

FINGERPRINT AUTHENTICATION SYSTEM FOR SERVER ROOM



**FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

BORANG PENGESAHAN STATUS LAPORAN

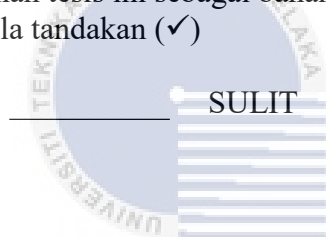
JUDUL: [FINGERPRINT AUTHENTICATION SYSTEM FOR SERVER ROOM]

SESI PENGAJIAN: [2020 / 2021]

Saya: NABILAH ZAYANI BINTI YAACOB

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

 SULIT

(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)

 TERHAD

(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)

 TIDAK TERHAD

nabilahzayani



(TANDATANGAN PELAJAR)

(TANDATANGAN PENYELIA)

Alamat tetap: 156, Jalan Bunga Raya,
3/1 Taman Cemara, 08000 Sungai
Petani, Kedah

DR. MOHD RIZUAN BIN BAHARON

Nama Penyelia

Tarikh: 03 SEPTEMBER 2021

Tarikh: 05 SEPTEMBER 2021

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak

FINGERPRINT AUTHENTICATION SYSTEM FOR SERVER ROOM

NABILAH ZAYANI BINTI YAACOB

B031810275



This report is submitted in partial fulfillment of the requirements for the
Bachelor of Computer Science (Computer Security) with Honour.

FAKULTI TEKNOLOGI MAKLUMAT DAN KOMUNIKASI
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled
[FINGERPRINT AUTHENTICATION SYSTEM FOR SERVER ROOM]
is written by me and is my own effort and that no part has been plagiarized
without citations.

STUDENT : NABILAH ZAYANI BINTI YAACOB Date : 3 SEPTEMBER 2021
([NAME OF STUDENT])



اونيورسيتي تيكنيكل مليسيا ملاك

— I hereby declare that I have read this project report and found
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
this project report is sufficient in term of the scope and quality for the award of
Bachelor of [Computer Science (Software Development)] with Honour.

A handwritten signature in black ink, appearing to be 'TS DR MOHD RIZUAN BIN BAHARON', is written over a horizontal line.

SUPERVISOR : _____ Date : 5 SEPTEMBER 2021
([TS DR MOHD RIZUAN BIN BAHARON])

DEDICATION

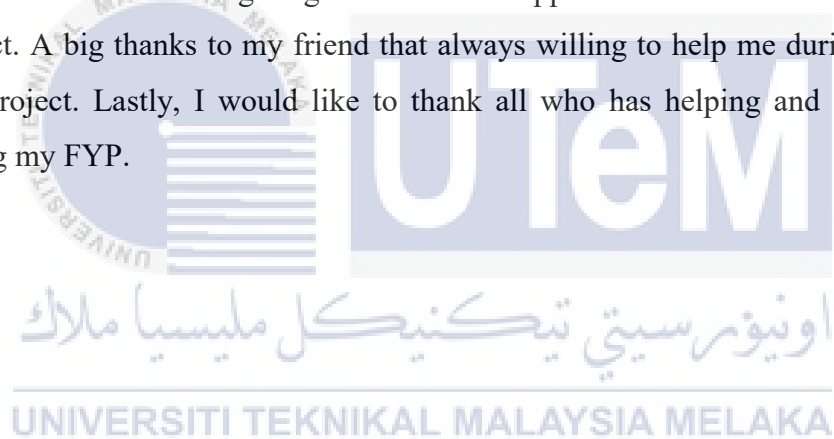
Specially dedicated to my beloved parents, Mr Yaacob bin Mat Zim and Mrs Zaini binti Zainol as well as to my siblings who always give the encouragement and support for me to complete this project. And not forgotten to my supervisor, Ts Dr Mohd Rizuan bin Baharon, who gave me a lot of guidance and advises throughout this project until it is successful. Lastly, thank you to all of you.



ACKNOWLEDGEMENTS

First and foremost, Alhamdulillah, thank you to Allah S.W.T for giving me spirit and strength to proceed with this project and going through all the problems to finally success to deliver it. I hereby would like to take this opportunity to thank the countless number of people who has involved in helping and assisting me while I completing this project and report in order to complete this degree.

Many thanks go to my supervisor, Ts Dr Mohd Rizuan bin Baharon for his support morally and physically, assistance, tolerance, guidance even when he is full with works as our faculty's head of department which proved to be invaluable as to completion of my project. Last but not least, I would like to thank my precious family who have been giving me ultimate support and motivation throughout my project. A big thanks to my friend that always willing to help me during completing this project. Lastly, I would like to thank all who has helping and supporting me during my FYP.



ABSTRACT

The Fingerprint Authentication System for Server Room is developed to protect a server room which considered as a critical infrastructure managed by an institution or an organization. This system mainly provides high security in accessing the server room. This system only allow an authorized user to access the server room. Hence, to access the server room employees need to record their fingerprint to the system in order to authenticate whether they are authorized user or not an authorized user. The administrators are able to monitor the system logs and when an unauthorized user tries to scan their fingerprint, a notification alert will be sent to the admin. Existing systems such as CA card scanner and password have several weaknesses. The key card may be easy to fit into the wallet but it is also easy to be stole or missing. Furthermore, passwords may be easily forgotten by the authorized user. This system offers many benefits to the user as it is convenient where the employees does not need to remember the password or bring the key card. Besides, the employee holds their own identity information themselves and the biometric links a person to an action. This Fingerprint Authentication System for Server Room has its own advantage compared to conventional fingerprint authentication system. This system is embedded with notification alert system that is implemented using Telegram. The administrator is allowed to identify an unauthorized user who has tries to access the room and allow the administrator to take a necessary action to protect the server room.

ABSTRAK

Sistem Pengesahan Jari untuk Ruang Pelayan (Server Room) dikembangkan untuk melindungi ruang pelayan yang dianggap sebagai infrastruktur kritikal yang dikendalikan oleh institusi atau organisasi. Sistem ini memberikan keselamatan yang tinggi dalam mengakses bilik pelayan. Sistem ini hanya membenarkan pengguna yang sah untuk mengakses bilik pelayan. Oleh itu, untuk mengakses ruangan pelayan, pekerja perlu merakam cap jari mereka ke sistem untuk mengesahkan sama ada pengguna sah atau bukan pengguna sah. Pentadbir dapat memantau log sistem dan apabila pengguna yang tidak sah berusaha merakam cap jari mereka, pemberitahuan peringatan akan dikirimkan kepada admin. Sistem yang ada seperti pengimbas kad CA dan kata laluan mempunyai beberapa kelemahan. Kad kunci mudah dimasukkan ke dalam dompet tetapi juga mudah dicuri atau hilang. Seterusnya, kata laluan mungkin mudah dilupakan oleh pengguna yang sah. Sistem ini menawarkan banyak faedah kepada pengguna kerana senang dan mudah di mana pekerja tidak perlu mengingat kata laluan atau membawa kad kunci. Selain itu, pekerja menyimpan maklumat identiti mereka sendiri dan biometrik menghubungkan seseorang dengan tindakan. Sistem Pengesahan Cap Jari ini untuk Bilik Pelayan mempunyai kelebihan tersendiri berbanding dengan sistem pengesahan cap jari konvensional. Sistem ini juga disertakan dengan sistem peringatan pemberitahuan yang dilaksanakan menggunakan Telegram. Pentadbir dibenarkan untuk mengenal pasti pengguna yang tidak dibenarkan yang telah cuba memasuki ruangan dan membenarkan pentadbir mengambil tindakan yang diperlukan untuk melindungi bilik pelayan.

TABLE OF CONTENTS

	PAGE
DEDICATION.....	III
ACKNOWLEDGEMENTS.....	IV
ABSTRACT.....	V
ABSTRAK.....	VI
TABLE OF CONTENTS.....	VII
LIST OF TABLES.....	XI
LIST OF FIGURES.....	XII
LIST OF ABBREVIATIONS.....	XIV
LIST OF ATTACHMENTS.....	XV
CHAPTER 1: INTRODUCTION.....	1
1.1 Project Background.....	1
1.2 Problem Statements.....	2
1.3 Project Questions.....	3
1.4 Objectives.....	3
1.5 Scope of the Project.....	3
1.6 Project Significance.....	3
1.7 Expected Outcome.....	4
1.8 Conclusion.....	4
CHAPTER 2: LITERATURE REVIEW.....	5
2.1 Biometric.....	5
2.2 How Does Biometric System Works?.....	7

2.3 Fingerprint Authentication.....	8
2.4 Fingerprint Minutiae (details).....	8
2.5 Why Fingerprint Authentication.....	10
2.6 Arduino Microcontroller.....	10
2.7 Fingerprint Module.....	11
2.8 ESP8266.....	12
CHAPTER 3: METHODOLOGY.....	14
3.1 Introduction.....	14
3.2 Project Methodology.....	14
3.2.1 Planning Phase.....	15
3.2.2 Requirement Analysis Phase.....	16
3.2.3 Design Phase.....	16
3.2.3.1 High Design Phase.....	16
3.2.3.2 Low Design Phase.....	16
3.2.3.3 Coding Phase.....	17
3.2.4 The System Prototype.....	17
3.2.5 Implementation Phase.....	17
3.2.6 Testing Phase.....	17
3.2.7 Maintenance Phase.....	18
3.3 Project Milestone.....	18
3.4 Block Diagram for Fingerprint System.....	20
3.4.1 Enrolment Phase.....	21
3.4.2 Verification Phase.....	22
3.5 Conclusion.....	23

CHAPTER 4: DESIGN	24
4.1 Introduction.....	24
4.2 Project Requirement.....	24
4.3 System Design.....	24
4.4 Process Flow.....	25
4.5 Hardware Requirements.....	25
4.5.1 Arduino Microcontroller.....	25
4.5.2 Fingerprint Scanner.....	26
4.5.3 ESP 8266.....	27
4.5.4 Breadboard.....	28
4.5.5 Jump Wires.....	29
4.5.6 LEDs.....	29
4.5.7 Resistors.....	30
4.6 Model Diagram.....	31
4.7 Conclusion.....	33
CHAPTER 5: IMPLEMENTATION	34
5.1 Introduction.....	34
5.2 Development Environment Setup.....	34
5.3 Hardware Development Setup.....	34
5.4 Software Development Setup.....	36
5.4.1 Fingerprint Authentication System for Server Room.....	36
5.5 Implementation Status.....	38
5.6 Conclusion.....	39
CHAPTER 6: TESTING	40

6.1 Introduction.....	40
6.2 Testing Plan.....	40
6.2.1 Testing Organization.....	40
6.2.2 Testing Schedule.....	41
6.3 Test Design.....	41
6.4 Test Result and Analysis.....	47
6.4.1 Arduino Uno connected with Fingerprint Sensor Test.....	47
6.4.2 Arduino IDE to enroll fingerprint Test.....	47
6.4.3 Save fingerprint in database Test.....	47
6.4.4 Fingerprint Authentication Test (Authorized User).....	48
6.4.5 Fingerprint Authentication Test (Unauthorized User).....	49
6.4.6 Notification Alert using Telegram Test.....	50
6.4.7 Comparison Confidence Level for each Fingerprint.....	52
6.5 Conclusion.....	53
CHAPTER 7: PROJECT CONCLUSION.....	54
7.1 Introduction.....	54
7.2 Project Summary.....	54
7.3 Challenges Project Development.....	55
7.4 Project Contribution.....	55
7.5 Conclusion.....	56
REFERENCES.....	57

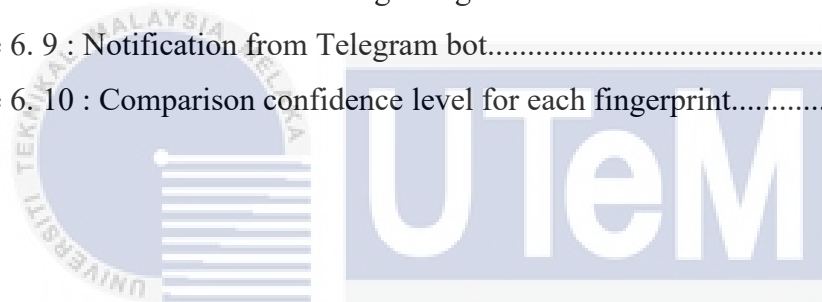
LIST OF TABLES

	PAGE
Table 5. 1 : Implementation Status.....	38
Table 6. 1 : List of testers.....	41
Table 6. 2 : Arduino Uno Test.....	42
Table 6. 3 : Fingerprint enrollment Test.....	43
Table 6. 4 : Fingerprint Authentication Test.....	44
Table 6. 5 : Node MCU ESP8266 Test.....	45
Table 6. 6 : Notification alert Test.....	46

LIST OF FIGURES

	PAGE
Figure 2. 1 : Taxonomy by Application type.....	6
Figure 2. 2 : Taxonomy by Technology Type.....	6
Figure 2. 3 : General procedure of biometric systems.....	7
Figure 2. 4 : Various stages in a typical minutiae algorithm.....	9
Figure 2. 5 : Arduino Microcontroller.....	11
Figure 2. 6 : Fingerprint Sensor Module.....	12
Figure 2. 7 : ESP8266 Module.....	13
Figure 3. 1 : A prototype model.....	15
Figure 3. 2 : اونيزر سیتی ٹیکنیکل ایما	19
Figure 3. 3 : Block Diagram for Fingerprint System.....	20
Figure 3. 4 : Flowchart Enrolment Phase.....	21
Figure 3. 5 : Flowchart of verification phase.....	22
Figure 4. 1 : Basic flow of the system.....	25
Figure 4. 2 : Arduino Microcontroller.....	26
Figure 4. 3 : Fingerprint Scanner.....	27
Figure 4. 4 : ESP8266 Module.....	28
Figure 4. 5 : Breadboard.....	28
Figure 4. 6 : Jump Wires.....	29
Figure 4. 7 : Light-emitting Diode (LEDs).....	30
Figure 4. 8 : Resistor.....	30
Figure 4. 9 : Circuit Diagram.....	31
Figure 4. 10 : Arduino Uno Circuit Diagram.....	32

Figure 4. 11 : ESP8266 Circuit Diagram.....	32
Figure 5. 1 : Arduino Uno Pinout.....	35
Figure 5. 2 : Set data rate for the sensor serial port.....	37
Figure 6. 1 : Connected to Fingerprint Sensor.....	47
Figure 6. 2 : Enroll fingerprint process.....	47
Figure 6. 3 : Fingerprint saved in database.....	47
Figure 6. 4 : Found ID with confidence level.....	48
Figure 6. 5 : Green Led for Authorized User.....	48
Figure 6. 6 : No match in database.....	49
Figure 6. 7 : Red Led for Unauthorized User.....	49
Figure 6. 8 : Chat box with bot using Telegram.....	50
Figure 6. 9 : Notification from Telegram bot.....	51
Figure 6. 10 : Comparison confidence level for each fingerprint.....	52



اونيورسيتي تيكنيكل مليسيا ملاك

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

LIST OF ABBREVIATIONS

FYP - **Final Year Project**



LIST OF ATTACHMENTS

		PAGE
Appendix A	Gantt Chart	59
Appendix B	Testing Results	61
Appendix C	System Coding	62



CHAPTER 1: INTRODUCTION

1.1 Project Background

Presently, the world has progressed in terms of information technologies and development of intelligent system that make life easier and safer. As a result, biometric technologies have given a considerable attention. Biometric procedures have evolved into a sophisticated and reliable means of identification that may aid in the development of something tremendously powerful for computing. Biometric is a subject in the field of science that automatically identify individuals based on their unique behavioral or physiological characteristics. One of it is fingerprints because of its ease of use, non-intrusiveness and reliability. The fingerprints are also unique for each of person even an identical twins.

The Fingerprint Authentication System is the most suitable to be used at server room because it can provide high security. The server room contains of the infrastructure that are important and necessary to support computing network systems, including design features like environmental control, fire suppression systems, power system redundancies, cable management and also airflow planning. It is also a collection of computer servers which usually maintained by an enterprise to accomplish any needs that the server should have. These facilities are equipped with high cost equipment. It can be only allow for the authorized users to enter and exit from this server room.

Besides, biometric system provides a securer solution comparing with key card identification or password verification because some of the server room may not have efficient security features to secure the room and the equipment in it. Currently, only a few of institutions that implement this type of security system while the others may using the key card and password verification. These type of security can be manipulated and stolen by unauthorized users. Hence, the Fingerprint Authentication System for Server Room is proposed

by using the Arduino to control the whole system that will be developed and a scanner for the fingerprint device.

Arduino is a free and open source microcontroller that can be readily programmed, erased, and reprogrammed. The Arduino platform was created to give students and professionals an affordable and simple approach to construct devices that can interact with the environment utilizing sensors and actuators. Next, like microcontrollers, it can operate as a small computer that accepts inputs and controlling output for a variety of electronic devices. Thus, it will let the administrator to be able to generate a database or report on the users that have entered the server room. This system may helps in eliminate the current problems and make the system more secure.

1.2 Problem Statements

The problems that occurs for this system to develop are :

The lack of security in the server room. There are some of the server room that still not have efficient security features to secure the room and the equipment in it. The factor that contribute to the lack of the security of the server room are

- a) Key Card Deficiency. Key card is easy to fit snuggly into wallet and portable to bring anywhere which it can be easily stolen by unauthorized user anytime. Many key cards can be easily hacked using inexpensive devices.
- b) Password. Authorized users need to enter user ID and password to enter the server room but they might also forget the password or the password can be stolen by any unauthorized user just by seeing it. Password also need to change frequently to avoid any attacks from the hackers.

1.3 Project Questions

1. How to develop a fingerprint authentication system for securing a server room?
2. How to notify the unauthorized access to the server room?
3. How to evaluate the functionality of the fingerprint authentication system?

1.4 Objectives

This project embarks on the following objectives:

1. To develop fingerprint authentication system by using Arduino Uno and fingerprint scanner.
2. To develop a notification alert system that integrate with the fingerprint authentication system by using ESP8266 and Telegram.
3. To evaluate the functionality of the fingerprint authentication system by using Arduino IDE.

1.5 Scope of the Project

The scope will be divided into two which are

1. Administrator - The system will required the admin to register information. The admin can also view the employee's admission.
2. Employee - The system required the employees to register the fingerprint information. Employees need to scan their fingerprint to enter the server room.

1.6 Project Significance

This Fingerprint Authentication System for Server Room will offer the following benefits to the community

1. Convenience - The user or employee no longer need to remember the password or bring the key card every time they wanted to enter the server room
2. Local Verification - The user hold their identity information themselves, hence there is unnecessary for them to verify identity
3. Great Security - The biometric link a person to an action . User identity is stored securely and tamper free

1.7 Expected Outcome

The Fingerprint Authentication System for Server Room will be built with Arduino and a scanner to ensure that it can scan and authenticate fingerprints for authorized users. Following that, the administrator will receive notifications about their employees' logs via their smartphone application after using the fingerprint scanner.

1.8 Conclusion

In summary, to remove the problems that have been occur in the existing system, the Fingerprint Authentication System for Server Room is proposed. This system will be improved from the current systems to make it more secure for the server room.

CHAPTER 2: LITERATURE REVIEW

2.1 Biometric

Biometrics are the measurements and calculations of a person's unique physical and behavioral features taken from their body. For thousands of years, humans have used bodily traits such as face, voice, and others to recognize one another. In the mid-nineteenth century, Alphonse Bertillon, the chief of the criminal identification team in Paris, devised and practised the idea of using body measurements to identify criminals. In computer science, this technology is used as a form of identification, access control and identifying individuals who are under surveillance.

Generally, biometrics identifiers are distinctive, which only measurable characteristics are used to label and describe any individual. Biometric identifiers often categorized as a physiological characteristics, which are related to the shape of the body. Fingerprints, eye retinas and irises, face patterns, and hand measurements are examples of physical traits. It is related to a person's pattern of behaviour, such as typing rhythm, keystroke, signature, and voice, for behavioral features. Every person can be accurately identified by their physical and behavioral attributes, according to the core assumption of biometric authentication. The term biometrics is derived from a Greek words bio, meaning life and metric, meaning to measure.

Biometrics is a term that refers to a measurable physical or behavioral trait of a person. Universality, uniqueness, permanence, collectable, and acceptability should all be met by the physical and behavioral qualities chosen to establish identity. It is divided into two categories: application type and technology type.

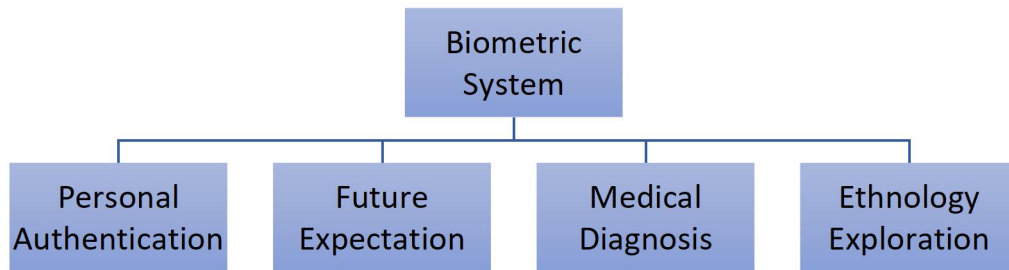


Figure 2. 1 : Taxonomy by Application type

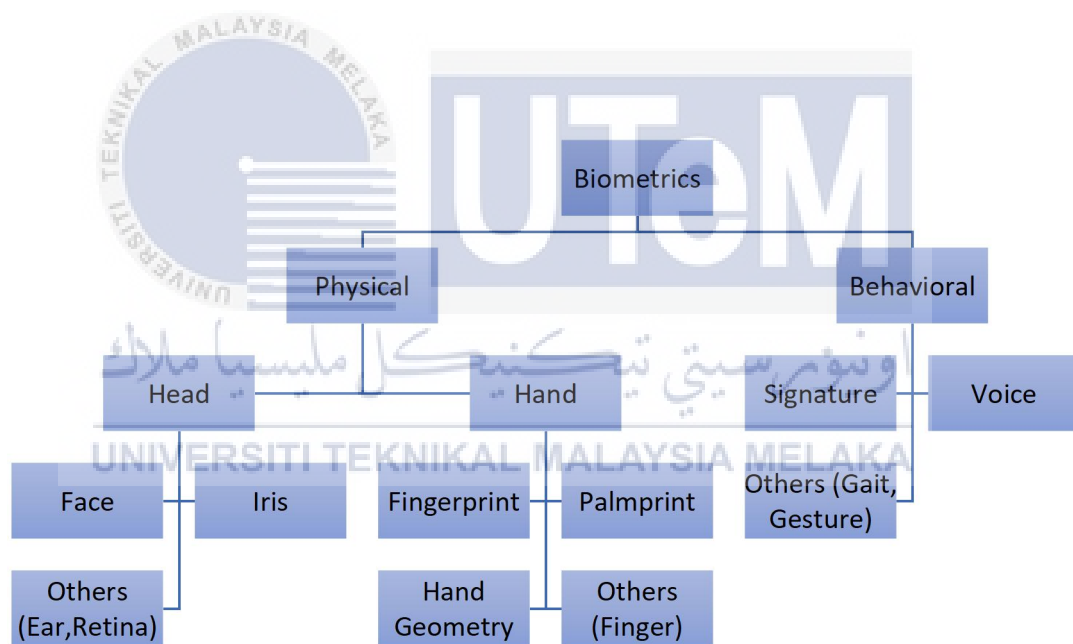


Figure 2. 2 : Taxonomy by Technology Type

2.2 How Does Biometric System Works?

Biometric system consists of two different parts which are enrollment part and identification part. Firstly, enrollment part needs to have user's characteristic registered to make sure it can be used as a basis when identification is performed. While identification part allows the user interface to have the end user's characteristics to be captured and verified. All the system follow the exact same function procedure even it may be based on different trait or characteristic. The enrollment part contains of sample capturing, feature extraction and storage while the identification part contains of four stages which are capture, feature extraction, comparison and decision.

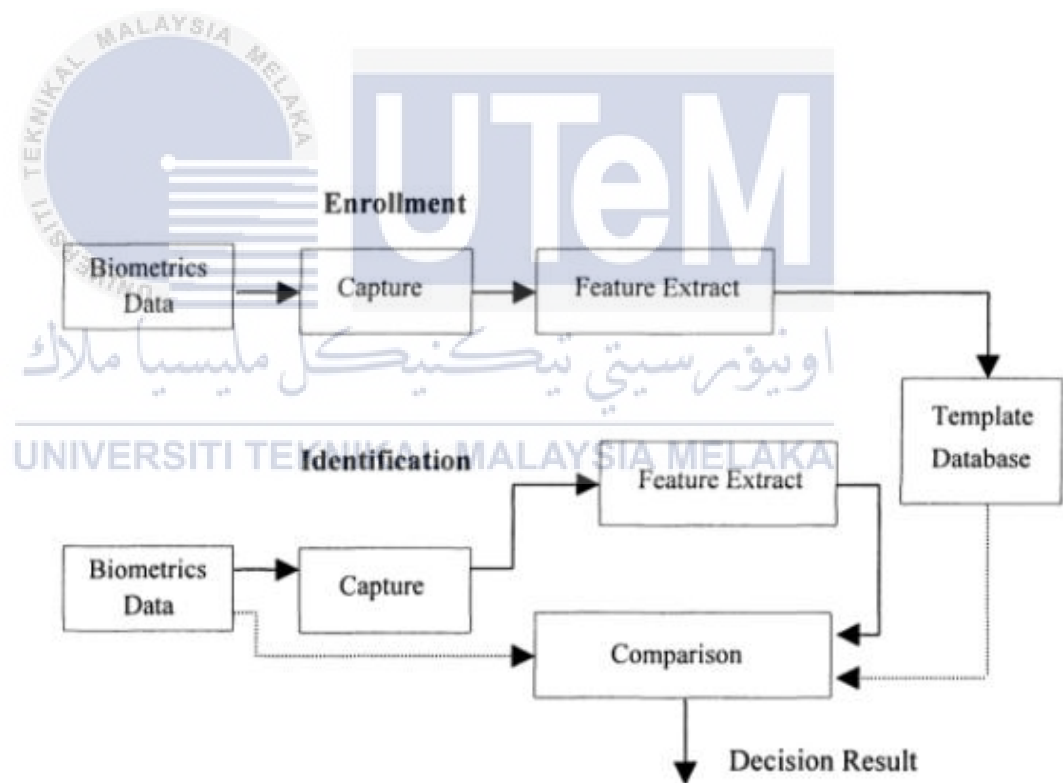


Figure 2. 3 : General procedure of biometric systems