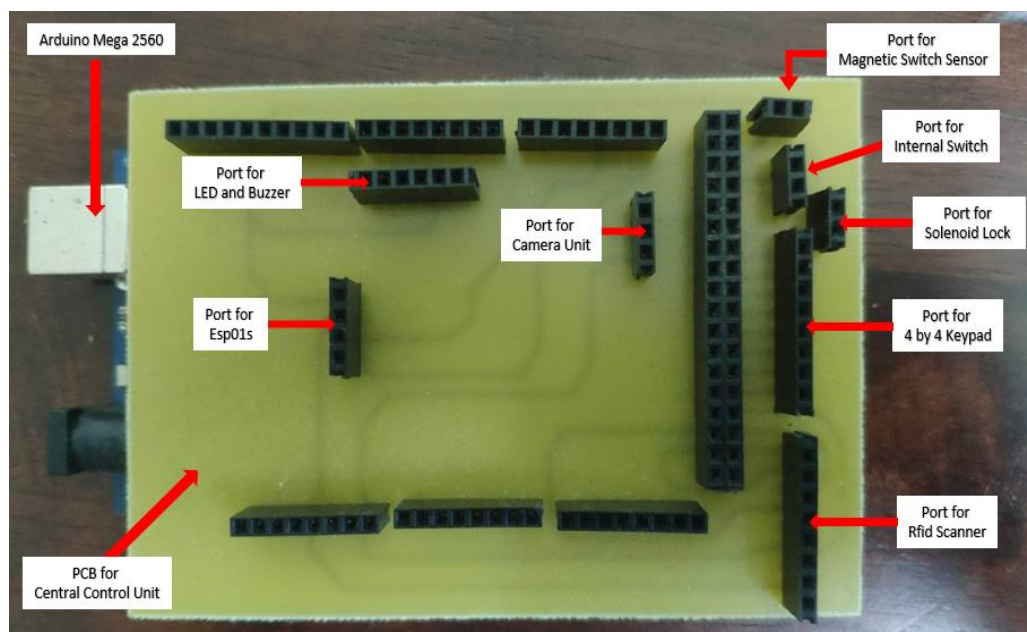


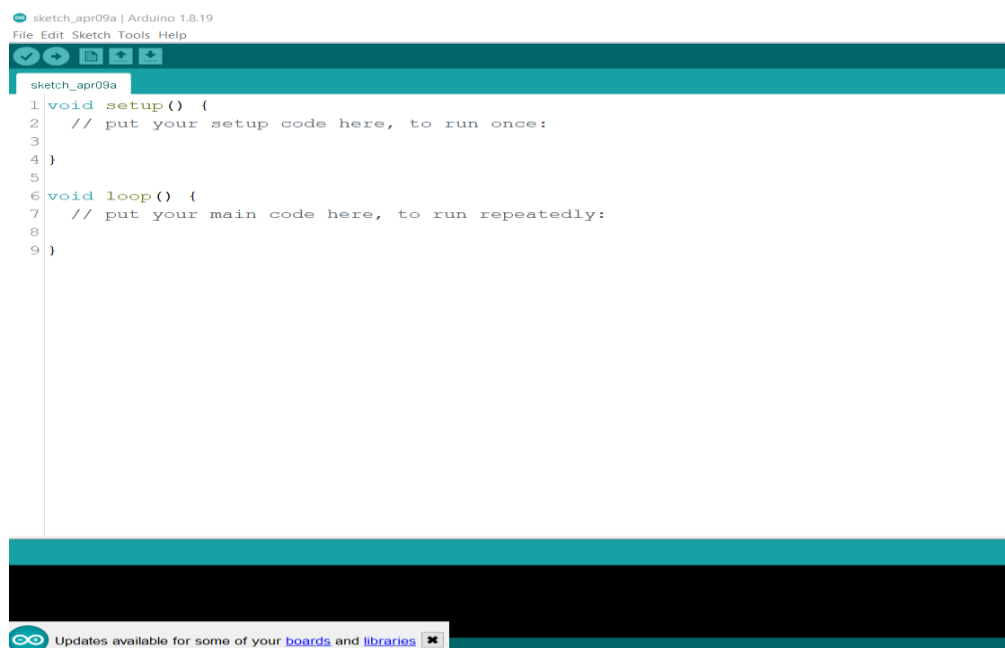
Figure 4.9: Appearance of Central Control Unit Build by Printed Circuit Board and Arduino Mega 2560

4.4 Project Software

The main language for the smart door access system is C language, and the programming language is uploaded by using Arduino IDE. The Blynk application is the mobile application for the system.

4.4.1 Programming Language and Program Tools

In this project, two types of microcontrollers have been used to build the smart door access system. Arduino Mega 2560 is used for the central control unit for the system, and the Esp32 cam module is used to build the camera unit for the system. Different companies manufacture both of them but use the same programming language and program tools. The C language is burned into Arduino Mega using Arduino IDE, shown in Figure 4.10. The Esp32 cam used the same language and IDE tools to program the microcontroller with some specific settings. The board in the Arduino IDE would need to be selected as ESP32 dev Module before uploading. This selection can be made by Tools, which are shown in Figure 4.11. Both microcontrollers' codes can be referred in Appendix A and Appendix B.



```
sketch_apr09a | Arduino 1.8.19
File Edit Sketch Tools Help
sketch_apr09a
1 void setup() {
2   // put your setup code here, to run once:
3
4 }
5
6 void loop() {
7   // put your main code here, to run repeatedly:
8
9 }
```

Updates available for some of your boards and libraries

Figure 4.10: Main Menu for Arduino IDE with Version 1.8.19

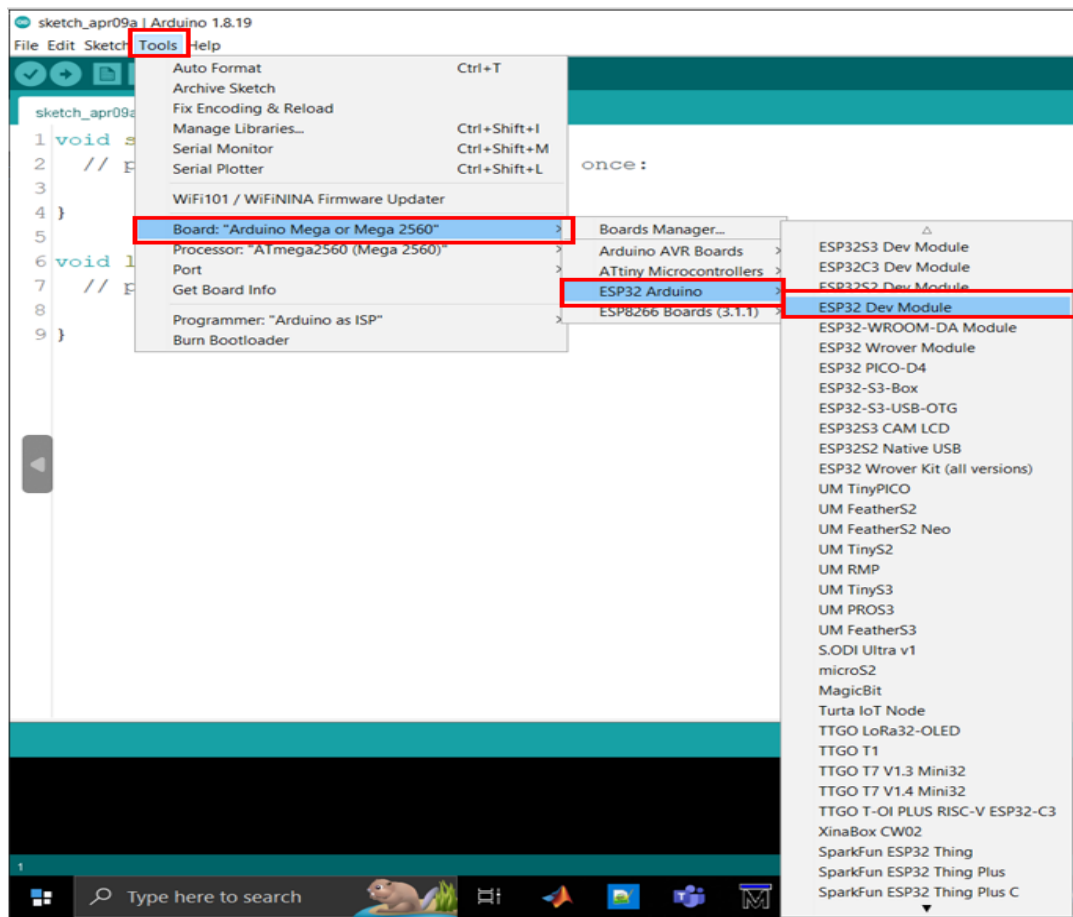


Figure 4.11: Selection of Board at Arduino IDE with Version 1.8.19

4.4.2 Mobile Application

According to subsection 3.5.2, the Blynk application can be downloaded at Google Play Store, so the user is not required to create their application to control the smart door access system. Figure 4.12 shows the login interface for Blynk mobile application. A user ID and password are required before login into the applications. After login into the application, the user can view any device linked to the mobile application, as shown in Figure 4.13. The devices are referred as the smart door access system of the project. The user can see the user interface for the door access system by clicking on the devices, as shown in Figure 4.14. The user interface contains two buttons: the unlock and the halt buttons. The unlock button allows the user to access the system without providing credentials. In contrast, the halt button halts the system for a certain period without accepting credentials or input signals.

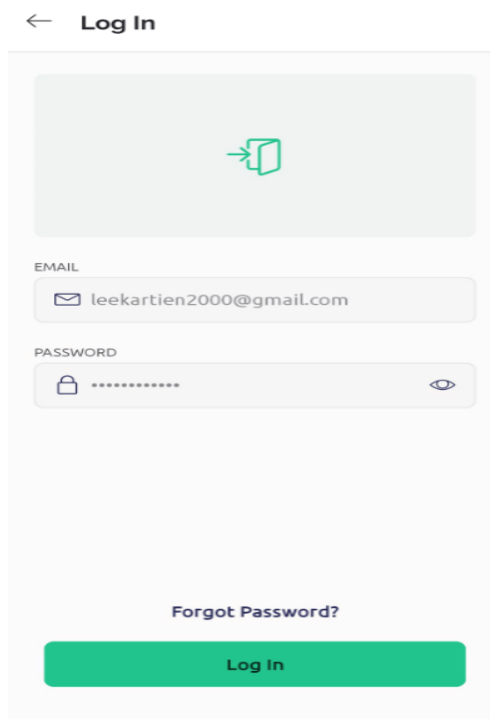


Figure 4.12: Login Interface of Blynk Mobile Application on Android Handphone

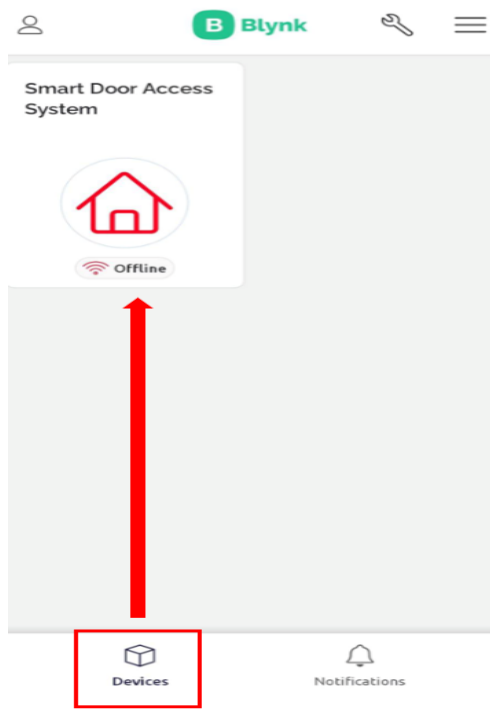


Figure 4.13: Devices Link to Blynk Mobile Application

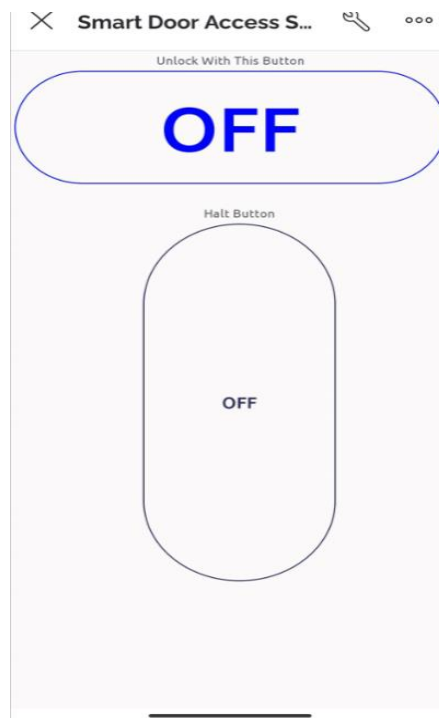


Figure 4.14: User Interface of Blynk Application for Smart Door Access System

As discussed before in subsection 3.6.2, the user interface for the mobile application is built by widgets, and they would need to link to datastream before they start functioning. Figure 4.15 shows the unlock button is linked to datastream Integer V0, while the halt button is linked to datastream Integer V1. Both buttons are selected as push mode, which means the button will return to normal after the finger is released from the screen. The unlock button and halt button will show ON when pressed and show OFF when not pressed by the user. The effect of pressing the button is shown in Figure 4.16.

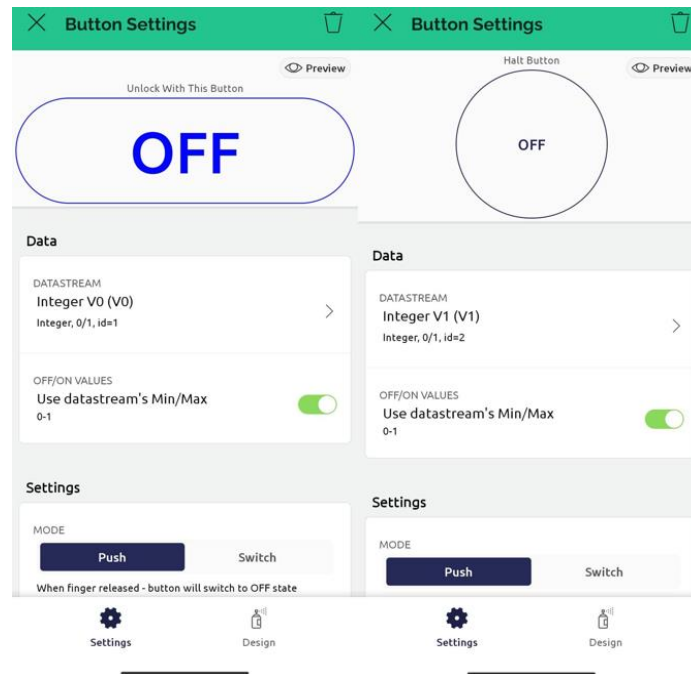


Figure 4.15: Datastream and Button Mode for Unlock Button and Halt Button

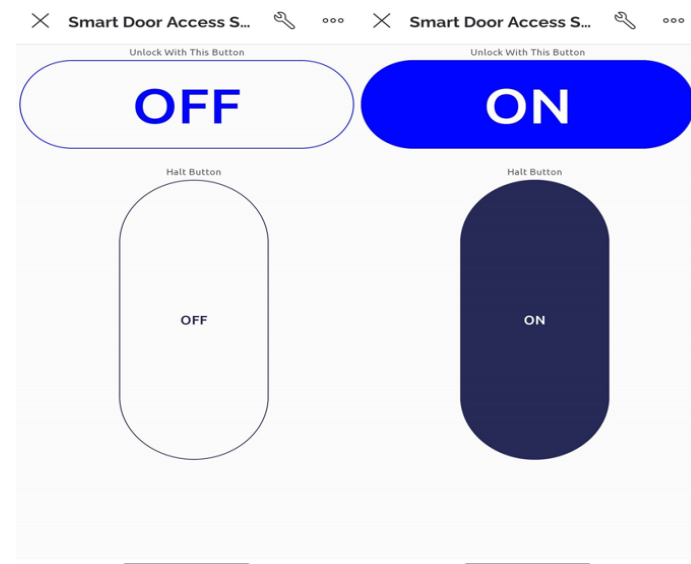


Figure 4.16: Effect of Pressing Unlock Button and Halt Button

Furthermore, the timeline feature of the Blynk mobile application can record the system's status and all the notifications. As mentioned in subsection 3.5.2, the Blynk application can notify the user, but the notification will be renewed once a second notification is received. Thus, the timeline feature collects all data for every

notification. The user can see the time, date, and information for different kinds of notifications within one single page, as shown in Figure 4.17. The timeline can also show a clear status of the system, whether it is connected to the internet or not. Figure 4.18 shows that the smart door access system was connected to WiFi on 6 March at 3.22 PM and disconnected at 5.19 PM on the same day. The following subsection will discuss about the mechanism of sensor for the system.



Figure 4.17: Information of Notification in Timeline Feature of Blynk Mobile Application

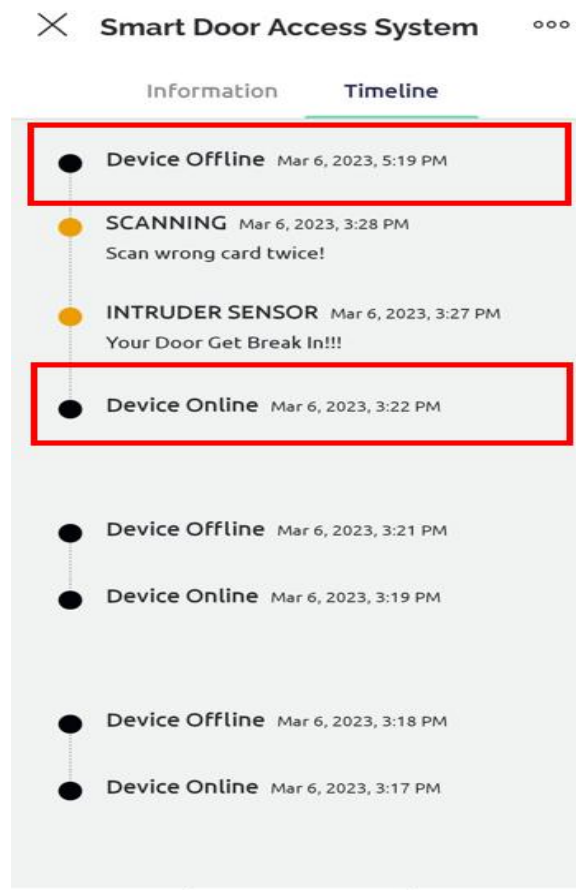


Figure 4.18: Status of Device in Timeline Feature of Blynk Mobile Application

4.5 Sensor Mechanism

The magnetic switch sensor mentioned in subsection 3.8 is used to guide the door for the smart door access system. It is the only sensor used for the system, but it has two functions. The first function acts as the door sensor, while the second is an intruder sensor for the system. The fragmented code for the door sensor is shown in Code Listing 4.1, while the fragmented code for the intruder sensor is shown in Code Listing 4.2.

Code Listing 4.2: Fragmented Code of Intruder Sensor for Pressing Internal Switch

```

magnetData=digitalRead(magnet); // read magnetic switch sensor signal
  if(magnetData ==1 && rfid_status == true && magnet_status == false)
  // magnet faw away will produce signal 1
  {
    digitalWrite(buzzer,HIGH);
    Blynk.logEvent("intruder", "Your Door Get Break In!!!");
  }
  if(magnetData == 0) // magnet ad the side will produce signal 0
  {
    digitalWrite(buzzer,LOW);
    digitalWrite(round1,LOW);
    digitalWrite(round2,LOW);
    counter=0;
  }

```

4.5.1 Door Sensor

The magnetic switch sensor works as the door sensor to monitor the door of the smart door access system. Usually, the magnetic switch sensor functions as an intruder sensor. Once the central control unit receives the correct input, it is switched to the door sensor. The correct input includes a signal from the internal switch, a signal from the reader unit or a signal from the Blynk mobile application. According to Code Listing 4.1, innerSignal becomes zero if a user presses the internal switcher. At the same time, the system will unlock the solenoid lock for three seconds and activate the door sensor. If the magnet moves away from the magnetic switch sensor, magnetData receives a high signal and calls the start_counting() function. After the fifth second of unlocking the solenoid lock, the function will notify the handphone and turn on the buzzer if the door is not closed correctly. The notification of the handphone for the door sensor is shown in Figure 4.19.

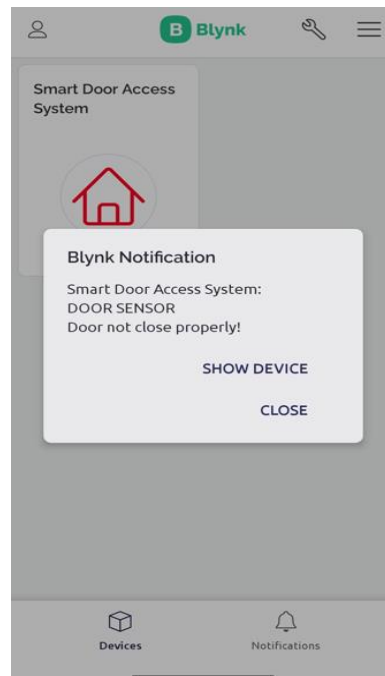


Figure 4.19: Notification of Door Sensor from Blynk Mobile Application

4.5.2 Intruder Sensor

The magnetic switch sensor is always ready as the intruder sensor for the smart door access system. If the door is opened improperly, the intruder sensor will trigger the central control unit to notify the handphone and turn on the buzzer as a warning signal. According to Code Listing 4.2, a notification for the intruder sensor will be sent if the magnet is far away from the magnetic switch, `rfid_status` is equal to true, and `magnet_status` is equal to false. These three conditions must be fulfilled simultaneously for sending the notification. There are three ways for the user to prevent fulfilling the condition: providing credentials to the reader unit, pressing the internal switch, or pressing the unlock button in the Blynk mobile application. If the user does not use any method mentioned in this paragraph to access the system, the central control unit will recognize the user as an intruder. Thus, the user registered under the Blynk mobile application will receive an intruder notification. The notification for the intruder sensor is shown in Figure 4.20, which the user will receive every second when the intruder sensor triggers the central control unit. The following subsection will discuss about the system analysis for the project.

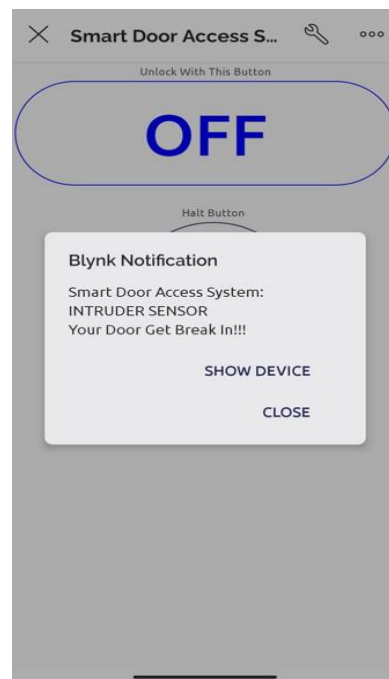


Figure 4.20: Notification of Intruder Sensor from Blynk Mobile Application

4.6 Overall System Analysis

The system is a word that came from the Greek word Systema, meaning arranging a relationship between any components to reach a specific objective or cause. System analysis is a procedure to collect and interpret facts, determine the problem and decompose the system into its components. Besides, system analysis is also considered a problem-solving technique to improve the system and ensure all system components work well to achieve their objective (Tutorialspoint, n.d.). This system analysis for the project is to test the reliability of the smart door access system. The analysis is time-dependent, which means it frequently varies due to the time usage of the door system or components. The equation below is used to calculate accuracy for analysing the whole system.

$$Accuracy = \frac{Correct\ output}{Number\ of\ sample\ taken} \quad (4.1)$$

4.6.1 Access Signal Analysis

According to subsection 3.3, the smart door access system supports up to three different access methods, which are accessible through double-factor authentication, mobile application, or internal switch methods. Thus, the analysis for this section covers all three methods. Every method is tested up to 30 times to determine the solidness and calculate the accuracy. From subsection 3.6.2, the double factor authentication is implemented using an RFID scanner and a 4x4 matrix keypad. The scanner must scan a card with an ID equal to C3 73 4E AD, and then the system will allow the user to key in a password via keypad. The password for the system is 12345AB, and the user is only allowed to access the system by providing the correct password. When both credentials are provided accurately, the central control unit will signal the L293D lock driver to unlock the solenoid lock. Out of 30 tests for double-factor authentication, the matrix keyboard is not responding for the 26th time. The solenoid lock is not unlocked after keying in 12345AB as the password, so the accuracy test for the 26th time is considered as a failure. Therefore, the correct output of this test is only successful 29 times, and the accuracy is 96.67%.

The reason for the fail respond of the keyboard is due to the mechanical issue of the button key. A group of push buttons forms the matrix keypad, and the button will generate fake open and close transitions after being pressed by the user. The program for the system gets fooled by the high transition of state changing because the transition is considered multiple presses for that button. Therefore, the central control unit fails to recognize the signal even though the user provides a correct password.

By pressing the unlock button shown in Figure 4.14, the solenoid lock will unlock for up to three seconds. This method does not require the user to provide credentials like a password or card ID but must have a Blynk account for the smart door access system. The unlock button in the mobile application is pressed up to 30 times to test the accuracy of the application. The accuracy test for the 14th and 29th tests is considered a failure due to the high delay in response. The solenoid lock still unlocks at the 14th and 29th tests, but it only gives the response after a few minutes of pressing. Therefore, the accuracy for the Blynk mobile application is 93.33%

because only 28 correct outputs are generated in this test. Control of the lock by using a mobile application is highly dependent on the internet connection. The system will not respond to the lock without an internet connection. So, the high delay in unlocking the solenoid lock is due to a poor WiFi connection to the central control unit.

According to subsection 3.6.3 a limit switch is used as the internal switch for the smart door access system. When the switch is pressed, the NO terminal will connect with the COM terminal. So, a signal will be generated to the central control unit and trigger the lock driver to unlock the solenoid lock. As usual, the internal switch is pressed up to 30 times to test the accuracy for unlock. The accuracy for the internal switch is 100% because 30 correct output is successfully generated in this test. All the access signal test data are tabulated and shown in Table 4.1.

Table 4.1: Accuracy of Three Different Access Signal

Access Signal	Accuracy	Comment
Double-Factor Authentication	96.67%	4x4 keypad is not responding at 26 th testing
Blynk Mobile Application	93.33%	High delay at 14 th test and 29 th test
Internal Switch	100%	

4.6.2 Lock Analysis

According to subsection 3.3, the smart door access system supports three ways to unlock the solenoid. The analysis of this section is to test the functionality of the L293D lock driver and solenoid lock. So, an easier way to unlock the solenoid lock is chosen: pressing the internal switch. The internal switch will send a signal to the central control unit to generate an unlock signal for the lock driver to unlock the solenoid lock. The solenoid lock will unlock for three seconds and then return to normal.

As discussed in subsection 3.7.1, the solenoid lock is made by a big coil of copper wire with an armature in the middle. The solenoid lock will draw large currents due to its mechanical design, so the current usage and power to unlock the lock is recorded in Table 4.2. These two data will help determine the energy consumption for the solenoid lock.

According to Table 4.2, 15 samples are taken to test the accuracy of the solenoid lock. The unlock status has shown that the solenoid successfully generated 15 correct outputs for this test and produced 100% accuracy for the lock analysis. The highest current used for unlocking is 318mA, while the lowest is 310mA. The power consumption for the solenoid during unlock period ranges from 4.03W to 4.134W.

Table 4.2: Accuracy of Solenoid Lock and Current Usage

No	Unlock Status		Voltage Supply (V)	Current (mA)	Power (W)
	Success	Fail			
1.	*		13	318	4.134
2.	*		13	317	4.121
3.	*		13	317	4.121
4.	*		13	317	4.121
5.	*		13	313	4.069
6.	*		13	312	4.056
7.	*		13	313	4.069
8.	*		13	312	4.056
9.	*		13	310	4.03
10.	*		13	313	4.069
11.	*		13	313	4.069
12.	*		13	312	4.056
13.	*		13	311	4.043
14.	*		13	312	4.056
15.	*		13	311	4.043

4.6.3 Fault Tolerance Analysis

From subsection 3.3, the smart door access system can detect and differentiate the wrong credential provided to the reader unit. When the wrong password or card ID is provided to the reader unit two times continuously, the system will provide a warning signal, send a notification and capture an image. Thus, the analysis for this section tests the reliability of the credential detection function of the smart door access system. The analysis is divided into two main parts, the first part is to detect the wrong password, while the second is to detect the wrong card ID. The testing is considered a success if the system can finish the progress of Signal or Effect from one to four, as mentioned in Table 4.3. After detecting the wrong password twice, the system must turn on the red LED and buzzer. Besides, the system must notify on the Blynk mobile application and trigger the camera unit to capture an image. The image will send to a receiver email and stored as crime evidence.

The first part of the fault tolerance analysis is to detect entering the wrong password twice. A correct card ID (C3 73 4E AD) will be provided to the scanner, then a wrong password (6789CDE) will be keyed into the system. This action must be performed twice to activate the system's credential detection function. Fifteen samples are taken in the first part of the analysis. From the observation in Table 4.3, the 4th and 11th test are considered as failure to detect the wrong password. This is because the system needs to complete the progress of the Signal or Effect. The camera unit of the system captures the image, but it is not received in the email. Therefore, 13 correct output is generated, and the accuracy for the first part of the analysis is 93.33% only. Failure to receive an image in the email is due to an internet connection or file corruption. When the camera unit successfully captures an image, it will convert it into a Still Picture Interchange File Format (SPIFF) file before sending it. File corruption can happen in this stage and cause the image to be unavailable for sending. Besides, the internet is essential for sending images to an email. If the WiFi connection is poor, it will cause the Esp32 cam module to fail to transfer the image.

The second part of the fault tolerance analysis is to detect scanning the wrong card ID twice. An RFID card with ID 10 2C BE 1A is continuously scanned on the

reader unit to activate the system's credential detection function. The step to activate the credential detection function for the second part differs from the first. This is because the wrong password is not required for the second part. A card with the wrong ID is enough to activate the function. As usual, fifteen samples are taken for the second test of this analysis. Through the observation in Table 4.3, the system can ideally detect the wrong card ID because there is no fail detection within the fifteen tests. Therefore, the accuracy for the second part of the analysis is 100%. The accuracy and comment for the fault tolerance analysis are tabulated and shown in Table 4.4.

Table 4.3: Status of Entering Wrong Password Twice and Scanning Wrong Card Twice

No	Enter Wrong Password						Scan Wrong ID					
	Signal or Effect				Status		Signal or Effect				Status	
	1	2	3	4	Success	Fail	1	2	3	4	Success	Fail
1.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
2.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
3.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
4.	Y	Y	Y	N		*	Y	Y	Y	Y	*	
5.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
6.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
7.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
8.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
9.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
10.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
11.	Y	Y	Y	N		*	Y	Y	Y	Y	*	
12.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
13.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
14.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	
15.	Y	Y	Y	Y	*		Y	Y	Y	Y	*	

1 = Red LED turn on // 2 = Buzzer turn on
3 = Receive notification // 4 = Receive image in email
Y = Yes, N = No

Table 4.4: Accuracy of Fault Tolerance Analysis

Access Signal	Accuracy	Comment
Enter Wrong Password	93.33%	Fail to receive image at 4 th and 11 th test
Scan Wrong ID	100%	

4.6.4 System Halting Analysis

The halt function is present in the smart door access system. The system will temporarily terminate by pressing the halt button shown in Figure 4.14. During temporary termination, the system does not accept any access signal. The system rejects receiving a signal from the reader unit, internal switch and Blynk mobile application before the termination is ended. The blue LED is turned on during temporary termination, as shown in Figure 4.21 and turned off after the termination period. The analysis for this section is to determine the functionality of the halt feature of the system. After pressing the halt button in the Blynk mobile application, the correct RFID card is scanned on the reader, but the system does not allow any key in password on the keypad.

Besides, when the internal switch is also pressed during the termination period, the solenoid lock does not unlock. When the unlock button of the mobile application is also pressed during the termination period, the solenoid lock remains unchanged. These three actions have been tested up to fifteen times, as shown in Table 4.5, and the halt function for the system is considered a success. This is because the solenoid lock remains unchanged even though the internal switch or unlock button is pressed. The user is also not allowed to key in a password after scanning with the correct card. Therefore, the accuracy shown in Table 4.6 is 100% for all three actions. The following subsection will discuss about the sensor analysis for the project.

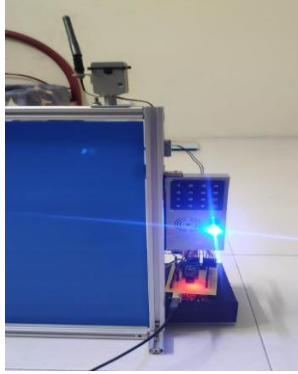


Figure 4.21: Blue LED Light Up during Temporary Termination

Table 4.5: Status of Solenoid Lock During Temporary Termination Period

No	Action					
	Double Factor Authentication (Scan RFID card)		Mobile Application (Press Unlock Button)		Internal Switch (Press Internal Switch)	
	Status of Lock		Status of Lock		Status of Lock	
	Unlock	Lock	Unlock	Lock	Unlock	Lock
1.		*		*		*
2.		*		*		*
3.		*		*		*
4.		*		*		*
5.		*		*		*
6.		*		*		*
7.		*		*		*
8.		*		*		*
9.		*		*		*
10.		*		*		*
11.		*		*		*
12.		*		*		*
13.		*		*		*
14.		*		*		*
15.		*		*		*

Table 4.6: Accuracy of Halt Feature Analysis

Access Signal	Accuracy	Comment
Double-Factor Authentication	100%	
Blynk Mobile Application	100%	
Internal Switch	100%	

4.6.5 Sensor Analysis

A magnetic switch sensor is used in the system to guide and monitor the door. There is only one magnetic switch sensor, but it has two functions. The first function acts as an intruder sensor, while the second is a door sensor. The magnetic switch sensor is always set as an intruder sensor during operation. If any correct access signal is provided, it will switch from the intruder sensor to the door sensor. Thus, the sensor analysis for this section is separated into two main parts. The first part is used to test the functionality of the intruder sensor, while the second part is for the door sensor.

No access signal will be provided to the smart door access system to test the intruder sensor. The door will be opened and closed directly up to fifteen times, which causes the magnet to move away from the magnetic switch sensor. Then, the system will turn on a buzzer and send an intruder notification directly to the user. The notification is sent every second to spam the user's handphone as the warning signal. According to Table 4.7, fifteen samples are collected on the intruder sensor test. The accuracy for the intruder sensor is 100% because fifteen correct output is generated from the test. The intruder Blynk notification is received fifteen times on the user's handphone.

One access signal is provided once for the door sensor test. For the first round of the test, a card ID (C3 73 4E AD) and password (12345AB) are provided to the reader unit of the system. The door opens after the solenoid lock is unlocked, causing the magnet to move to away from the magnetic switch sensor. The system will turn on a buzzer and send a door sensor notification after the fifth second of unlock period.

The door sensor notification is only received by the user every minute, and it is not spamming on the user's handphone every second. The process for the second and third rounds is the same as the first rounds. However, the access signal for the second round is by pressing unlock button in the Blynk mobile application, while the access signal for the third round is by pressing the internal switch. From the observation in Table 4.7, the door sensor was tested up to fifteen times, and fifteen correct outputs were generated. This is because the Blynk mobile application received fifteen notifications on this test. Therefore, the accuracy for the door sensor is 100%, and both accuracies are tabulated in Table 4.8. The following subsection will discuss the cost analysis for the project.

Table 4.7: Status of Blynk Notification for Intruder Sensor and Door Sensor

No	Intruder Sensor					Door Sensor				
	Access Signal Provided			Blynk Notification		Access Signal Provided			Blynk Notification	
	1	2	3	Receive	Not Receive	1	2	3	Receive	Not Receive
1.				*		Y			*	
2.				*			Y		*	
3.				*				Y	*	
4.				*		Y			*	
5.				*			Y		*	
6.				*				Y	*	
7.				*		Y			*	
8.				*			Y		*	
9.				*				Y	*	
10.				*		Y			*	
11.				*			Y		*	
12.				*				Y	*	
13.				*		Y			*	
14.				*			Y		*	
15.				*				Y	*	

1 = Double Authentication factor (Card ID and Password)
 2 = Blynk Mobile Application (Unlock button)
 3 = Internal switch
 Y = Yes, N = No

Table 4.8: Accuracy of Sensor Analysis

Sensor	Accuracy	Comment
Intruder Sensor	100%	
Door Sensor	100%	

4.7 Project Cost Analysis

The Table 4.9 lists all the item costs used to build the door system. It has been categorized into four main parts: device and component part, door model part, 3D printing part, and printed circuit board part. The total cost of the door system is RM 257.67, but it is not the actual cost for the door system. The reason is that main objective of this project is to design a smart door access system only. The door model is built for demonstration purposes during a presentation or promoting the door system, so the cost for the door model part should be excluded from the actual cost. Therefore, the actual cost for a smart door access system is RM170.47. Table 4.10 shows what type of cost should be included in the total and actual costs.

Table 4.9: Cost for Every Item Use to Build Smart Door Access System

Device and Component					
No	Item	Unit	Unit Price (RM)	Total Price (RM)	Comment
1.	Arduino Mega 2560	1	74.9	74.9	
2.	Esp01s	1	7.9	7.9	
3.	Esp01 serial adaptor	1	5.58	5.58	
4.	Magnetic switch sensor	1	3.9	3.9	
5.	Esp32 cam module	1	24.9	24.9	Include external antenna and cable
6.	Solenoid lock	1	10.09	10.09	
7.	4 by 4 matrix keypad	1	6.5	6.5	
8.	RC522 scanner	1	6.29	6.29	A type of RFID scanner
9.	Limit switch	1	1.8	1.9	
10.	L293D	1	2.9	2.8	
11.	RGB LED	1	0.3	0.3	
12.	330-ohm resistor	3	0.10	0.3	
13.	5V buzzer	1	0.89	0.89	
14.	Male to female jumper	1	0.9	0.9	One pack has 40 wires
15.	Male header pin	1	0.5	0.5	One pack has 40 pins
16.	Female header pin	1	0.5	0.5	One pack has 40 pins
17.	Female header pin 1x8P	5	0.87	4.35	One pack has 8 pins
18.	Female header pin 1x10P	1	0.87	0.87	One pack has 10 pins
19.	Female header pin 2x18P	1	1.73	1.73	One pack has 10 pins with 2 rows
20.	IC socket 16 pin	1	0.3	0.3	

			Total	155.4	
Door Model					
1.	Aluminium profile (Size 2020)	180	0.19	34.2	RM0.19 for every 1cm
2.	Interior bracket	12	2.95	35.4	
3.	Nylon hinge	2	4.5	9	
4.	T-head bolt screw	6	1.05	6.3	M5 size with 16mm
5.	Corrugated plastic sheet	1	2.3	2.3	
			Total	87.2	
3D Printing					
1.	Case for reader unit	48g	0.057	2.74	RM0.057 for every 1 gram
2.	Case for camera unit	17g	0.057	0.97	RM0.057 for every 1 gram
3.	Board for solenoid lock	3g	0.057	0.171	RM0.057 for every 1 gram
			Total	3.88	
Printed Circuit Board					
1.	Central control unit (11x8) cm, single layer	1	6.52	6.52	Price from JLC PCB
2.	Lock driver (3x3.1) cm, single layer	1	4.67	4.67	Price from JLC PCB
			Total	11.19	

Table 4.10: Difference Between Total Cost and Actual Cost for Smart Door Access System

No.	Cost of System	Included Cost	Amount (RM)	Total (RM)
1.	Total Cost	Device and Component	155.4	
2.		Door Model	87.2	
3.		3D Printing	3.88	
4.		Printed Circuit Board	11.19	
				257.67
1.	Actual Cost	Device and Component	155.4	
2.		3D Printing	3.88	
3.		Printed Circuit Board	11.19	
				170.47

4.8 Summary

In this chapter, the results for hardware and software has been discussed. The Fritzing is selected as the simulation software to test and verify the basic idea for the smart door access system. The prototype model for the project has been successfully built out and shown in this chapter. The prototype door model for the system contains one reader unit on the right-hand side and a camera unit at the top right of the door model. The L293D driver controls the solenoid lock and both act as output devices for the prototype model. A printed circuit board is plugged into the top of Arduino Mega 2560, which is the system's central control unit.

The main language used for the system is C language. It is compatible with a central control unit (Arduino Mega 2560) and a camera unit (Esp32 cam module). Arduino IDE is used to upload the code for both device units. The system uses a magnetic switch sensor to guide and monitor the door. Typically, the magnetic

sensor act as the intruder sensor. If someone tries to open the door without using the proper access method, the system will send an intruder notification to the user who owns the Blynk mobile application. The magnetic sensor turns into a door sensor if the user uses the proper way to access the system. The system will only send a door sensor notification to the mobile application if the door does not close after the fifth second of the unlock session.

An overall system analysis has been done to test the functionality and reliability of the project. The analysis has covered credentials analysis, lock analysis, halt feature analysis, fault tolerance analysis, and sensor analysis. Although the system is imperfect, the accuracies are at least 90%. The cost analysis for the whole project is stated at the end of the chapter. Two main costs have been calculated in the cost analysis, which are total and actual costs. The total cost for this project is RM257.67, while the actual cost is RM170.47. The actual cost is much less than the total cost because the cost for the door model is excluded from the project's actual cost.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter will discuss the conclusion of the whole project. The weaknesses of the smart door access system will be mentioned in this chapter, and the methods to improve the weaknesses are given as the recommendations.

5.2 Conclusion

In conclusion, the three main objectives of the project have been achieved. The project's first objective is to design a system that can support multiple access method. The system of this project supports three different access methods. The user must provide the reader unit with two credentials (password and card ID) to access the system. Besides, the user can also press the unlock button in the Blynk mobile application for access. The internal switch of the system allows the user to exit from the building through a single press action. The second objective of the system is to boost the safety rate by sending a notification to the end user if the system is aware of any danger. The system will notify the user through the Blynk mobile application and trigger the camera unit to capture an image if the wrong password or card ID is provided twice. The project's third objective is to unlock the system through a mobile application with a long-distance range. Another restriction for the third objective is that it is only useable for the user registered under the system. Therefore, the door

system of the project uses the Blynk mobile application to unlock and halt the system. The user that does not have the login ID and the password is not allowed to use the mobile application from the Blynk platform.

The prototype model of the project has been built for this project. The model contains a central control unit, reader unit, camera unit, door sensor, internal switch and one solenoid lock with the driver. The Arduino Mega 2560 is the main microcontroller used to build this project. For the software, the Blynk IoT platform works as the mobile application for the project. The smart door access system is built by combining the hardware and software mentioned in this paragraph. An overall system analysis has been tested on this project to determine the reliability and functionality of the door system. The system analysis has covered all the software and hardware used to build the system.

Besides, the accuracy is also being calculated along with the system analysis. The access signal analysis contains three different analyses and three accuracies, which is double factor authentication (96.67%), Blynk mobile application (93.33%), and internal switch (100%). The accuracy for the lock analysis and halt feature analysis is the same, which is 100%. The analysis for fault tolerance is separated into two parts. The first part is wrong password detection with 93.33% accuracy, while the second is wrong card ID detection with 100% accuracy. Two different analyses are contained in the sensor analysis, which is the intruder and door sensor analysis. Both sensor testing has an accuracy of 100%. A cost analysis has been done in the results part to determine the spending for the whole project. The total cost for the whole project is RM257.67, and the actual cost is RM170.47. The actual cost is much lower because the cost for the door model is not included in this cost. The following subsection will discuss the limitations of the project.

5.3 Limitations of Project

The limitation of the project is that the smart door access system needs to be more convenient. A door access system's advantage is replacing the key with something

that is easier to carry, like a thin card, small tag or mobile app. However, the user still needs to use one hand to scan the card or take out a phone to press the icon. It is inconvenient if the user carries many things with two hands or is rushing to enter the building.

Furthermore, the project needs to be more eco-friendly for the environment. The system is always in ready mode and causes energy waste. This is because the system uses the same amount of energy whether there is a user or not. Even though electricity is a renewable energy on earth, but the way of generating electricity is not purely eco-friendly. Some countries still uses burning coal to produce electricity. This method will pollute the earth due to the exposure of harmful gas to the surrounding. Thus, reducing the consumption of electricity will help to save the earth.

Besides, the project needs to be more intelligent as a smart door access system. The system is fixed to specific rules for door opening. The door cannot open more than five seconds after the unlock period. If the door still opens after five seconds, the user will receive a mobile application on the Blynk application. Even though the user is still standing in front of the door, the system also does not allow the door to open for more than five seconds.

In addition, the size of the whole system is too big and not convenient for installation. The system is built with a combination of a few devices separately. The devices communicate through a wire connection, so it causes the system to occupy much space and take more time to install for each part. Workers need to install the reader, camera, or central control units one by one before connecting them. This procedure will waste much time and requires more space from the building to locate all the devices for the system. The following subsection will discuss about the recommendations for the project.

5.4 Recommendations for Project

Four methods are proposed to solve the weaknesses mentioned in the limitations and to improve the project.

5.4.1 Biometric Technology

Integrate biometric technology into the smart door access system to “Free User Hand”. The biometric technology is a technique which utilizes the unique biometric characteristic of humans as a credential. The technology will extract faces, fingerprints, or voices from humans and compare them with a database. As long as the database is matched, people are allowed to access the system; otherwise, the people are denied access. The project can integrate a sound recognition sensor or face recognition sensor on the reader unit. So users can replace the card with their face or access the system by speaking a specific sentence on the sound recognition sensor. Besides, biometric technology also increases the safety of the door access system because it is harder to copy or imitate faces and sounds from a human. The card or tags can be easily stolen and copied with a handheld RFID writer since the device is cheap and easily found on the market.

5.4.2 Energy Saving Mode

Implement sleep mode on the central control unit of the system to reduce unnecessary power consumption. The system will not activate the reader, camera, or sensor under sleep mode. All these devices are ready to receive or send a signal if the system detects a user. Therefore, more energy is consumed during accessing period, and lesser energy is used for the waiting period. There are many ways to implement energy-saving modes. For example, the use of GPS to activate the system. The door access system can detect the user's distance from the building through GPS, so it will activate the whole system and get ready for operation as long as the user enters the

setting range. If the user is far from the building or does not stay within the setting range, the door access system will go into sleep mode to save energy.

5.4.3 Human Detection Function

Implement a function to detect the presence of the user to let the system become more intelligent. The system can scan whether there is a user or not in the front or at the back of the door. Thus, the user can leave the door open without triggering the door sensor detection. The door sensor detection will only trigger the system if a user is not near the door and the door is not closed correctly for a certain period. An image processing method can implement this detection function by adding a camera on the door to scan the user's face for every access action. If the camera scans that a user is at the front or back of the door, the system allows the user to open the door for more than five seconds. Users will only receive the notifications if they do not close the door and fail to be detected by the camera after five seconds. This method lets users automatically control the door opening session using their faces.

5.4.4 Full Custom Build Printed Circuit Board

Full customization of the printed circuit board gives high flexibility to control board size, arrangement of devices, and selection of components. Since the central control unit of the project is made from the combination of a piece of PCB with Arduino Mega 2560, it causes the size to become bulky. The size of the microcontroller board is already fixed by Arduino company and has significantly less space for modification. The PCB must also follow the size of Arduino Mega 2560 for compatibility. Thus, the central control unit for the system looks thick and cannot solder other devices directly on the Arduino Mega 2560. Other devices like the reader unit, magnetic switch sensor, or lock need a jumper wire to build a connection with the Arduino Mega 2560.

If full customization is used to build the system, many devices can be built on a single board. The camera, reader, and sensor can be combined with the central control unit. Besides, customization allows a designer to replace most of the Dual In Line Package (DIP) components with Surface Mount Device (SMD) components to save space and energy. Usually, the size of SMD components is smaller than DIP components, and they will consume less energy. The designer also allows arranging the best place to locate devices or components on the printed circuit board without wasting any corner of the printed circuit board. Figure 5.1 shows that Tuya company manufactured a door access system in a thin and compact size. The door access device combines the camera unit, lock unit, keypad unit, and fingerprint sensor within one box.



Figure 5.1: Digital Camera Door Lock from Tuya Company (tuya, n.d.)

REFERENCES

- Amazon, n.d. *DIY malls 1pcs 4x4 Matrix Membrane Keyboard Module +5pcs 16 Keys Keypad*. [electronic print] Available at: <<https://www.amazon.com/DIYmalls-Matrix-Membrane-Keyboard-Module/dp/B09CT7H7HY>> [Accessed 17 March 2023].
- Aqib, 2018. *RFID and Keypad Door Lock and Alert System Using Arduino*. [online] Available at: <https://create.arduino.cc/projecthub/muhammad-aqib/rfid-and-keypad-door-lock-and-alert-system-using-arduino-60f050?ref=tag&ref_id=lock&offset=0> [Accessed 15 July 2022].
- Arduino, n.d. *What is Arduino*. [online] Available at: <<https://www.arduino.cc/en/Guide/Introduction>> [Accessed 3 July 2022].
- Ashwak, 2021. *ESP32 vs ESP8266 – Which One to Choose*. [online] Available at: <<https://www.electronicshub.org/esp32-vs-esp8266/>> [Accessed 8 July 2022].
- Biometric Solutions, 2021. *Fingerprint Recognition*. [online] Available at: <<https://www.biometric-solutions.com/fingerprint-recognition.html>> [Accessed 16 August 2022].
- Blynk, 2022. *Introduction*. [online] Available at: <<https://docs.blynk.io/en/>> [Accessed 14 August 2022].
- Blynk, 2022. *Template*. [electronic print] Available at: <<https://blynk.cloud/dashboard/152720/products>> [Accessed 14 August 2022].
- Catie, 2020. *Door Access Control System: Uses, Options and Pricing* [electronic print] Available at: <<https://www.360connect.com/product-blog/door-access-control-system/>> [Accessed 30 August 2022].
- Chris, 2021. *8 Advantage of Arduino over Raspberry Pi*. [online] Available at: <<https://chipwired.com/arduino-advantages-over-raspberry-pi/>> [Accessed 3 July 2022].
- cie, n.d. *What is Access control?*. [online] Available at: <<https://cie-group.com/how-to-av/videos-and-blogs/access-control-systems>> [Accessed 20 June 2022].

Current Technologies, 2021. *The evolution of Access Control*. [online] Available at <<https://www.getcurrent.net/blog/the-evolution-of-access-control>> [Accessed 20 June 2022].

ElectronicWings, 2019. *Raspberry Pi Introduction*. [online]. Available at: <<https://www.electronicwings.com/raspberry-pi/raspberry-pi-introduction>> [Accessed 6 July 2022].

EPS Security, 2020. *Unlocking door security: A quick history of the lock, key, and modern day access control systems*. [online] Available at <<https://www.epssecurity.com/news/business-security/unlocking-door-security-a-quick-history-of-the-lock-key-and-modern-day-access-control-systems/#:~:text=The%20first%20%E2%80%9Caccess%20control%E2%80%9D%20device%3A%20the%20door%20lock&text=Archaeologists%20have%20discovered%20primitive%20locks,more%20familiar%20to%20modern%20eyes>> [Accessed 20 June 2022].

IMPINJ, n.d. *Types of RFID Systems*. [online] Available at: <<https://www.impinj.com/products/technology/how-can-rfid-systems-be-categorized>> [Accessed 23 August 2022].

Jayant, 2016. *Arduino vs Raspberry Pi: Difference between the two*. [online]. Available at: <<https://circuitdigest.com/article/arduino-vs-raspberryp-pi-difference-between-the-two#:~:text=Raspberry%20Pi%20is%2040%20times,for%20most%20of%20the%20functions>> [Accessed 8 July 2022].

Joseph, J., 2022. *Types of Arduino Boards – Quick Comparison on Specification and Features*. [online] Available at: <<https://circuitdigest.com/article/different-types-of-arduino-boards>> [Accessed 3 July 2022].

Joseph, J., 2022. *Types of Arduino Boards – Quick Comparison on Specification and Features*. [electronic print] Available at: <<https://circuitdigest.com/article/different-types-of-arduino-boards>> [Accessed 4 July 2022].

kynix, 2018. *RFID Technology: A Brief Introduction*. [electronic print] Available at: <https://www.kynix.com/Blog/Basic-Introduction-and-Future-Development-Trend-Analysis-of-RFID-Technology.html?utm_source=google&utm_medium=cpc&utm_campaign=D-T-0815&utm_term=&adgroupid=140141246316&gclid=CjwKCAjwmJeYBhAwEiwAXlg0AXpw6jBjSEevhXKwPwzPYx8dW--0Cfe2T68uuy9wH11ciZ4nQnguxoC_4cQAvD_BwE#ii-structure-of-rfid-system> [Accessed 30 August 2022].

kynix, 2018. *RFID Technology: A Brief Introduction*. [online] Available at: <https://www.kynix.com/Blog/Basic-Introduction-and-Future-Development-Trend-Analysis-of-RFID-Technology.html?utm_source=google&utm_medium=cpc&utm_campaign=D-T-0815&utm_term=&adgroupid=140141246316&gclid=CjwKCAjwmJeYBhAwEiwAXlg0AXpw6jBjSEevhXKwPwzPYx8dW--0Cfe2T68uuy9wH11ciZ4nQnguxoC_4cQAvD_BwE#ii-structure-of-rfid-system> [Accessed 20 August 2022].

Last Minute ENGINEERS, 2022. *Control DC Motors with L293D Motor Driver IC & Arduino*. [online] Available at: <<https://lastminuteengineers.com/l293d-dc-motor-arduino-tutorial/>> [Accessed 17 March 2023].

Last Minute ENGINEERS, 2022. *Control DC Motors with L293D Motor Driver IC & Arduino*. [electronic print] Available at: <<https://lastminuteengineers.com/l293d-dc-motor-arduino-tutorial/>> [Accessed 17 March 2023].

Last Minute ENGINEERS, 2022. *Interface 4x3 & 4x4 Membrane Keypad with Arduino*. [online] Available at: <<https://lastminuteengineers.com/arduino-keypad-tutorial/#:~:text=known%20as%20Multiplexing,-.How%20Does%20the%20Matrix%20Keypad%20Work%3F,4%20%2B%203%20%3D%207%20pins>> [Accessed 17 March 2023].

MAG, 2021. *FR300 Face Recognition Reader*. [online] Available at: <https://magnet.com.my/wp-content/uploads/download-center/MAG_FR300_Face-Recognition-Reader_Specification-Sheet.pdf> [Accessed 12 July 2022].

MAG, 2022. *Introduction who are we*. [online] Available at: <<https://magnet.com.my/about-us/introduction/?nowprocket=1>> [Accessed 11 July 2022].

MAG, 2022. *Touchless Access Enjoy the convenient of handsfree*. [electronic print] Available at: <<https://magnet.com.my/solution/touchless-access/>> [Accessed 30 August 2022].

MAG, 2022. *Touchless Access Enjoy the convenient of handsfree*. [online] Available at: <<https://magnet.com.my/solution/touchless-access/>> [Accessed 12 July 2022].

Maker.io., 2018. *Raspberry Pi Comparison: Which Pi is Right for My Application*. *Digi-Key Electronics*, [blog] 5 February. Available at: <<https://www.digikey.my/en/maker/blogs/2018/how-to-pick-the-right-raspberry-pi>> [Accessed 8 July 2022].

Mohahan, V., 2022. *How to Create Your First Iot Project – Arduino Cloud Tutorial with Arduino Nano 33 Iot*. [online] Available at: <https://circuitstate.com/tutorials/how-to-create-your-first-iot-project-arduino-cloud-tutorial-with-arduino-nano-33-iot/#What_is_Arduino_IoT_Cloud> [Accessed 13 August 2022].

- Mohahan, V., 2022. *How to Create Your First Iot Project – Arduino Cloud Tutorial with Arduino Nano 33 Iot*. [electronic print] Available at: <[https://circuitstate.com/tutorials/how-to-create-your-first-iot-project-arduino-cloud-tutorial-with-arduino-nano-33-iot/#What is Arduino IoT Cloud](https://circuitstate.com/tutorials/how-to-create-your-first-iot-project-arduino-cloud-tutorial-with-arduino-nano-33-iot/#What%20is%20Arduino%20IoT%20Cloud)> [Accessed 13 August 2022].
- Natasha, S. B. M. Z. 2012. *Door access System-Arduino Based*. Degree. Universiti Teknologi Petronas.
- Newman, R. M., 2010. *Security and Access Control Using Biometric Technologies*. Boston: Course Technology Cengage Learning, Australia.
- prajwalsn, 2022. *RFID and Password Based Door Lock System*. [online] Available at: <<https://create.arduino.cc/projecthub/prajwalsn/rfid-and-password-based-door-lock-system-b04915>> [Accessed 15 July 2022].
- Project Hub, n.d. *Arduino Iot Cloud*. [online] Available at: <<https://create.arduino.cc/projecthub/products/arduino-iot-cloud?page=2>> [Accessed 13 August 2022].
- Proto Supplies, 2023. *L293D Dual H-Bridge Motor Driver*. [electronic print] Available at: <<https://protosupplies.com/product/l293d/>> [Accessed 17 March 2023].
- RANDOM NERD TUTORIALS, 2019. *Monitor Your Door Using Magnetic Reed Switch and Arduino*. [electronic print] Available at: <<https://randomnerdtutorials.com/monitor-your-door-using-magnetic-reed-switch-and-arduino/>> [Accessed 25 March 2023].
- RANDOM NERD TUTORIALS, 2020. *ESP32-CAM Video Streaming and Face Recognition with Arduino IDE*. [online] Available at: <<https://randomnerdtutorials.com/esp32-cam-video-streaming-face-recognition-arduino-ide/>> [Accessed 25 March 2023].
- Rascagneres, P., 2020. *Fingerprint cloning: Myth or reality*. [electronic print] Available at: <<https://blog.talosintelligence.com/2020/04/fingerprint-research.html>> [Accessed 17 August 2022].
- Rathnayake, P., 2021. *Interfacing 4x4 Matrix Keypad with PIC16F877A using MM74C922 Encoder*. [electronic print] Available at: <<https://pabasararathnayake.medium.com/interfacing-4x4-matrix-keypad-with-pic16f877a-using-mm74c922-encoder-42e7809e797a>> [Accessed 17 March 2023].
- Santos, S., 2021. *ESP32 vs ESP8266- Pros and Cons*. [electronic print] Available at: <<https://makeradvisor.com/esp32-vs-esp8266/>> [Accessed 30 August 2022].
- Santos, S., 2021. *ESP32 vs ESP8266- Pros and Cons*. [online] Available at: <<https://makeradvisor.com/esp32-vs-esp8266/>> [Accessed 9 July 2022].

- Soderby, K., 2022. *Getting Started With the Arduino iot Cloud*. [online] Available at: <<https://docs.arduino.cc/arduino-cloud/getting-started/iot-cloud-getting-started#esp32--esp8266>> [Accessed 13 August 2022].
- Teja, R., 2021. *Getting Started with ESP32/ Introduction to ESP32*. [online] Available at: <<https://www.electronicshub.org/getting-started-with-esp32/>> [Accessed 8 July 2022].
- The Engineering Knowledge, 2023. *Introduction to Arduino Mega 2560: 5 Features You Need to Know*. [electronic print] Available at:<<https://www.theengineeringknowledge.com/arduino-mega-2560-5-features-you-need-to-know/>> [Accessed 17 April 2023].
- Triggs, R., 2022. How fingerprint scanners work: Optical, capacitive, and ultrasonic explained. [online] Available at: <<https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>> [Accessed 16 August 2022].
- Triggs, R., 2022. How fingerprint scanners work: Optical, capacitive, and ultrasonic explained. [electronic print] Available at: <<https://www.androidauthority.com/how-fingerprint-scanners-work-670934/>> [Accessed 30 August 2022].
- Tutorialspoint, n.d. *System Analysis and Design – Overview*. [online] Available at: <<https://www.tutorialspoint.com/system-analysis-and-design/system-analysis-and-design-overview.htm>> [Accessed 11 April 2023].
- tuya, n.d. *iLockey Smart Lock with Camera Door bell iLockey Newest Fingerprint Door Lock with Camera Wi-Fi*. [electronic print] Available at: <<https://expo.tuya.com/product/1024020>> [Accessed 13 April 2023].
- VANMA, 2022. *Vanma Electronic Padlock*. [electronic print] Available at: <<https://www.lockmanage.com/product/electronic-padlock/vanma-electronic-padlock-wm2000c/>> [Accessed 30 August 2022].
- Vanma, 2022. *What is Vanma lock*. [online] Available at: <<https://www.lockmanage.com/vanma-lock/?gclid=CjwKCAjw2rmWBhB4EiwAiJ0mtYwVVisM69T7kEU42fbntp5TA6gDKFIjDkIocidf4zi95O1p15QgOBoCQZQQA vD BwE>> [Accessed 11 July 2022].
- Wu, E., 2020. *Comparing Raspberry Pi Compute Module 4(CM4) and Cm3+, What has been changed from Cm3+*. [electronic print] Available at: <<https://www.seeedstudio.com/blog/2020/10/30/comparing-raspberry-pi-compute-module-4cm4-and-cm3-what-has-been-changed-from-cm3/>> [Accessed 30 August 2022].

APPENDICES

APPENDIX A: Code of Smart Door Access System

```
#include <SPI.h>
#include <MFRC522.h>
#define RST_PIN 49 // reset pin of Rc522 scanner
#define SS_PIN 53 // ss pin of Rc522 scanner
MFRC522 mfrc522(SS_PIN, RST_PIN);
String MasterTag = "C3734EAD"; // REPLACE this Tag ID with your Tag ID!!!
String tagID = ""; // store card I during operation
int wrong_Counter=0; // Counter use to count wrong RFID scan
int N=2; // Number of times can be wrong for RFID scanner
byte readCard[4];

int halt; // use to save data from integer V1
int a; // counter for halt feature

int greenLed = 7; // pin connect to green led
int redLed = 6; // pin connect to red led
int buzzer = 5; // pin connect to buzzer
int blueLed = 4; // pin connect to blue led

int lockPin = 31; // pin connect to L293D to control solenoid lock

int innerSwitch = 25; // pin connect to internal switch
```

```

int innerSignal; // data use to store digitalRead of innerSwitch

int magnet = 23; // pin connect to magnetic switch sensor
int magnetData; // use to store data from magnet sensor
int counter; // counter use to for magnetic switch sensor

boolean magnet_status = false; // status for magnetic sensor
boolean rfid_status = true; // status for rfid scanner

int cam_trigger = 28; // digital pin use to trigger esp32 cam

#include <Wire.h>
#include <Keypad.h>
const byte rows=4; // define how many rows for keypad
const byte cols=4; // define how many column for keypad
char hexakeys[rows][cols]= // define array to represent keys on keypad
{
  {'1','2','3','A'},
  {'4','5','6','B'},
  {'7','8','9','C'},
  {'*','0','#','D'}
};

byte rowpins[rows] = {41,43,45,47}; // row1, row2, row3, row4,
byte columnpins[cols] = {33,35,37,39}; // column1, column2, column3, column4,
Keypad
mykeypad=Keypad(makeKeymap(hexakeys),rowpins,columnpins,rows,cols); // give
mykeypad as name for 4x4 keypad
#define Password_length 8 // length for password n+1
char pwd_keyIn[Password_length]; // use to store password key in from keypad
char pwd_master[Password_length] = "12345AB"; // correct password use for
comparison
byte pwd_counter = 0; // counter for keypad

```

```

char customkey; // use to hold hold key input
int wrong_keypadCounter = 0; // counter use to calculate amount of wrong inputs
int M = 2; // Number of times can be wrong for 4x4 keypad

#include <ESP8266_Lib.h>
#include <BlynkSimpleShieldEsp8266.h>
#define BLYNK_PRINT Serial
#define BLYNK_TEMPLATE_ID "TMPLNASH3cQI" // template ID from Blynk
char auth[] = "F20zgO7f1TJB6xql7TtulTQJG1jIH-jG"; // auth token from Blynk
char ssid[] = "lkt";// Your WiFi credentials.
char pass[] = "123456789";// Set password to "" for open networks.
#define EspSerial Serial1 // Hardware Serial on Mega, by changing the number at
Serial1 to 2 or 3 can change the UART port
#define ESP8266_BAUD 9600
ESP8266 wifi(&EspSerial);

////////////////////////////////////
BLYNK_WRITE(V0) // function mobile application
{
  int pinValue = param.asInt();
  if (pinValue == 1)
  {
    unlock();
    magnetData=digitalRead(magnet);
    delay(100);
    while(magnetData == 1)
    {
      start_counting();
      magnetData = digitalRead(magnet);
    }
  }
}
////////////////////////////////////

```



```
BLYNK_WRITE(V1) // function for halt feature
{
  halt = param.asInt();
  while(halt ==1 && a<10)
  {
    digitalWrite(blueLed,halt);
    a=a+1;
    Serial.print(a);
    delay(1000);
  }
  a=0;
  digitalWrite(blueLed,LOW);
}
////////////////////////////////////
void setup()
{
  SPI.begin(); // SPI bus
  mfrc522.PCD_Init(); // MFRC522

  Serial.begin(9600);
  pinMode(redLed,OUTPUT);
  pinMode(greenLed,OUTPUT);
  pinMode(buzzer,OUTPUT);
  pinMode(blueLed,OUTPUT);

  pinMode(lockPin,OUTPUT);

  pinMode(innerSwitch,OUTPUT);
  digitalWrite(innerSwitch,HIGH);

  pinMode(magnet,OUTPUT);
  digitalWrite(magnet,HIGH);
}
```

```

EspSerial.begin(ESP8266_BAUD);
delay(10);
Blynk.begin(auth, wifi, ssid, pass);

pinMode(cam_trigger,OUTPUT);
}/// for void setup

void loop()
{
////////////////////////////////////
innerSignal=digitalRead(innerSwitch); // read internal switch signal
if(innerSignal == 0)
{
unlock();
magnetData=digitalRead(magnet);
delay(100);
while(magnetData == 1)
{
start_counting();
magnetData = digitalRead(magnet);
}
}
////////////////////////////////////

magnetData=digitalRead(magnet); // read magnetic switch sensor signal
if(magnetData ==1 && rfid_status == true && magnet_status == false)
{
digitalWrite(buzzer,HIGH);
Blynk.logEvent("intruder", "Your Door Get Break In!!!");
}
if(magnetData==0) // magnet at the side will produce signal 0
{
digitalWrite(buzzer,LOW);
counter=0;
}
}

```

```
    }  
    //////////////////////////////////////  
    if(rfid_status == true) // scan card here  
    magnet_status= false;  
    {  
    while (getID())  
    {  
    if (tagID == MasterTag)  
    {  
    accessSign();  
    wrong_Counter=0;  
    rfid_status=false;  
    }  
    else  
    {  
    wrong_Counter=wrong_Counter+1;  
    deniedSign();  
    if(wrong_Counter == N)  
    {  
    Blynk.logEvent("rfid", "Scan wrong card twice!");  
    digitalWrite(cam_trigger,HIGH);  
    delay(1000);  
    digitalWrite(cam_trigger,LOW);  
    warning();  
    wrong_Counter=0;  
    }  
    }  
    delay(200);  
    } //for while loop  
    }  
    //////////////////////////////////////  
    if(rfid_status==false)// key in password here  
    {
```

```
customkey= mykeypad.getKey();
if(customkey)
{
  pwd_keyIn[pwd_counter]=customkey;
  pwd_counter++;
}
if(pwd_counter == Password_length-1)
{
  if(!strcmp(pwd_keyIn,pwd_master))
  {
    accessSign();
    wrong_keypadCounter=0;
    unlock();
    magnetData=digitalRead(magnet);
    delay(100);
    while(magnetData == 1)
    {
      start_counting();
      magnetData = digitalRead(magnet);
    }
    rfid_status=true;
  }
  else
  {
    wrong_keypadCounter=wrong_keypadCounter+1;
    deniedSign();
    rfid_status=true;
    magnet_status=true;
    if(wrong_keypadCounter == M)
    {
      Blynk.logEvent("key", "Enter wrong password twice!");
      digitalWrite(cam_trigger,HIGH);
      delay(400);
    }
  }
}
```

```

    digitalWrite(cam_trigger,LOW);
    warning();
    wrong_keypadCounter=0;
  }
}
clearData();
}

if(customkey == '#')
{
  clearData();
}
}/// for (rfid_status == false)
  Blynk.run();

}/// for (void loop)

////////////////////////////////////
boolean getID() // function to read new tag if available
{
  // Getting ready for Reading PICCs
  if ( ! mfrc522.PICC_IsNewCardPresent())
  { //If a new PICC placed to RFID reader continue
    return false;
  }
  if ( ! mfrc522.PICC_ReadCardSerial())
  { //Since a PICC placed get Serial and continue
    return false;
  }
  tagID = "";
  for ( uint8_t i = 0; i < 4; i++)
  { // The MIFARE PICCs that we use have 4 byte UID
    //readCard[i] = mfrc522.uid.uidByte[i];

```

```

tagID.concat(String(mfrc522.uid.uidByte[i], HEX)); // Adds the 4 bytes in a single
String variable
}
tagID.toUpperCase();
mfrc522.PICC_HaltA(); // Stop reading
return true;
}
/////////////////////////////////////////////////////////////////
void warning()// function use to show warning sign if scanning or key in wrong
password more than N times
{
digitalWrite(buzzer,LOW);
delay(300);
digitalWrite(redLed,HIGH);
digitalWrite(buzzer,HIGH);
delay(1500);
digitalWrite(redLed,LOW);
digitalWrite(buzzer,LOW);
}
/////////////////////////////////////////////////////////////////
void unlock()// function use to control L293D
{
digitalWrite(lockPin,HIGH);
delay(2000);
digitalWrite(lockPin,LOW);
}
/////////////////////////////////////////////////////////////////
void accessSign() // function use to give LED signal that represent access is success
{
digitalWrite(greenLed,HIGH);
for(int a=0;a<2;a++)
{
digitalWrite(buzzer,HIGH);

```


APPENDIX B: Code of Camera Unit

```
/* == Including the libraries */
#include "esp_camera.h"
#include "SPI.h"
#include "driver/rtc_io.h"
#include "ESP32_MailClient.h"
#include <FS.h>
#include <SPIFFS.h>
#include <WiFi.h>
#define emailSenderAccount    "lktFYPSender@gmail.com"
#define emailSenderAppPassword "aapsyvhoneohufdlh"
#define smtpServer            "smtp.gmail.com"
#define smtpServerPort        465
#define emailSubject           "Smart Door Access System_EVIDENCE"
#define emailRecipient         "leekartien2000@gmail.com"
/* = Defining the Camera Model and GPIO */
#define CAMERA_MODEL_AI_THINKER
#if defined(CAMERA_MODEL_AI_THINKER)
    #define PWDN_GPIO_NUM    32
    #define RESET_GPIO_NUM  -1
    #define XCLK_GPIO_NUM    0
    #define SIOD_GPIO_NUM    26
    #define SIOC_GPIO_NUM    27

    #define Y9_GPIO_NUM       35
    #define Y8_GPIO_NUM       34
    #define Y7_GPIO_NUM       39
    #define Y6_GPIO_NUM       36
    #define Y5_GPIO_NUM       21
```

```

#define Y4_GPIO_NUM    19
#define Y3_GPIO_NUM    18
#define Y2_GPIO_NUM    5
#define VSYNC_GPIO_NUM 25
#define HREF_GPIO_NUM  23
#define PCLK_GPIO_NUM  22
#else
  #error "Camera model not selected"
#endif

#define FILE_PHOTO "/photo.jpg" //--> Photo File Name to save in SPIFFS

#define pin_Pir 12 //--> PIR Motion Detector PIN
#define pin_Led 4 //--> On-Board LED FLash

/* ===== Variables for network */
// REPLACE WITH YOUR NETWORK CREDENTIALS
const char* ssid = "lkt";
const char* password = "123456789";

SMTPData smtpData; //--> The Email Sending data object contains config and data
to send

/* _Subroutine to turn on or off the LED Flash */
void LEDFlashState(bool state) {
  digitalWrite(pin_Led, state);
}

/* __ Subroutine for LED Flash blinking */
// Example :
// LEDFlashBlink(2, 250); --> blinks 2 times with a delay of 250 milliseconds.
void LEDFlashBlink(int blink_count, int time_delay) {
  digitalWrite(pin_Led, LOW);
  for(int i = 1; i <= blink_count*2; i++) {

```

```

digitalWrite(pin_Led, !digitalRead(pin_Led));
delay(time_delay);
}
}
bool PIR_State() {
    bool PRS = digitalRead(pin_Pir);
    return PRS;
}

/* _ Function to check if photos are saved correctly in SPIFFS */
bool checkPhoto(fs::FS &fs) {
    File f_pic = fs.open(FILE_PHOTO);
    unsigned int pic_sz = f_pic.size();
    Serial.printf("File name: %s | size: %d\n", FILE_PHOTO, pic_sz);
    return (pic_sz > 100);
    f_pic.close();
}

/* _ Subroutine for formatting SPIFFS */
// This subroutine is used in case of failure to write or save the image file to SPIFFS.
void SPIFFS_format() {
    bool formatted = SPIFFS.format();
    Serial.println();
    Serial.println("Format SPIFFS...");
    if(formatted){
        Serial.println("\n\nSuccess formatting");
    }else{
        Serial.println("\n\nError formatting");
    }
    Serial.println();
}

/* _ Subroutine for Capture Photo and Save it to SPIFFS */

```

```

void capturePhotoSaveSpiffs( void ) {
    camera_fb_t * fb = NULL; //--> pointer
    bool Status_save_photo = 0; //--> Boolean indicating if the picture has been taken
correctly

    /* - Take a photo with the camera */
    Serial.println();
    Serial.println("Taking a photo...");
    do {
        LEDFlashState(true);
        delay(2000);
        fb = esp_camera_fb_get();
        if (!fb) {
            Serial.println("Camera capture failed.");
            Serial.println("Carry out the re-capture process...");
        }
        LEDFlashState(false);
    } while ( !fb );
    Serial.println("Take photo successfully.");

    /* -Save photos to SPIFFS */
    do {
        LEDFlashBlink(0,250); //--> The LED Flash blinks 2 times with a duration of 250
milliseconds, which means it starts the process of saving photos to SPIFFS.

        /* : Photo file name */
        Serial.printf("Picture file name: %s\n", FILE_PHOTO);
        File file = SPIFFS.open(FILE_PHOTO, FILE_WRITE);

        /* : Insert the data in the photo file */
        if (!file) {
            Serial.println("Failed to open file in writing mode.");
            SPIFFS_format();

```

```

    capturePhotoSaveSpiffs();
    return;
}
else {
    file.write(fb->buf, fb->len); // payload (image), payload length
    Serial.print("The picture has been saved in ");
    Serial.print(FILE_PHOTO);
    Serial.print(" - Size: ");
    Serial.print(file.size());
    Serial.println(" bytes.");
}

file.close(); //--> Close the file

/* :check if file has been correctly saved in SPIFFS */
Serial.println("Checking if the picture file has been saved correctly in SPIFFS...");
Status_save_photo = checkPhoto(SPIFFS);
if (Status_save_photo == 1) {
    Serial.println("The picture file has been saved correctly in SPIFFS.");
} else {
    Serial.println("The picture file is not saved correctly in SPIFFS.");
    Serial.println("Carry out the re-save process...");
    Serial.println();
}

} while (!Status_save_photo);

esp_camera_fb_return(fb); //--> return the frame buffer back to the driver for reuse.
LEDFlashBlink(0,1000); //--> The LED Flash flashes once with a duration of 1
second, which means that the process of capturing photos and saving photos to
SPIFFS has been completed.
}

```

```
/* _ Subroutine to get the Email sending status */
// Callback function to get the Email sending status
void sendCallback(SendStatus msg) {
  Serial.println(msg.info()); //--> Print the current status
}

/* _ Subroutine for send photos via Email */
void sendPhoto( void ) {
  LEDFlashBlink(0,250); //--> The LED Flash blinks 3 times with a duration per 250
  milliseconds, which means it starts the process of sending photos via email.
  Serial.println("Sending email...");

  // Set the SMTP Server Email host, port, account and password
  smtpData.setLogin(smtpServer, smtpServerPort, emailSenderAccount,
  emailSenderAppPassword);

  // Set the sender name and Email
  smtpData.setSender("ESP32 Security System", emailSenderAccount);

  // Set Email priority or importance High, Normal, Low or 1 to 5 (1 is highest)
  smtpData.setPriority("High");

  // Set the subject
  smtpData.setSubject(emailSubject);

  // Set the email message in HTML format
  smtpData.setMessage("<h2>Photo captured with ESP32-CAM and attached in this
  email.</h2>", true);

  // Set the email message in text format
  //smtpData.setMessage("Photo captured with ESP32-CAM and attached in this
  email.", false);

  // Add recipients, can add more than one recipient
```

```

smtpData.addRecipient(emailRecipient);
//smtpData.addRecipient(emailRecipient2);

// Add attach files from SPIFFS
smtpData.addAttachFile(FILE_PHOTO, "image/jpg");

// Set the storage type to attach files in your email (SPIFFS)
smtpData.setFileStorageType(MailClientStorageType::SPIFFS);

// sendCallback
smtpData.setSendCallback(sendCallback);

// Start sending Email, can be set callback function to track the status
if (!MailClient.sendMail(smtpData))
Serial.println("Error sending Email, " + MailClient.smtpErrorReason());

// Clear all data from Email object to free memory
smtpData.empty();

// The LED Flash flashes 1 time with a duration per 1 second,
// which means that the process of sending photos via email has been completed
(regardless of whether the photo was successfully sent or not).
LEDFlashBlink(1,1000);
delay(2000);
}

/* _VOID SETUP() */
void setup() {
// put your setup code here, to run once:
WRITE_PERI_REG(RTC_CNTL_BROWN_OUT_REG, 0); //--> disable
brownout detector

Serial.begin(115200);

```

```

Serial.println();

pinMode(pin_Pir, INPUT);
pinMode(pin_Led, OUTPUT);
LEDFlashBlink(0, 250); //--> The LED Flash blinks 2 times with a duration per 250
milliseconds, which means the process to stabilize the PIR sensor is started.
Serial.println("Wait 60 seconds for the PIR sensor to stabilize.");
Serial.println("Count down :");
for(int i = 5; i > -1; i--) {
  Serial.print(i);
  Serial.println(" second");
  delay(1000);
}
Serial.println("The time to stabilize the PIR sensor is complete.");
Serial.println();

/* ----- Connect to Wi-Fi */
WiFi.begin(ssid, password);
Serial.print("Connecting to WiFi...");
while (WiFi.status() != WL_CONNECTED) {
  LEDFlashBlink(4,250);
  Serial.print(".");
}
LEDFlashState(false);
Serial.println();
Serial.print("Successfully connected to ");
Serial.println(ssid);

/* ----- Print ESP32 Local IP Address */
Serial.print("IP Address: http://");
Serial.println(WiFi.localIP());
Serial.println();

```



```
/* ----- Starting to mount SPIFFS */
Serial.println("Starting to mount SPIFFS...");
if (!SPIFFS.begin(true)) {
  Serial.println("An Error has occurred while mounting SPIFFS");
  Serial.println("ESP32 Cam Restart...");
  ESP.restart();
}
else {
  Serial.println("SPIFFS mounted successfully");
}

/* ----- Camera configuration. */
camera_config_t config;
config.ledc_channel = LEDC_CHANNEL_0;
config.ledc_timer = LEDC_TIMER_0;
config.pin_d0 = Y2_GPIO_NUM;
config.pin_d1 = Y3_GPIO_NUM;
config.pin_d2 = Y4_GPIO_NUM;
config.pin_d3 = Y5_GPIO_NUM;
config.pin_d4 = Y6_GPIO_NUM;
config.pin_d5 = Y7_GPIO_NUM;
config.pin_d6 = Y8_GPIO_NUM;
config.pin_d7 = Y9_GPIO_NUM;
config.pin_xclk = XCLK_GPIO_NUM;
config.pin_pclk = PCLK_GPIO_NUM;
config.pin_vsync = VSYNC_GPIO_NUM;
config.pin_href = HREF_GPIO_NUM;
config.pin_sscb_sda = SIOD_GPIO_NUM;
config.pin_sscb_scl = SIOC_GPIO_NUM;
config.pin_pwdn = PWDN_GPIO_NUM;
config.pin_reset = RESET_GPIO_NUM;
config.xclk_freq_hz = 20000000;
config.pixel_format = PIXFORMAT_JPEG;
```

```

if(psramFound()){
  config.frame_size = FRAMESIZE_UXGA; //--> FRAMESIZE_ +
QVGA|CIF|VGA|SVGA|XGA|SXGA|UXGA
  config.jpeg_quality = 20;
  config.fb_count = 2;
} else {
  config.frame_size = FRAMESIZE_SVGA;
  config.jpeg_quality = 12;
  config.fb_count = 1;
}

/* ----- Initialize camera */
Serial.println();
Serial.println("Camera initialization...");
esp_err_t err = esp_camera_init(&config);
if (err != ESP_OK) {
  Serial.printf("Camera init failed with error 0x%x", err);
  Serial.println("ESP32 Cam Restart...");
  ESP.restart();
}
Serial.print("Camera initialization was successful.");
Serial.println();

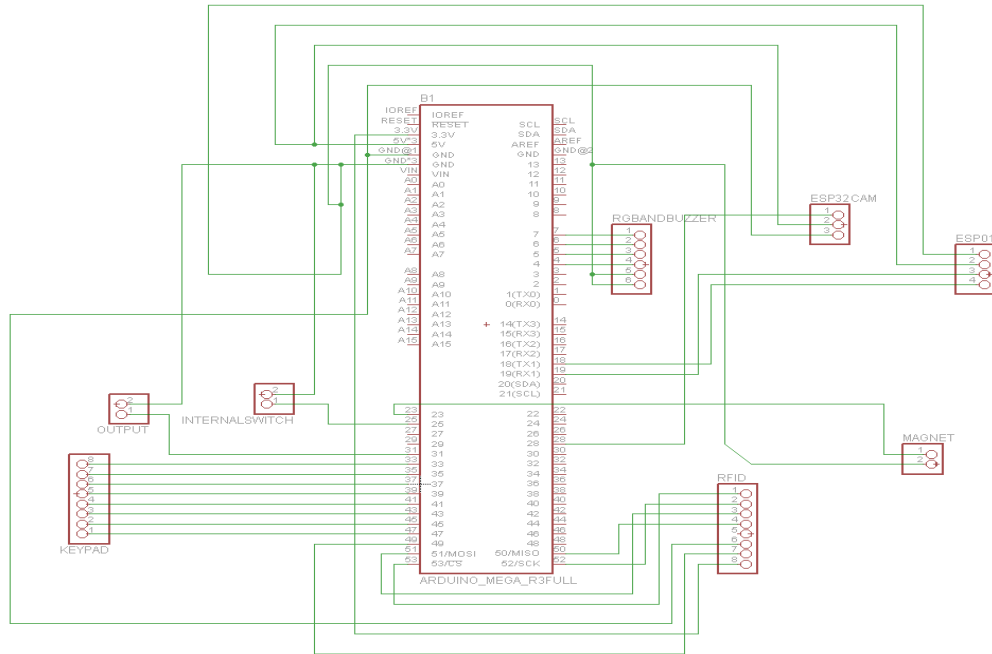
  LEDFlashBlink(2, 1000); //--> The LED Flash blinks 2 times with a duration per 1
second, which means the Setup process is complete.
}

/* _ VOID LOOP() */
void loop() {
  if(PIR_State() == 1) {
    capturePhotoSaveSpiffs(); //--> Calling the capturePhotoSaveSpiffs() subroutine.
    sendPhoto(); //--> Calling the sendPhoto() subroutine.
  }
}

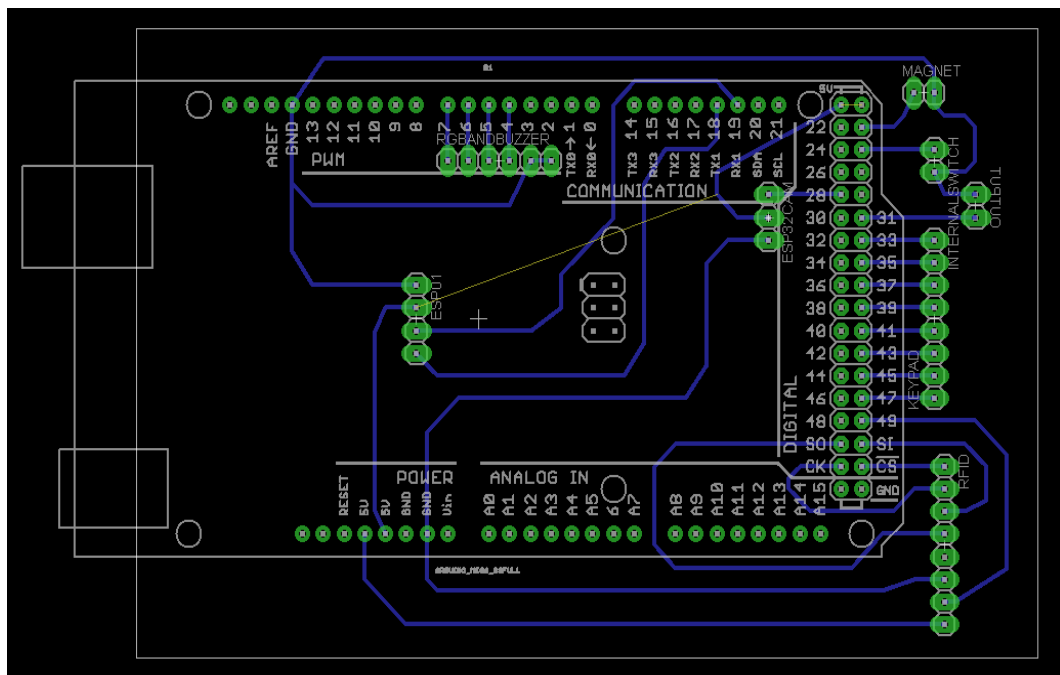
```

```
}  
  delay(1);  
}
```

APPENDIX C: Printed Circuit Board of Central Control Unit

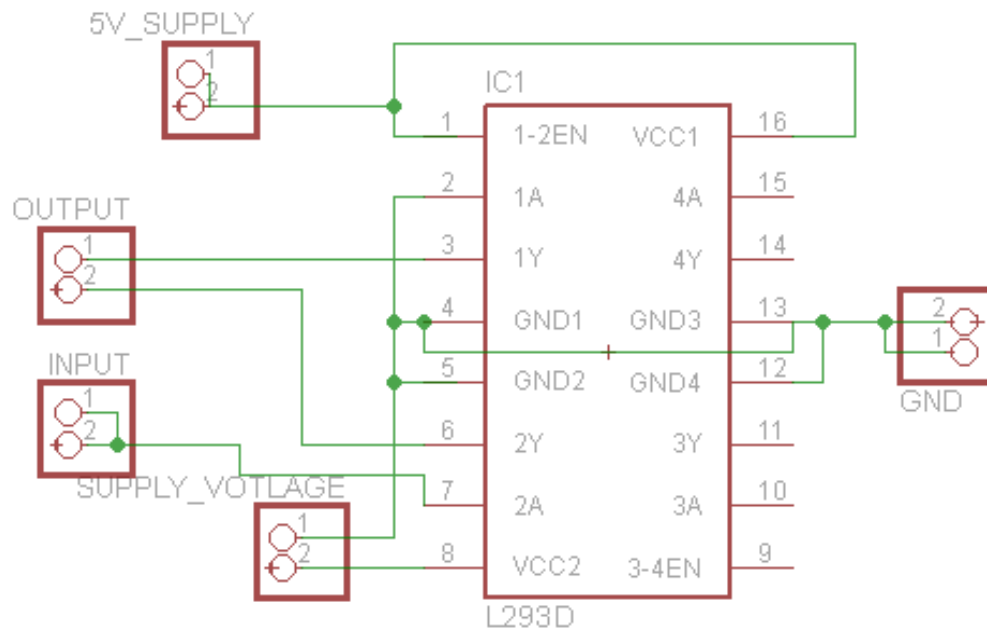


Schematic Diagram of Central Control Unit

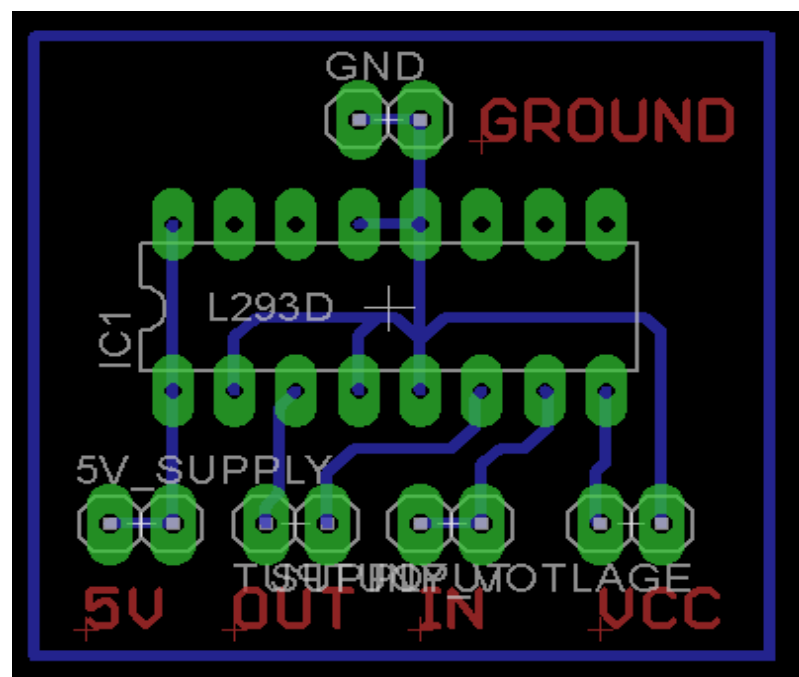


Layout Diagram of Central Control Unit

APPENDIX D: Printed Circuit Board of Lock Driver



Schematic Diagram of Lock Driver



Layout Diagram of Lock Driver