



**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**

**BORANG PENGESAHAN STATUS LAPORAN  
PROJEK SARJANA MUDA II**

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

Sesi Pengajian : **1/20222023**

Saya **MUHAMMAD HAIQAL BIN SAIFUL NIZAM** mengaku membenarkan laporan Projek Sarjana Muda ini disimpan di Perpustakaan dengan syarat-syarat kegunaan seperti berikut:

1. Laporan adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan laporan 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)

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

**TIDAK TERHAD**

Disahkan oleh:



(TANDATANGAN PENULIS)

Alamat Tetap: NO88, LORONG SERI KELEDANG ½, TAMAN SERI KELEDANG, 71700 MANTIN, NEGERI SEMBILAN.

(COB DAN TANDATANGAN PENYELIA)

Ir. Ts. Dr. MOHD FAUZI BIN AB RAHMAN

Pensyarah Kanan

Jabatan Teknologi Kejuruteraan Elektronik dan Komputer  
Fakulti Teknologi Kejuruteraan Elektrik dan Elektronik  
Universiti Teknikal Malaysia Melaka

Tarikh: 13 JANUARY 2023

Tarikh: 13 JANUARY 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.

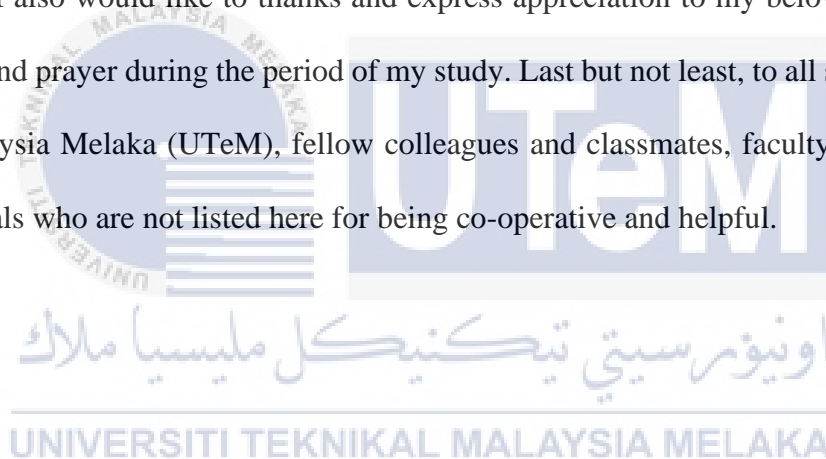


## ACKNOWLEDGEMENTS

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

|   |            |
|---|------------|
| <b>ABSTRAK</b>  | <b>i</b>   |
| <b>ACKNOWLEDGEMENTS</b>   | <b>iii</b> |
| <b>TABLE OF CONTENTS</b>  | <b>iv</b>  |
| <b>LIST OF TABLES</b>   | <b>vi</b>  |
| <b>LIST OF FIGURES</b>  | <b>vii</b> |
| <b>LIST OF APPENDICES</b>   | <b>ix</b>  |
| <b>LIST OF SYMBOLS</b>  | <b>7</b>   |
| <b>LIST OF ABBREVIATIONS</b>  | <b>8</b>   |
| <b>CHAPTER 1 INTRODUCTION</b>   | <b>9</b>   |
| 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         |
| <b>CHAPTER 2 LITERATURE REVIEW</b>  | <b>14</b>  |
| 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         |
| <b>CHAPTER 3 METHODOLOGY</b>  | <b>29</b>  |
| 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        |
| <b>CHAPTER 4</b> | <b>RESULTS AND DISCUSSION</b>               | <b>38</b> |
| 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        |
| <b>CHAPTER 5</b> | <b>CONCLUSION AND FUTURE WORKS</b>          | <b>49</b> |
| 5.1              | Conclusion                                  | 49        |
| 5.2              | Future Works                                | 49        |
|                  | <b>REFERENCE</b>                            | <b>50</b> |
|                  | <b>APPENDICES</b>                           | <b>51</b> |



## 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

|               |                              |
|---------------|------------------------------|
| $\mu\text{V}$ | Microvolts                   |
| $\alpha$      | Alpha                        |
| $\beta$       | Beta                         |
| $\gamma$      | Gamma                        |
| $\Delta$      | Delta                        |
| $\theta$      | Theta                        |
| Hz            | Hertz                        |
| V             | Volt                         |
| dB            | Daubechies                   |
| $\psi$        | Wavelet coefficients         |
| $\tau$        | Tau                          |
| VCC           | Voltage Common<br>Collector  |
| GND           | Ground                       |
| RX            | Receiver                     |
| TX            | Transmitter                  |
| $a$           | Scaling Parameter            |
| $b$           | Location of the<br>Parameter |
| %             | Percentage                   |



## LIST OF ABBREVIATIONS

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

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

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. <sup>5</sup> |
| 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  |

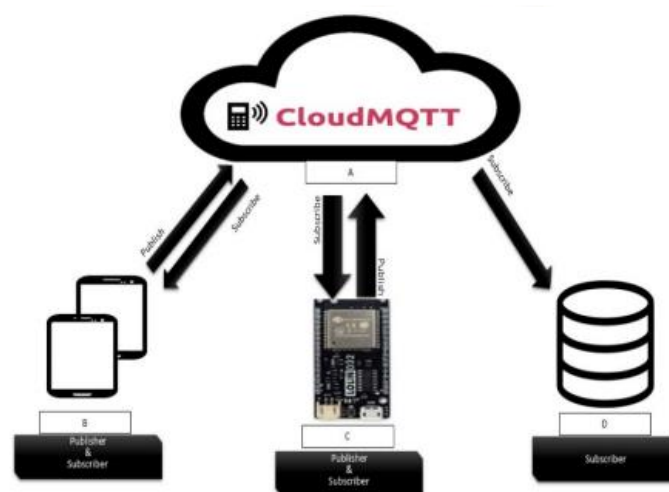


Figure 2.1 : Architecture Design