CLOUD AND FINGERPRINT BASED LICENSE AUTHENTICATION SYSTEM

A PROJECT REPORT

submitted to

University of Kashmir

By

Nayeem Tariq Magray	**15203135016**
Syed Yasir Rafi	**15203135046**
Aabid Hassan Najar	**15203135052**
Kaisar Ali Dar	**15203135065**
Waseem Ahmad Mir	**15203135048**

In partial fulfilment of the award of the degree

Of

BACHELOR OF TECHNOLOGY / ENGINEERING

In

ELECTRONICS AND COMMUNICATION ENGINEERING

Department of Electronics and Communication Engineering

University of Kashmir

SRINAGAR

DECEMBER 2019

UNIVERSITY OF KASHMIR

SRINAGAR

CERTIFICATE

This is to certify that the project entitled "**CLOUD AND FINGERPRINT BASED LICENSE VERIFICATION AND AUTHENTICATION SYSTEM**" submitted by **NAYEEM TARIQ MAGRAY, SYED YASIR RAFI, AABID HASSAN NAJAR, KIASAR ALI DAR AND WASEEM AHMAD MIR** to SSM College of Engineering and Technology, Divar Parihaspora, Pattan in partial fulfilment of the award of the degree of Bachelor of Engineering in Electronics and Communication Engineering is a bonafide record of the project work carried out by them.

ER. MANZOOR AHMAD MIR
H.O.D (Department of ECE)

Majid Darvesh
(Project guide)

PROF. (DR.) SAJAD HUSSAIN
PRINCIPAL

ACKNOWLEDGMENT

"Achievement is finding out what you would be doing, what you have to do. The higher the summit, higher will be the climb." It has been rightly said that we are built on the shoulders of others but the satisfaction that accompanies the successful completion of any task would be incomplete without the mention of the people who made it possible.

We express our deep sense of gratitude towards **MR. MANZOR AHMAD MIR**, HOD, Department of ECE & **MR. MAJID DARVESH,** PROFESSOR, Department of ECE who have been a constant source of inspiration for us throughout this work.

I would like to thank **MR. ARSHID IQBAL KHAN,** PROFESSOR, University of Kashmir for providing the facilities for the completion of Project work. Because of which we were able to learn the minute aspects of our project work.

At last we want to share our sincere gratitude to all those who helped me in completion of this project. During the work we faced many challenges due to my lack of knowledge and experience, but these people helped us to get over from all the difficulties and in final compilation of our Idea to a shaped sculpture.

Abstract

Index Term: *Fingerprint identification, Fingerprint verification, Wi-Fi technology, Google Firebase (Cloud)*

This project provides the design method of fingerprint based driving license authentication system. The system includes terminal fingerprint acquisition, fingerprint matching and verification process, wireless transmission, Google Firebase (Cloud). The current system involves manual verification of license which is difficult to monitor. The issues of forgery of licenses by some people are a serious issue from the security point of view. The issues regarding the fake identity have been raised. In order to overcome such problems and to achieve the simple and high real-time system, we are proposing a low-cost and high-performance wireless driving license verification function, which provides a new wireless driving license system which will be helpful for traffic police and RTOs.

CONTENTS **Page**

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

To start with the project, it is essential to know the requirements and scope of the project. For a country which ranks second in the global population, keeping the track of each person is very essential. Developed countries like USA, UK, and other developed countries, have implemented 24 hours traffic surveillance but the cost incurred is too high. Instead of that we can implement "Cloud And Fingerprint Based Driving License Authentication".

The fingerprint scanning is most convenient method and has a lot of advantages, such as its unique, permanent, good, anti-fake and easy to use. So it is recognized increasingly by people. Recently while **"ADHAR CARD"** was introduced the finger prints were collected. The data of fingerprints of each person is stored. In same way, we have also created a real time database, which contains fingerprint and other details of the license holders. The most prominent feature is that we can track the previous violations so that the data can be used while dealing with the situations like "High Alert". This Project Single headedly deals with the problems like "**Identity Theft"** and "**Document Forgery".**

The working conditions in which it is to be used creates most of the complications as we can't make the device delicate and bulky. So the wireless technology is used so that the device can be used as a handheld device which enhances its usability.

For wireless communication we are using Wi-Fi module. Wi-Fi technology is an emerging technology developed in recent years. Comparing with some existing wireless communication technologies, Wi-Fi is advantageous in terms of low-power and low-cost. It is very suitable for application to wireless sensor networks. With reliable wireless performance and battery operation, Wi-Fi gives you the freedom and flexibility to do more. The device if produced at larger scale will not be costly and will be compact enough to be handled easily.

Aiming at the disadvantages of traditional manual driving license verification system, a design method of wireless driving license verification system is proposed. It achieves license verification by fingerprint identification. It is low-cost, low-power and provides high performance.

CHAPTER 2

EXISTING SYSTEM

The present driving license checking system is not an efficient way for authenticating licenses because nowadays anyone can produce a counterfeit license easily and it's very difficult for traffic police to identify whether driving license is genuine or counterfeit. Recently in an Indian newspaper, The Indian Express claimed that over 50 million motorists driving with fake license. Almost every third driving license in India could be ‘bogus’ with a staggering number of over 50 million people driving on roads with fake documents, according to official data.

Also, if a person forgets to carry his driving license or loses it, he will get penalized.

Drawbacks of existing system

- Document forgery.
- Identity theft.
- Lack of security.
- No record of previous violations committed by the driver.

Fig 2.1: Fake License Cards

Chapter 3

PROPOSED SYSTEM

Our proposed system consists of Fingerprint module, Wi-Fi module, Microcontroller and Cloud (Real-time Database). Fingerprint module is used to realize fingerprint collecting. Wi-Fi module is used to send and receive data from the database. To control all these external devices along with LCD, a microcontroller is used. Database is used to store the pre-recorded finger prints and data related to those and realize fingerprint extraction and matching in order to verify the license.

When a person is needed to be verified as a license holder his fingerprint is scanned. If the fingerprint scanned matches with the stored fingerprint in database, license is verified and data related will be displayed. If it does not match then the person is not licensed.

Advantages of Proposed System

- Efficient and highly secure.
- No concern of losing or carrying a driving license.
- Any change in person's data can be done only in database and it's a real time database i.e., any change in data present in database will be reflected on system within few seconds.
- Since fingerprints are the composition of protruding sweat glands, everyone has collection of wavy, curvy shape unique fingerprints. They do not change naturally.
- Fingerprint recognition or identification equipment is relatively less costly compared to other biometric system and R&D investments are very robust in this field.
- It avoids fraud & duplication.

CHAPTER 4

SYSTEM DESIGN

The system includes: Fingerprint module, Microcontroller NodeMCU with in built Esp8266 Wi-Fi module, 20x4 LCD, Power supply and Google Firebase.

4.1 BLOCK DIAGRAM

The block diagram consists of a fingerprint module that captures each person's fingerprint and converts it into binary form and assigns a unique ID to it. The sensor forms the core part of the fingerprint module. The fingerprint module is connected to the NodeMCU. The NodeMCU processes this ID and sends it to Google firebase through Wi-Fi module in-built on the NodeMCU. In Google firebase, the received ID is matched with the IDs stored in the Google firebase. If there is match, the Google firebase forwards all the details for this particular ID to the NodeMCU. The NodeMCU processes these details and then displays on the LCD. However, if there is no match in the Google firebase then "No Data Found" will be displayed on the LCD.

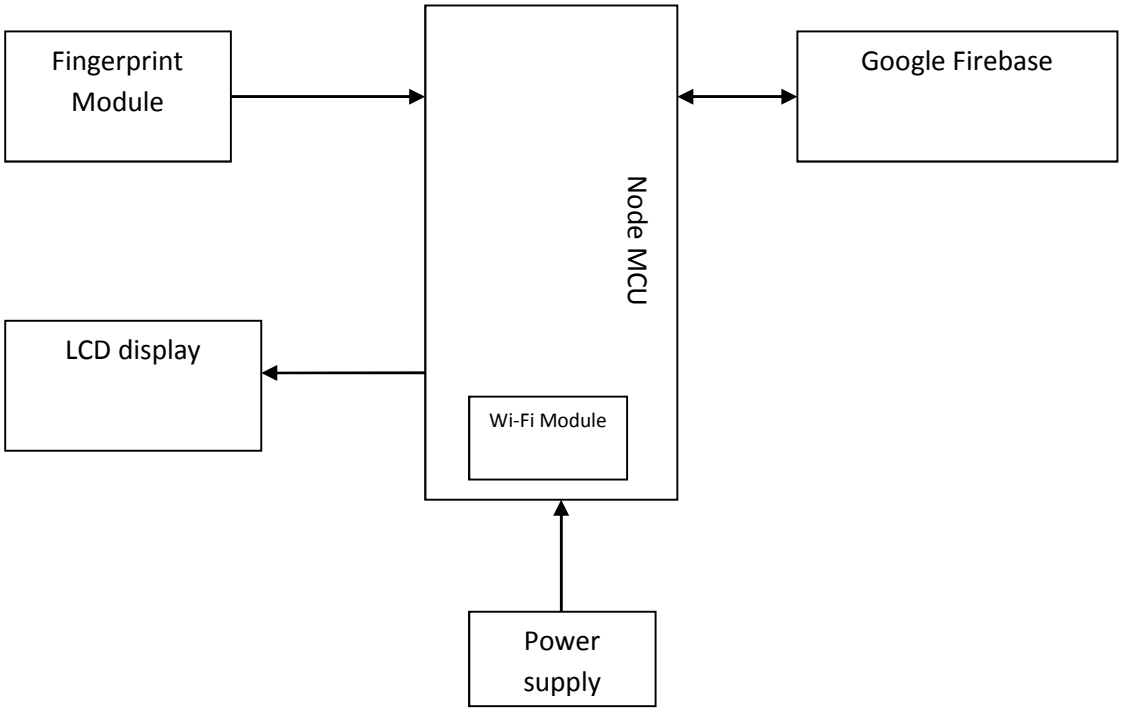


Fig4.1: Block Diagram

CHAPTER 5

COMPONENT DESCRIPTION

The hardware consists of following components:

- LCD display.
- Fingerprint Module.
- NodeMCU with inbuilt Esp8266 Wi-Fi module.
- Power Supply.

5.1 LCD Display:

LCDs are broadly used in electronics projects as they are good for displaying information like License holder data from our project, and also they are very cheap.

It has 16 pins and the first one from left to right is the Ground pin. The second pin is the VCC which we connect the 5 volts pin on the NodeMCU Board. Next is the Vo pin on which we can attach a potentiometer for controlling the contrast of the display. Next, the RS pin or register select pin is used for selecting whether we will send commands or data to the LCD. For example if the RS pin is set on low state or zero volts, then we are sending commands to the LCD like: set the cursor to a specific location, clear the display, turn off the display and so on. And when RS pin is set on High state or 5 volts we are sending data or characters to the LCD. Next comes the R / W pin which selects the mode whether we will read or write to the LCD. Here the write mode is obvious and it is used for writing or sending commands and data to the LCD. Next is the E pin which enables the writing to the registers, or the next 8 data pins from D0 to D7. So through this pins we are sending the 8 bits data when we are writing to the registers. And the last two pins A and K, or anode and cathode are for the LED back light.

Since the NodeMCU doesn't have that many pins, therefore we use **I2C protocol** which uses just 4 pins of NodeMCU to interface it with the 16pin LCD Display.

I2C (Inter-Integrated Circuit) is serial bus interface connection protocol. It is also called as **TWI** (two wire interface) since it uses only two wires for communication. Those two wires are **SDA** (serial data) and **SCL** (serial clock). I2C is acknowledgment based communication protocol i.e. transmitter checks for an

acknowledgment from the receiver after transmitting data to know whether data is received by receiver successfully.

I2C works in two modes namely,

- Master mode
- Slave mode

SDA (serial data) wire is used for data exchange in between master and slave device. **SCL** (serial clock) is used for the synchronous clock in between master and slave device.

Master device initiates communication with a slave device. Master device requires slave device address to initiate conversation with a slave device. Slave device responds to master device when it is addressed by a master device.

NodeMCU has I2C functionality support on its GPIO pins. Due to internal functionality on ESP-12E, we cannot use all its GPIOs for I2C functionality.

Master Device: NodeMCU

Slave Device: LCD Display

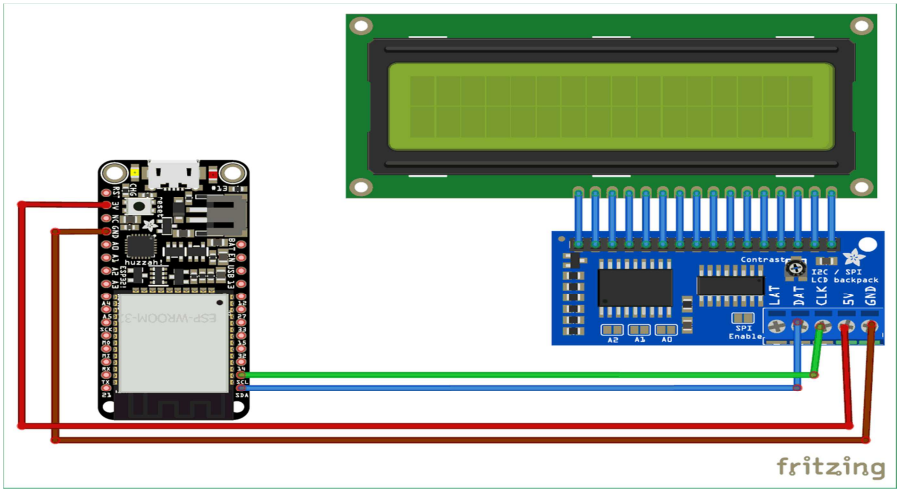


Fig5.1: Interfacing LCD with NodeMCU using I2C protocol

5.2 NodeMCU:

NodeMCU is an open source LUA based firmware developed for ESP8266 Wi-Fi chip. By exploring functionality with ESP8266 chip, NodeMCU firmware comes with ESP8266 Development board/kit i.e. NodeMCU Development board. NodeMCU Dev Kit/board consists of ESP8266 Wi-Fi enabled chip. The **ESP8266** is a low-cost Wi-Fi chip developed by Espressif Systems with TCP/IP protocol. It uses the 2.4 GHz band and it can operate with baud rates from 250 kbps up to 2 Mbps. If used in open space and with lower baud rate its range can reach up to 100 meters. The power consumption of this module is just around 12mA during transmission, which is even lower than a single LED. The operating voltage of the module is from 1.9 to 3.6V, but the good thing is that the other pins tolerate 5V logic, so we can easily connect it to an Arduino without using any logic level converters.

ESP8266 pinning, or in other words, NodeMCU comes with USB input. The NodeMCU is formed by an ESP12E, which still has an ESP8266EX inside it.

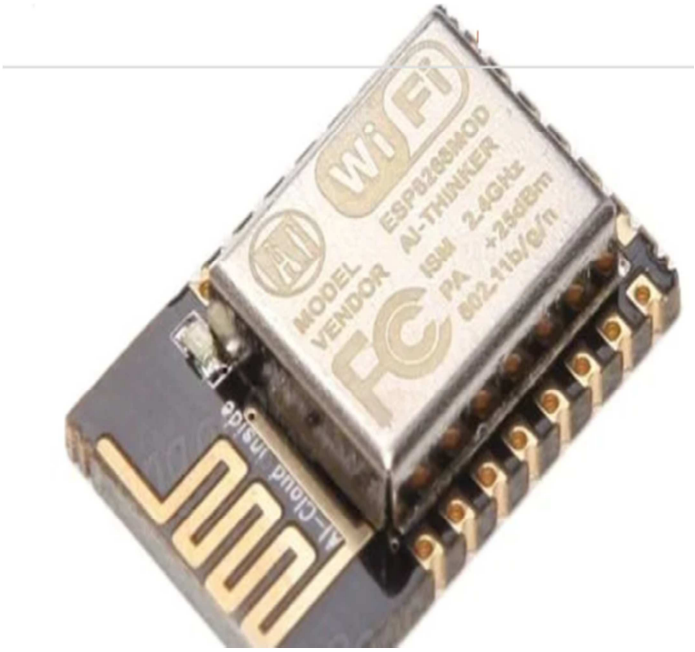


Fig5.2 ESP8266EX

The term NodeMCU usually refers to the firmware, while the board is called Devkit. NodeMCU Devkit 1.0 consists of an ESP-12E on a board, which facilitates its use. It also has a voltage regulator, a USB interface.

The ESP-12E is a board created by AI-THINKER, which consists of an ESP8266EX inside the metal cover.

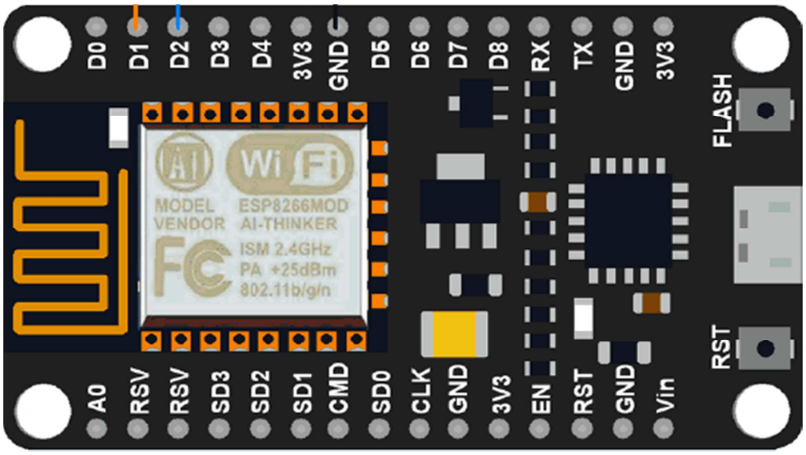
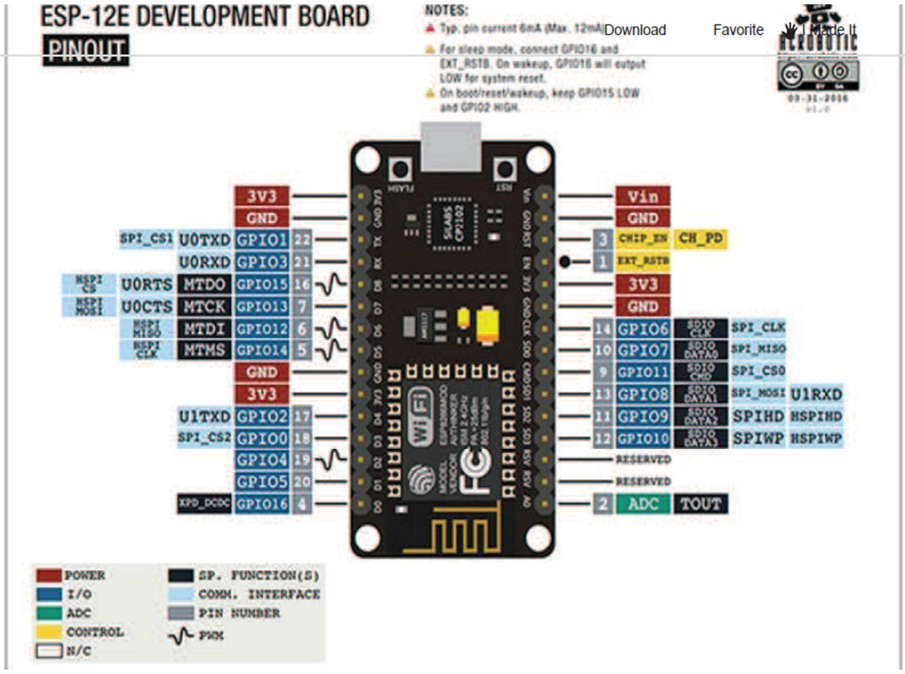


Fig5.3 NodeMCU Devkit 1.0

5.2.1 NodeMCU 1.0 ESP-12E Pin out:-



5.2.2 ESP8266EX:-

Espressif's ESP8266EX delivers highly integrated Wi-Fi SoC solution to meet users' Continuous demands for efficient power usage, compact design and reliable performance in the Internet of Things industry. With the complete and self-contained Wi-Fi networking capabilities, ESP8266EX can perform either as a standalone application or as the slave to a host MCU. WhennESP8266EX hosts the application, it promptly boots up from the flash. The integrated highspeed cache helps to increase the system performance and optimize the system memory. Also, ESP8266EX can be applied to any microcontroller design as a Wi-Fi adaptor through SPI/SDIO or UART interfaces. ESP8266EX integrates antenna switches, RF balun, power amplifier, low noise receive amplifier, filters and power management modules. The compact design minimizes the PCB size and requires minimal external circuitries.

Besides the Wi-Fi functionalities, ESP8266EX also integrates an enhanced version of Tensilica's L106 Diamond series 32-bit processor and on-chip SRAM. It can be interfaced with external sensors and other devices through the GPIOs. Software Development Kit (SDK) provides sample codes for various applications.

Espressif Systems' Smart Connectivity Platform (ESCP) enables sophisticated features including:

• Fast switch between sleep and wakeup mode for energy-efficient purpose;

• Adaptive radio biasing for low-power operation

• Advance signal processing

• Spur cancellation and RF co-existence mechanisms for common cellular, Bluetooth, DDR, LVDS, LCD interference mitigation

Wi-Fi Key Features:

- 802.11 b/g/n support
- 802.11n support (2.4 GHz), up to 72.2 Mbps
- Defragmentation
- 2 x virtual Wi-Fi interface
- Automatic beacon monitoring (hardware TSF)
- Support Infrastructure BSS Station mode/SoftAP mode/Promiscuous mode
- Antenna diversity

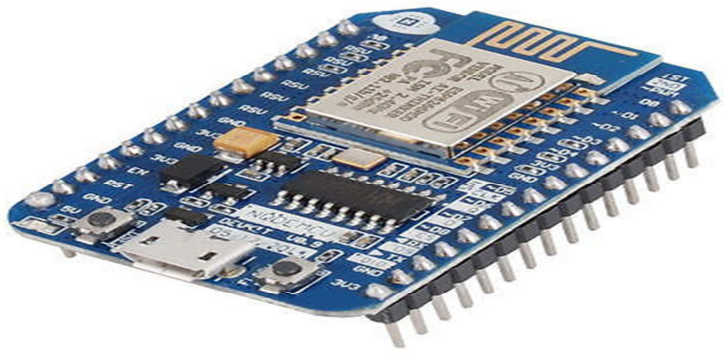


Fig5.4: NodeMCU with ESP8266EX

5.2.3 Specifications:-

Table 1-1. Specifications

Categories	Items	Parameters
Wi-Fi	Certification	Wi-Fi Alliance
	Protocols	802.11 b/g/n (HT20)
	Frequency Range	2.4G – 2.5G (2400M – 2483.5M)
	TX Power	802.11 b: +20 dBm
		802.11 g: +17 dBm
		802.11 n: +14 dBm
	Rx Sensitivity	802.11 b: –91 dbm (11 Mbps)
		802.11 g: –75 dbm (54 Mbps)
		802.11 n: –72 dbm (MCS7)
	Antenna	PCB Trace, External, IPEX Connector, Ceramic Chip
Hardware	CPU	Tensilica L106 32-bit processor
	Peripheral Interface	UART/SDIO/SPI/I2C/I2S/IR Remote Control
		GPIO/ADC/PWM/LED Light & Button
	Operating Voltage	2.5V – 3.6V
	Operating Current	Average value: 80 mA
	Operating Temperature Range	–40°C – 125°C
	Package Size	QFN32-pin (5 mm x 5 mm)
	External Interface	-
Software	Wi-Fi Mode	Station/SoftAP/SoftAP+Station
	Security	WPA/WPA2
	Encryption	WEP/TKIP/AES
	Firmware Upgrade	UART Download / OTA (via network)
	Software Development	Supports Cloud Server Development / Firmware and SDK for fast on-chip programming
	Network Protocols	IPv4, TCP/UDP/HTTP
	User Configuration	AT Instruction Set, Cloud Server, Android/iOS App

5.2.4 ESP8266EX Radio:

ESP8266EX radio consists of the following blocks.

- 2.4 GHz receiver
- 2.4 GHz transmitter
- High speed clock generators and crystal oscillator
- Bias and regulators
- Power management

2.4 GHz Receiver

The 2.4 GHz receiver down-converts the RF signals to quadrature baseband signals and converts them to the digital domain with 2 high resolution high speed ADCs. To adapt tovarying signal channel conditions, RF filters, automatic gain control (AGC), DC offset cancelation circuits and baseband filters are integrated within ESP8266EX.

2.4 GHz Transmitter

The 2.4 GHz transmitter up-converts the quadrature baseband signals to 2.4 GHz, and drives the antenna with a high-power CMOS power amplifier. The function of digital calibration further improves the linearity of the power amplifier, enabling a state of art performance of delivering +19.5 dBm average TX power for 802.11b transmission and +18 dBm for 802.11n (MSC0) transmission.

Additional calibrations are integrated to offset any imperfections of the radio, such as:

- Carrier leakage
- I/Q phase matching
- Baseband nonlinearities
- These built-in calibration functions reduce the product test time and make the test
- equipment unnecessary.

Clock Generator

The clock generator generates quadrature 2.4 GHz clock signals for the receiver and transmitter. All components of the clock generator are integrated on the chip,

including all inductors, varactors, loop filters, linear voltage regulators and dividers. The clock generator has built-in calibration and self test circuits. Quadrature clock phases and phase noise are optimized on-chip with patented calibration algorithms to ensure the best performance of the receiver and transmitter.

5.2.5 Wi-Fi

ESP8266EX implements TCP/IP and full 802.11 b/g/n WLAN MAC protocol. It supports Basic Service Set (BSS) STA and SoftAP operations under the Distributed Control Function (DCF). Power management is handled with minimum host interaction to minimize active duty period.

4.2.5a Wi-Fi Radio and Baseband

The ESP8266EX Wi-Fi Radio and Baseband support the following features:

- 802.11b and 802.11g
- 802.11n MCS0-7 in 20 MHz bandwidth
- 802.11n 0.4 μs guard-interval
- up to 72.2 Mbps of data rate
- Receiving STBC 2x1
- Up to 20.5 dBm of transmitting power
- Adjustable transmitting power
- • Antenna diversity

5.2.5b Wi-Fi MAC

The ESP8266EX Wi-Fi MAC applies low-level protocol functions automatically, as follows:

- 2 × virtual Wi-Fi interfaces
- Infrastructure BSS Station mode/SoftAP mode/Promiscuous mode
- Request To Send (RTS), Clear To Send (CTS) and Immediate Block ACK
- Defragmentation
- CCMP (CBC-MAC, counter mode), TKIP (MIC, RC4), WEP (RC4) and CRC
- Automatic beacon monitoring (hardware TSF)

- Dual and single antenna Bluetooth co-existence support with optional simultaneous
- receive (Wi-Fi/Bluetooth) capability

5.2.6 Power Management

ESP8266EX is designed with advanced power management technologies and intended for mobile devices, wearable electronics and the Internet of Things applications.

The low-power architecture operates in the following modes:

- Active mode: The chip radio is powered on. The chip can receive, transmit, or listen.
- Modem-sleep mode: The CPU is operational. The Wi-Fi and radio are disabled.
- Light-sleep mode: The CPU and all peripherals are paused. Any wake-up events
- (MAC, host, RTC timer, or external interrupts) will wake up the chip.
- Deep-sleep mode: Only the RTC is operational and all other part of the chip are
- powered off.

5.3 Fingerprint module:

In today's world, the need for effective security is evident. Without effective security, many everyday activities are compromised. Specific security concerns include: Protecting computer systems, PDA's, mobile phones, Internet appliances and similar devices from unauthorized access or use.

Protecting motor vehicles and other valuable items from unauthorized access or use preventing theft and fraud in financial transactions, in particular electronic transactions, including credit card payments and payments via the internet. Restricting access to workplaces warehouses and secures areas, such as military installations, to authorized personnel. Screening access to public transportation, in particular air travel. Authenticating the identity of an individual in drivers' licenses, health cards, ID cards and similar administrative documents.

A major factor in ensuring security is the unique identification of individuals, or the authentication that a person is who he or she claims to be. This must be done reliably, rapidly, non-intrusively and at reasonable cost. Currently, this has been done by methods such as security tokens (passports, badges, etc.), secure knowledge (passwords pin codes, signature, etc.) or recognition by a guardian (doorkeeper). These traditional approaches are all limited with respect to the above criteria. A promising approach for the future is biometrics. Biometrics offers a convenient, reliable and low-cost means of identifying or authenticating individuals, and can be implemented in unsupervised and remote situations. Biometrics seeks to identify individuals uniquely by measuring certain physical and behavioral characteristics and extracting a sample (also called a sampled template or live template) from these measurements in a standard data format. This sample is compared with a template (also called an enrolled template or signature), based on the same characteristics, that has been established as the unique identity of that individual and stored in the security system. a close match between sample and template confirms the identity of the individual. Attention has been focused on a small number of physical characteristics that can identify individuals uniquely, notably voice, gait, face, iris and retina patterns, palm prints and fingerprints. (DNA is excluded from this list because DNA sampling is intrusive and slow.) Work is proceeding to develop electronic recognition systems based on all of these. This project focuses on fingerprints as the most advanced mature and well-developed option. Based on centuries of experience and extensive research, fingerprints are at present considered to be the most reliable biometric for uniquely identifying an individual. In spite of some recent legal challenges in the USA, they are still regarded as giving proof of identity beyond reasonable doubt in almost all cases. The majority of the biometric- based security systems in operation today are based on fingerprint recognition.

Finger chip ic for fingerprint image capture combines detection and data conversion circuitry in a single rectangular cmos die. It captures the image of a fingerprint as the finger is swiped vertically over the sensor window. It requires no external heat, light or radio source.

Through a USB interface to transfer digital images of the fingerprint to the computer controlled technology to support the bio key SDK build out tools. Require

authentication for laptop computers, desktop computer or other personal computing devices, it is the ideal accessory.

5.3.1 Fingerprint Sensing and Matching:

1. Sensing

Fingerprints can be sensed using countless technologies. The historical "ink & paper" technique, still used by many law enforcements organizations, involves applying ink to the fingertip surface, rolling the finger from one side of the nail to the other side on a card, and finally scanning the card to generate.

Fig 5.4 Fingerprint

2. **How The Fingerprint Is Recognized And Stored In The Database**

During the enrollment phase, the fingerprint sensor scans the user's fingerprint and converts it into a digital image or template. the minutiae withdraw processes the fingerprint image to identify specific details known a minutia points that are used to distinguish different user's.

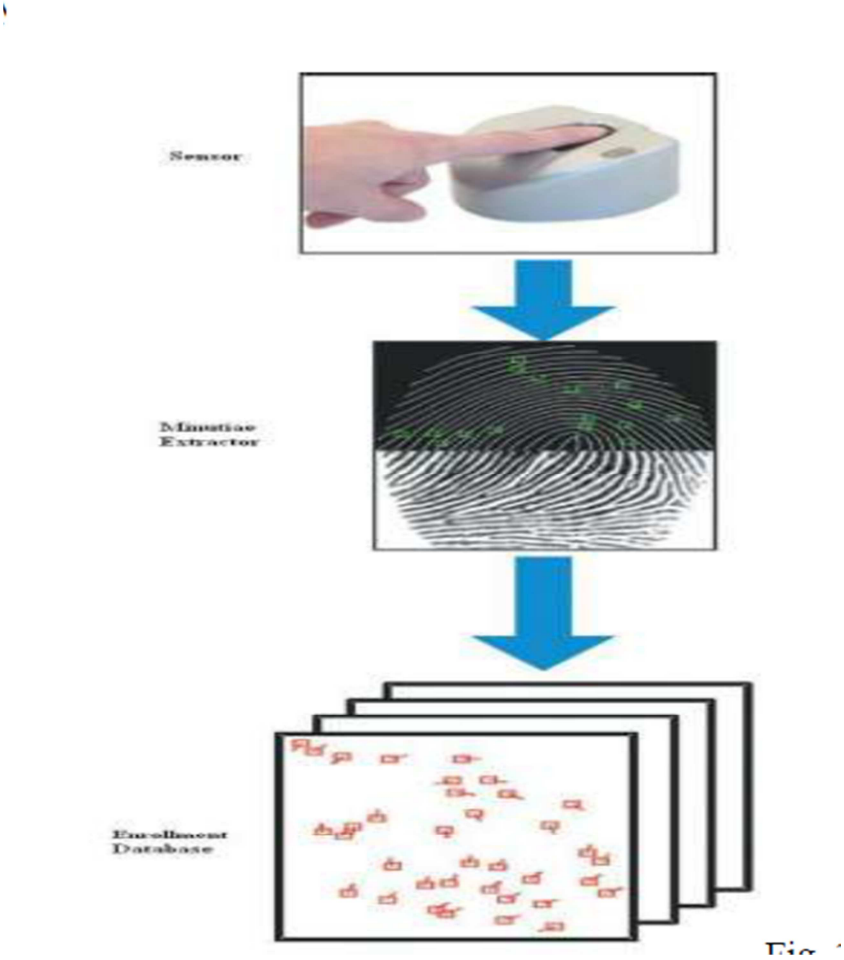


Fig 5.5 Fingerprint Scanning

Minutia points represent positions where friction ridges end abruptly or where a ridge branches into two or many more ridges. a typical good-quality fingerprint template contains 20-70 minutiae points; the actual number depends on the size of the finger sensor surface and how the user places his or her finger on the sensor. The system stores the minutiae information position and direction along with the user's demographic information as a template in the enrollment database. During the identification phase, the user puts the finger on the same sensor, generating a new fingerprint image or template called query print. Minutiae points are carried out from the query print, and the matcher module compares the set of query minutia with the stored minutia templates or image in the enrollment database to find the number of similar minutia points. Because of variations present in finger placement and pressure applied to the sensor, the minutia points take out from the template and query

fingerprints must be lined up, or submitted before matching. After line up the fingerprints, the matcher decides the number of pairs of matching minutiae-two minutiae points that have similar location and directions. the system decides the user's identity by comparing the match score to a threshold set by the administrator.

3. How The Database Accepts The Fingerprint Image:

At first the fingerprint image i.e., the gray scale image

(A) Is converted into an orientation field.

(B) And then into a binary image.

(C) And at last the minutiae.

(D) Is matched and stored in the database.

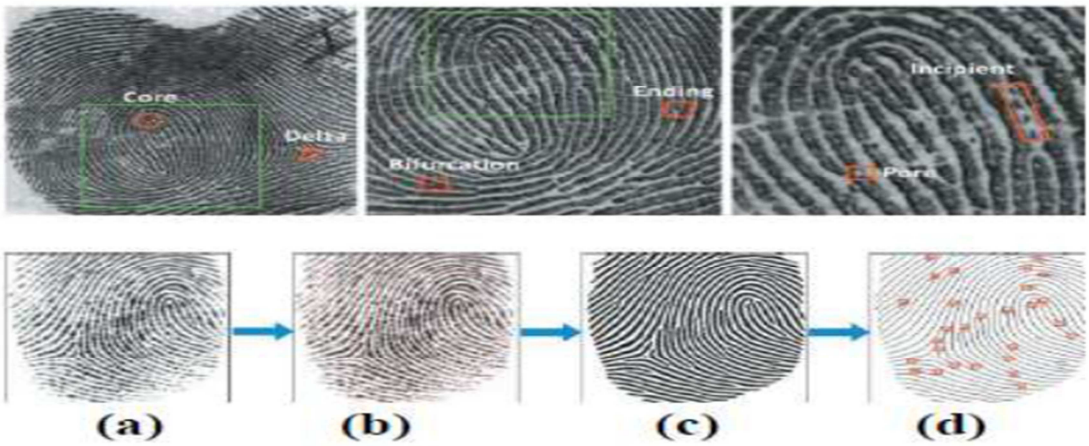


Fig. 5.6 Fingerprint Image

4. Matching

A fingerprint matching sensor module computes a match score between two fingerprints, which should be more for fingerprints from the same finger and less for those from different fingers. Fingerprint matching is a difficult pattern - recognition problem due to large intra class variation (variations in a fingerprint template of the same finger) and large interclass similarity (similarity between a fingerprint template from different fingers). Intra class variations are caused by finger pressure and placement- rotation, translation, and correct area-with respect to the sensor and the condition of the finger such as skin dryness and cuts. At the same time, inter class similarity can be large due to there are the only types of major fingerprint patterns.

Most of the fingerprint - matching algorithms adopt one out of four approaches;

image correlation, phase, skeleton, and minutiae. Minutiae-based recognitions commonly used, primarily because

- Forensic examiners are depending on minutiae to match by comparing fingerprints for more than 100 years.
- Minutiae-based representation is storage efficient, and evidence about suspect identity based on mated minutiae is admissible in courts of law.

The current culture in minutiae matching is to use local minutiae structures to quickly find a coarse alignment.

Between two fingerprints and then integrate the local matching results at a global level. This kind of matching algorithm typically consists of four steps, as the figure shows. First, the algorithm computes pair wise similarity between minutiae of two fingerprints by comparing minutiae examiners that are invariant to rotation and translation. Next, it line ups two fingerprints according to the most common minutiae pair. The algorithm then establishes minutiae correspondence-minutiae that close enough both in location and direction are deemed to be corresponding (mated) minutiae. Finally, the algorithm computes a matching score to reflect the degree of match between two fingerprints based on factors such as the no. of matching minutiae, the percentage of matching minutiae in the overlapping area of two fingerprints, and the flawless regularity of ridge count between matching minutiae.

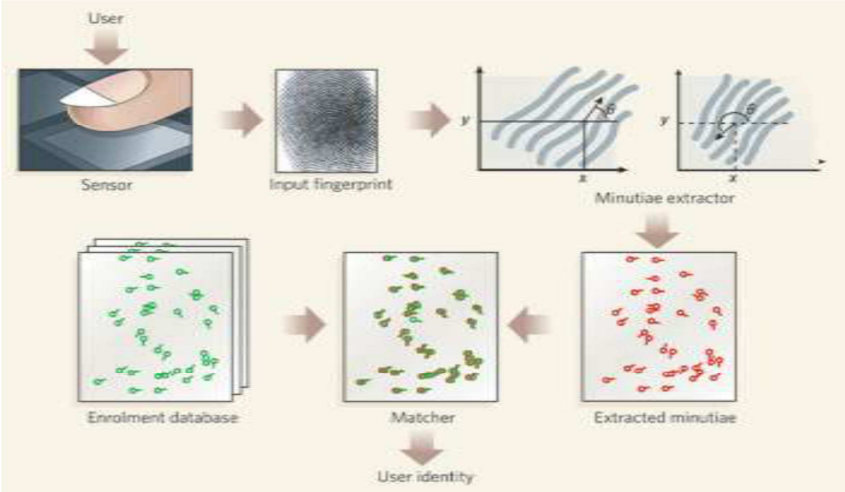


Fig. 5.7 Fingerprint Matching Process

5.3.2 How To Overcome Duplication

1. **Altered / Fake Fingerprints**

People may alter their fingerprints in different ways for many reasons. For example, an unauthorized user may use a fake finger that imitates a legitimate user's fingerprint template to access a computer system. Criminals may cover their fingers with fake fingerprints made of substances glue or they may intentionally mutilate their fingers to avoid being identified by automated systems or even human experts. an essential countermeasure to thwart the use of inanimate or fake fingers is aliveness detection – checking if the finger is "live" by measuring and analyzing various vital signs of the finger such as pulse, perspiration, and deformation. While software-based aliveness detection solutions that complement existing fingerprint scanners may be more cost effective, they have not yet shown much promise. To deal with different fingers, a mutilation detector should be added, and once difference between two or mutilation is detected, attempt should be made to identify the subject either by restoring the genuine fingerprints or using the only the unaltered areas of the fingerprints. With the adoption of multiple biometric features in large scale recognition systems such as the fbi's ngi, multi- biometrics will be powerful tool to handle altered fingerprints and system used by many other investigative agencies.

2. **Uniqueness Of The Fingerprints**

The" fingerprint" which is formed on the tip of the finger by the visible wavy shape pattern the skin takes is absolutely unique to its owner. Every person living on the earth has a different shape of structure of fingerprints. All the people who have lived throughout history also had a different structure of fingerprint. These fingerprints remain unchanged throughout one's lifetime unless a great injury occurs. That is why the fingerprint is accepted as a very important identity card and used for this purpose around the world. However, 200 years ago, the fingerprint was not so important, because it was only invented in the late 19^{th} century that each human have different fingerprints.

In 1880, an English scientist named Henry Faulds stated in an article published that

the fingerprints of people did not change in their whole life span, and that suspects could be convicted by the fingerprints they left on surfaces such as glossy surfaces.
In 1884, for the first time a murder case was solved by police with the help of fingerprints. Since then, fingerprints have become a more important method of identification of a human. in the 19th century, however, people most probably had never thought that the curvy shapes on their fingertips had some meaning or considered them worthy of note.

***3.* How To Overcome For Injured Fingerprint**

The accidental injuries are common. Although the injured fingerprint will get its own true image after it get cured. But for security purpose we must take 2 images of the fingerprint from 2 different fingers.

4.3.3 R307 Fingerprint Scanner:

R307 Fingerprint Module consists of optical fingerprint sensor, high-speed DSP processor, high-performance fingerprint alignment algorithm, high-capacity FLASH chips and other hardware and software composition, stable performance, simple structure, with fingerprint entry, image processing, fingerprint matching, search and template storage and other function.
This finger print module captures each person’s fingerprint as data. The sensor forms the core part of the fingerprint module. This in turn is connected to a NodeMCU microcontroller. This provides a unique ID to each data. The microcontroller stores the captured data and sends through the Wi-Fi transmitter module for further processing.

FIG 4.8 Fingerprint Sensor Module R307

Power	DC 4.2V-6V	**Interface**	UART(TTL logical level)/ USB 2.0
Working current	Typical: 50mA	**Matching Mode**	1:1 and 1:N
Baud rate	(9600*N)bps, N=1～12 (default N=6)	**Character file size**	256 bytes
Image acquiring time	<0.5s	**Template size**	512 bytes
Storage capacity	1000	**Security level**	5 (1, 2, 3, 4, 5(highest))
FAR	<0.001%	**FRR**	<0.1%
Average searching time	< 1s (1:1000)	**Window dimension**	19mm*21mm
Working environment	Temp: -10℃- +40℃	**Storage environment**	Temp: -40℃- +85℃
	RH: 20%-85%		RH: <85%
Outline Dimention	Split type	Module: 44.1*20*23.5 mm	

Specification Table

4.3.2a Operation Principle

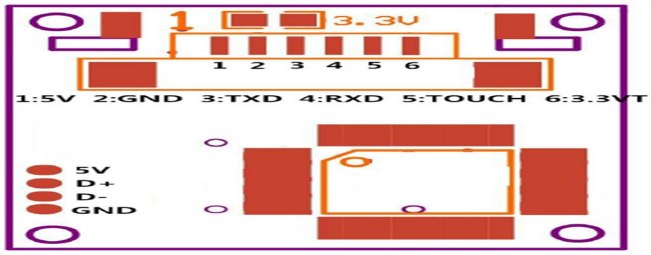
Fingerprint processing includes two parts: fingerprint enrollment and fingerprint matching (the matching can be 1:1 or 1: N). When enrolling, user needs to enter the

finger two times. The system will process the two time finger images, generate a template of the finger based on processing results and store the template.

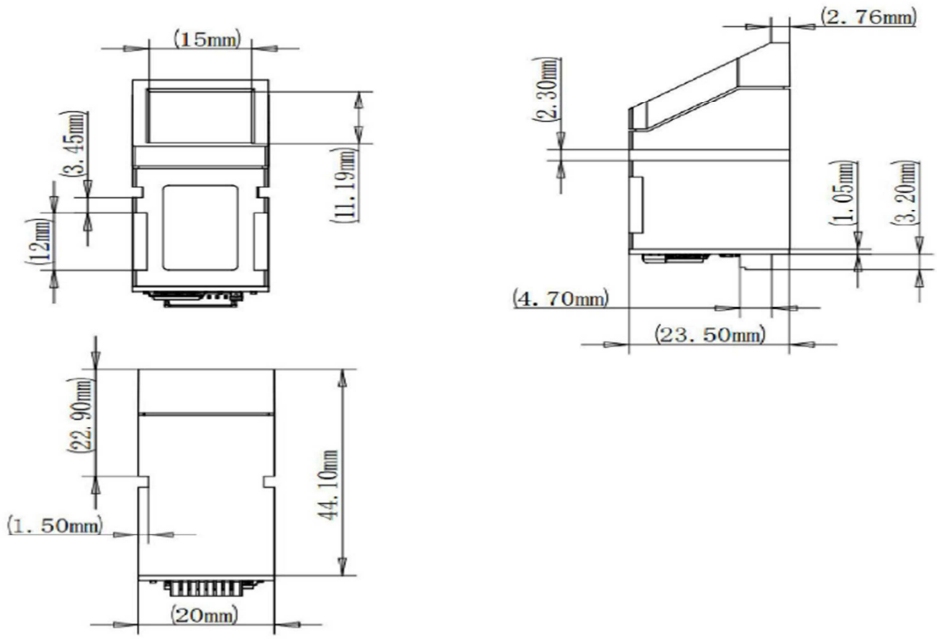
When matching, user enters the finger through optical sensor and system will generate a template of the finger and compare it with templates of the finger library. For 1:1 matching, system will compare the live finger with specific template designated in the Module; for 1:N matching, or searching, system will search the whole finger library for the matching finger. In both circumstances, system will return the matching result, success or failure.

5.3.2.b Hardware Interface

- **Exterior Interface**



- **Dimension**



- **Serial Communication**

When the FP module communicates with user device, definition of J1 is as follows:

Pin Nmuber	Name	Type	Function Description
1	5V	in	Power input (DC4.2V - 6V)
2	GND	-	Signal ground. Connected to power ground
3	TXD	out	Data output. TTL logical level
4	RXD	in	Data input. TTL logical leve
5	Touch	out	Finger detection signal（maximum output current: 50mA）
6	3.3V	in	Finger detection power (DC3.3V - 5V、about 5uA)

- **Hardware connection**

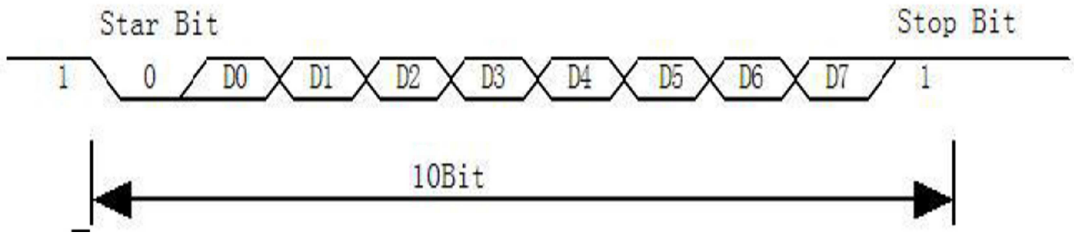
Via serial interface, the Module may communicate with MCU of 3.3V or 5V power: TXD (pin 3 of P1) connects with RXD (receiving pin of MCU), RXD (pin 4 of P1) connects with TXD (transferring pin of MCU). Should the upper computer (PC) be in RS-232 mode, please add level converting circuit, like MAX232, between the Module and PC.

- **USB Communication**

Pin Nmuber	Name	Type	Function Description
7	5V	in	Power input
8	D+	out	USB data output.
9	D-	in	USB data input.
10	GND	—	Signal ground.

- **Serial communication protocol**

The mode is semiduplex asychronism serial communication. And the default baud rate is 57600bps. User may set the baud rate in 9600～115200bps. Transferring frame format is 10 bit: the low-level starting bit, 8-bit data with the LSB first, and an ending bit. There is no check bit.



- **Reset time**

At power on, it takes about 200ms for initialization. During this period, the Module can't accept commands for upper computer

5.3.2c System Resources

To address demands of different customer, Module system provides abundant resources at user's use.

- **Notepad**

Notepad 512-byte memory is set aside in flash for User's notepad. The notepad is divided into 16 pages logically, 32 bytes per page. The host can access any page by instruction GR_WriteNotepad or GR_ReadNotepad.

Note: when written, the whole page is taken as a whole and its former contents will be replaced.

- **Buffer**

There are an image buffer and two 512-byte-character-file buffers within the RAM space of the module. Users can read & write any of the buffers by instructions.

Note: Contents of the above buffers will be lost at power-off.

- **Image buffer**

Image Buffer serves for image storage and the image format is 256*288 pixels, form is BMP.

When transferring through UART, to quicken speed, only the upper 4 bits of the pixel is transferred (that is 16 grey degrees). And two adjacent pixels of the same row will form a byte before the transferring. When uploaded to PC, the 16-grey-degree image

will be extended to 256-grey-degree format. That's 8-bit BMP format.
When transferring through USB, the image is 8-bit pixel, that's 256 grey degrees.

- **Character file buffer**

Character file buffer, CharBuffer1, CharBuffer2, can be used to store both character file and template file.
Fingerprint Library
System sets aside a certain space within Flash for fingerprint template storage, that's fingerprint library. Contents of the library remain at power off.
Capacity of the library changes with the capacity of Flash, system will recognize the latter automatically. Fingerprint template's storage in Flash is in sequential order. Assume the fingerprint capacity N, then the serial number of template in library is 0, 1, 2, 3 … N. User can only access library by template number.

- **System Configuration Parameter**

To facilitate user's developing, Module opens part system parameters for use. And the basic instructions are SetSysPara & ReadSysPara. Both instructions take Parameter Number as - 5 - www.hzgrow.comparameter. When upper computer sends command to modify parameter, Module first responses with original configurations, then performs the parameter modification and writes configuration record into Flash. At the next startup, system will run with the new configurations.

- **Baud rate control (Parameter Number: 4)**

The Parameter controls the UART communication speed of the Module. Its value is an integer N, N= [1, 12]. Corresponding baud rate is 9600*N bps。

- **Security Level (Parameter Number: 5)**

The Parameter controls the matching threshold value of fingerprint searching and matching. Security level is divided into 5 grades, and corresponding value is 1, 2, 3, 4, 5. At level 1, FAR is the highest and FRR is the lowest; however at level 5, FAR is the lowest and FRR is the highest.

- **Data package length (Parameter Number: 6)**

The parameter decides the max length of the transferring data package when communicating with upper computer. Its value is 0, 1, 2, 3, corresponding to 32 bytes, 64 bytes, 128 bytes, 256 bytes respectively.

- **System status register**

System status register indicates the current operation status of the Module. Its length is 1 word, and can be read via instruction *ReadSysPara*. Definition of the register is as follows:

Bit Num	15 4	3	2	1	0
Description	Reserved	ImgBufStat	PWD	Pass	Busy

Note:
Busy：1 bit. 1: system is executing commands; 0: system is free;
Pass：1 bit. 1: find the matching finger; 0: wrong finger;
PWD：1 bit. 1: Verified device's handshaking password.
ImgBufStat：1 bit. 1: image buffer contains valid image.

- **Module password**

At power-on reset, system first checks whether the handshaking password has been modified. If not, system deems upper computer has no requirement of verifying password and will enter into normal operation mode. That's, when Module password remains the default, verifying process can be jumped. The password length is 4 bytes, and its default factory value is 0FFH, 0FFH, 0FFH, 0FFH. Should the password have been modified, *refer to instruction SetPwd*, then Module (or device) handshaking password must be verified before the system enter into normal operation mode. Or else, system will refuse to execute and command. The new modified password is stored in Flash and remains at power off. - 6 - www.hzgrow.com

- **Module address**

Each module has an identifying address. When communicating with upper computer, each instruction/data is transferred in data package form, which contains the address item. Module system only responds to data package whose address item value is the

same with its identifying address. The address length is 4 bytes, and its default factory value is 0xFFFFFFFF. User may modify the address via instruction *SetAdder*. The new modified address remains at power off.

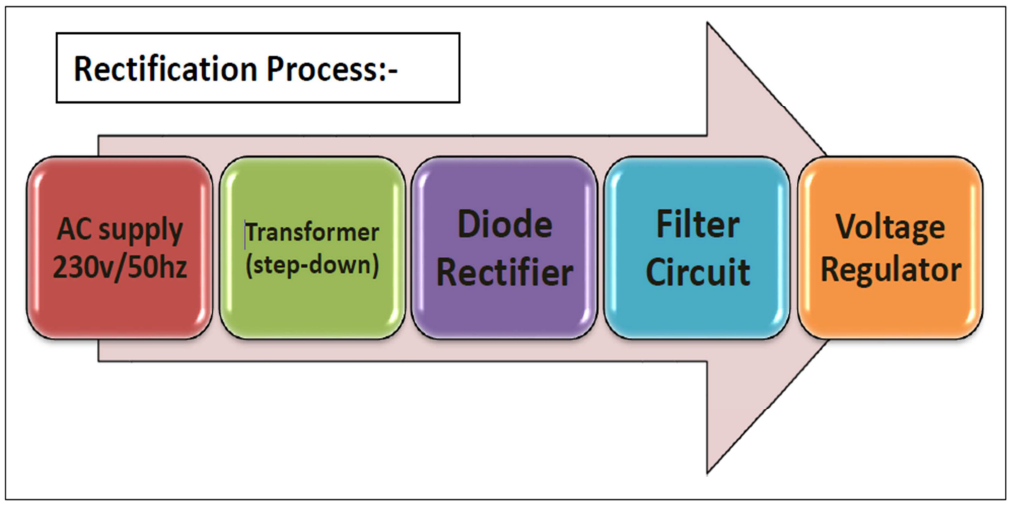
- **Random number generator**

Module integrates a hardware 32-bit random number generator (RNG) (without seed). Via instruction *GetRandomCode*, system will generate a random number and upload it.

5.4 Power supply:

- **Rectification:**

The diode is an ideal and simple device to convert AC into DC. The process is called rectification. We shall focus our attention on some performance measure of a rectifier:



- **Transformer:**

A Transformer is a static piece of equipment used either for raising or lowering the voltage of an AC supply with a corresponding decrease and increase in current. It essentially consists of two windings primary and secondary, wound on a common

laminated magnetic core as shown in figure.

N1: no. of turns in primary coil

N2: no. of turns in secondary coil

If N1< N2:- Step-up transformer

N1> N2:- Step-down transformer

The following points may be noted carefully:-

1. The transformer action is based on the law of electromagnetic induction.
2. There is no electrical/physical connection between the primary & secondary windings. The ac power transferred from primary to secondary through magnetic flux.
3. There is no change in frequency i.e. output power has the same frequency as the input power.
4. The losses that occur in transformer are:
    - Core losses- eddy current & hysteresis losses.
    - Copper losses-in the resistance of a winding.

Relation b/w voltages and no. of turns is:

(V1/V2) = (N1/N2)

Fig 5.4.1 Transformer

- **Checking of Transformer:**

1. **Cold check (**without connecting power supply**):-**

a) **Insulation of Cu wire (short circuit):-** if the circuit is short than its resistance will be "0".

b) **Test for open circuit: -** if the winding is break (open) from anywhere than it will show very high "infinite" resistance.

c) **Insulation b/w winding and core & b/w primary and secondary windings: -** these are tested using "Multimeter". If multimeter shows some value/produces sound when connect to two terminals means insulation is not proper b/w both terminals. Otherwise it will produce no sound.

2. Hot Check(using power supply**):-**

Rating error:- It is to verify whether output of a transformer is according to its rating(voltage and current) or not**.** It is identified by measuring Voutput and Ioutput using multimeter. **The** transformer which we have used is given bellow:

type:- 12-0-12

- **Full Wave Rectifier:**

A Full Wave Rectifier Circuit produces an output voltage or current which is purely DC or has some specified DC component. Full wave rectifiers have some fundamental advantages over their half wave rectifier counterparts. The average (DC) output voltage is higher than for half wave, the output of the full wave rectifier has much less ripple than that of the half wave rectifier producing a smoother output waveform.

- **Full Wave Bridge Rectifier**

Another type of circuit that produces the same output waveform as the full wave rectifier circuit above is that of the **Full Wave Bridge Rectifier**. This type of single phase rectifier uses four individual rectifying diodes connected in a closed loop "bridge" configuration to produce the desired output. The main advantage of this bridge circuit is that it does not require a special centre tapped transformer, thereby reducing its size and cost. The single secondary winding is connected to one side of

the diode bridge network and the load to the other side as shown below.

The Diode Bridge Rectifier:-The four diodes labelled D1 to D4 are arranged in "series pairs" with only two diodes conducting current during each half cycle

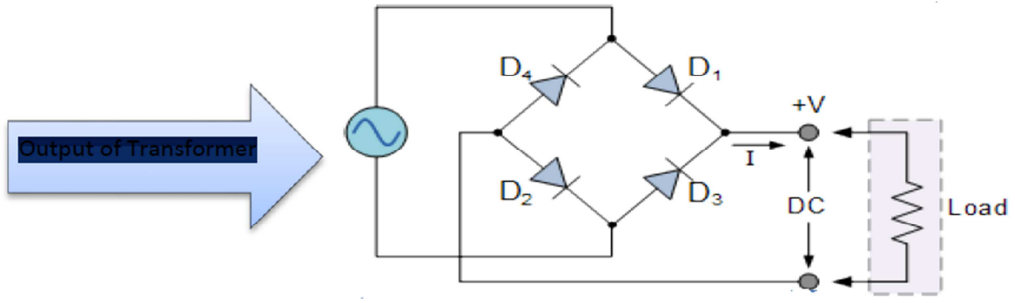
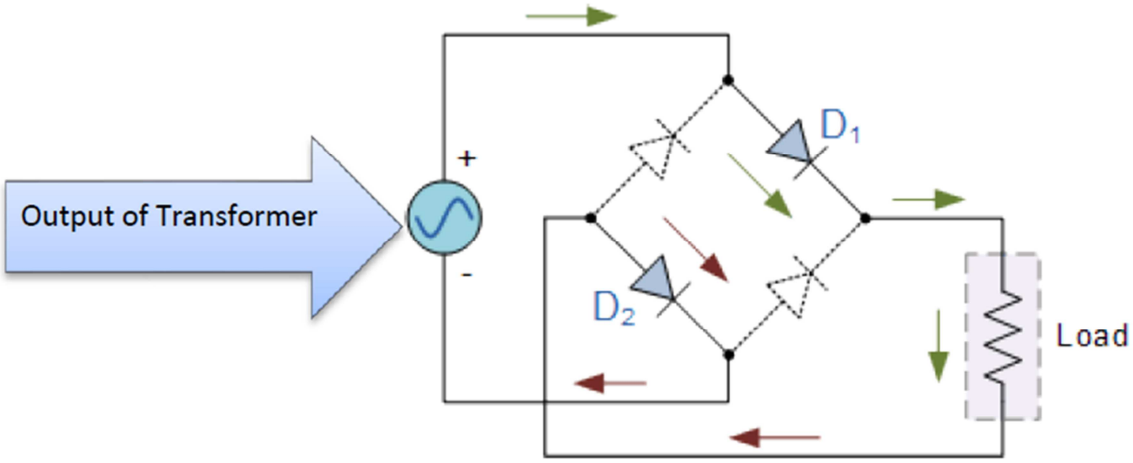


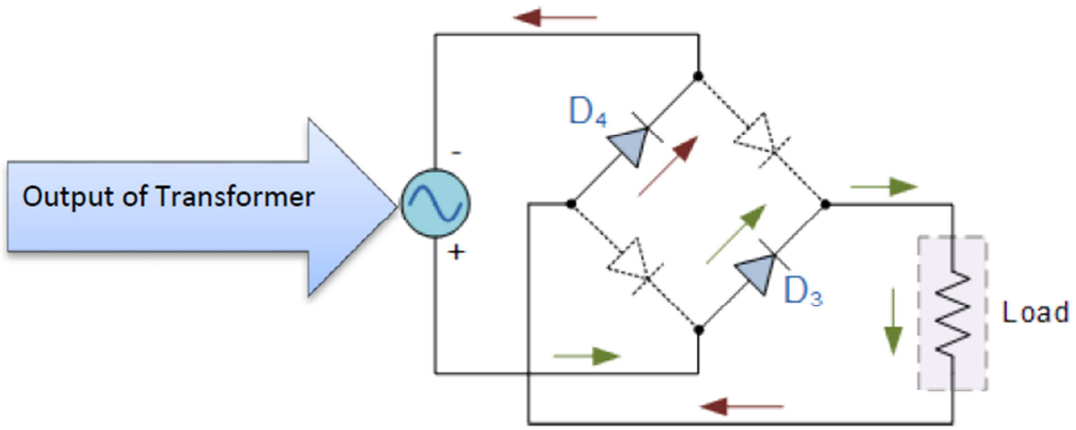
Fig 5.4.2 Full **Wave Bridge Rectifier**

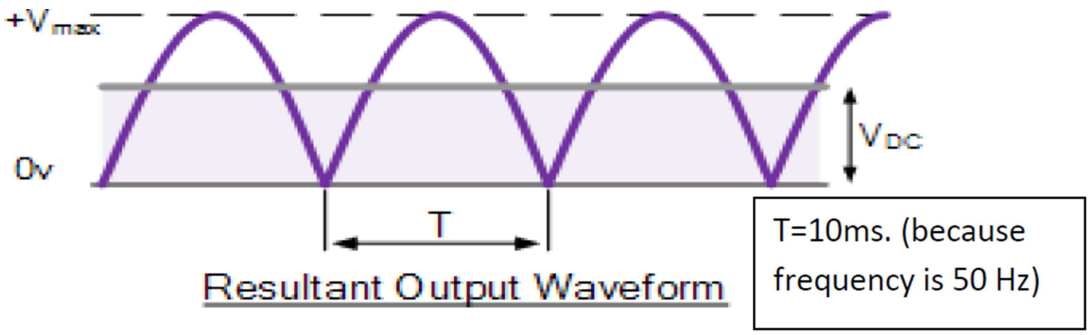
- **Working of Full Wave Bridge Rectifier:-**

The **Positive Half-cycle**: During the positive half cycle of the supply, diodes **D1** and D2conduct in series while diodes D3 and D4 are reverse biased and the current flows through the load as shown below.



The **Negative Half-cycle:** During the negative half cycle of the supply, diodes D3 and D4 conduct in series, but diodes D1 and D2 switch "OFF" as they are now reverse biased. The current flowing through the load is the same direction as before.



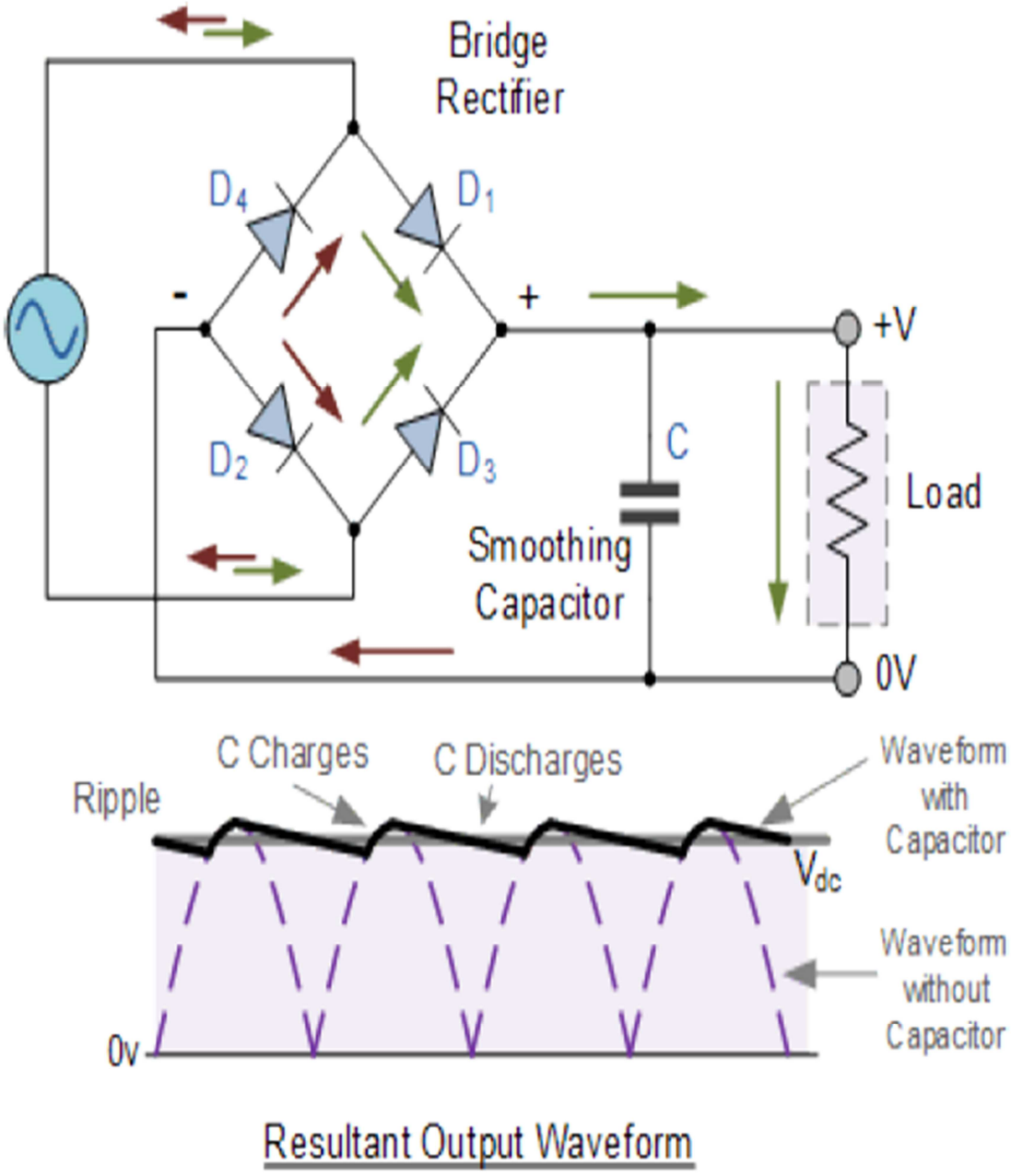


$$V_{d.c.} = \frac{2V_{max}}{\pi} = 0.637V_{max} = 0.9V_{RMS}$$

- **CAPACITOR FILTER:**

We saw in the previous section that the single phase half-wave rectifier produces an output wave every half cycle and that it was not practical to use this type of circuit to produce a steady DC supply. The full-wave bridge rectifier however, gives us a greater mean DC value (0.637 Vmax) with less superimposed ripple while the output

waveform is twice that of the frequency of the input supply frequency. We can therefore increase its average DC output level even higher by connecting a suitable smoothing capacitor across the output of the bridge circuit as shown below.



- **Formulas to find capacitor value**:-

There are so many ways to find capacitor values . the formulas mostly used are:-

1) Q=CV

C=IL/(2.f.ΔV)

2). Q=CV

C=Q/ΔV

C=I.td/ΔV {because Q=I.t}

Now we have to find values of I(current) , td(discharging time period) and ΔV(ripple voltage) .

For current:

I = current rating of transformer

ΔV(ripple voltage):

ΔV= Vm-value of voltage assumed in input of regulator which is sufficient to give required output

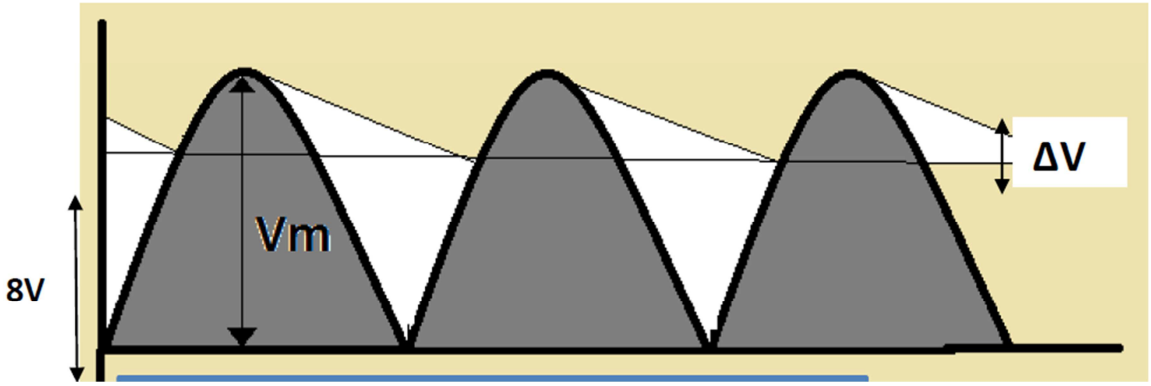


Fig 5.4.3 Calculation to obtain less ripple waveform

td(discharging time period):-

the above waveform is sin wave so

v=Vm.Sinɵ

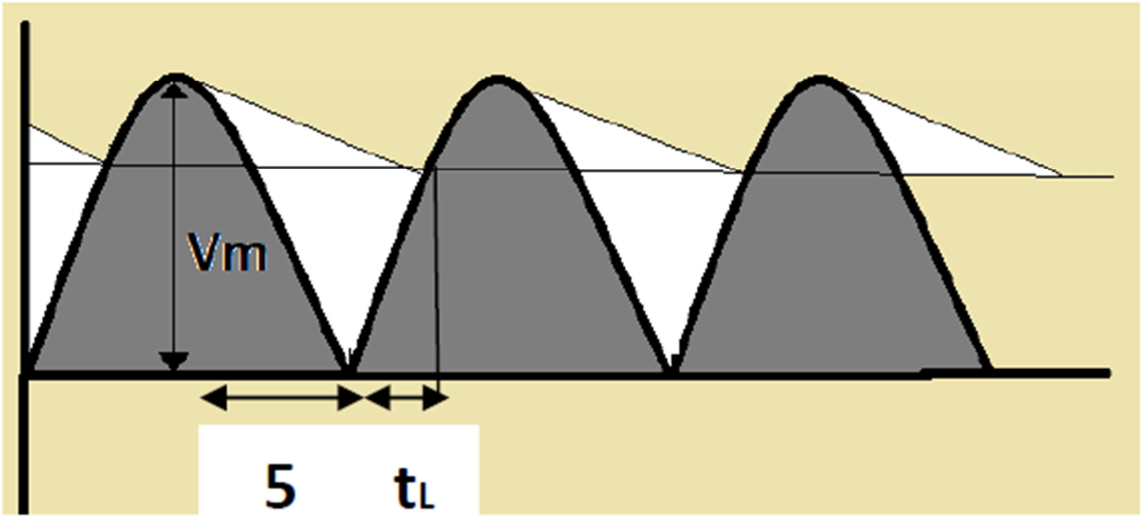
let instantaneous value of voltage v=8V

8= Vm.Sinɵ

Ɵ=sin^(-1)(8/Vm)

As at 180˚ angle; time is 10ms (because the frequency of wave is 50Hz)

So at angle Ɵ ; time =(10/180) Ɵ



So from above figure it is clear that

td(discharging time period) = 5+Tl.....eq.(1)

now to find values of capacitor for Vm=18.2V

& RL= 18.4Ω

Q=CV

C=Q/ΔV

C=I.t/ΔV where ΔV= Vm-8= 18.2-8= 10.2V

& IL=1Amp

So C=1.t/10.2……..eq.(2)

To find "td"

v=Vm.Sinθ

let instantaneous value of voltage v=8V

8= Vm.Sinθ

Θ=sin^(-1)(8/Vm)

sin Θ=8/18.2 Θ=26.075

As at 180˚ angle; time is 10ms (because the frequency of wave is 50Hz)

So at angle Θ ; time =(10/180) Θ

time =(10/180) 26.075 t=1.4486ms

from eq.(1)

now td =5+1.4486 td =6.4486ms

from eq..(2)

C =1*6.4486/10.2 C=632.17μ*f*

But because of safety purpose we are using 2000μf capacitor.

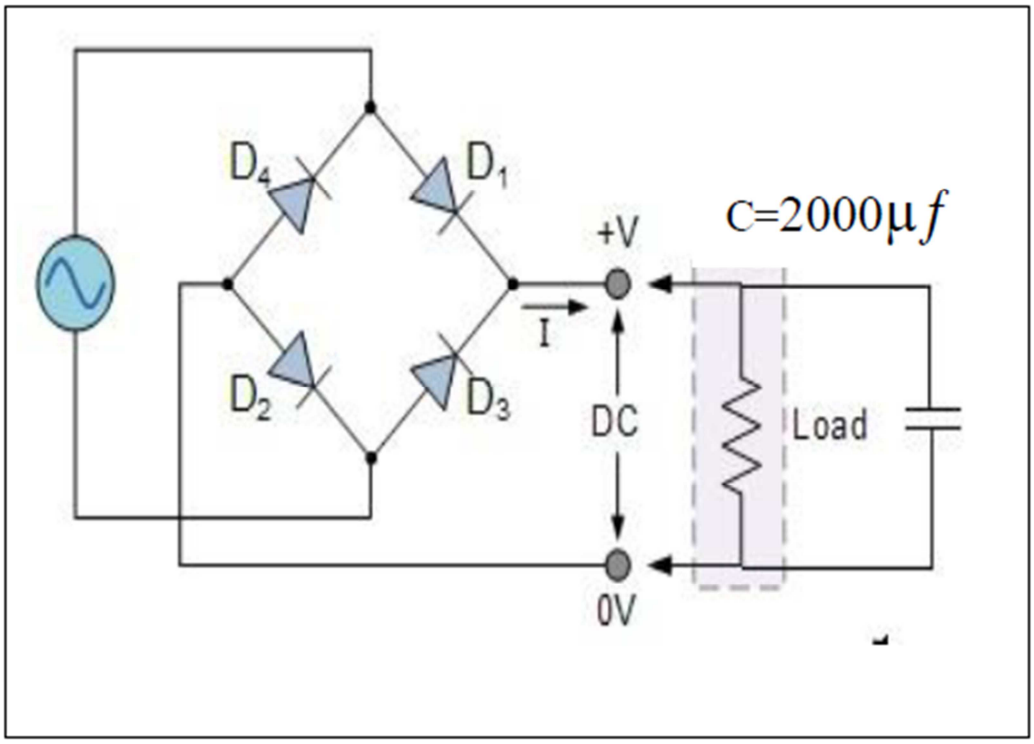


Fig. 5.4.4:- Image showing circuit of capacitive filter and output pulse from capacitor filter

Voltage across capacitor:-

Vp=24.88V

Vrms=24.88/(2√3)

Vrms=7.18223Volt

Till there are some ripples in the output waveform. So we have to use some IC's like LM7805 to obtain perfect DC wave. Now the next step is to put a voltage regulator IC in the circuit.

- **Voltage Regulator:**

Regulated DC Power Supply using adjustable Voltage Regulator LM7805:

It gives a constant direct voltage across its output terminals

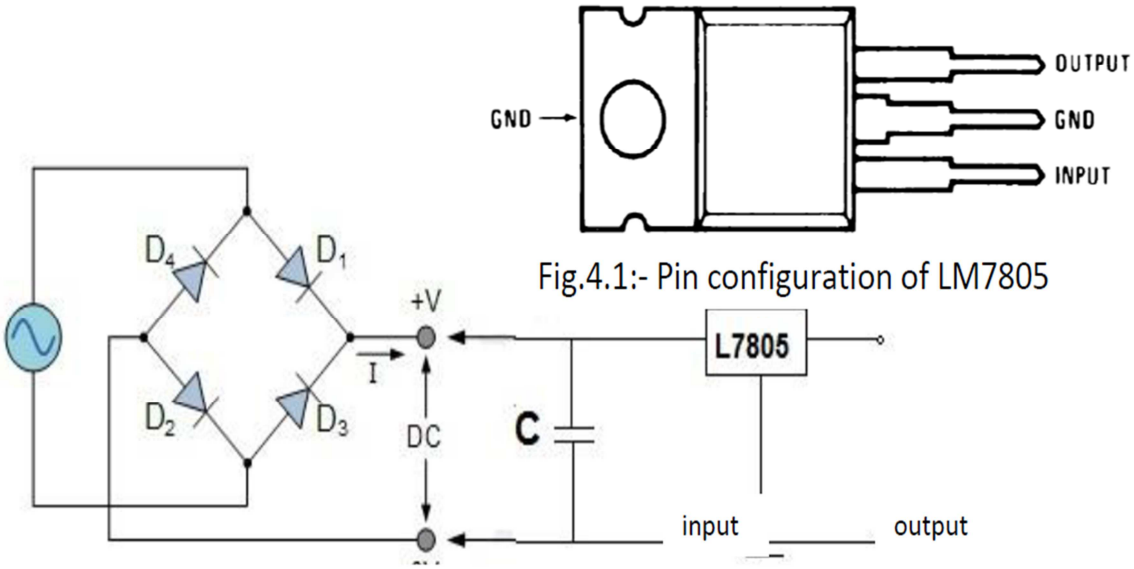


Fig.4.1:- Pin configuration of LM7805

Fig.5.2:- Rectifier circuit with LM7805 voltage regulator

Output of IC-LM7805 **VDC=5.050Volt**

Load regulation for LM7805

S. NO.	R_L(Load Resistance)	I_{DC}	V_{output}
1.	9.8Ω	368.40 mA	5.02V
2.	31.2 Ω	140.0 mA	5.04V
3.	49.6 Ω	92.9 mA	5.08V
4.	72.4 Ω	242.9 mA	4.98V
5.	100.9 Ω	181.2 mA	4.84V
6.	123.2 Ω	153.7 mA	4.82V
7.	123.6 Ω	153.7 mA	4.8V
8.	220 Ω	22.9 mA	4.995V
9.	560 Ω	9.24 mA	5.024V
10.	2.2K Ω	2.35 mA	5.021V
11.	4.6K Ω	1.07 mA	5.018V

TABLE 5.1: Variation of output voltage with changing the load RL

CHAPTER 6

CLOUD / REAL-TIME DATABASE

We have used Google firebase to store the details of a license holder. It provides many features like Authentication & Security, Real-time Database & File Storage.

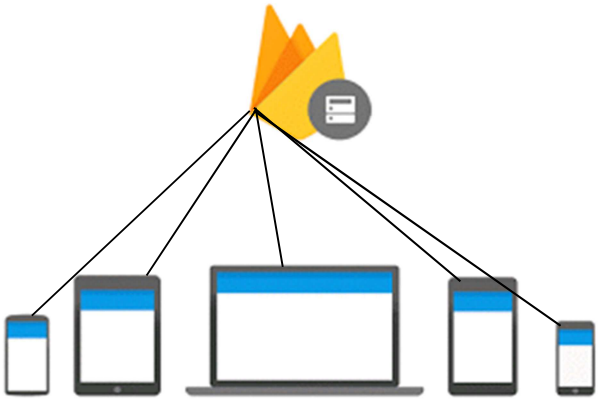
6.1 Google Firebase:

Firebase is a mobile and web app development platform that provides developers with a plethora of tools and services to help them develop high-quality apps, grow their user base, and earn more profit. It provides many features like Authentication & Security, Real-time Database & File Storage, Analytics, Push Notifications, AdMod and many others.

Back in 2011, before Firebase it was a start-up called Envolve. As Envolve, it provided developers with an API that enabled the integration of online chat functionality into their website. What's interesting is that people used Envolve to pass application data that was more than just chat messages. Developers were using Envolve to sync application data such as a game state in real time across their users. This led the founders of Envolve, James Tamplin and Andrew Lee, to separate the chat system and the real-time architecture. In April 2012, Firebase was created as a separate company that provided Backend-as-a-Service with *real-time functionality.* After it was acquired by Google in 2014, Firebase rapidly evolved into the multifunctional behemoth of a mobile and web platform that it is today.

Firebase offers many services but for our project we use particular service called Real-time Database. The Firebase Real-time Database is a cloud-hosted NoSQL database that lets you store and sync between your users in real-time. The Real-time Database is really just one big JSON object that the developers can manage in real-time.

With just a single API, the Firebase database provides your app with both the current value of the data and any updates to that data.



Real-time syncing makes it easy for your users to access their data from any device, be it web or mobile. Real-time Database also helps your users collaborate with one another. Another amazing benefit of Real-time Database is that it ships with mobile and web SDKs, allowing you to build your apps without the need for servers. When your users go offline, the Real-time Database SDKs use local cache on the device to serve and store changes. When the device comes online, the local data is automatically synchronized.

6.1.1 Database Rules

With Firebase Real-time Database, your Database rule is your server side security. You need to be very careful and aware of who has access to your database. It is

important that no one gains access to your data that shouldn't. By default, the Firebase Real-time Database rules allow any authenticated user to read and write all the data, this is probably not what you want your app to do. The Firebase Real-time Database provides a flexible, expression-based rules language with JavaScript-like syntax to easily define how your data should be structured, how it should be indexed, and when your data can be read from and written to. Combined with our authentication services, you can define who has access to what data and protect your users' personal information from unauthorized access. By default, your database rules require Firebase Authentication and grant full read and write permissions only to authenticated users. The default rules ensure your database isn't accessible by just anyone before you get a chance to configure it.

6.1.2 Firebase UI

Firebase is a suite of integrated products designed to help you develop your application, grow an engaged user base, and earn more money. It includes tools that help you build your app, such as a real-time database, file storage, and user authentication, as well as tools to help you grow and monetize your app, such as push notifications, analytics, crash reporting, and dynamic links. You can think of Firebase as a set of Lego bricks that you can use to build your masterpiece. Just like bricks, Firebase is relatively unopinionated, since there are an infinite number of ways to combine the pieces and we're not going to tell you that certain ways are wrong.

FirebaseUI is built on Firebase and provides developers simple, customizable, and production ready native mobile bindings on top of Firebase primitives to eliminate boilerplate code and promote Google best practices In the Lego analogy, FirebaseUI is a set of pre-built kits with instructions that you can take off the shelf and tweak to suit your needs. You can see how we used the individual components of Firebase to build FirebaseUI because FirebaseUI is open source. FirebaseUI has to be opinionated--we're telling you how we think the bricks should go together, so we make some choices. But because FirebaseUI is open source, you can go in and change what we're doing to better suit your individual needs. If you're building a Lego city, you'd rather pull a bunch of houses from a pre-build collection and modify slightly to suit your needs than start from scratch and design each building by hand, right?

FirebaseUI let's you do exactly this, which is why we include it in our sample apps and examples. Developers (ourselves included) are lazy--we want the best reuse of our code and the most concise examples, and FirebaseUI allows us to provide really high quality examples that translate to really good user experiences at a fraction of the development cost.

- **How to save user profile data**

  Every authenticated user has a Firebase uid that's unique across all providers and is returned in the result of every authentication method. A good way to store your user's data is to create a node to keep all the user's data and to protect it using your security rules

- **Database**

```
{
   "users": {
      "uid1" : {
         "name": "Steve",
         "surname": "Jobs"
      },
      "uid2" : {
         "name": "Bill",
         "surname": "Gates"
      }
   }
}
```

- **Security**

```
{
    "rules": {
        "users": {
            "$uid": {
                // If node's key matches the id of the auth user
                ".write": "$uid == auth.uid"
            }
        }
    }
}
```

The $uid in the above rules is a so-called "dollar variable", which ensures that the rules under it are applied to all child nodes of users. For more information see the

documentation on Using $ Variables to Capture Path Segments.

- **Why save user data in the database**

Firebase Authentication allows the users of your app to sign-in with social providers or their email and password. But what if you want to store additional information about a user, beyond what Firebase Authentication allows you to specify? Or what if you want to display a list of the users in your app? Firebase Authentication doesn't have an API for this. Most developers solve this problem by storing the additional information in a separate database.

- **Handling User Account Data in the Real-time Database**

The Firebase author system is the source of a users uid, displayName, photoURL, and maybe email. Password based accounts set these *persistent* values in the auth system via the .update Profile method. Storing these values in the Realtime Database, rDB, users node poses the issue of stale data. Display names, for example, may change. To keep these values in synch use local storage in concert with .onAuthStateChange.

on every .onAuthStateChange

• getItem('displayName') and getItem('photoURL')

• compare to user.displayName and user.photoURL if different

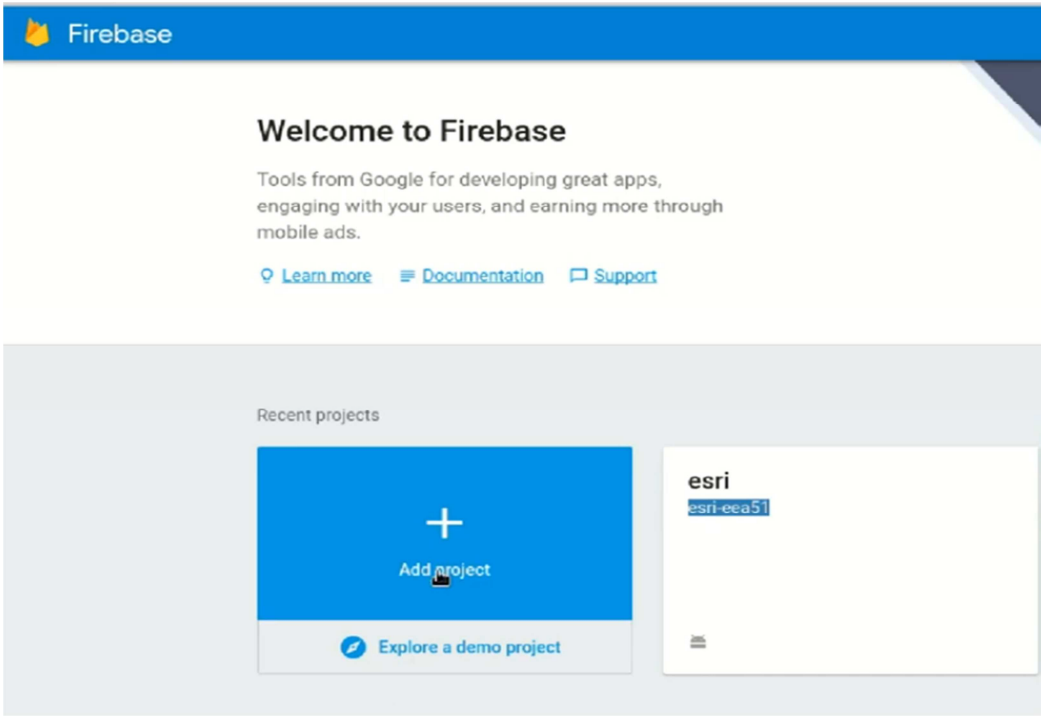
○ setItem('displayName') and setItem('photoURL')

○ db.ref.child('users').update the values of displayName and/or photoURL

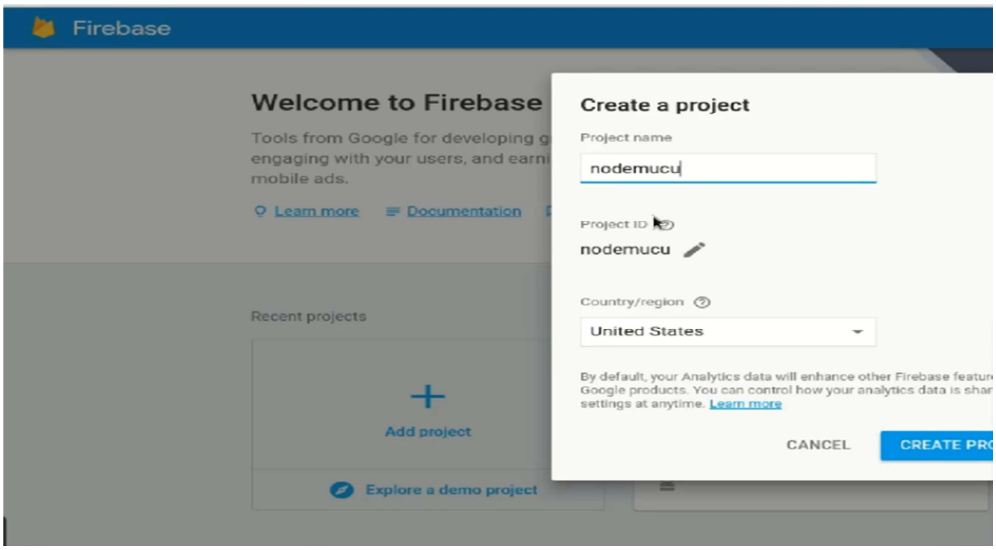
•.onAuthStateChange fires on every page load or reload, as well as on every auth state change. It potentially fires often, e.g. multi page apps. However reading and writing to local storage is synchronous and very fast so there will be no noticeable impact on app performance.

6.1.3 Setting up Google Firebase for NodeMCU:

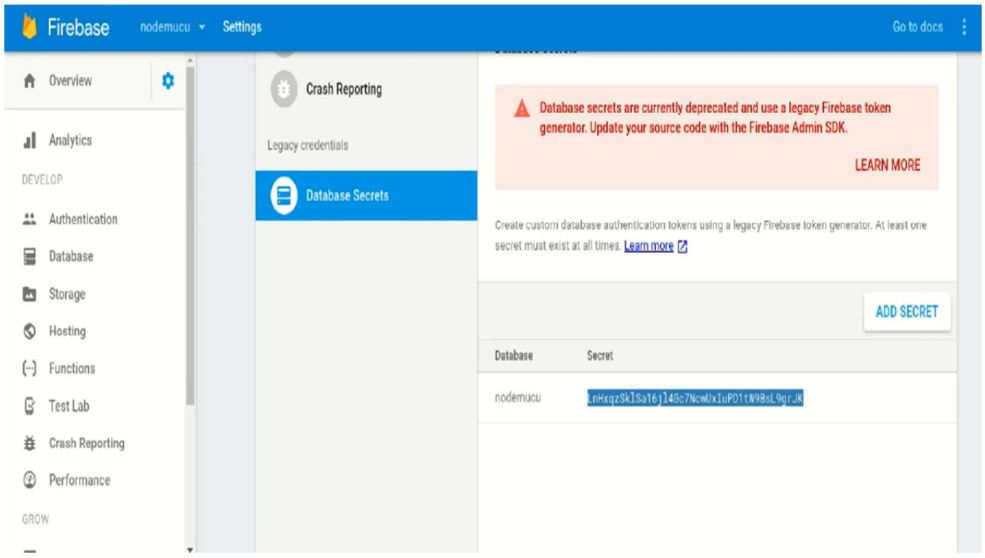
1. Firstly, go to firebase dashboard and create a new project using the '**Add Project**' button.



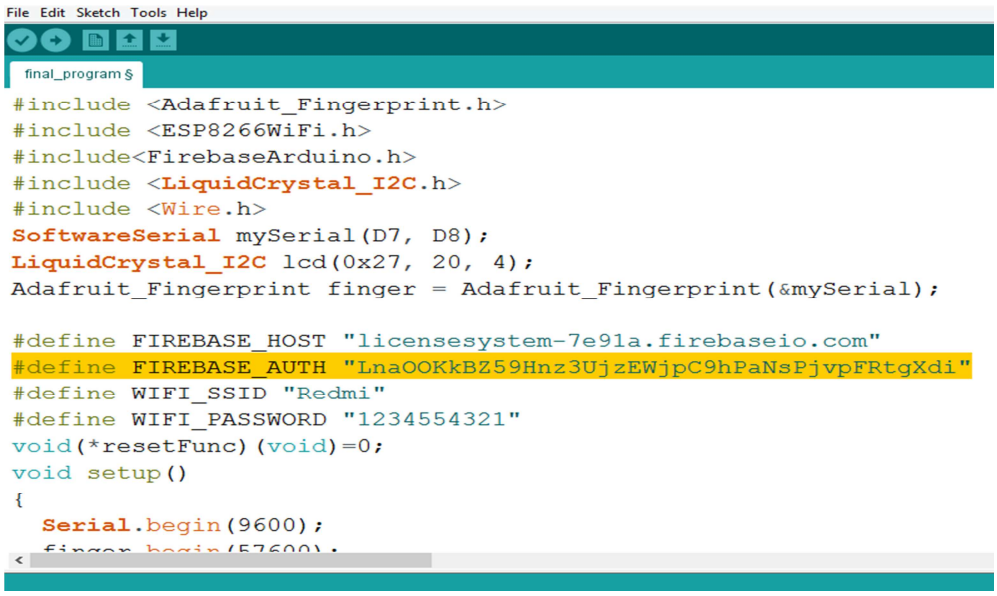
2. Create a new project by adding the name of your app for example I put mine as '**NodeMCU**' then choose your region and press **'Create Project'**.



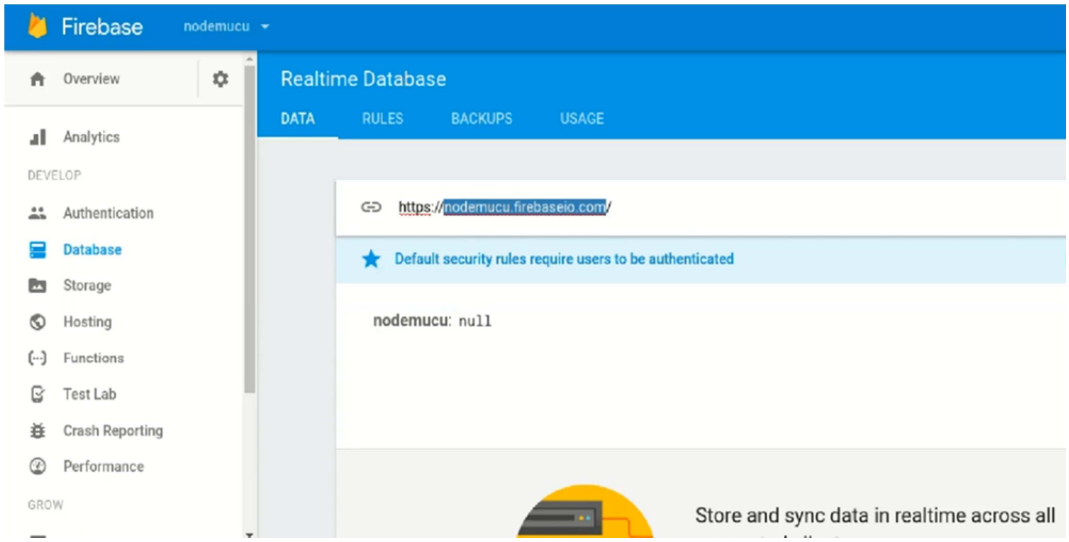
3. After creating the project, click on **Overview** and in the Overview, click on **Project settings**. In project setting, click on **Service Accounts** and in service accounts, click on **Database Secrets** and click on show to get **Secret.**



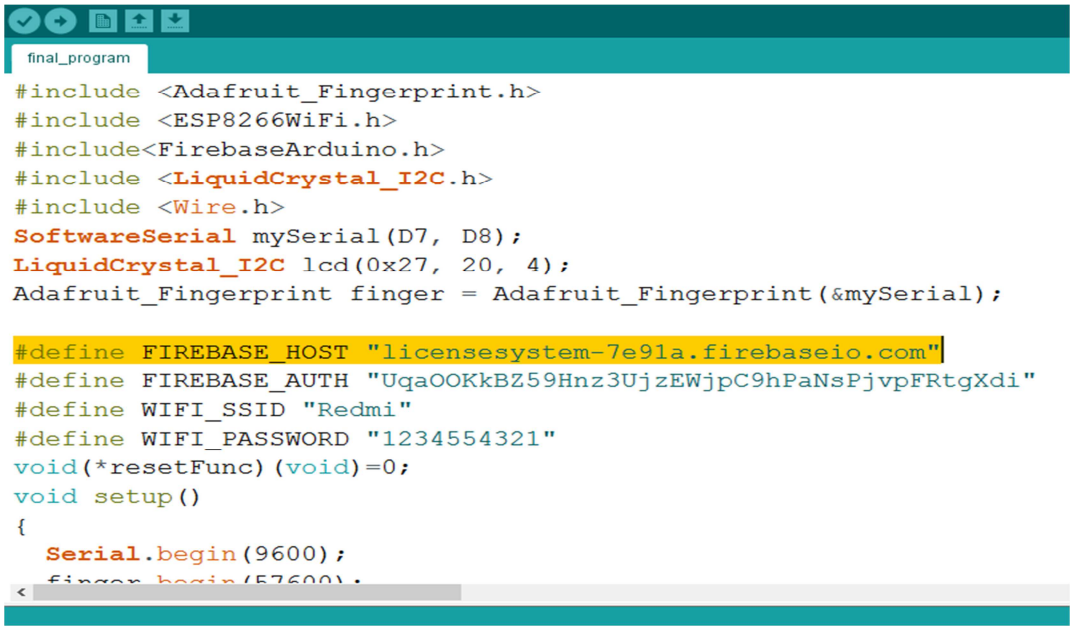
4. Copy the **Secret** and paste it to **FIREBASE_AUTH** on **Arduino IDE.**



5. Now click on **Database,** copy the shown **URL.**

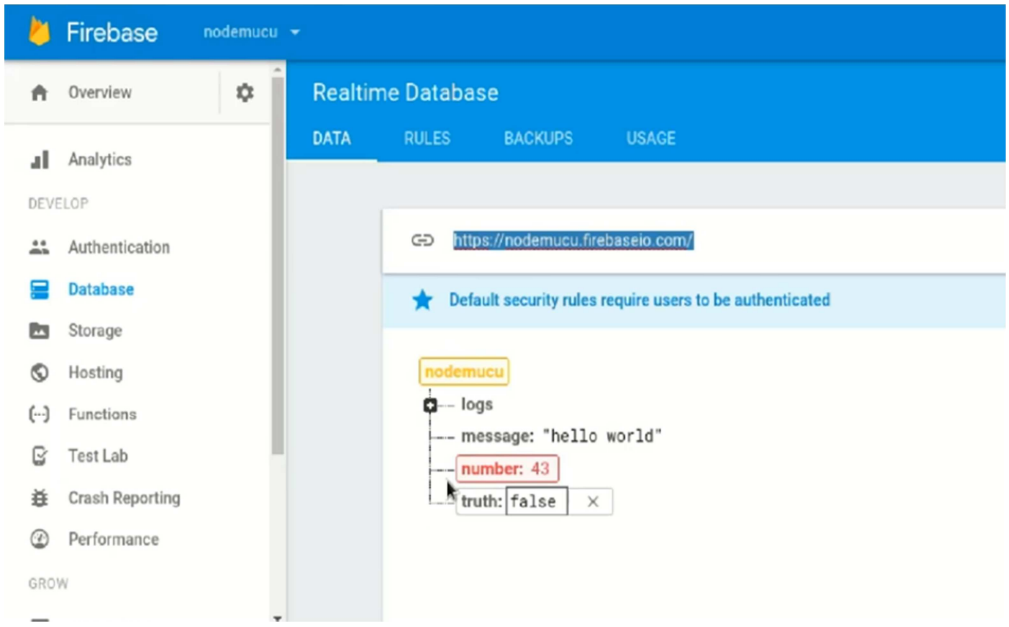


6. Paste this URL to **FIREBASE_HOST** on **Arduino IDE**



7. After entering these parameters on **Arduino IDE,** upload the program on NodeMCU and NodeMCU will start communicating with Google Firebase.

8. Now click on **Database**, and then click on Plus sign to license details.



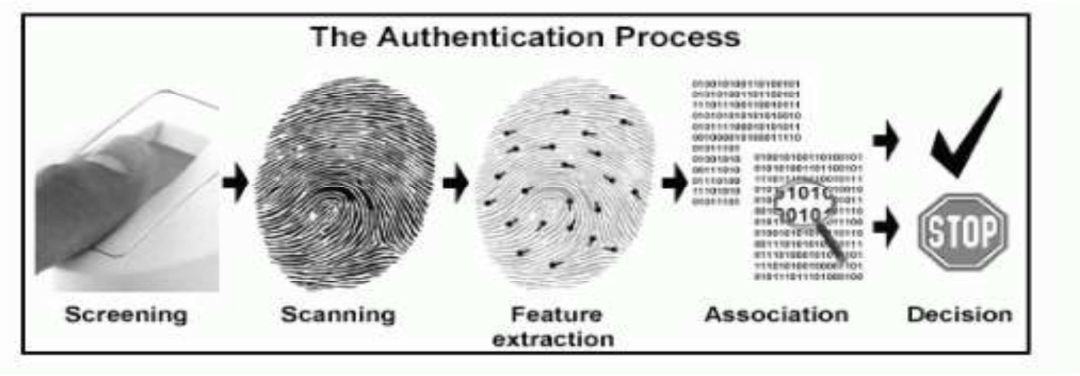
CHAPTER 7

WORKING OPERATION

The working of this project is very simple. This project consists of a Fingerprint module, Microcontroller NodeMCU with inbuilt Esp8266 Wi-Fi module, 20x4 LCD, Power supply and Google Firebase. The main functional unit of this project is NodeMCU, which acts as a processor. The NodeMCU has its own memory where the program is uploaded and stored, and all the other components are interfaced with it.

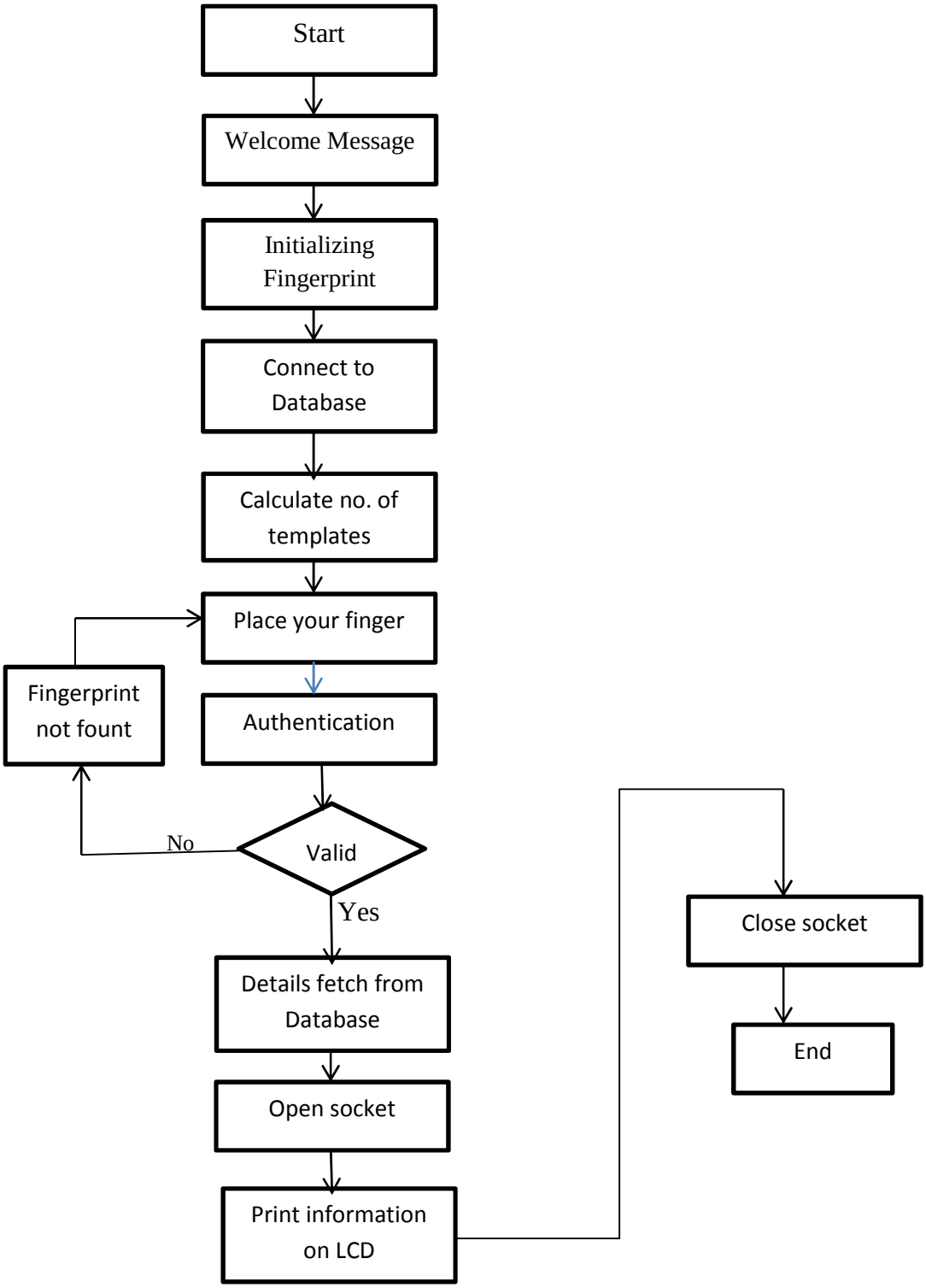
Working of project:

1. When power on, a welcome message is displaced on the LCD display.
2. ESP8266 connects to the available Wi-Fi hotspot.
3. NodeMCU initializes the R307 Fingerprint module and then connects to the Google firebase.
4. Now NodeMCU calculates the number of templates.
5. After all the above operations are successful, NodeMCU displays ‘Place your finger’ on the LCD.
6. Person places the finger on fingerprint module, fingerprint module scans and captures the fingerprint then matches that fingerprint with stored fingerprints. If the match is found, then the ID is generated and forwarded to NodeMCU.



7. NodeMCU sends this ID to Google firebase. Firebase searches for this ID and if ID is found, then the information about this ID is forwarded to NodeMCU and NodeMCU after processing the data and then details of the license holder will be displayed it on LCD
8. If no match is found, no ID will be generated and no details will be displayed.

7.1 Flowchart



Conclusion

Automated fingerprint identification systems is been successfully used around the globe for various application like law-enforcement, passport and adhar etc.., and new Fingerprint matching applications are emerging day by day. The fingerprint is and will always be the dominant biometric attribute, and many identity management and access control applications will continue to dependable on fingerprint recognition because of its performance, large databases, and the availability of compact and cheap fingerprint readers. Further, fingerprint proof is acceptable in court's to convict criminals. In this project we have proposed method based on “minutiae-based" algorithm for efficient, accurate and more secured system because of following features:

1. Universal
2. Unique
3. Persistence
4. Collectable
5. Acceptability
6. Circumvention
7. Performance

Thus the Proposed system provides wireless driving license verification with fingerprint acquisition and verification through Real-time Database. It can automatically realize functions such as information acquisition of fingerprint, processing, and wireless transmission, fingerprint matching, and driving license verification. In order to achieve the simple and high real-time system, it realized low-cost and high-performance wireless driving license verification function, which provided a new wireless driving license verification system.

References

1. J. Feng, “Combining Minutiae Descriptors For Fingerprint Matching,” Pattern Recognition, Jan. 2008, Pp. 342-352
2. H.C.Lee And R.E.Gaensslen. Eds., Advances In Fingerprint Technology, CRC Press 2001.
3. Salil Prabhakar, Sharath Panknti & A.K. Jain," Biometric Recognition: Security & Privacy Concerns", IEEE Security & Privacy, April 2003.
4. Jun Gao, Huo-Ming Dong, Dingguo Chen, Long Gan & Wen Wen Dong,″ Research On Synergetic Fingerprint Classification And Matching″, International Conference On Machine Learning And Cybernencs, November 2003.
5. David Silcock,AnnaSunter Chris van Lottum, Ross Silcock Limited, Kris Beuret, " Unlicensed Driving: A Scoping Study to Identify Potential Areas for Further Research Foundation for Road Safety Research".
6. Hugh Wimberly; Lorie M. Liebrock "Fingerprint Authentication to Reduce System Security: An Empirical Study" 2011 IEEE Symposium on Security and Privacy Year: 2011 Pages: 32 – 46..
7. K. Al-Begain, I. Awan and D. D. Kouvatsos, “Analysis of GSM/GPRS Cell with Multiple Data Service Classes,” Wireless Personal Communications, Vol. 25, No. 1, 2003,pp. 41-57.