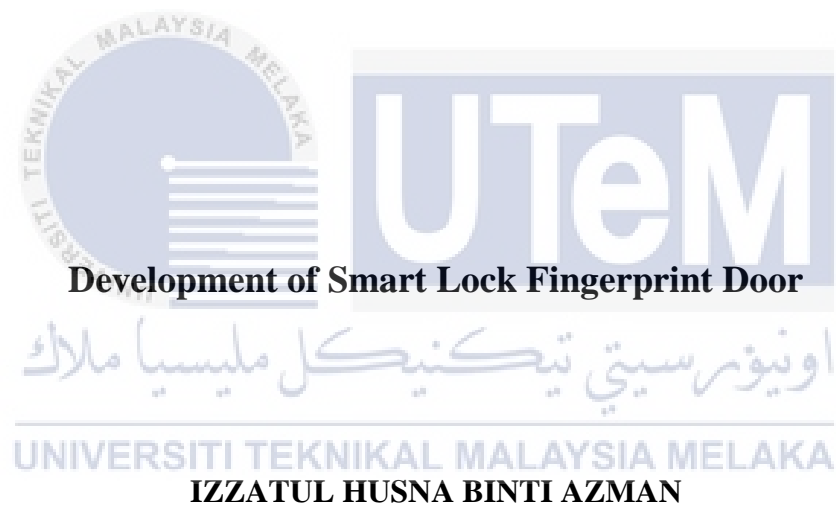




Faculty of Electrical and Electronic Engineering Technology



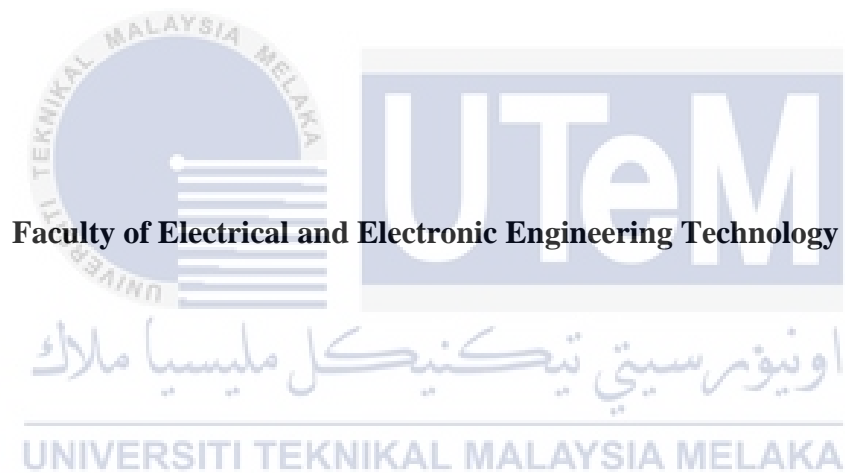
Bachelor of Computer Engineering Technology (Computer Systems) with Honours

2021

Development of Smart Lock Fingerprint Door

IZZATUL HUSNA BINTI AZMAN

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



UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

BORANG PENGESAHAN STATUS LAPORAN PROJEK SARJANA MUDA

Tajuk: Development of Smart Lock Fingerprint Door

Sesi Pengajian: 2021

Saya **IZZATUL HUSNA BINTI AZMAN** mengaku membenarkan Laporan PSM ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka (UTeM) dengan syarat-syarat kegunaan seperti berikut:

1. Laporan PSM adalah hak milik Universiti Teknikal Malaysia Melaka dan penulis.
2. Perpustakaan Universiti Teknikal Malaysia Melaka dibenarkan membuat salinan untuk tujuan pengajian sahaja dengan izin penulis.
3. Perpustakaan dibenarkan membuat salinan laporan PSM ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. **Sila tandakan (X)

SULIT*

Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia sebagaimana yang termaktub dalam AKTA RAHSIA RASMI 1972.

TERHAD* Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan.

TIDAK TERHAD

Yang benar,

Disahkan oleh penyelia:



Azman Awang Teh

IZZATUL HUSNA
BINTI AZMAN

Mr. AZMAN BIN AWANG TEH

Alamat Tetap:

Cop Rasmi Penyelia

NO. 13, JALAN 1/2,
TAMAN PENGGAWA,
45300 SUNGAI BESAR
SELANGOR



Tarikh: 10/1/2022

Tarikh: 10/1/2021

اونيورسيتي تيكنيكل مليسيا ملاك
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

*Jika Laporan PSM ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan PSM ini

DECLARATION

I declare that this project report entitled “Development of Smart Lock Fingerprint Door“ 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 : IZZATUL HUSNA BINTI AZMAN

Date : 10/1/2022



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 Computer Engineering Technology (Computer Systems) with Honours.

Signature

: *Azman Awang Teh*

Supervisor Name

: Mr. AZMAN BIN AWANG TEH

Date

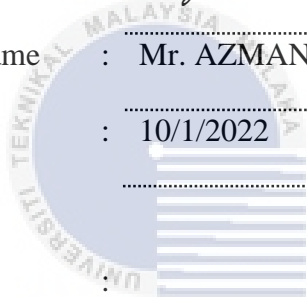
: 10/1/2022

Signature

Co-Supervisor

Name (if any)

Date



اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

DEDICATION

*This report is dedicated to my parents, supervisor, lecturers and friends,
who have always been there for me when I needed them.*

They have also taught me to pursue my dreams

with patience, love, and support,

especially on the path of my project.



ABSTRACT

The "Smart Lock Fingerprint door" is a device that is primarily intended for use with Bluetooth connectivity and a biometric scanner for user authentication. This gadget eliminates the need for the user to carry lock/unlock keys. Without the user's presence, the user may unlock it with a fingerprint and operate the lock system over Bluetooth connectivity. Biometric authentication, such as fingerprints, gives mechanisms for enforcing trustworthy system records and protecting an individual's right to privacy. This study shows research about the development of smart lock fingerprint doors and proposes a system with different features with the extension of wireless control via Bluetooth connectivity and as a rechargeable device. The purpose of this device is to restrict access to just those who are authorised. It is designed using both hardware and software technology. An emergency beep sound is generated to protect the system by sounding a buzzer if an unauthorised user attempts to enter it and a solenoid lock will be used as the locking device.



ABSTRAK

"Pintu Cap Jari Kunci Pintar" adalah peranti yang terutamanya bertujuan untuk digunakan dengan sambungan Bluetooth dan pengimbas biometrik untuk pengesahan pengguna. Alat ini menghapuskan keperluan untuk pengguna membawa kunci / membuka kunci kekunci. Tanpa kehadiran pengguna, pengguna boleh membuka kuncinya dengan cap jari dan mengendalikan sistem kunci atas sambungan Bluetooth. Pengesahan biometrik, seperti cap jari, memberikan mekanisme untuk menguatkuasakan rekod sistem yang boleh dipercayai dan melindungi hak individu untuk privasi. Kajian ini menunjukkan penyelidikan mengenai pembangunan pintu cap jari kunci pintar dan mencadangkan sistem dengan ciri-ciri yang berbeza dengan pelanjutan kawalan wayarles melalui sambungan Bluetooth dan sebagai peranti yang boleh dicas semula. Tujuan peranti ini adalah untuk menyekat akses kepada hanya mereka yang diberi kuasa. Ia direka menggunakan teknologi perkakasan dan perisian. Bunyi bip kecemasan dijana untuk melindungi sistem dengan membunyikan buzzer jika pengguna yang tidak dibenarkan cuba memasukinya dan kunci solenoid akan digunakan sebagai peranti penguncian.

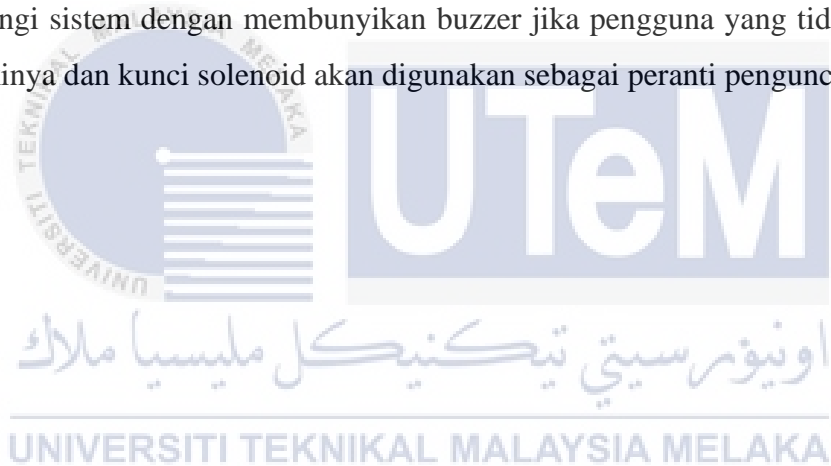


TABLE OF CONTENTS

	PAGE
DECLARATION	
APPROVAL	
DEDICATIONS	
ABSTRACT	i
ABSTRAK	ii
TABLE OF CONTENTS	i
LIST OF TABLES	ii
LIST OF FIGURES	iii
LIST OF APPENDICES	v
CHAPTER 1 INTRODUCTION	1
1.1 BACKGROUND	1
1.2 PROBLEM STATEMENT	2
1.3 PROJECT OBJECTIVE	2
1.4 SCOPE OF PROJECT	3
CHAPTER 2	4
2.1 INTRODUCTION	4
2.2 RELATED TOPICS	4
2.3 RELATED RESEARCH	6
2.4 COMPARISON TABLE	16
2.5 SUMMARY	18
CHAPTER 3	19
3.1 INTRODUCTION	19
3.2 METHODOLOGY	20
3.2.1 REQUIREMENT ANALYSIS AND PLANNING PHASE	20
3.2.2 SYSTEM DESIGN PHASE	25
3.2.3 IMPLEMENTATION PHASE	26
3.2.4 TESTING PHASE	27
3.3 SUMMARY	27
CHAPTER 4	28
4.1 INTRODUCTION	28
4.2 PROJECT ENVIRONMENT SETUP	30
4.3 PROJECT CONFIGURATION MANAGEMENT	36
4.4 DESIGN OF SAMRT LOCK FINGERPRINT DOOR	39

CHAPTER 5	44
5.1 INTRODUCTION	44
5.2 PROJECT SUMMARY	44
REFERENCES	46
APPENDICES	48
APPENDIX A: SOURCE CODE FOR FINGERPRINT ENROLMENT	48
APPENDIX B: SOURCE CODE FOR FINGERPRINT VERIFICATION	52
APPENDIX C SOURCE CODE FOR BLUETOOTH LOCK	56
APPENDIX D: GANTT CHART FYP1	58
APPENDIX E: GANTT CHART FYP2	59

LIST OF TABLES

TABLE	TITLE	PAGE
Table 2.1	Comparison of different platform	16
Table 2.2	Comparison between Mobile Website Application and Mobile Application.	17



LIST OF FIGURES

FIGURE	TITLE	PAGE
Figure 2.1:	August Door Lock application on Android smartphone	6
Figure 2.2:	August Door Lock	7
Figure 2.3:	Kwikset Kevo Lock	7
Figure 2.4:	Arduino Nano microcontroller	10
Figure 2.5:	Arduino Uno R3 Microcontroller	10
Figure 2.6:	Raspberry Pi	10
Figure 2.7:	Fingerprint Sensor AS608	11
Figure 2.8:	Bluetooth module HC-05	12
Figure 2.9:	Solenoid Lock	13
Figure 2.10:	System Block Diagram	14
Figure 2.11:	Flowchart of Smart Fingerprint Lock Door System	15
Figure 3.1:	Waterfall Model	20
Figure 3.2:	Arduino Uno R3	21
Figure 3.3:	Fingerprint Sensor	22
Figure 3.4:	Bluetooth Module	22
Figure 3.5:	Solenoid Lock	23
Figure 3.6:	18650 Lithium-Ion batteries	23
Figure 3.7:	Smart Phone	24
Figure 3.8:	Flowchart of Smart Fingerprint Lock Door System	25
Figure 3.9:	Block diagram of Smart Lock Fingerprint Door	26
Figure 4.1:	Bluetooth Ap Design	29
Figure 4.2:	Circuit Design	29
Figure 4.3:	Full Board Connection Project	39
Figure 4.4:	Fingerprint and Solenoid Lock	39
Figure 4.5:	Overall output	40
Figure 4.6:	Fingerprint matched	40

Figure 4.7: Fingerprint not matced

41

Figure 4.8: Unknown error occured

42



LIST OF APPENDICES

APPENDIX	TITLE	PAGE
Appendix A	SOURCE CODE FOR FINGERPRINT ENROLMENT	48
Appendix B	SOURCE CODE FOR FINGERPRINT VERIFICATION	52
Appendix C	SOURCE CODE BLUETOOTH LOCK	56
Appendix D	GANTT CHART FYP1	57
Appendix E	GANTT CHART FYP2	58



CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

Smart Lock Fingerprint access has been widely used for securing the important property of organizations or individuals. In reference to traditional security systems, entry to the lock system needs the user to have a key, a security password, an RFID card, or an ID card. These security mechanisms, however, have flaws, such as being forgotten or taken by unauthorized individuals. Thus, with the advancement of technology, this has already been implemented in our smart homes with smart lock fingerprint doors.

Biometric authentication has been proved to be the most secure authentication method when compared to facial recognition and RFID cards. Since the skin on our palms and soles exhibits a stream-like series of edges on each fingerprint, which is unusual and invariable, bio-measurement approval ends up being possibly the greatest feature. As a result, each individual's fingerprint becomes a unique ID. Thus, if the door is linked to wireless control by registered users as the backup package, high security will be guaranteed.

As a means of access, a fingerprint scanner was employed. The authorized user's fingerprints were enrolled. The patterns of the thumb and index finger were scanned and saved on the system. The user's fingerprint must match the pattern of the thumb and index finger to get access. If the mismatched fingerprint is recognized, the system display via serial monitor that the fingerprint not found and the lock remain off.

1.2 PROBLEM STATEMENT

Along with the arrival of the smart home era, smart locks have quietly become the first line of protection for security, as if they have become the key to security. However, there will undoubtedly be a number of issues and problems when using an intelligent door lock. For example, simple penetration leads to poor security, and dealing with the lock-in in one way, which is the standard key, is difficult because there is no other option.

Besides, the incidence of human mistakes such as losing a key while holding several keys, which exposes them to loss or theft, and forgetting to close the lock, which the lock can not do on its own because it is mechanical and does not rely on electromechanical. Nowadays, the most common smart door is by using an RFID card scanner door lock, which is not very effective due to the risk of being lost, stolen, or forgotten, and it still exists, as previously stated, in the same way as the key. Hence, human error should be minimized at all costs to ensure that no unintended incidents or mistakes occur, and that the safety of our houses can be ensured.

1.3 PROJECT OBJECTIVE

The main aim of this project are:

- a) To develop a smart lock fingerprint door system which also works on a wireless controller via Bluetooth connectivity.
- b) To monitor the user's safety by using a biometric reader (fingerprint), the new user can also be registered under the owner's control.
- c) To analyze the security performance of the smart lock fingerprint door system.

1.4 SCOPE OF PROJECT

This project is based on a smart lock door system with the addition of fingerprint biometric authentication, which is also limited to the users' personal properties. Based on research, the design and implementation scope of this project will be limited to designing and developing a robust, at the same time, low-cost home control device via smartphone application that will work with the Arduino Uno via Bluetooth connectivity. Hence, to allow the Arduino Uno to run specific features, C and C++ programming languages will be used to install and program the required operating system.

Besides, the overall purpose of a smart lock door system is to be able to scan the user's fingerprints and provide a secured framework via both software and hardware. The projects also highlight the process of assembling several circuits on an electronic board that functions by playing a specific role in the door control mechanism and is also responsible for communicating with any Arduino Uno as a computational device. The access system via hand-free door lock can then be developed as an example method where a user's smart phone can be detected via Bluetooth by developing systems for the interface between the application, microcontroller, and database.

Following the enrolment of users' fingerprint data, the user who does not exist in the database and is not registered is unable to access the door lock and must simultaneously press the door button, and a notification will appear in the application for the admin to give the verification to decide whether to open the door or not. At the end of the system flow, the output of the microcontroller will be represented by the solenoid lock, a serial monitor display and LED that will be handled and determined by the mobile application.

CHAPTER 2

LITERATURE REVIEW

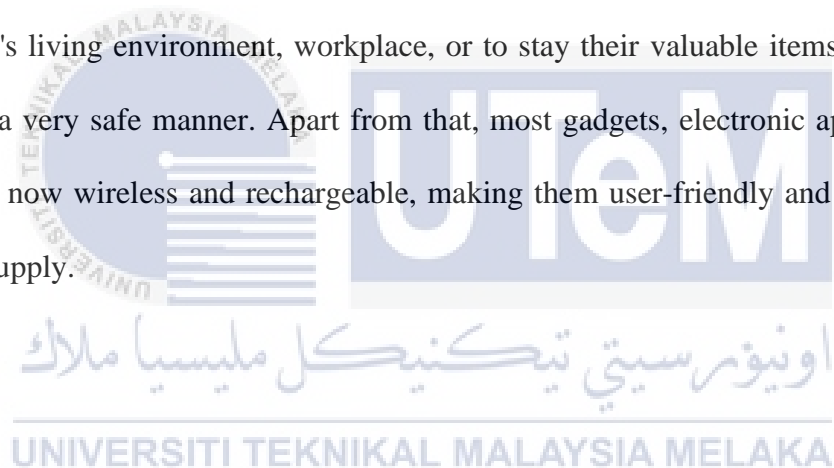
2.1 INTRODUCTION

In this chapter, the subject that associated with development of smart lock fingerprint door are going to be discussed well supported some review of some previous works, journals and articles. Several subtopics are discussed during this chapter, including related work, a critical overview of the present project, the intent, the approach, and therefore the conclusion. Furthermore, during this chapter we are going to also get to analyse any problems with the smart lock fingerprint door before come up with the solutions and concepts to beat the problems.

2.2 RELATED TOPICS

Many door access control systems utilized in banks, hospitals, schools, and residential buildings are operated by hand by various security services employed by the assorted organisations through the utilization of handles and locks with keys to work the locks. This system's validity, authenticity, and safety aren't ensured because an attacker will easily hack the lock by breaking or duplicating the key to get entry into a house. Keys could also be broken during use, necessitating replacement on several occasions, incurring extra costs for the user (Umar, 2018). However, Smart Lock Door System with specification of using biometric fingerprint-based identification which is more secured compared to other access control. supported (Md.Shahinur Rahman, 2019), fingerprint-based authentication has proven to be one among the foremost effective biometric methods for true identification additionally united of the foremost accurate standards for private identification. Biometric access control encompasses a higher level of authentication than traditional keys. Fingerprints are intricate,

one-of-a-kind, and long-lasting. It's used as a long-term identification marker. This sort of method even have been implemented for verifying the banking card and ID card. By using fingerprint- based access system may be implemented system using Android apps by Bluetooth. Supported by (Agbo David O., 2017), it'll bind to many computers, solving synchronisation issues besides also useful when transferring information between two or more devices that are near one another in low-bandwidth situations. Android application that implemented also able to allow users or owner to verify access via the appliance either for the unidentified and unenrolled users besides using password authentication system. As proposed by (Malabika Sarma, 2020) in her research paper, the system's multiple levels of protection will assist the user in ensuring precise security. The most explanation for the given device is to guard the user's living environment, workplace, or to stay their valuable items and essential documents in a very safe manner. Apart from that, most gadgets, electronic appliances, and equipment are now wireless and rechargeable, making them user-friendly and not reliant on direct power supply.



2.3 RELATED RESEARCH

As stated (Aleksander IBRO, 2019), the concept behind modern smart locks is to mix the functionality offered by simple and safe access control mechanisms with the convenience of internet networking and remote. There are some products on the market that have these systems, and that they had discuss two of them, reflecting on the features they need and any possible drawbacks. There are August Door Locks and Kwikset Kevo Locks. (Aleksander IBRO, 2019) The hardware on the lock, as seen in Figure 2.3.2, may signify whether or not the door is totally locked. There are many models available, each with a distinct price. A number of the costlier models have a webcam that enables people to work out who is at the outside door and whether or not they wish to open it for them. So as for the code to Figure 2.3.1, the recipient must have the smartphone download. August door locks have indeed been listed one among the simplest smart door lock solutions. they need a smartphone application that enables users to look the background of operation, like who locked and unlocked it at various times, as seen in Figure 2.3.1 users may grant digital keys to many friends from the smartphone app. So as for the sensor within the lock to sense those once they are nearby, whoever they share the code with must have the smartphone application.

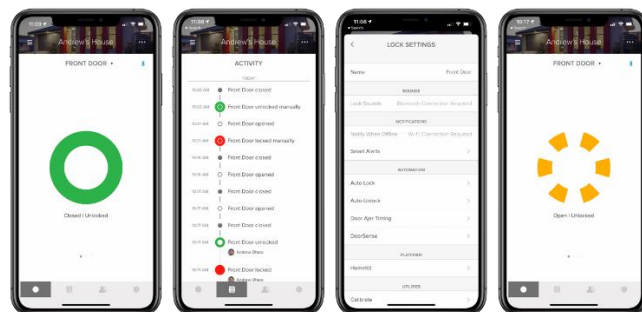


Figure 2.1: August Door Lock application on Android smartphone

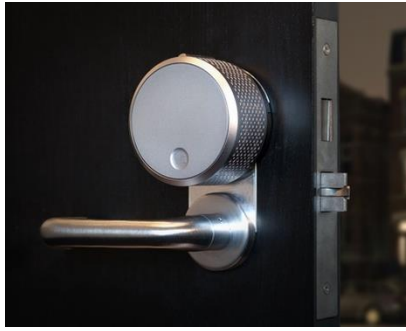


Figure 2.2: August Door Lock

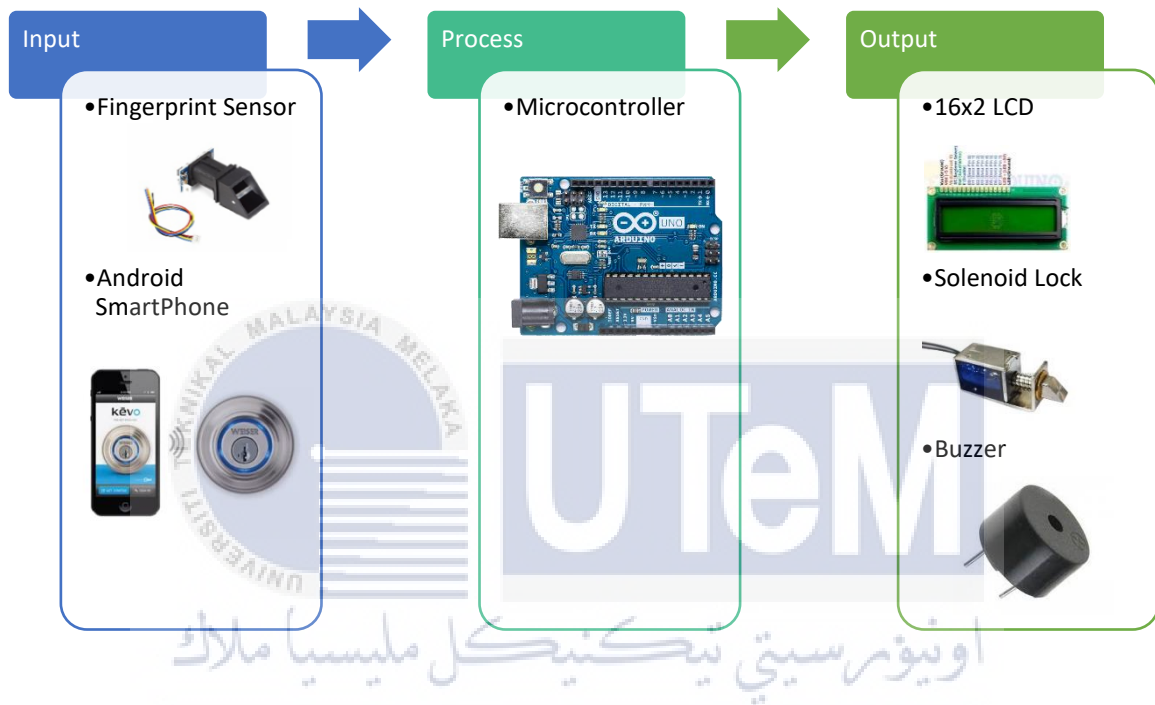
As for Kwikset Kevo Locks, as seen in Figure 2.3.4, are another popular brand of door locks where the locks have similar features, except to open the doorway, they use a wireless keypad. Since each user has their own access code, the lock's corresponding smartphone application may include a history of the lock's operation supported by (Aleksander IBRO, 2019). Owner or user can simply provide a replacement access code to friends or temporary users who need access to the house and set a cut-off date for the temporary user to access the lock. Users can't open the door supported proximity to their phone because everybody must use an access code.



Figure 2.3: Kwikset Kevo Lock

(Md.Shahinur Rahman, 2019) has stated in his research paper that with a standard lock, users cannot let any of their friends or guests to enter their home and open it if their doors are locked. If users lose their keys, they must either hire a locksmith or break the lock. This is this intelligent locking device comes into play. A lock that is permitted by a biometric reader and a person's fingerprint. This guarantees that the lock has been approved by a biometric reader and a person's fingerprint. This implies that only those

with registered fingerprint IDs may get access to the doors. Not only that, but the individual may wirelessly unlock his door from anywhere on the local area network. Hence this proposed project also will concentrate on automation and the usage of an embedded programming system to run. This lock system has some features, the basic two of which are wireless controller and fingerprint authentication.



As for microcontroller or platform which played a main role is that this system implementation there are several thought that has been proposed supported the research paper that I've got been studied. The Arduino microcontroller is the series' central processing unit (CPU). To perform specific functions, the microcontroller will be connected with other circuits. The Arduino microcontroller is powered by the IC ATmega328P-PU and operates by loading a previously developed and ready-to-use software. Stated by (Malabika Sarma, 2020), the biometric device employs an ATmega328P-based Arduino Uno, which is attached to an optical fingerprint sensor R305 for scanning the finger and a 16x2 LCD for providing instructions to users. The customer has the choice of enrolling two fingerprints with separate ID numbers. The

primary id is assigned to show on/off control circuitry, while the second id is assigned to access the home's door lock. If the automation system is turned on, the Android phone will be paired to the system's Bluetooth computer with a password, and therefore the equipment connected to the system will be remotely controlled using the Android app installed on the Smartphone. Besides (Karthik A Patil, 2020) also has stated in their research that they proposed Arduino Nano They picked Arduino Nano since it is a versatile working device that provides physical security by leveraging a biometric sensor found in a smartphone. The Arduino Nano board, like the Arduino UNO board, uses a comparable microcontroller, such as the Atmega328p. As a result, they may use similar software. The main contrast between these two is their size, due to the fact that the Arduino Uno board is double the size of the Arduino Nano board. As a result, Uno boards consume more system space. The Nano requires a tiny USB wire to be programmed, whereas the UNO can be programmed with a USB connection. According to (Dr. Mohd. Abdul Muqet, 2019), The Raspberry Pi analyses the information from the fingerprint module, then if the analysis is accurate, the system unlocks the door using a solenoid lock and permits entrance to the owner. It even has Wi-Fi and Built - in Bluetooth capabilities, allowing it to charge more powerful devices through USB ports. The Raspberry Pi 3 board is shown in Figure 2.3.6. A processor and graphics chip, as well as programme memory (RAM) and other interfaces and ports for external devices, are all found on the Raspberry Pi board.

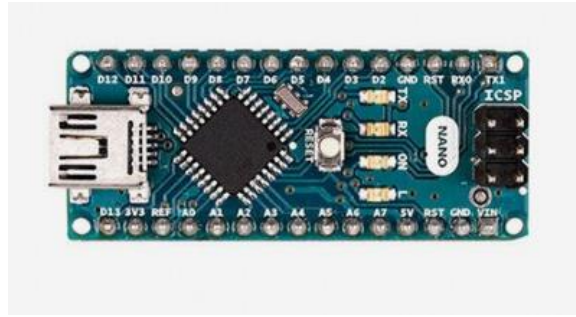


Figure 2.4: Arduino Nano microcontroller

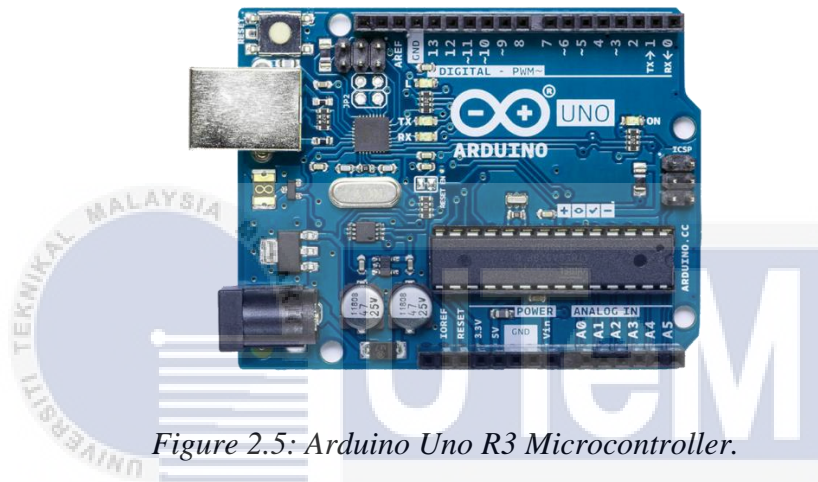


Figure 2.5: Arduino Uno R3 Microcontroller.



Figure 2.6: Raspberry Pi

According to the journal (K.Rajesh, 2019), fingerprint processing is divided into two stages: fingerprint registration and fingerprint matching (the matching can be 1:1 or 1:N). The user must enter his or her fingers twice when registering. The system will process the two-time finger pictures, generate a finger template based on the findings of the