



Faculty of Electrical and Electronic Engineering Technology



**DEVELOPMENT OF AN IOT BASED SMART DOOR SECURITY
SYSTEM WITH A BIOMETRIC SENSOR USING A
MICROCONTROLLER**

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

MUHAMMAD HAIQAL BIN SAIFUL NIZAM

**Bachelor of Electronics Engineering Technology (Industrial Electronics)
With Honors**

2023

DEVELOPMENT OF AN IOT BASED SMART DOOR SECURITY SYSTEM WITH A BIOMETRIC SENSOR USING A MICROCONTROLLER

MUHAMMAD HAIQAL BIN SAIFUL NIZAM

**A project report submitted
in partial fulfillment of the requirements for the degree of
Bachelor of Electronics Engineering Technology (Industrial Electronics) with Honours**



Faculty of Electrical and Electronic Engineering Technology

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I declare that this project report entitled “DEVELOPMENT OF AN IOT BASED SMART DOOR SECURITY SYSTEM WITH A BIOMETRIC SENSOR USING A MICROCONTROLLER” is the result of my own research except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature :



Student Name :

MUHAMMAD HAIQAL BIN SAIFUL NIZAM

Date :

13 JANUARY 2023

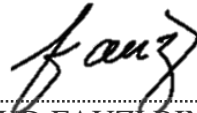


APPROVAL

I hereby declare that I have checked this project report and in my opinion, this project report is adequate in terms of scope and quality for the award of the degree of Bachelor of Electronics Engineering Technology (Industrial Electronics) with Honours.

Signature

:



Supervisor Name

:

IR. TS. DR. MOHD FAUZI BIN AB RAHMAN

Date

:

13 JANUARY 2023



DEDICATION

This thesis is dedicated to Saiful Nizam bin Ahmad and Norlily bte Mohd Nor, my beloved parents for their constant love, encouragement and inspiration. To my supervisor IR. TS. DR. Mohd Fauzi bin Ab Rahman who never giving up to taught and guide me to complete my project. To my helpful classmate and housemate who are always keep supporting me.



ABSTRACT

Security has always been a key concern in both the home and the workplace, and numerous measures have been implemented to solve the issue. Most main door lock security systems have many gaps that can be exploited to get access to desired locations, posing a threat to a secure lifestyle and a healthy working environment. Terrorism and unwanted access to places have also become serious issues in recent years, necessitating the implementation of a security system to prevent unauthorized access, particularly in shared access environments. This study presents a design and prototype of a biometric fingerprint-based door lock system that takes this into the report. Biometric technologies, such as fingerprints, give instruments for enforcing trustworthy system logs and safeguarding an individual's right to privacy. When RFID cards or passwords are shared or stolen, door lock mechanisms based on RFID or passwords can be readily infiltrated, necessitating the use of a biometric-based security system for facilities with shared access. Fingerprints of authorized users are enrolled and confirmed in the proposed system to grant access to a facility that is used by various users. User can also be deleted from the system, and a new user can be added. This project put in place a centralized control system that allows us to manage who has access to particular rooms and who doesn't.

ABSTRAK

Keselamatan sentiasa menjadi kebimbangan utama di rumah dan tempat kerja, dan pelbagai langkah telah dilaksanakan untuk menyelesaikan isu tersebut. Kebanyakan sistem keselamatan kunci pintu utama mempunyai banyak jurang yang boleh dieksploitasi untuk mendapatkan akses ke lokasi yang diingini, menimbulkan ancaman kepada gaya hidup yang selamat dan persekitaran kerja yang sihat. Keganasan dan akses yang tidak diingini ke tempat-tempat juga telah menjadi isu serius dalam beberapa tahun kebelakangan ini, yang memerlukan pelaksanaan sistem selamat untuk menghalang akses tanpa kebenaran, terutamanya dalam persekitaran akses dikongsi. Kajian ini membentangkan reka bentuk dan prototaip sistem kunci pintu berasaskan cap jari biometrik yang mengambil ini dalam laporan. Teknologi biometrik, seperti cap jari, memberikan instrumen untuk menguatkuasakan log sistem yang boleh dipercayai dan melindungi hak individu untuk privasi. Apabila kad atau kata laluan RFID dikongsi atau dicuri, mekanisme kunci pintu berdasarkan RFID atau kata laluan boleh dengan mudah menyusup, memerlukan penggunaan sistem keselamatan berasaskan biometrik untuk kemudahan dengan akses dikongsi. Cap jari pengguna yang dibenarkan didaftarkan dan disahkan dalam sistem yang dicadangkan untuk memberikan akses kepada kemudahan yang digunakan oleh pelbagai pengguna. Seorang pengguna juga boleh dipadamkan daripada sistem, dan pengguna baharu boleh ditambah. Kami telah menyediakan sistem kawalan berpusat yang membolehkan kami mengurus siapa yang mempunyai akses ke bilik tertentu dan siapa yang tidak. Ini ialah alat kerja yang fleksibel berdasarkan peranti Arduino UNO yang menggunakan teknologi penderia cap jari untuk memberikan keselamatan fizikal.

ACKNOWLEDGEMENTS

First and foremost, Alhamdulillah thanks Allah for giving me good health, spirit, patience, determination and blessing me far more than I deserve. Without Him, I would not be able to complete my dissertation in time.

Secondly, I would like to express my gratitude and appreciation to my supervisor, IR.TS.DR. MOHD FAUZI BIN AB RAHMAN for his guidance, support, encouragement, advise and most importantly for not giving up on me during the completion of this project.

Thirdly, I also would like to thank and express appreciation to my beloved parent and family for their love and prayer during the period of my study. Last but not least, to all staffs at the Universiti Teknikal Malaysia Melaka (UTeM), fellow colleagues and classmates, faculty members, as well as other individuals who are not listed here for being co-operative and helpful.



TABLE OF CONTENTS

ABSTRAK	i
ACKNOWLEDGEMENTS	iii
TABLE OF CONTENTS	iv
LIST OF TABLES	vi
LIST OF FIGURES	vii
LIST OF APPENDICES	ix
LIST OF SYMBOLS	7
LIST OF ABBREVIATIONS	8
CHAPTER 1 INTRODUCTION	9
1.1 Background	9
1.2 Problem Statement	11
1.3 Project Objective	11
1.4 Scope of Project	12
1.5 Contribution of Research	12
1.6 Thesis Outline	13
CHAPTER 2 LITERATURE REVIEW	14
2.1 Introduction	14
2.2 Literature Review	14
2.2.1 Door Security System For Home Monitoring Based On ESP32	14
2.2.2 Keypad/Bluetooth/GSM Based Digital Door Lock Security System	16
2.2.3 Automatic Door Lock System	17
2.2.4 IoT Security Applied on a Smart Door Lock Application	18
2.2.5 IoT Based Smart Home Security System With Alert and Door Access Control	21
2.2.6 IoT Enabled Door Lock System	23
2.2.7 Door Access and Security System Based on IoT	25
2.3 Summary	28
CHAPTER 3 METHODOLOGY	29
3.1 Introduction	29
3.2 Methodology	29
3.3 Flowchart of This Project	30
3.4 Block Diagram	31
3.5 Hardware Implementation	32
3.6 Software Implementation	33
3.6.1 Blynk Application	33
3.7 Gantt Chart	34

3.8	Summary	37
CHAPTER 4	RESULTS AND DISCUSSION	38
4.1	Introduction	38
4.2	Result of Developing Process	38
4.2.1	Circuit Construction	38
4.2.2	Hardware Design	39
4.2.3	Application Design	41
4.3	Data Analysis	43
4.3.1	Biometric Sensor Accuracy and Speed Reading	43
4.3.2	Wet and Dry	45
4.3.3	Clean and Dust Surface	46
4.4	Summary	48
CHAPTER 5	CONCLUSION AND FUTURE WORKS	49
5.1	Conclusion	49
5.2	Future Works	49
REFERENCE		50
APPENDICES		51



LIST OF TABLES

TABLE	TITLE	PAGE
Chapter 2		
Table 2.1:	Hardware Module	15
Table 2.2:	Comparison On Previous Project	27
Chapter 4		
Table 4.1:	Finger and Pressure Test Result	44
Table 4.2:	Wet and Dry Test	46
Table 4.3:	Clean and Dust Surface Test	47



LIST OF FIGURES

FIGURE	TITLE	PAGE
CHAPTER 2		
Figure 2.1 :	Architecture Design	15
Figure 2.2:	Block Diagram	17
Figure 2.3:	System Block Diagram	18
Figure 2.4:	Infrastructure of IoT Ecosystem	19
Figure 2.5:	Naïve Architechture of the Smart Door Lock	20
Figure 2.6 :	Block Diagram	22
Figure 2.7:	Block Diagram	23
Figure 2.8:	Block Diagram	24
CHAPTER 3		
Figure 3.1:	Flowchart of This Project	30
Figure 3.2:	Block Diagram of This Project	31
Figure 3.3:	Hardware Design	32
Figure 3.4:	Blynk Application	34
Figure 3.5:	Gantt Chart	36
CHAPTER 4		
Figure 4.1:	Overview of The Project Circuit	39
Figure 4.2:	Circuit Setup in An Electrical Box	40
Figure 4.3:	Hardware Design of The Project	40
Figure 4.4:	User Interface	41
Figure 4.5:	Automation Setup	42
Figure 4.6:	Name of The Finger	43

Figure 4.7: Example of The Fingerprint Pressure	44
Figure 4.8: The Speed of The Biometric Sensor Sense With Various Pressure	45
Figure 4.9: The Speed of The Biometric Sensor Sense With Wet and Dry Condition	46
Figure 4.10: The Speed of The Biometric Sensor Sense With Clean and Dust Surface	47



LIST OF APPENDICES

APPENDIX	TITLE	PAGE
	Appendix 1: Gantt Chart	50
	Appendix 2: Turnitin Result	53
	Appendix 3: Programme	60



LIST OF SYMBOLS

μV	Microvolts
α	Alpha
β	Beta
γ	Gamma
Δ	Delta
θ	Theta
Hz	Hertz
V	Volt
dB	Daubechies
ψ	Wavelet coefficients
τ	Tau
VCC	Voltage Common Collector
GND	Ground
RX	Receiver
TX	Transmitter
a	Scaling Parameter
b	Location of the Parameter
%	Percentage

LIST OF ABBREVIATIONS

IoT	Internet Of Thing
ID	Identification
GPI O	General Purpose Input/Output
PIR	Passive InfraRed
WIF I	Wireless Fidelity
LAN	Local Area Network
LED	Light Emitting Diode
GSM	Global System for Mobile Communications
SM S	Short Message Service
PIC	Peripheral Interface Controller
API	Application Programming Interface
LCD	Liquid Crystal Display
IC	Integrated Circuit
SD	Secure Digital
USB	Universal Serial Bus
GPS	Global Positioning System
CPU	Central Processing Unit
IDE	Integrated Development Environment
UA RT	Universal Asynchronous Receiver Transmitter
BLE	Bluetooth Low Energy
UI	User Interface

CHAPTER 1

INTRODUCTION

1.1 Background

Many firms have found that automated integration and permissions systems are crucial in preventing security risks. Everything is now linked to the system, and anybody may access data from anywhere on the earth. As a result, information hacking is a serious problem. Because of these risks, having some form of personal identification (ID) to access one's own personal information is essential. At various points throughout the guarded space, various methods are introduced to track the individual's movement and limit their access to sensitive zones. [1] Password and ID card approaches are the most often used standard individual ID systems. However, a secret password is now quite trivial to crack, and recognised Identification cards may be misplaced, making these approaches exceedingly questionable.[2]

Biometric authentication technology has long been used in a number of contexts as a dependable security solution. Fingerprints, eye iris, retinal, voice, and face recognition are all examples of biometric technology.[3] These diverse ways each have distinct focal points and downsides that must be considered while designing a biometric system, such as the system's unwavering quality, worth, adaptability, the demand for physical touch with the checking device, and many other factors. Fingerprints are one of several biometrics used to identify people and verify their identities. For more than a century, fingerprints have been used to help people adjust to the judicial system. When studying fingerprints for matching purposes, the correlation of a few highlights of the print pattern is necessary. Patterns are among them.

The Internet of Things (IoT) is a worldwide infrastructures that combines intelligent services with situational awareness and enables cross-network communication between things and between humans and intelligent things.[4] Machine to Machine communication differs from IoT in that a person is responsible for communicating on behalf of people rather than controlling the equipment or intelligent instruments directly.

In this project, efforts have been made to use biometric and Internet Of Things (IoT) formulas at a time to increase the safety and security of access to the entity's automatic sensing and verification of an accessible identity, as well as the automatic operation of action in the event of valid access. To gain access to the security system, a person must place his finger on the sensor and wait for his fingerprint to be validated. They can also use their smartphone or computer with an internet connection to lock or unlock the door lock system.[5].

1.2 Problem Statement

There are numerous occasions where a thief has broken into a home and the homeowner is unaware. Homeowners are unaware that someone has been standing in front of their door for some time, attempting to open it and break in. Aside from the usual manner, a keyed door can be easily opened by an unauthorized person or a burglar with the correct key. They will be able to steal everything valuable in the room or building. The primary motivation for constructing this project is to eliminate the use of the key when unlocking the door.

While a smart door locking system with a load sensor is built for homes, homeowners can feel secure about their home security even when they are not at home. This is because the door lock system will notify them if the system detects an unusual presence in front of the entrance. The homeowner can then open their smartphone, which is connected to the system, and watch the scenario. This is the benefit that IoT and smart phones provide to individuals.

1.3 Project Objective

The purpose of this project is as follows :

- a) To develop a smart door lock prototype and test its functionality.
- b) To analyze the smart door lock's effectiveness in terms of speed to accessing the door.
- c) To design a smart door lock security system based on the use of Internet Of Things (IoT) using microcontroller.

1.4 Scope of Project

This project's scope is as described in the following:

- a) Smart door lock security system prototype will be built and controlled through a smartphone and fingerprint sensor.
- b) To create a software and hardware work implementation.
- c) Only enrolled users are identified by the system when they use a biometric fingerprint. As a result, unauthorized users are allowed to access the premises via the application.
- d) Five fingers will be used in three type of pressure which is low pressure, medium and high pressure to test the speed of the biometric sensor read the fingerprint.
- e) The best two finger then will be test in two condition of sense which is in dry/wet and clean/dust surface of the biometric sensor.

1.5 Contribution of Research

This project's contributions are made in the following areas::

- i) For starters, it offers collision detection and alarm functions. This is to identify an intruder who tries to gain in by physically forcing the lock open.
- ii) It also has security and monitoring functions using IoT technologies.
- iii) This proposed system provides a low equipment cost and easy to configure. This system is also reliable and easy to use.
- iv) The system also prevents unauthorized user from use random finger since all the data will be recorded.
- v) Certain task can be performed by user without the needs of touching the fingerprint sensor and system.

1.6 Thesis Outline

Based on the previously mentioned objectives and the strategy offered, this report is divided into five (5) chapters, the contents of which are summarised below:

- Chapter 1. Introduction. This chapter discusses the study's background, research problems, objectives, scopes, contributions, and significance of the research.
- Chapter 2 . Literature review. This chapter begins with a summary of the application field of an IoT Based Smart Door Security System With a Biometric Sensor Using a Microcontroller. This chapter also goes through the features, characteristic and technologies used in this project.
- Chapter 3. Methodology. This chapter presents the methodology that is used in this project. This project's flow is demonstrated to effectively achieve the purpose.. In addition, the hardware used to construct the smart door security system is covered in the Hardware Development section, whilst the software and approach utilised in the recognition system is discussed in the Software Development section.
- Chapter 4. Result. The created models are tested in this chapter in real time for performance, accuracy, and security of the system.
- Chapter 5. Conclusion and future works. This chapter summarises the main conclusions and achievements of the research conducted in this study, along with future research directions.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The market is now inundated with door lock security solutions. These systems are studied in order to gather knowledge about the project that was built. Even if today's market systems are more complex and compatible with new technology, the notion must still be derived from a literature research. The literature review works assist in exposing and developing skills in finding information from a variety of sources. These abilities are critical for solving problems that have arisen or will arise in the future.

2.2 Literature Review

2.2.1 Door Security System For Home Monitoring Based on ESP32

A door is one of the first lines of defence in maintaining the house's physical security. A robber can quickly enter and take the contents of a house if the door can be easily opened. A door used to simply have a physical key to lock or unlock it, but as technology advanced, a more modern door was invented, particularly the digital door, which can lock or unlock doors without the use of a physical key.[6] When the house is unoccupied, however, the digital door can be smashed or damaged, and the inhabitants will only find out when they return home. To ensure the house's security, the occupants will always keep the door secured when leaving or entering the residence.[6] However, occasionally when leaving the house, the residents forget to lock the door or are unsure if they have closed the door or not.

Microcontroller ESP32, Arduino programming language, and an Android-based

mobile application are used to create the system. The ESP32 microcontroller is used to connect all of the electronic devices in one place.[7] Because ESP32 has two cores, one for running wifi functions and the other for executing uploaded programmes, it is utilised. A wifi and bluetooth module, as well as 36 GPIO, are included in the ESP32 . The memory on the ESP32 is quite huge. The ESP32 consumes low power and contains an inbuilt touch sensor, making it ideal for developing door security systems.[6] PIR sensors are used to detect motion, and a magnetic sensor is used to determine if the door is open or closed. The system design strategy for the proposed home security system is discussed in this section.

Table 2.1 : Hardware Module

No	Name	Description
1.	Adaptor	Adaptor to supply electricity 12V to system from stopkontak
2.	Step Down	Step Down to reduce voltage from 12V to 5V
3.	PCB Board	To connect all device
4.	ESP 32	Using Wemos LOLIN D32, 2.4 GHz Wi-Fi and Bluetooth combo chip. TSMC low power 40nm technology. ⁵
5.	Button Reset	Buton to reset ESP32
6.	PIR Sensor	PIR Sensor for movement detection
7.	LED	LED used as a power indicator and wifi indicator
8.	Magnetic Sensor	Magnetic Sensor to state the door status
9.	Internal Touch Sensor	To find out if the door is opened from inside
10.	Mosfet	Mosfet for automatic switches
11.	Alarm Buzzer	Alarm Buzzer to tinging when the door forced open
12.	Electric Strike	Electric Strike to lock or unlock the door

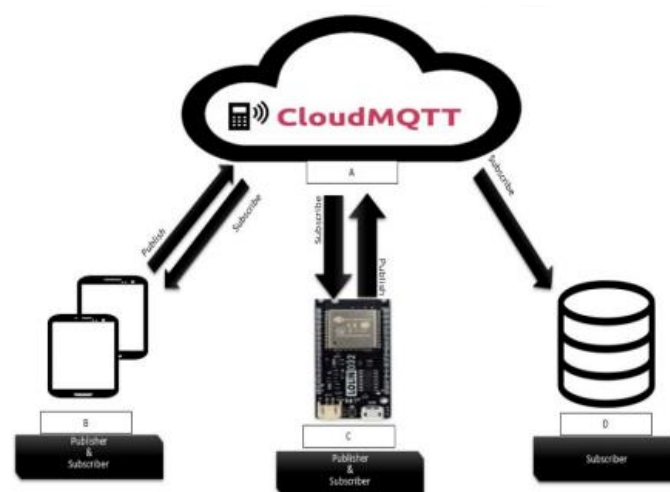


Figure 2.1 : Architechture Design

The design of the architecture comprises the choosing of electronics equipment as well as the integration of all components. The hardware design for our security monitoring system is depicted in Figure 2.1. Table 2.1 defines the specifications of each component in Figure 1. Figure 2.1's number matches to the order of elements in Table 2.1. This project utilise an ESP32 with a Lolin D32 Board for the processing module. This board has a wireless LAN module for connectivity. The Arduino programming language is used to compile the ESP32. Two LEDs are utilized, with the first serving as a power indication. If the appliance is electrified, the ESP32 will send a command to the red LED to turn on. Second, green LEDs serve as WiFi indications. If the ESP32 is not connected to WiFi, it will send a signal to the green LED to flicker until it is. To detect motion, the ESP32 employs a PIR sensor. The ESP32 gathers the data from the detector to determine the status of the door. The buzzer siren module is used by ESP32 to emit a warning. The electric strike module is used by ESP32 to lock and open the door.

2.2.2 Keypad/Bluetooth/GSM Based Digital Door Lock Security System

In today's world, it is crucial to have a security system with different sensors and an alarm system in residential communities. This project created a security alarm system with many sensors for smoke, fire, intrusion, and application operation. A central monitoring system was installed to offer continuous sensor indication. For successful communication, transmitters were linked to sensors and receivers to a monitoring system[8]. The central monitor will then display the indication for each transmitter linked to a certain sensor. This project presented a home security system that used GSM/GPRD technology services to manage door locks via a short message service (SMS). Also this project design and

development of PIC supported security system with the GSM system for sending the alert message on mobile for continues three unsuccessful attempts of password[3].

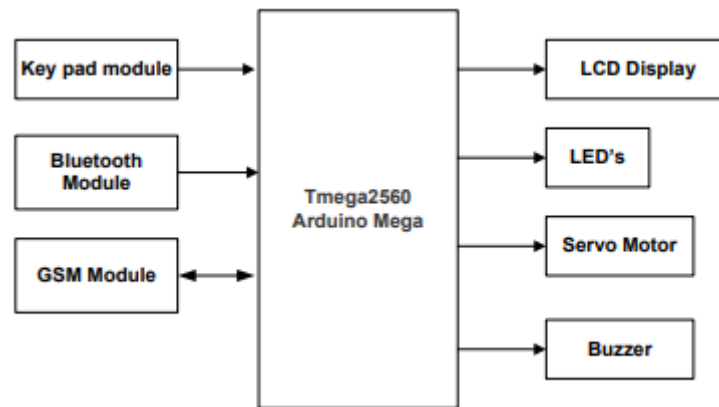


Figure 2.2 : Block Diagram

Figure 2.2 present time door security is the most important and so this project designed and implemented a digital door lock system which works in three different modules. From figure 2.2, the keypad module user can directly enter the 4 digit password to lock and unlock the door. In bluetooth module, first this project establish connection between their smart phone and door lock system bluetooth kit, then enter the password to lock/unlock door. Bluetooth module range is approximately 10 meters. GSM module is the most secured mode in which the owner has to enter the password through his mobile via text message to open or close the lock.[8] The main advantage of GSM module is that it enables user to lock/unlock the door from remote location. The main advanced feature in all three modules is that if unknown person enters three consecutive wrong passwords, it will send an alert message on GSM mobile number of the owner which is stored in arduino program and also start the buzzer alarm for security alert of the society.

2.2.3 Automatic Door Lock System

To open the lecture room door, this project will employ SMS or text message. Lecturers can send text messages to the system to open the lecture room door. The system will recognise it and perform a safety check. The system receiver will be used to receive SMS messages. For the receiver, a Sony Ericsson K700i phone was used. The microcontroller will then read the signal and check if it is the correct person to open the door or not. If the correct person sends the SMS, the door lock circuit will be activated. It will not open the door if the SMS is not from an authorised individual.

The electromagnetic principle is used to construct the door lock circuit. It will have a magnetic core and will transform into a magnet when electricity is applied.[1] This magnet will serve as the door's locking mechanism. In addition, safety precautions are taken into mind. At all times, the door will be locked. If someone sends the correct SMS to the system, it will automatically open. The door will open once a specified amount of time has passed, and the user must close it within that period.



Figure 2.3 : System Block Diagram

Figure 2.3 shows that the system receiver will be used to receive SMS messages. For the receiver, a Sony Ericsson K700i phone was used based on figure 2.3. The microcontroller will then read the signal and check if it is the correct person to open the door or not. If the correct person sends the SMS, the door lock circuit will be activated. It will not open the door if the SMS is not from an authorised individual.

2.2.4 IoT Security Applied on a Smart Door Lock Application

Companies prefer to focus on time-to-market and launching products as quickly as possible in the IoT sector, rather than developing a secure, meaningful solution. As a result, many IoT devices have insufficient protection against many types of harmful assaults.[8] IoT security is a developing issue, and while there has been a lot of research done on the subject, there hasn't been much effort done on implementations or standardizations that could help alleviate the problem.



Figure 2.4 : Infrastructure of IoT Ecosystem

As shown in Figure 2.4, the overall structure is depicted. The foundation of the IoT ecosystem can be divided into three parts: user interaction point, sensors and actuators, and delegate and relay. The following are the three:

- 1) User Interaction Point: The dynamic component that connects the end user to the end device is known as the user interaction point. The objects in this section can be compared to a laptop or a smartphone that the user can manage. A third-party

application that can be installed allows the user to control the unit (Smartphone, laptop, etc.).

- 2) Delegate & Relay: A cloud service that gathers the logic for numerous IoT devices supports and maintains some IoT system end devices. The computation is the responsibility of this group. Routers and sensors can also fill this role, collaborating with the cloud to combine and transfer various collaborations via various communication channels.
- 3) Sensors and Actuators: These are the components of the system that respond to orders, carry out interactions, and modify its state. A camera may begin recording, a Smart TV may switch on, a coffee machine may begin brewing, and so forth.

The smart door lock will be in charge of unlocking an office space's entrance. The front door is on the third story of a massive structure, and it connects the office to a stairwell and several elevators. The smart lock should be able to handle a high volume of traffic while also remaining functional in the given context.[1] Only authorised persons in the space between the stairs, elevator, and the door should be able to open the door. This necessitates the door lock having a precise sense of the user's location.

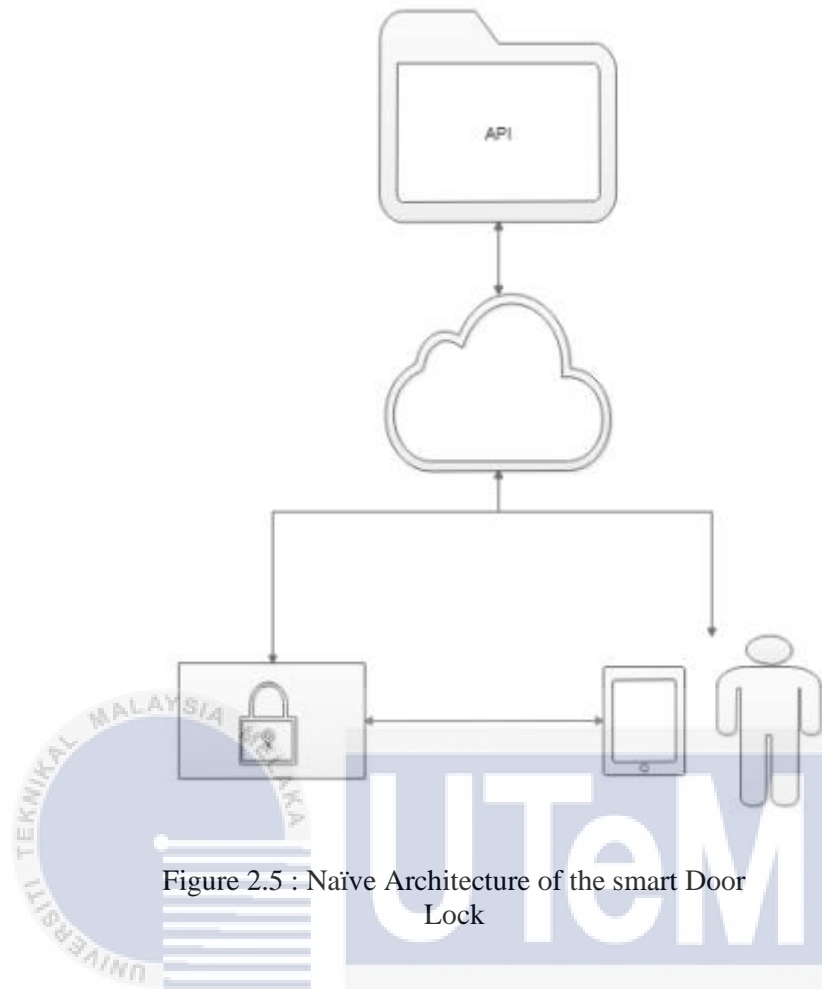


Figure 2.5 : Naïve Architecture of the smart Door Lock

Figure 2.5 depicts a naive system overview of the smart door. The user application will only connect with the lock through Bluetooth to see if a specific user is nearby. Separate communication channels will exist between the lock and the application, which will securely communicate data to the API via a cloud service. The API will accept a variety of requests and respond by sending commands to the digital lock or providing feedback to the user application.

2.2.5 Iot Based Smart Home Security System with Alert and Door Access Control

For a wide range of commercial and security applications, an efficient, low power consumption, and low cost embedded access control system for Smart home security and

remote monitoring based on motion detection is critical. Smart home security control systems are gradually being adopted in several nations.[9] Microprocessors are now found in the majority of home and workplace products with which we interact. Although all of these appliances have some sort of user interface, many users are upset by how difficult it is to operate the complicated functionality of their gadgets.

The goal of this project is to create a framework that allows people to interact with appliances using a different user interface device that they currently own. Smart phones are ideal candidates for providing interfaces because they are widely available, have communication capabilities that allow them to connect to appliances, and are currently being used for a variety of purposes[9]. The most crucial aspect of any home security system is recognising visitors who enter and exit through the entrance. An entrance guard can be handled remotely, and the most natural approach to perform security is to detect visitors at the door and warn the user by mobile phone.

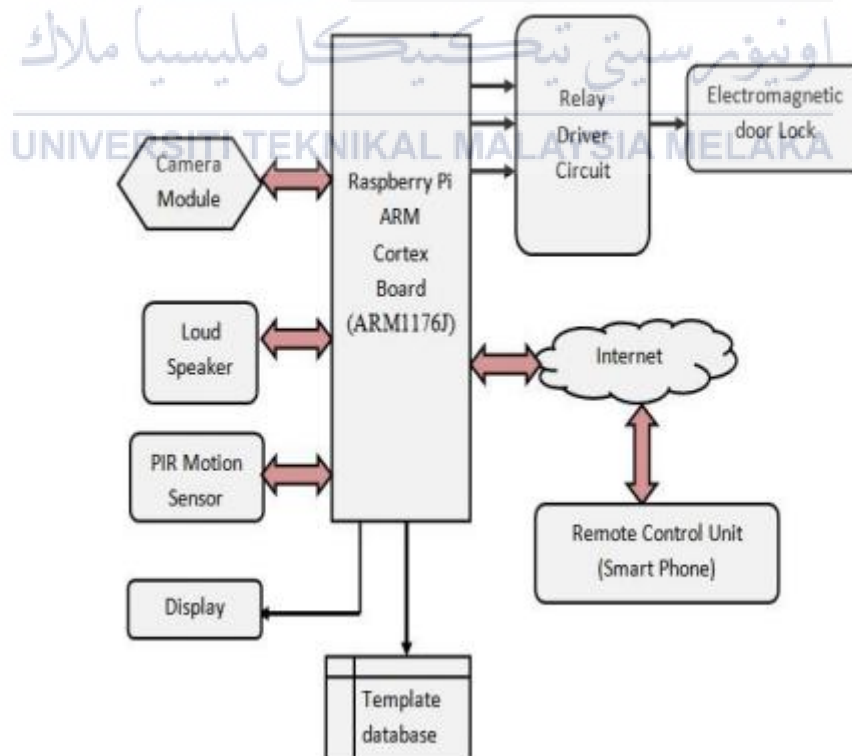


Figure 2.6 : Block Diagram

Figure 2.6 depicts the Smart Home Security System's system architecture. The entire security system to be put at the specified location is made up of Raspberry Pi, PiCamera, and Power supply. The Raspberry Pi's GPIO pins are connected to a PIR motion sensor. For setting up the Raspberry web server, the user can use an LCD monitor. A loudspeaker is connected to the Raspberry Pi's audio jack. To control an electromechanical door lock, a relay driver circuit with the IC ULN2003 is connected to the Raspberry Pi. The image recorded can be saved on an SD card or a USB pen drive attached to the Raspberry Pi with the time and date.

2.2.6 Iot Enabled Door Lock System

A GPS-based smart door lock is devised in this study. The ultimate goal of this study is to create a door lock system that does not require manual input from the user while still remaining secure. However, the purpose of this paper is limited to evaluating the viability of using GPS for location-based lock to accomplish the aforementioned goal.[10] The Android-based application outlined in is used to control the smart home. The smart lock design and implementation, as well as the testing results, are detailed in this paper.

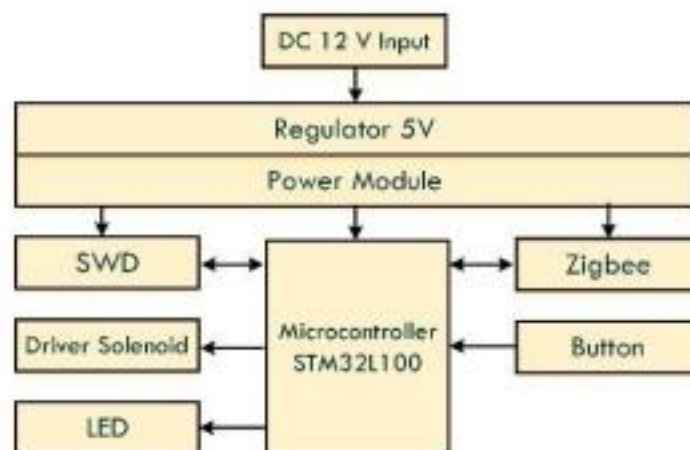


Figure 2.7 : Block Diagram

The door lock functions as an on/off switch that is activated based on the user's proximity to the door. The lock system is built around a battery-powered STM32L100 microcontroller that controls a 12 VDC/630 mA solenoid and an Xbee module that receives signals from the central host.[10] TIP 102 transistor is used to control the solenoid by switching the state of the solenoid using its cut-off and saturation modes. The system also includes components such as a DC power jack, a microUSB port for development, a switch, and reset and mode buttons. Figure 2.7 shows a block diagram of the door lock hardware.



2.2.7 Door Access and Security System Based on IoT

Security has become a major concern in both public and commercial institutions, with many security methods suggested and created for a variety of critical operations. Information, property, and theft or crime prevention are all made possible by security systems. Security solutions have become a must in everything from data centres to banks.[11]

This project proposed a revolutionary access monitoring and control system based on IoT and a finger print door lock. Users can live a safe and convenient life by implementing this system. The goal of the study is to create a high-security system. The prototype's implementation demonstrates that the proposed system can be a good practical option for access monitoring and control.[11] Apart from the intrinsic door security given by traditional door locks, our system takes security a step further by protecting homes and other applications from various unnatural conditions such as burglary, fire, gas leakage, and other calamities.

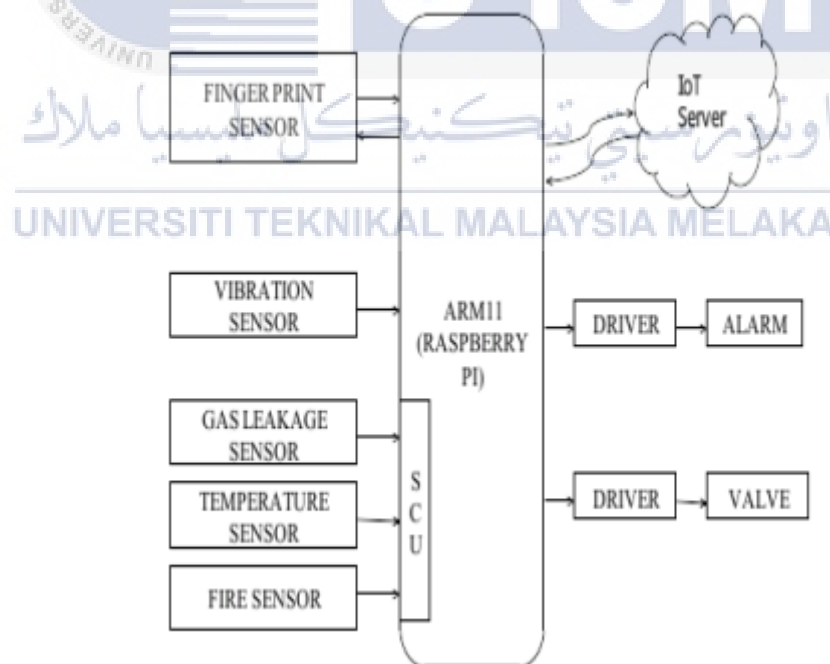


Figure 2.8 : Block Diagram

The IoT-based door lock system is depicted in Figure 2.8. The Raspberry Pi2 model B CPU, which controls all of the project's components, is the project's beating heart. The authorised user is identified via a fingerprint sensor. IoT is linked to the system via the internet.[3] During dangerous situations, the sensors send a signal to the processor. When the sensors are engaged or unauthorised people try to access the door, the buzzer will sound. A valve is a motor that controls the operation of a door, such as opening and closing it.



Table 2.2: Comparison On Previous Project

Author('s)	Title	Hardware Used	Software Used	Method	Dataset Source
Andreas, Cornelio Relivan Aldawira and Handhika Wiratama	Door Security System For Home Monitoring Based on ESP32[5]	-ESP32 -PIR Sensor -Magnetic Sensor -Internal Touch Sensor	-Door Lock Software -System Mobile Apps	-MQTT Brokers	-Science Direct
S. Umbakar, G.Rajput and P. Harnane	Keypad / Bluetooth / GSM Based Digital Door Lock Security System[2]	-Bluetooth Module HC05 -Arduino -Servo Motor	-Arduino IDE	-Bluetooth Application	-Department of Electronic Engineering RAIT Nerul Navi-Mumbai
Mohd Helmi, Alsukran Bin Abd Malik	Automatic Door Lock System[3]	-Sony Ericsson K700i -PIC16F84A	-THRSim11	-Internal ClockBus	-University Teknologi Malaysia
Kristoffer Djupso And Masar Almosawi	IoT Security Applied On A Smart Door Lock Application[1]	- Microcontroller -Bluetooth Transmitter		-Computing Concept	- Examensarbete Inom Teknik Grundniva Stockholm
Shaik Anwar and D. Kishore	IoT Based Smart Home Security System With Alert and Door Access Control Using Smart Phone[9]	-Raspberry Pi3 -Electro Magnetic Door Lock	-Python	-Remote Monitoring -Controlling ECU	-Aditya College Of Engineering And Technology Surampallem India
Irfan Gani	IoT-Enabled Door Lock System[7]	- Microcontroller STM2L100	-MINDS Applications	-MINDS System	-International Journal of Advanced Computer Science And Application
G. Sowjanya And S. Nagaraju	Design And Implementation Of Door Access Control And Security System Based on IoT[8]	-Raspberry Pi		-IoT Server	-University of Bonn

2.3 Summary

To be conclude, this chapter has explained and compared other previous project that most similar to this project. Many data that have been collect in previous project such as in title, software and hardware used, method and others. Based on the table 2.2, combination in biometric fingerprint sensor and IoT concept has never been used. This will be an advantage to this project to implement the combination of method to unlock the door.



CHAPTER 3

METHODOLOGY

3.1 Introduction

This part will briefly discuss the progress of the project. The following will be an overview of the smart door lock security systems with biometric fingerprint and followed by a thorough clarification on the development of hardware and software.

3.2 Methodology

An Arduino uno microcontroller is the major controller of the system. The power source for this microcontroller comes from the regulator circuit that is being constructed. To programme the microcontroller by using Arduino IDE programmer.

The door lock solenoid is used as the door lock mechanism. This solenoid lock is using 12Vdc as an input and will be connect with relay circuit to get signal from microcontroller.

3.3 Flowchart

A flowchart depicts the sequence of actions or movements of people or things in a complex system or activity. A graphical representation of a computer programme in respect to its sequence of functions is also included (as distinct from the data it processes). As shown in Figure 3.1, this is a flowchart of this project which start with an input such as sensor, keypad, and applications to connect with microcontroller.

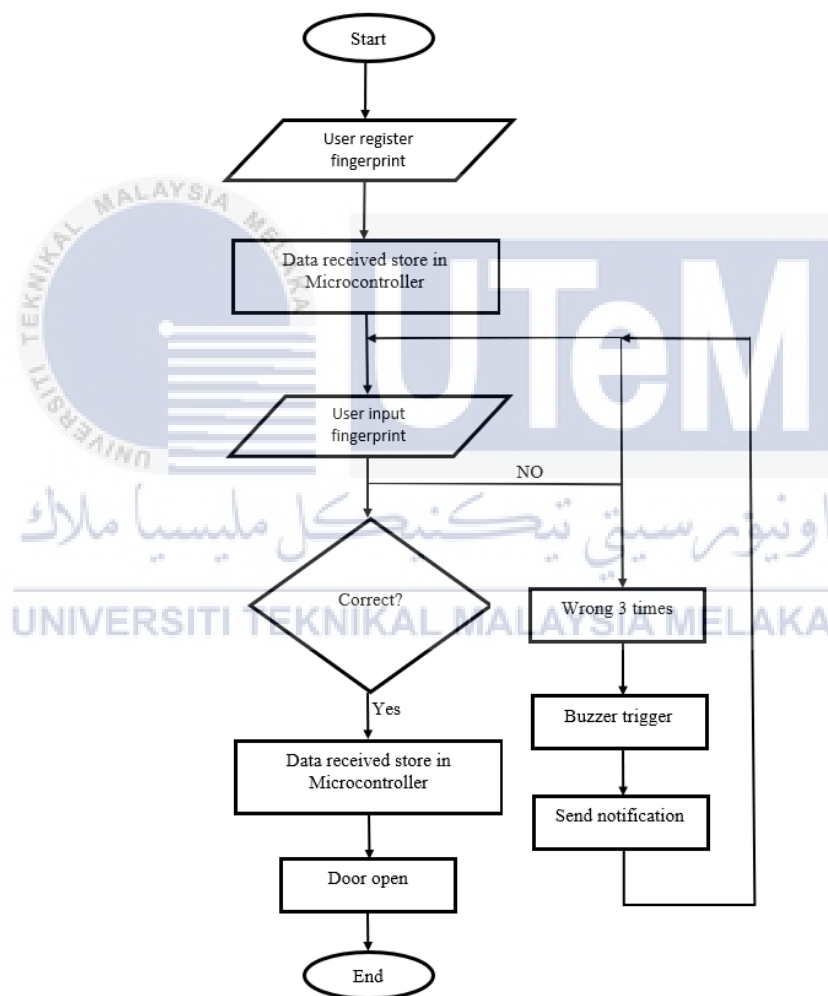


Figure 3.1 : Flowchart of This Project

As shown in Figure 3.1, this is a flowchart of this project which start with an input such as sensor and applications to connect with microcontroller. If the condition of input is

correct, the Arduino will process and proceed to the output which is the solenoid will retract. But if the condition is false, the Arduino will process and no action will be taken and solenoid will maintain in locked position.

3.4 Block Diagram

Figure below shows block diagram for this project. The input is microcontroller which is this project use Arduino as a microcontroller.

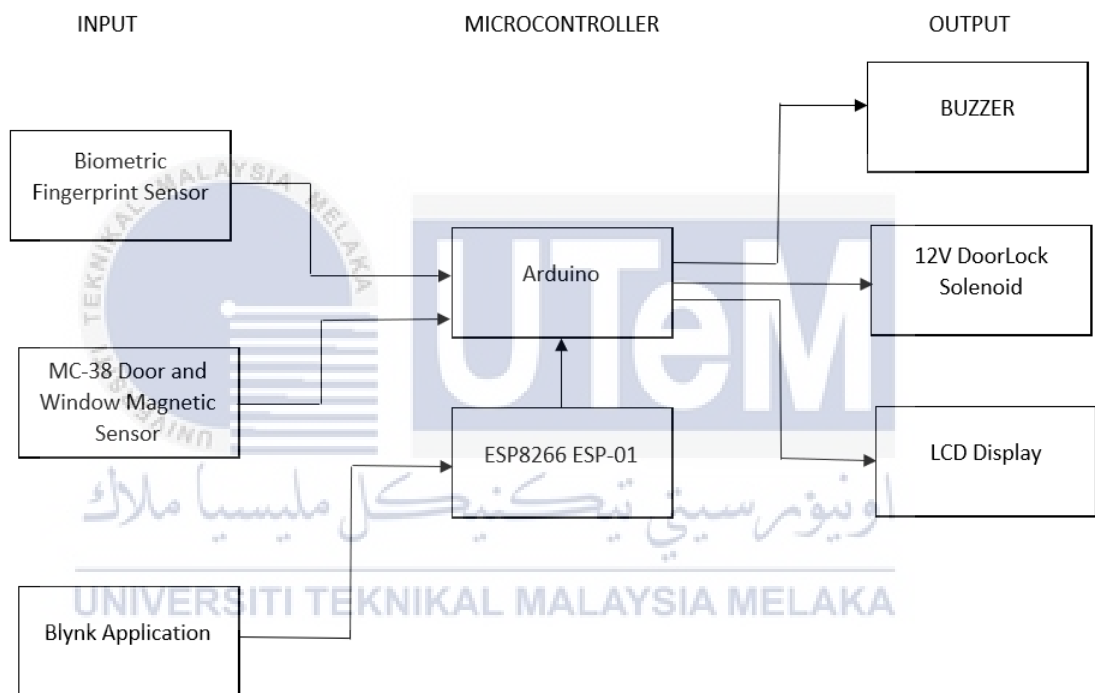


Figure 3.2 : Block Diagram For This Project

Figure 3.2 shows block diagram for this project. The input is microcontroller which is this project use Arduino as a microcontroller. ESP8266 ESP-01 is used to connect the system over the internet. This project has four input and three output. The biometric fingerprint sensor and mc-38 door and window magnetic sensor will be connected to an Arduino while esp8266 esp-01 will be controlled using application. The output will be taken to buzzer, 12v door lock solenoid and lcd display.

3.5 Hardware Implementation

The fingerprint sensor used in this project is an optical type. There are two other types of fingerprint sensors which is capacitive, which can be found in smart phones, and ultrasonic, which is still in the testing phase. Both of these options are expensive, so this project stick with the optical type.

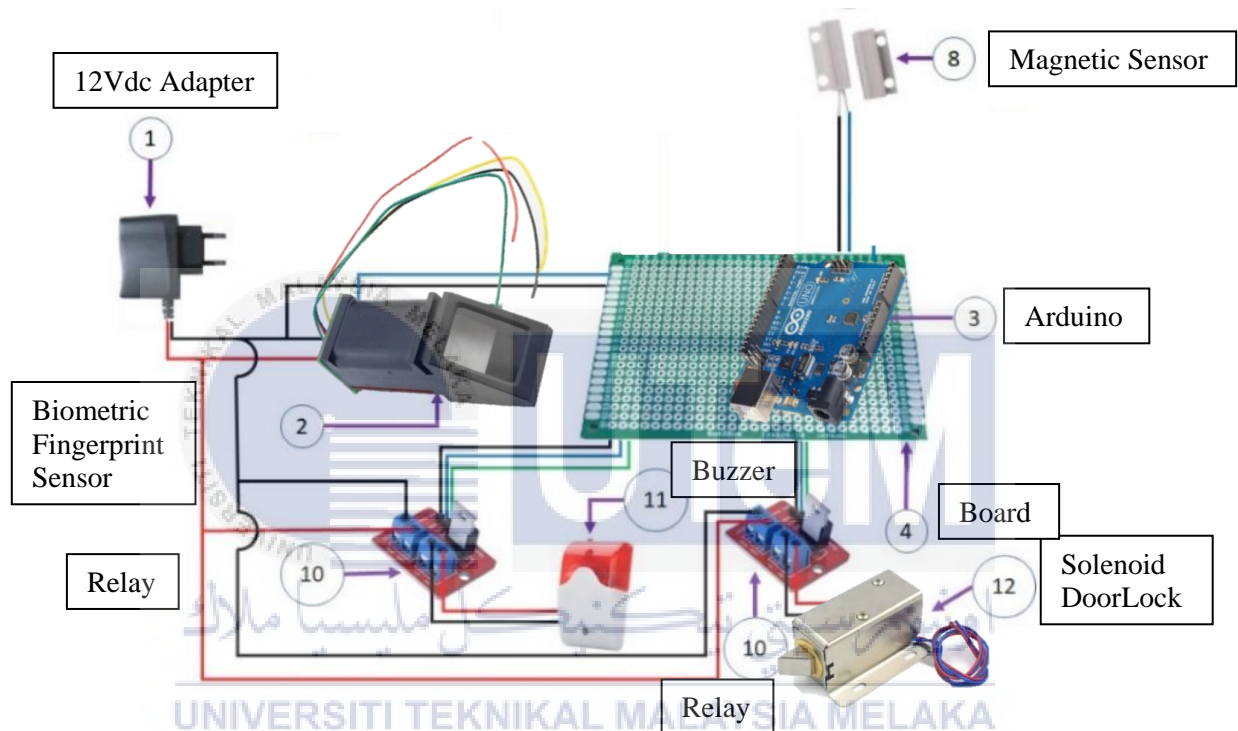


Figure 3.3: Hardware Design

Figure 3.3 shows hardware design for this project. The optical fingerprint sensor works by taking a snapshot of our fingerprint, then matching it with stored data using a specific algorithm and displaying the result. This sensor needs power supply range 3.8V to 7Vdc to operated. Operation current for typical using is 65mA and using UART interface. This sensor only needs average searching time less than 1second.

For the locking system, this project will use DC door lock solenoid. Door lock solenoid need 12Vdc power supply to working. Door lock solenoid will be connected to normally open pin 5v relay and 12V supply. Arduino pinout will trigger relay contact and the 12V supply

will supply the solenoid to lock or unlock.

IoT system in this project will use ESP8266 ESP-01 as the wifi module. The wifi module will be put together in the system box. It will receive data from application and transfer the data to Arduino to process it. Later, Arduino will make a decision to lock or unlock the 12V door lock solenoid.

3.6 Software Implementation

3.6.1 Blynk Application

The Internet of Things inspired the design of the Blynk. It can handle hardware online, present sensor data, save it, visualise it, and do a number of other intriguing things. The blynk platform focuses on 3 components: blynk applications, blynk servers, and blynk libraries. Blynk shares API and UI with all supported hardware and devices. Blynk transfers data over Wi - fi connectivity, Bluetooth and BLE, Ethernet, USB (Serial), GSM, and other methods.

Blynk can control microcontroller such as Raspberry Pi, Arduino or PIC either in platform android or iOS. It's a digital dashboard where you may drag and drop widgets to create the graphical interface for a project. It is easy to put everything together. Blynk is not bound to any particular board or shield. Instead, it works with whatever hardware you have on your system. Blynk will get online and ready for the Internet of Things whether Arduino or Raspberry Pi is linked to the Internet by Wi-Fi, Ethernet, or this new ESP32 chip.

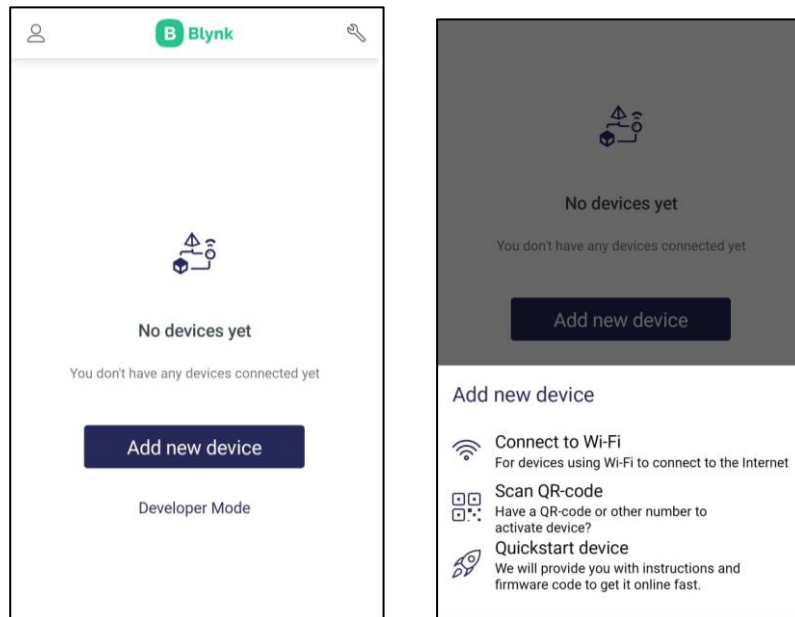


Figure 3.4: Blynk Application

3.7 Gantt Chart

Activities	1	2	3	4	5	6	7	8	9	10	11	12	13	14
PSM1 briefing									M					
Find related project									I					
Find journals or research paper									D					
Chapter 1									S					
Do comparison table from previous project									E					
Flow chart and block diagram for the project									M					
Chapter 2									B					
Finalise component used and design project									R					
Chapter 3									E					
Chapter 4									A					
Draft report submission									K					
Slide presentation														

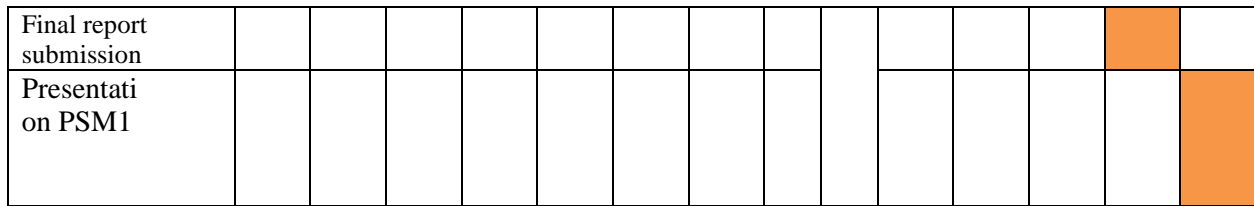


Figure 3.5: Gantt Chart

A gantt chart, which is shown in Figure 3.4, is one of the most common and simple methods to represent activities (tasks or events) versus time. The activities are listed on the left side of the chart, and a time scale is provided at the top. Each action is represented by a bar, the placement and length of which indicate the start, duration, and finish dates of the activity.

Based on figure 3.4, this report need 13 weeks to be done. Briefing for this PSM1 is on first week. To find the related previous project, its takes 5 weeks from first week to week 5 while to find journals or research paper it tooks 4 weeks from week 2 to week 5. Chapter 1 writed in week 4 to week 6. After that, for comparison table, flowchart and block diagram took 2 week to be done. Chapter 2 from week 7 to week 10. Next, this projects component is be finalized in week 10 to 12. This task working same with written for chapter 3 and 4. Final report will be submitted in week 13 and presentation in week 14.

3.8 Summary

The recommended methodology for developing a new, effective, and integrated door lock security system is presented in this chapter. The fundamental goal of the suggested methodology is to provide a simple, secure, and effective estimation that does not result in a significant loss of accuracy in the results. The system proposed in this report can monitor and control the door in a variety of ways, including remotely, granting door access to trusted people who can control the door, receiving notification that the door is still open after the time limit has passed, and turning on the alarm if the door is forced open.



CHAPTER 4

RESULTS AND DISCUSSIONS

4.1 Introduction

This chapter presents the final results for this project. Final results in this situation is when this project result comes when the trully project is done. The verb result refers to what happens as a result of some action. A solution to a problem, especially one reached through computation or testing, is sometimes referred to as a result. The consequence of an action or the way something concluded is defined as a result.

4.2 Result of Developing Process

4.2.1 Circuit Construction

A software called Proteus Design Suite was used to sketch the schematic circuit in order to depict the connection of the rough idea of the circuit. Proteus is a software tool suite that is mainly used for electronic design automation. Electronic design engineers and technicians primarily use the software to create schematics and electronic prints for the fabrication of printed circuit boards. This circuit diagram shows an overview of all the components used in this project, including the input, process, and output.

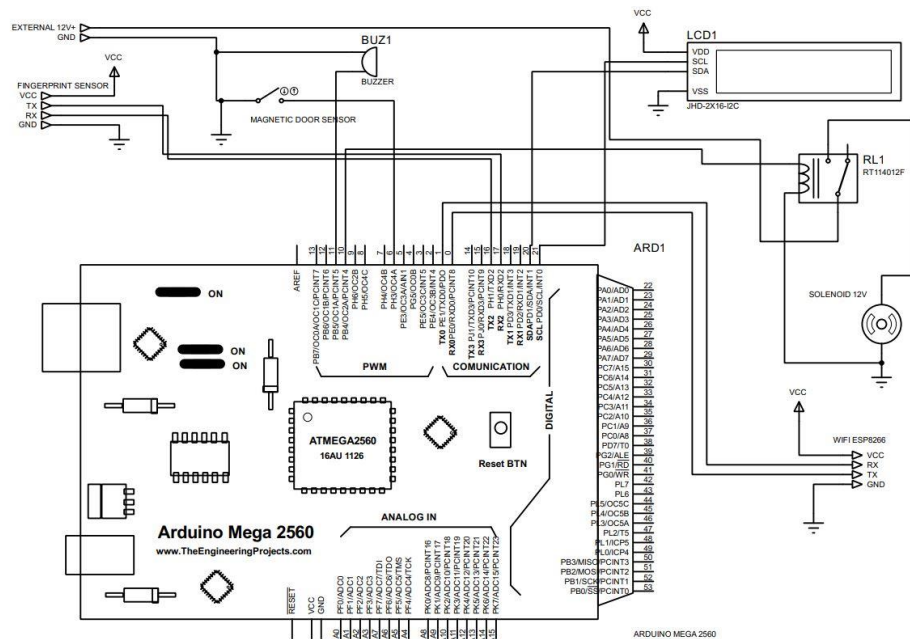


Figure 4.1: Overview of the project circuit

Before the final project circuit was depicted in Figure 4.1 above, Arduino Mega was utilized as a replacement programmer of FDTI and any other USB to TTL converter to setup the ESP8266-WiFi module. The code was uploaded using the Arduino IDE, and the ESP8266-WiFi module will store it because it has its own memory.

4.2.2 Hardware Design

A tidier circuit was designed on a breadboard for hardware design, with wire jumpers connected to each component. In order for the circuit to operate, a 12V AC-DC power supply was used. A small-scale circuit was built to achieve one of the project's main goals: to create a user-friendly device that is simple to install. The project prototype is small enough to fit into a small electrical box based on Figure 4.2 below.

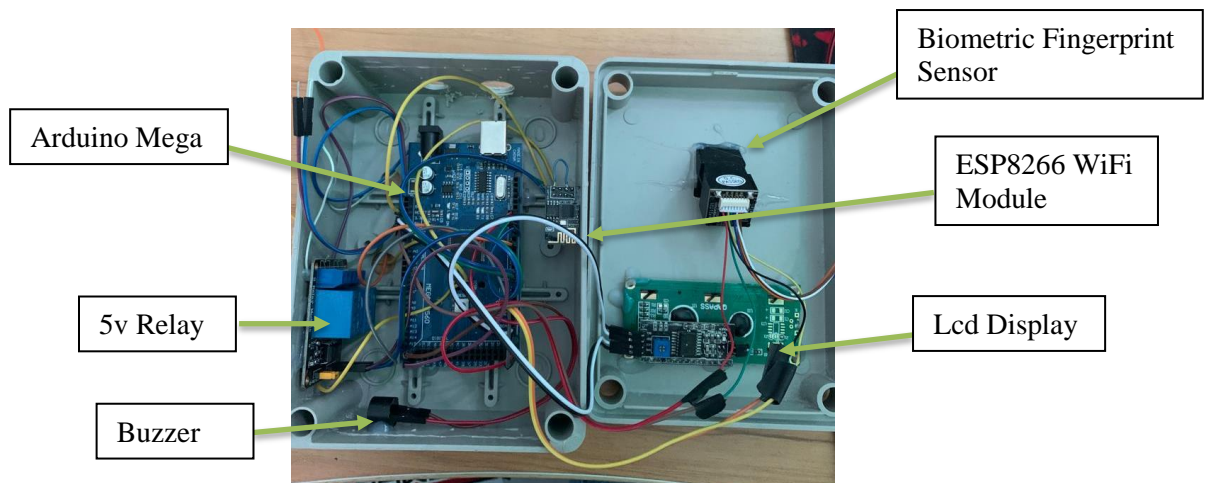


Figure 4.2: Circuit setup in an electrical box

Figure 4.3 below show full design of the projects hardware. Prototype of a door was made by using used wooden pallet. The electrical box with circuit inside were installed and attached at the side of the prototype. A dc 12v solenoid attached upper side of the door while the magnetic door sensor were installed between the door and the door frame.

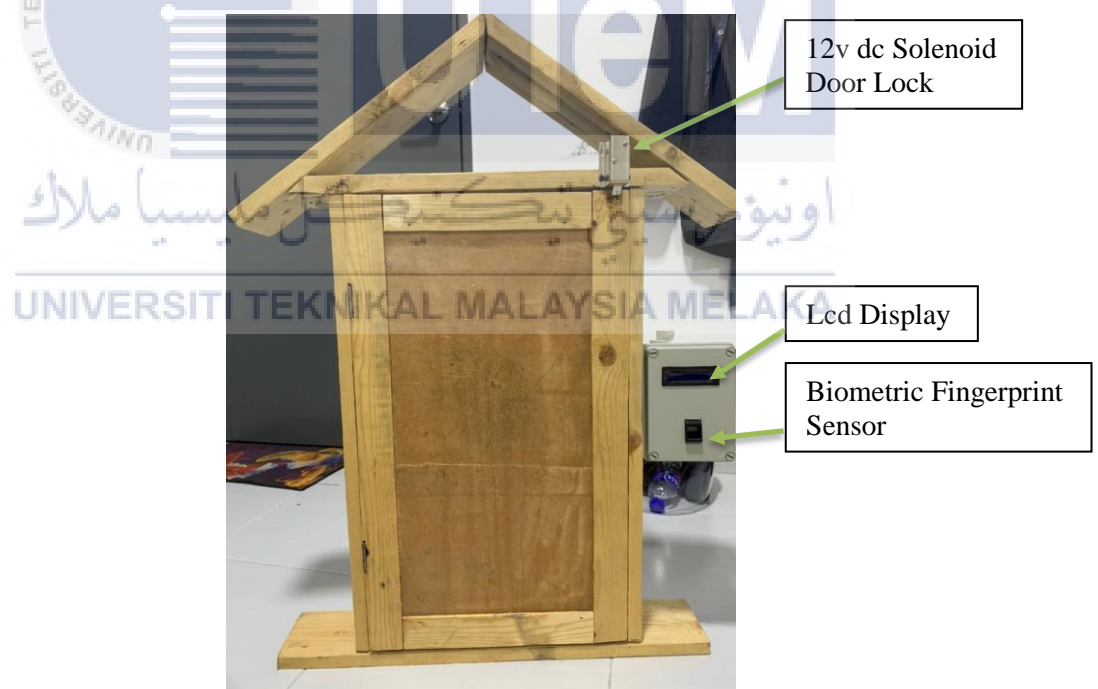


Figure 4.3: Hardware design of the project

4.2.3 Application Design

Blynk is available for both Android and iOS devices. The user interface and API for Blynk are identical on all supported devices and hardware. Widgets are widely known because of their simplicity of use and ability to be controlled through the virtual pin function. Users can access the Blynk cloud service via a variety of methods, including WiFi, BLE & Bluetooth, GSM, Ethernet, and USB.

Overall, even for beginners, integrating hardware and cloud servers with Blynk is simple. After downloading Blynk, users should first sign up and register their email account. Following that, as shown in the figure below, the user can begin designing a new project.

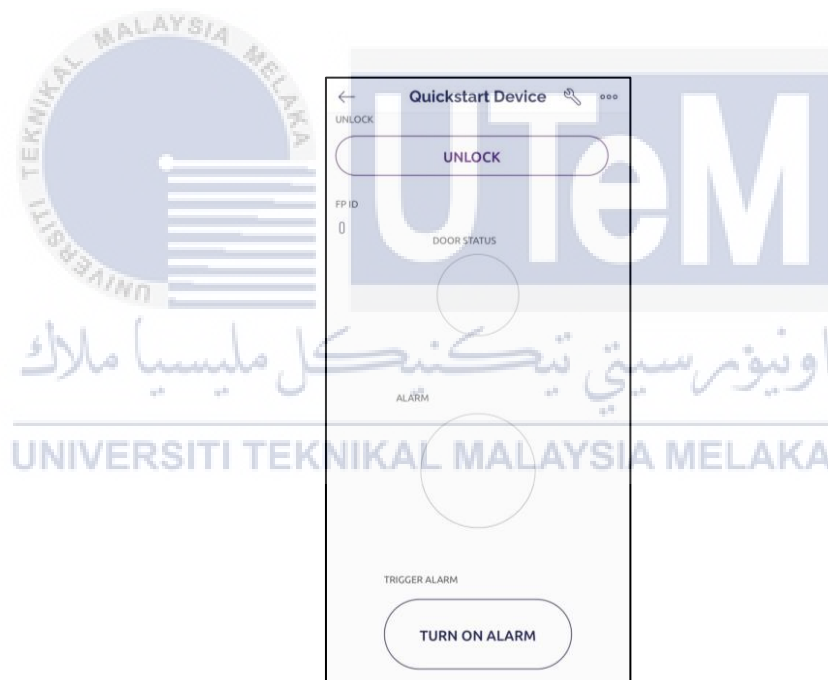


Figure 4.4: User Interface

After connected to WiFi and first setup in Blynk application, user need to configure and design the user interface. Figure 4.4 shows the user interface for this project. First button in for unlock the door which means if user triggered the button, 12v dc solenoid door lock will retract and after a second, solenoid will automatically return to initial position. Below the button is door

status led. If magnetic door sensor is not attached to another magnetic, red led will turn on.
following with button for trigger alarm and alarm status.

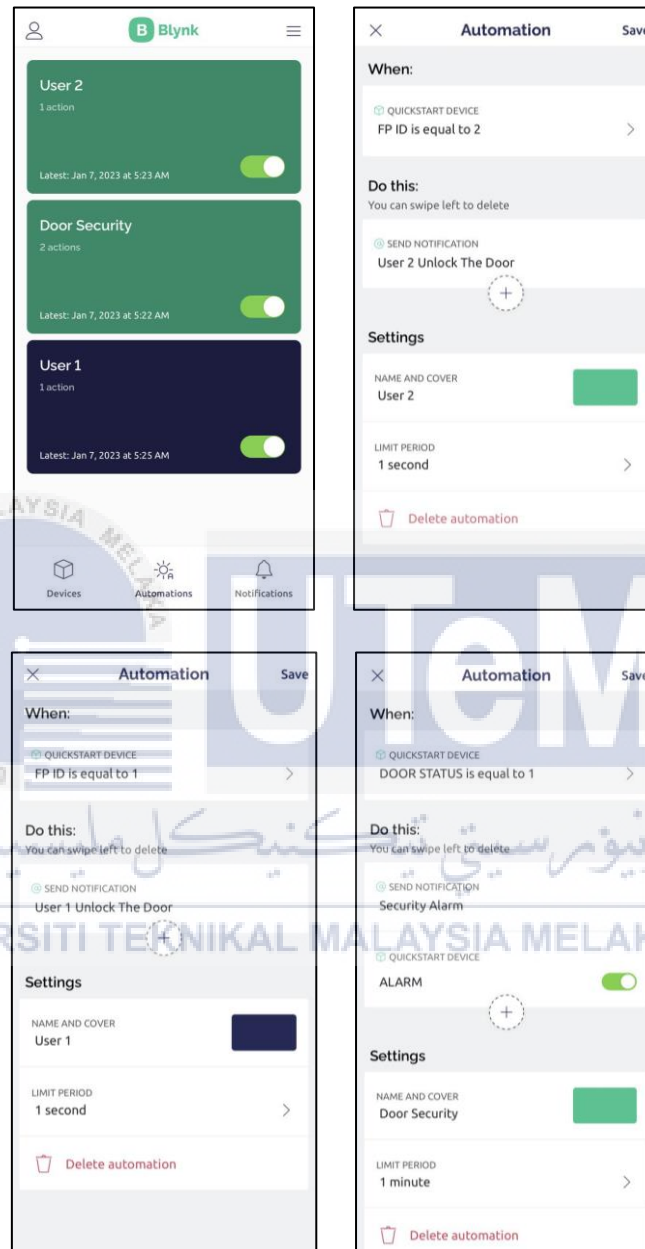


Figure 4.5: Automation setup

Figure 4.5 above show the setting for automation in Blynk application. First and second automation is when the biometric sensor sense that user 1 or user 2 scan their fingerprint, people with access to the apps can get a notification show who is access the door. Next automation is when door status is turn on for 1 minute which means the door is open, alarm will be triggered.

4.3 Data Analysis

Data analysis is one of the process used to obtain information that can be used to make an option. It came with a variety of approaches and techniques to achieve the desired outcome. A frequent test was run to analyse the pattern of each data set collected from the project. A better data analysis obtained from the right data analysis technique and tools can result in a successful project at the end of the process.

4.3.1 Biometric Sensor Accuracy and Speed Reading

This project used five fingers in three way of pressure on the sensor which is in low, medium and high pressure to test the accuracy and speed of biometric sensor read the fingerprint data. The biometric sensor work simultaneously with door lock solenoid where at certain pressure on the sensor will affect the speed of solenoid retracted. But if the biometric sensor failed to read more than three times, the buzzer that connected to the system will turn on. Figure 4.6 below shows the name of the finger. Starting with thumb finger, index finger, middle finger, ring finger and little finger.

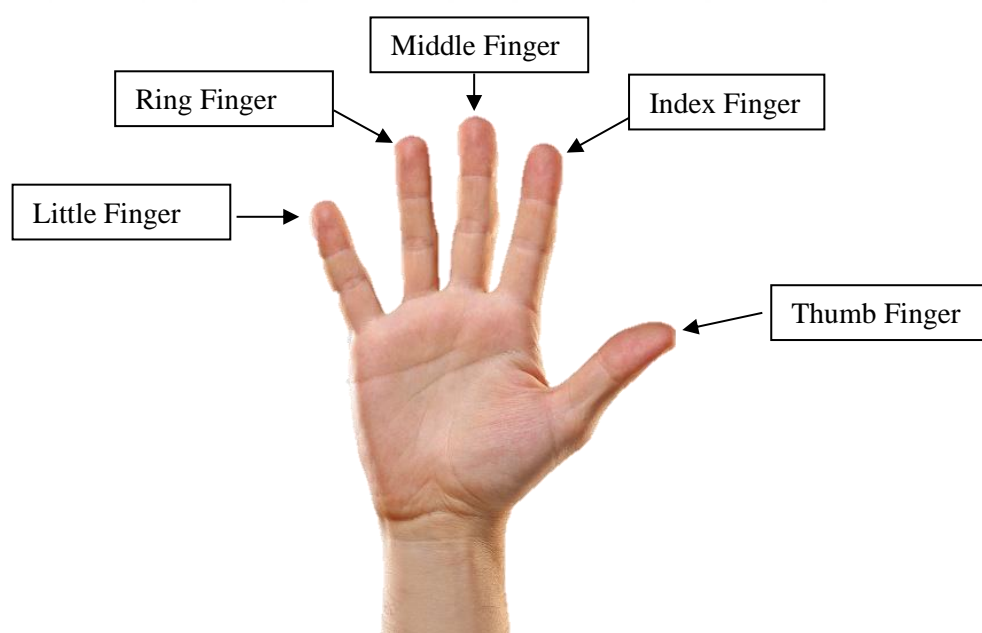


Figure 4.6: The name of the finger

Three pressure will be tested in this experiment which is low pressure, medium pressure and high pressure. The pressure example is based on the Figure 4.7 below while the result of the experiment are shown in table 4.1 below.



Figure 4.7: Example of the fingerprint pressure

Table 4.1: Finger and Pressure Test Result

Type of Finger	Low (sec)	Medium (sec)	High (sec)
Thumb Finger	0.73	0.54	0.33
Index Finger	0.75	0.53	0.31
Middle Finger	0.79	0.61	0.36
Ring Finger	0.8	0.69	0.43
Little Finger	0.91	0.7	0.48

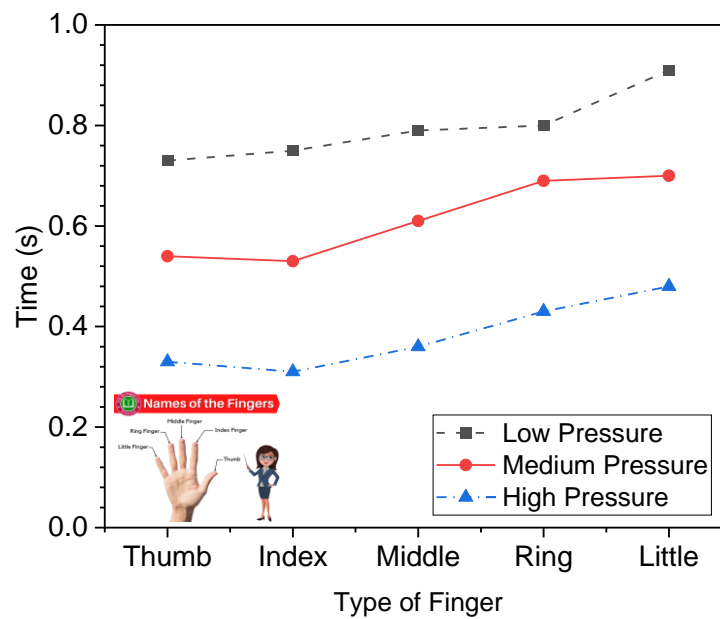


Figure 4.8: The speed of the biometric sensor sense with various pressure

Based on figure 4.8, this project has been tested with different finger and different pressure. Each finger tested with three types of pressure which is in low pressure, medium pressure and high pressure. Based on the graph that has been obtained, the index finger with high pressure leads the speed of the other fingers. The little finger with low pressure takes the longest time to retract the solenoid door lock.

4.3.2 Wet and Dry

In this test, the best two fingers which is thumb finger and index finger will be used to run two condition of test. The condition of the test are wet and dry test. Every test will be tested in high pressure. Time will be recorded to compare the speediness of the biometric sensor to sense the finger. Table 4.2 shows the result of the test.

Table 4.2: Wet and Dry Test

Type of Finger	Wet (sec)	Dry (sec)
Thumb Finger	0.44	0.3
Index Finger	0.5	0.32

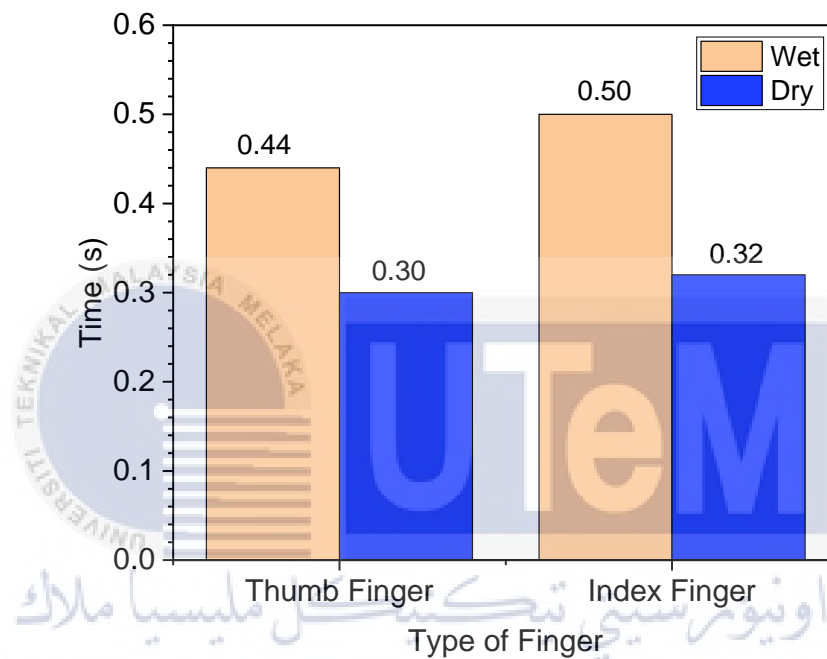


Figure 4.9: The speed of the biometric sensor sense with wet and dry condition.

Figure 4.9 show the result for wet and dry test to thumb and index finger in high pressure. Based on the figure, the biometric sensor will sense index finger in dry condition faster than other. Thumb with wet condition take longest time for biometric sensor to sense the finger.

4.3.3 Clean and Dust Surface

For the next experiment, this project will use thumb finger and index finger with dry and high pressure condition. Accuracy and speed of the sensor to sense the finger will be tested with clean and dust condition of the biometric sensor surface. Table 4.3 below shows the result of the test. Time will be recorded in sec to find out the speediness of the sensor.

Table 4.3: Clean and Dust Surface Test

Type of Finger	Clean (sec)	Dust (sec)
Thumb Finger	0.29	0.52
Index Finger	0.31	0.6

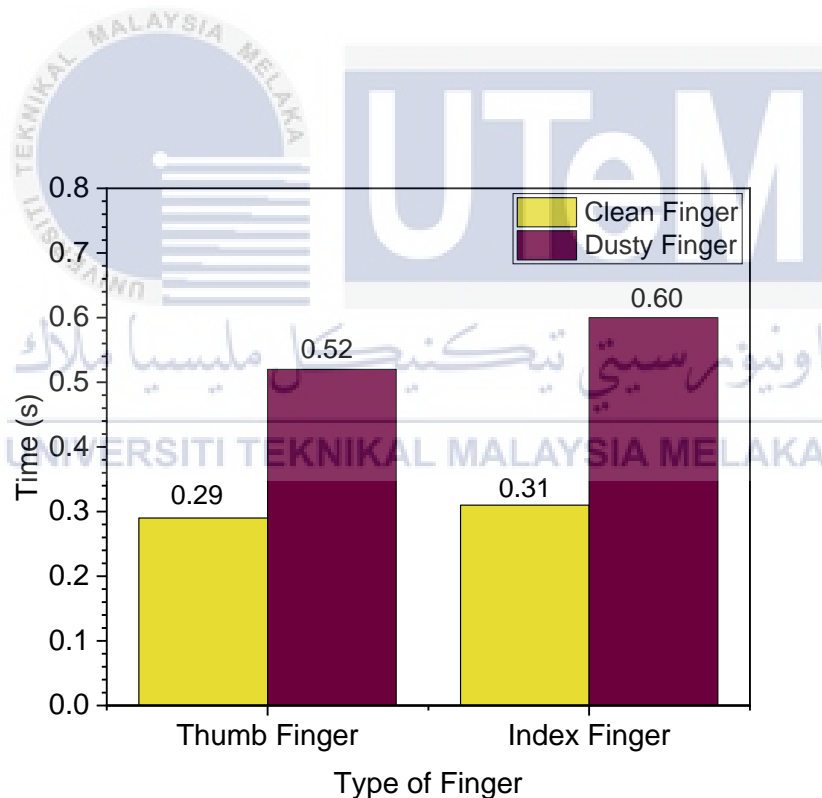


Figure 4.10: The speed of the biometric sensor sense with clean and dust condition of the surface.

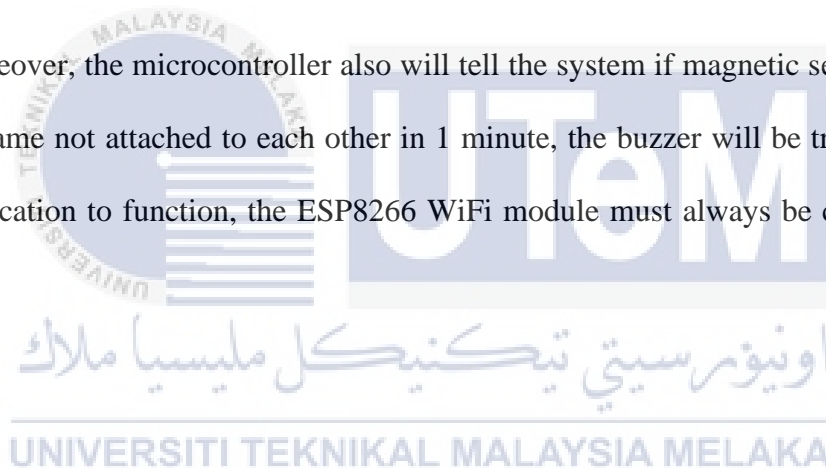
By referring to the Figure 4.10, the clean surface of the sensor does not take too long for the sensor to sense the fingerprint and then to retract the door lock solenoid. Using index finger on the dust surface will take longest time to retract the solenoid door lock.

4.4 Summary

When the device receives a DC 12v voltage, the action for this project begins. The adapter will provide 12V DC to the solenoid door lock and microcontroller. This project will then scan and connected to WiFi to obtain an Internet connection. Once connected to WiFi and the Blynk App, this project will begin to prepare for the user to scan their fingerprint.

Next, after user scan their fingerprint correctly, solenoid door lock will retract and door can be unlocked. But if non accessible person want to access the door, authorized user need unlock the solenoid door lock using their smartphone with access to the internet by using Blynk application.

Moreover, the microcontroller also will tell the system if magnetic sensor at the door and door frame not attached to each other in 1 minute, the buzzer will be triggered. For the Blynk application to function, the ESP8266 WiFi module must always be connected to the internet.



CHAPTER 5

CONCLUSION AND FUTURE WORKS

5.1 Conclusion

Security systems have become a significant part of human existence in recent years. This system was created in order to match the need in the security system, which is high nowadays. The Automatic Door Lock System was created to assist users in unlocking their doors without the usage of a key. To open the door, this system uses a biometric fingerprint sensor, a keypad, and an application. This approach adds to the security system's capabilities while also assisting the consumer in achieving greater life security.

The objectives of this thesis has been achieve which is the projects prototype has been developed and already test its functionality. Next, in this thesis, the smart door locks effectiveness in terms of speed to accessing the door also has been analyzed and get the best result using dry thumb finger in high pressure and clean surface of the scanner. IoT for this project also has been designed to get more features and to make user easy to unlocked the solenoid door lock.

The goal of learning application technology was achieved in this project. Later, this information can be applied to a more complex system. Furthermore, many talents have been developed through this project, not only in terms of software and hardware, but also in terms of the ability to search for vital data.

5.2 Future Works

In conclusion, this thesis accomplished all of its objectives. For the future works, this project will build a physical prototype of IoT Based Smart Door Security System. The project also will be added with RFID, magnetic sensor and alert buzzer to alert other residents or workers in that area.

Magnetic sensor will be placed at the door and doors frame. If door was open, the buzzer will alert if the door not close in 3 to 5 minutes. RFID function is to make an easy way to authorized person without having trouble in sense their fingerprint. User just need to touch the card and the door will easily can be opened.



REFERENCES

- [1] W. T. Barajas, F. Simat, S. Anwar, and D. Kishore, "IJERT-IOT based Smart Home Security System with Alert and Door Access Control using Smart Phone Net work Operat ions Procedures Net work and Temperat ure Monit oring Syst em Menggunakan Raspbe... IOT based Smart Home Security System with Alert and Door Acce," *IJERT J. Int. J. Eng. Res. Technol.*, vol. 5, no. 12, 2016, [Online]. Available: www.ijert.org
- [2] I. Journal, M. Patil Bhushan, M. Mahajan Vishal A, M. Suryawanshi Sagar A, M. Pawar Mayur B, and U. R. Patole, "IRJET-Automatic Door Lock System using PIN on Android phone Automatic Door Lock System using PIN on Android phone," *Int. Res. J. Eng. Technol.*, 2008, [Online]. Available: www.irjet.net
- [3] L. O. W. H. U. I. Qi, "DEVELOPMENT OF SMART DOOR LOCK USING," 2019.
- [4] O. Doh and I. Ha, "A Digital Door Lock System for the Internet of Things with Improved Security and Usability," vol. 109, pp. 33–38, 2015, doi: 10.14257/astl.2015.109.08.
- [5] I. Journal, K. A. Patil, N. Vittalkar, P. Hiremath, and M. A. Murthy, "IRJET-Smart Door Locking System using IoT Cite this paper Smart Door Locking System using IoT," *Int. Res. J. Eng. Technol.*, 2020, [Online]. Available: www.irjet.net
- [6] Andreas, C. R. Aldawira, H. W. Putra, N. Hanafiah, S. Surjarwo, and A. Wibisurya, "Door security system for home monitoring based on ESsp32," *Procedia Comput. Sci.*, vol. 157, pp. 673–682, 2019, doi: 10.1016/j.procs.2019.08.218.
- [7] S. Umbarkar, G. Rajput, S. Halder, P. Harnane, and S. Mendgudle, "Keypad/Bluetooth/GSM Based Digital Door Lock Security System," no. January, 2017, doi: 10.2991/iccasp-16.2017.102.
- [8] D. Show, "Automatic door lock system mohd helmi alsyukran bin abd malik universiti teknologi malaysia".
- [9] I. Gani *et al.*, "IoT-Enabled Door Lock System Related papers Prot ot ype of Smart Lock Based on Int ernet Of T hings (IOT) Wit h ESP8266 IoT-Enabled Door Lock System," *IJACSA) Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, 2019, [Online]. Available: www.ijacsa.thesai.org
- [10] S. N. G.Sowjanya M.Tech, "Access Control and Security System Based on Iot," *M.Tech, Embed. Syst. Vignan's L. Inst. Technol. Sci. Guntur, A.P, India*, no. DESIGN AND IMPLEMENTATION OF DOOR ACCESS CONTROL AND SECURITY SYSTEM BASED ON IOT, pp. 1–4, 2016.
- [11] A. R. Syafeeza, M. K. Mohd Fitri Alif, Y. Nursyifaa Athirah, A. S. Jaafar, A. H. Norihan, and M. S. Saleha, "IoT based facial recognition door access control home security system using raspberry pi," *Int. J. Power Electron. Drive Syst.*, vol. 11, no. 1, pp. 417–424, 2020, doi: 10.11591/ijped.v11.i1.pp417-424.

APPENDICES

Appendix 1: Gantt Chart BDP 2

Activities	1	2	3	4	5	6	7	8	9	10	11	12	13	14
BDP briefing									M I D S E M					
Study for hardware														
Simulating expected outcomes														
Construct assembler process simulation														
Built Arduino and Blynk coding														
Draw schematic design														
Simulate the Arduino circuit														

[illegible]