A Remote User Authentication Scheme for Home Access

by

Pradip Tilala
201511045

A Thesis Submitted in Partial Fulfilment of the Requirements for the Degree of

MASTER OF TECHNOLOGY
in
INFORMATION AND COMMUNICATION TECHNOLOGY
to

Dhirubhai Ambani Institute of Information and Communication Technology

April 2017

Declaration

I hereby declare that

i) the thesis comprises of my original work towards the degree of Master of Technology in Information and Communication Technology at Dhirubhai Ambani Institute of Information and Communication Technology and has not been submitted elsewhere for a degree,

ii) due acknowledgment has been made in the text to all the reference material used.

Pradip Tilala

Certificate

This is to certify that the thesis work entitled A REMOTE USER AUTHENTICATION SCHEME FOR HOME ACCESS has been carried out by PRADIP TILALA for the degree of Master of Technology in Information and Communication Technology at *Dhirubhai Ambani Institute of Information and Communication Technology* under our supervision.

Dr. Anil K. Roy
Thesis Supervisor

Prof. Maniklal Das
Thesis Co-Supervisor

Acknowledgments

This thesis presents not only my work, but also motivation and support of some people around me. I would like to thank them who directly or indirectly helped me, in accomplishing this.

First of all, I want to express my deepest gratitude to my supervisor Dr. Anil K. Roy and Prof. Maniklal Das for providing a continuous guidance and motivation during the complete period of my thesis work. I would also like to thank my evaluation committee members, Prof. Sanjay Srivastava and Prof. Gagan Garg for their constructive criticism, which shaped my thesis better.

I am thankful to my friends Nishith Kotak and Abhishek Jani for their help. I would like to thank my father Mr. Govindbhai Tilala, mother Mrs. Sudhaben Tilala and brother Mr. Mehul Tilala for motivating me with their selfless love and invaluable trust in me.

Pradip Tilala
August 01, 2017

Contents

Abstract

Digital home security systems are becoming inevitable in modern lifestyle. For the purpose of safety, smart systems are required to be developed that themselves could recognize the legitimate visitor and only then allow him/her the access to the door. We propose a smart home access system architecture for the door lock system. This system controls the door lock via android smartphone App using WiFi as the communication protocol, WeMos D1 WiFi module embedded in the lock and the online PHP web server. With the help of cloud-based messaging service, it is easy to send a message to remote android mobile. This aspect removes the need to embed GSM module with a smart lock system. To keep track of the door status and the events like door smashing, keeping door open for a long time, we have used the accelerometer and magnetometer respectively. This system keeps itself in LAN of the home router. It avoids the access to the system from outside the LAN. The smartphone App has a password for secure access to the lock system. This system verifies the password of the user and then sends an OTP to the mobile App using cloud-based secure messaging service. Different possible scenarios have been considered to check the system's performance in real time. Memory space consumption and the time taken by the system in use are the challenging aspects in a home access system. The security aspect of the system does not affect much to the operation time of the system. So, the system is efficient from the time perspective and easy to use by novice user as its mobile App.

List of Tables

List of Figures

Chapter 1

Introduction

Nelson Mandela truly recognized, "Freedom would be meaningless without security in the home and the streets [1]." For the purpose of the safety, one of the systems that can be developed, itself verifies the visitor's identity with the owner and then only allows the visitor the access to the door [4].

Digital home security systems are becoming inevitable in a modern lifestyle where there may be situations when there is nobody inside the house, and yet the owner of the house wants to allow the access to the house to some bonafide visitor. Since such systems allow access only to the bonafide visitors, it acts as an efficacious deterrent in the case of break-ins and robberies. On the flip side, anybody having the access code of such digital home security system may be seen as the bonafide visitor. Therefore, these systems are prone to potential misuse too, in which case a person with malafide intention can hack the access code of this digital home security system and hence get the access to the house without anybody noticing or suspecting it. But the good thing is that statistics show that burglars are less likely to attempt to break into a home in which there is a home security system installed [5]. Also, in the case of those burglars who are smart enough to attempt a break-in into a house with a digital home security system, the likelihood of them being apprehended is substantially higher than them getting away.

Security Statistics
Following global home security statistics [5] that incite us to define our problem statement:

- Every 13 second, a home intrusion is committed.
- More than 2 million home burglaries are reported each year in United States.
- Police usually only clear 13% of all reported burglaries due to lack of witnesses or physical evidence.
- About 66 percent of all break-ins are residential.
- Homes without security systems are up to 300% more likely to be broken into.
- Nearly 30 percent of all break-ins are through an open and unlocked window or door.
- About 95% of intrusions needed some amount of force to break-in.

- The type of tools used to intrude are mostly simple; a screwdriver, pliers, pries bars, and small hammers are the most common.
- Identity theft is the rapidly increasing crime in the U.S.A.
- 85% of break-ins are from non-professionals that are usually more desperate and dangerous.
- Only about 17 percentage of the residences in U.S.A. have a security system.
- Insurance agencies can offer discounts up to 20% for auto insurance when a home security system is installed.

The situation in India is no more different than above mentioned statistics. Maximum number of cases of properties stolen were registered in residential premises (2,12,438 out of 6,22,116 cases) followed by highways/road (89,102 cases) which accounted for 34.1% and 14.3% of total such cases registered in the country during 2015 respectively [2]. Maximum cases of 'Criminal trespassing /Burglary' and 'Theft' took place in residential premises [3].

Keeping this in mind we propose a home access system that comprises of the android smartphone App, online server, and WiFi module attached to the door lock. This system is enabled with the digital key authentication with widely used security algorithm SHA1. It works with two-step verification, first verifies the user password and then it needs an OTP to unlock the door. The Firebase messaging service runs on an android App which is installed on the visitor's smartphone who wants an access to the home. This user-friendly App makes it easy-to-use for any novice user. The use of various event-based sensors like accelerometer makes such system to detect intrusion. It detects the tapping or smash on the door by an intruder. Door status becomes important during events when the user is locking or unlocking the door and in cases where door left unlocked for some time without anybody entering. To keep vigil of the open/closed status of the door and the unusual events like door smashing, keeping door open for a long time, we use the accelerometer and magnetometer, respectively. The door status checked by the comparing the current magnetometer reading and the value stored for door close threshold parameter. This decreases the break-ins due to open or unlock door to a major extent. The system is also useful in cases where we want to give access to a visitor who is having the android phone with this App installed by using one-time registration of user by one of the family members to the house. The registration/digital key generation is handled by the server which also reduces the need for a large number of computations at the WiFi module. We used WeMos D1 WiFi module which is low cost, WiFi enabled, having full stack implementation of TCP/IP, with 32-bit controller and 1MB of space. It has no non-volatile memory space; this memory can be extended by using the external EEPROM memory. We interface the secure cloud messaging service in such system to interact with the mobile device instead of using the SMS. This messaging service can also be implemented on the iOS devices very easily. This system specially useful for smart city with reliable WiFi and the Internet availability. This system is easy to install, time efficient and handy to new users.

Chapter 2

Home Access System in Technical Literature

This chapter includes the literature survey and the analysis of different methodologies to accomplish this purpose. This chapter comprises of the different design approaches and the drawbacks of the existing solutions that needs to be overcome for the efficient and user-friendly system.

2.1 The Concept of Home Access System [4]

The home automation is an application of the Internet of Things (IoT). This system connects various household devices to the user end which makes it easy to access and control various systems like ventilation, auto-lighting, auto-controlling, air conditioning and home access systems.

Accommodating access control to some bonafide/regular users and also to once-in-a-while users, such as, guests, delivery men, etc. is the primary need of such application.

From usability point, interface or UI of such application must be very user friendly even to a novice user. The access to the system must be convenient and secure to users. The Number of smartphone App users has expeditiously been increasing, and various handy and useful Apps are being added to play stores every day. Therefore, an access control system for achieving home security, comprising of smartphone, Apps, door locks and mobile devises is a practical requirement of modern digital societies.

2.2 Wireless Access Monitoring and Control System Based on Digital Door Lock [6]

A door lock system has been proposed [6] on a ZigBee network. They developed different modules for various purposes. The module for human detection detects a human at the door which is achived by a ZigBee tag. They also suggested an idea to use an additional sensor device to extend the system to the house monitoring and security system. This system can be extended to additional services by connecting the mobile phone and home networking system.

Some of the key points that can be extended are as follows:

- This proposed system uses the ZigBee tag for user authentication. The user has to keep this tag with him whenever he wants access to the house. If we could integrate this technology with the existing technologies like mobile device then also it would be convenient to use the system.
- This system has the human detection module that also detects the movements of the people. Such functionalities could also be integrated and put on a module without the need of developing a separate module.
- In the case of lost tag, tag id has to be removed from the registration list. Otherwise, it can be used for untrusted access to the system.
- We can improve this system by integrating it with a mobile application. If the mobile device is misplaced, it is easy to block the user from the system that prevents the misuse of the application.

2.3 A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System [7]

A home automation system is presented that includes GSM, Internet, and speech recognition algorithm. They presented the design and the implementation of the whole system with interactive web GUI. Some of the key points are as follows:

- GSM used in this system for interaction with lock due to its broad coverage. It is also text-based protocol to have access to the system. They are also using the Internet to access the system. In case if identity and password theft the whole system could be brought down. Two-step verification of the user with credentials and OTP can be included. This aspect of the authentication can also be implemented with the cloud messaging services.

2.4 Different Devices for Authentication in Home Access Systems

The different known devices used for smart lock security reasons.

- Pass code based locking system consists of the keypad. Intruder can crack the code after several tries and different combinations. It's very user-friendly and convenient [8].
- Smart card used with the pass code to unlock. It unlocks the door after scanning the card. It's quiet convenient to operate, but difficult to operate in case if card lost. There is also a possibility that secrets stored in a card can be extracted or clone the card [9].
- Bluetooth locking system has the advantage that it's convenient to use without the need of any pass code after it gets connected with the lock device. We have to carry extra device if this system is not integrated with our mobile device Bluetooth [10].

- RFID-based system uses the passive infrared which activates and verifies the user identity and then unlocks the door [11].

2.5 Securing the Internet of Things: Standardization Perspective [12]

The Internet of Things (IoT) is the next wave of innovation that assures to improve our daily life based on smart sensors and intelligent objects working together. The devices can now be connected to the Internet through IP (Internet Protocol) connectivity, thus allowing them to be controlled and managed at any time and at any location. Security is a key aspect for IoT networks. However, proprietary security solutions do not help in devising a consistent security perception to facilitate IoT devices to communicate securely with each other in an inter-operable mode. This paper covers a view of the attempts in the Internet Engineering Task Force (IETF) to standardize security aspects for the IoT ecosystem. It also presents an comprehensive review of the different communication security solutions for IoT, specially the standard security protocols to be used in combination with the Constrained Application Protocol (CoAP), an application protocol specially fitted to the needs of adapting to the limitations of IoT devices. Since Datagram Transport Layer Security (DTLS) has been selected as the channel security underneath CoAP, this paper also summarizes the recent standardization efforts to adapt the DTLS for IoT applications.

Chapter 3

Proposed Work

This chapter includes the problem statement with the overall proposed work that has been carried out. It also determines bifurcations of the entire work in different modules that also includes whole architecture, the description about various components used in the experimental setup of the home access system. It is really necessary to describe the features of the components that are used in the designing of the system.

3.1 Problem Definition

There may be situations when nobody is inside the house, but the owner of the house wants to allow the access of the house to some bonafide visitor [4]. For example, their kids are returning back from their school. The visitor needs to seek the permission of the house-owner to enter the house. In such case, the smart way to verify the identity of the visitor and to provide him/her with the electronic key to unlock the door is possible by a digital door lock system along with a mobile App.

We are proposing a digital home security system that has two parts a) a digital lock that is integrated on the entry door of the house and b) a mobile App that is installed on the smartphones of the bonafide users and visitors of the house. All these smartphones have Internet access and the digital lock has a WiFi module in it. The digital lock authenticates the registered user using server or visitor and provides the OTP to the visitor on his/her mobile App which is used to unlock the door.

The home access system or the digital lock comprises of different sensors to detect the intrusion. The accelerometer which is embedded in the door lock detects if the door lock has been smashed in an attempt to break in. On the other hand if some intruder opens the door lock by some malafide means to enter the house, the magnetometer attached to the lock detects the unauthorized opening of the door. Also, if the visitor unlocks the door but doesn't open it(i.e., the door is in closed state), this is also detected by magnetometer and locks the door again after 2 minutes.

The networked door lock, in such cases, notifies the user (or the owner of the house) of the unauthenticated access to the home. User can also use this android App when user lost his/her physical keys. In such cases, user can easily download or use this App to unlock the door.

3.2 System Architecture

Architecture of the home access system includes the user's smartphone, WeMos D1 WiFi module [14], database server and the Firebase cloud messaging service (FCM) [15].

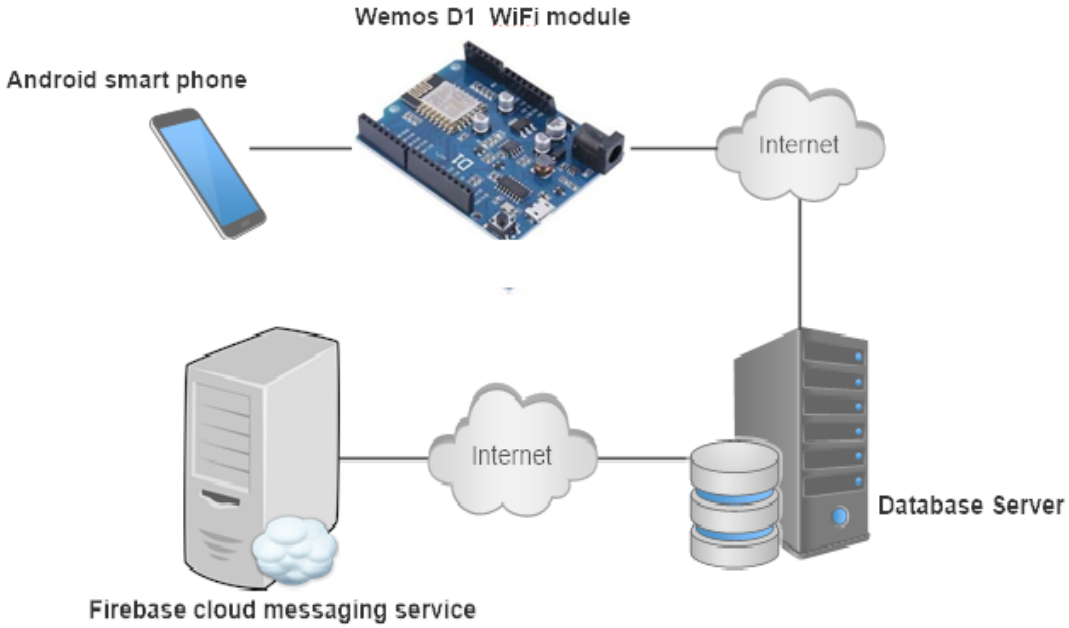


Figure 3.1: Architecture of the home access system

The front end of the home access system has three components described as follows:

Android smartphone: The home access system App developed for android smartphone is user friendly. This App has two buttons, first button click sends authenticated request to server and the other button click sends the OTP received by android smartphone to the WiFi module.

Server: The server authenticates the user request and then generates OTP against that request. Server sends the OTP to the user through the android App using the FCM service by Google [15]. FCM service uses the secured Transmission Layer Security (TLS) channel to communicate with the android App. It handles the requests made by WiFi module

WiFi module in the digital door lock: WiFi module has a shared secret, attaches the hash of the secret and the timestamp with the request made by android App. Thus the server can verify that the request is coming from the WiFi module and then verifies the user by computing the hash of the identity, password of user stored at database and the timestamp.

3.3 Components Description

This section includes a brief description about different components used in the proposed system of the home access system.

3.3.1 WeMos D1 WiFi ESP8266 Development Module

We have used an Arduino UNO compatible WiFi module based on ESP8266EX [13]. The WeMos D1 WiFi ESP8266 [14] chip offers the following features:

- **TCP/IP stack:** The ESP8266EX chip comes with TCP/IP stack and micro controller unit capability.
- **Compatibility with Arduino integrated development environment (IDE) :** It is platform independent, thereby, can be used with any OS like Linux, windows, etc.
- **Memory specifications:** A 32 bit RISC CPU running at 80MHz, 1MB flash memory, 64Kb of instruction RAM and 96Kb of data RAM.
- **WiFi capabilities:** It supports IEEE 802.11 b/g/n WiFi standards. This makes it more compatible for use in WiFi scenarios.

We have used the WiFi module as it is Arduino compatible and has the WiFi capability. It has the full TCP/IP stack that can be used with the server and the android smartphone for data transfer.

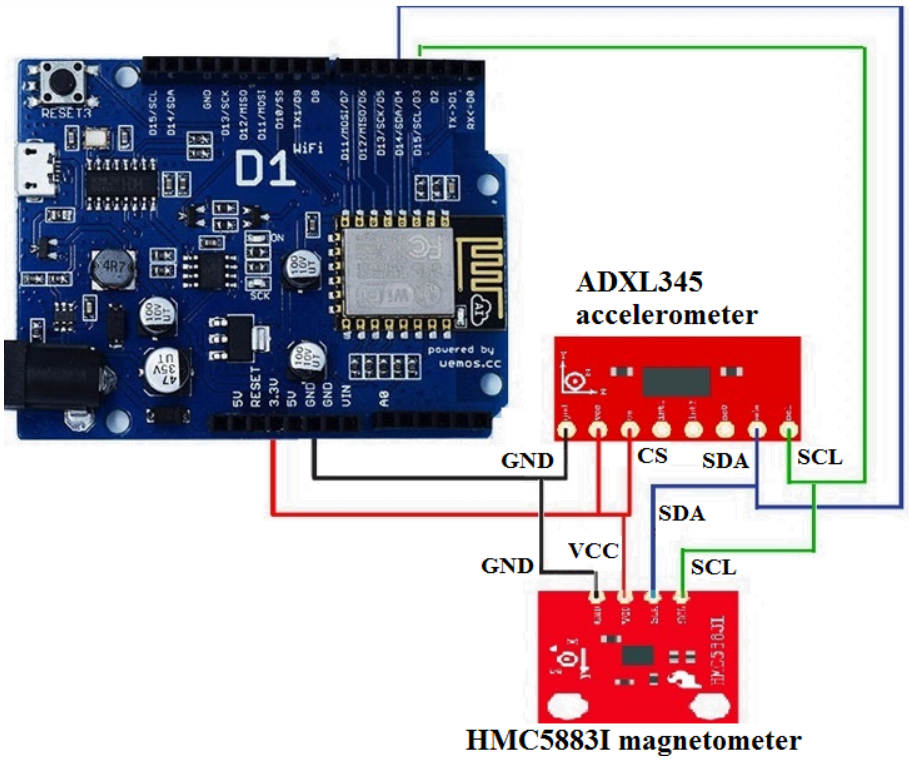


Figure 3.2: Schematic of the digital lock.

3.3.2 Accelerometer

The ADXL345 is a compact, thin, low power, 3-axis accelerometer with resolution (13-bit) measurement capability at up to 16 g [16]. Digital output data is formatted as 16-bit two's complement and is accessible either through a SPI (3- or 4-wire) or I^2C digital interface. It is well suited for mobile applications. It measures the constant acceleration of gravity in tilt-sensing applications. The ADXL345 is well suited to measure the constant acceleration of gravity in tilt-sensing applications, as well as dynamic acceleration resulting from motion or shock. Its high resolution (4 mg/LSB) enables measurement of inclination changes less than 1.0°. It has the following features:

- **Ultra Low operating Power:** It's low as 23 μA in measurement mode, 0.1 μA in standby mode at 2.5V
- SPI (3 and 4 wire) and I^2C digital interfaces.
- Tap and double tap detection.
- Activity/inactivity monitoring.
- 10,000 g shock survival

We have used the accelerometer to detect the tapping or smash on the door by any intruder. The accelerometer detects the tapping with threshold of more than or equals to 3g (G force due to gravity).

3.3.3 Magnetometer

The Honeywell HMC5883L is a surface-mount, multi-chip module designed for low-field magnetic sensing with a digital interface for applications such as low-cost compassing and magnetometry [17]. The HMC5883L includes high-resolution HMC118X series magneto-resistive sensors plus an ASIC containing amplification, automatic degaussing strap drivers and offset cancellation. The features of HMC5883L are as follows:

- **Simple interface:** I^2C protocol.
- 2.16 to 3.6V DC supply range and low current draw.
- 5 Milli-gauss resolution
- It enables 1° - 2° degree compass heading correctness.

We have used the magnetometer to detect whether door is opened when it is in unlocked status. We have used the compass heading to detect the degree of movement from the closed position of the door.

3.3.4 DS1307 Real-Time Clock

The DS1307 serial Real Time Clock (RTC) [18] uses an I^2C, serial, bidirectional bus to read and write.

Features and benefits: [18]
It provides all timekeeping functionalities as follows:

- The RTC provides year with leap-year, day of the week, month, date of the month, hours, minutes, seconds and the UNIX timestamp (It's the number of seconds lapsed since the Unix epoch (from 1st January, 1970 at UTC). It is valid up-to year 2100 and operates with leap year compensation.
- It operates with I^2C serial interface.
- It automatically detects power fail and operates from battery backup.
- It supports wide range of applications with industrial temperature range of -40°C to +85°C.
- Low power operation increases battery backup run time (it consumes less than 500nA when operates using battery backup).
- The RTC supports either the 24 hour or 12 hour clock format with am/pm indication.

The RTC used in our use-case to keep the time of the different events like locking, unlocking, opening and closing of the door. We use the time, to mark the event of tapping and also sends the timestamp with the alert messages to user.

Chapter 4

Methodology

This chapter describes the functionalities of different components that have been implemented in the architecture and the issues that have been faced while implementing them. It also includes sequence diagram and working of the implemented model.

4.1 Sequence Diagram

The sequence diagram shows different independent entities and the flow of the requests between them for OTP generation. Here, user through mobile App requests the OTP to the WiFi module which forwards the request to server that generates OTP and sends to mobile App using the Firebase cloud messaging service. The user submits the OTP received by the mobile App. The OTP is verified by the server and notification is displayed on the mobile App.

4.1.1 For Bonafide User

Steps for the authentication of family members and OTP request handling are as shown in figure 4.1 and explained briefly as follows:

1. The family member install an App and enters the digital key provided by lock company to enable App for further use.
2. Server stores digital key with key type as "member type" for further validation of user for OTP request.
3. The user connects to the WiFi module access point.
4. Then, clicks the OTP request button. The App automatically sends a request packet comprising of user identity, the SHA1 digest of digital key and timestamp (As shown in step 5 and 6 of figure 4.1).
5. The WiFi module receives this request and check for the proper arguments and attach the SHA1 digest of the secret stored in WiFi module, random number and the timestamp. It sends this to the server(As shown in step 7 and 8 of figure 4.1).
6. Server verifies the user with a digital key. Then, generates OTP.

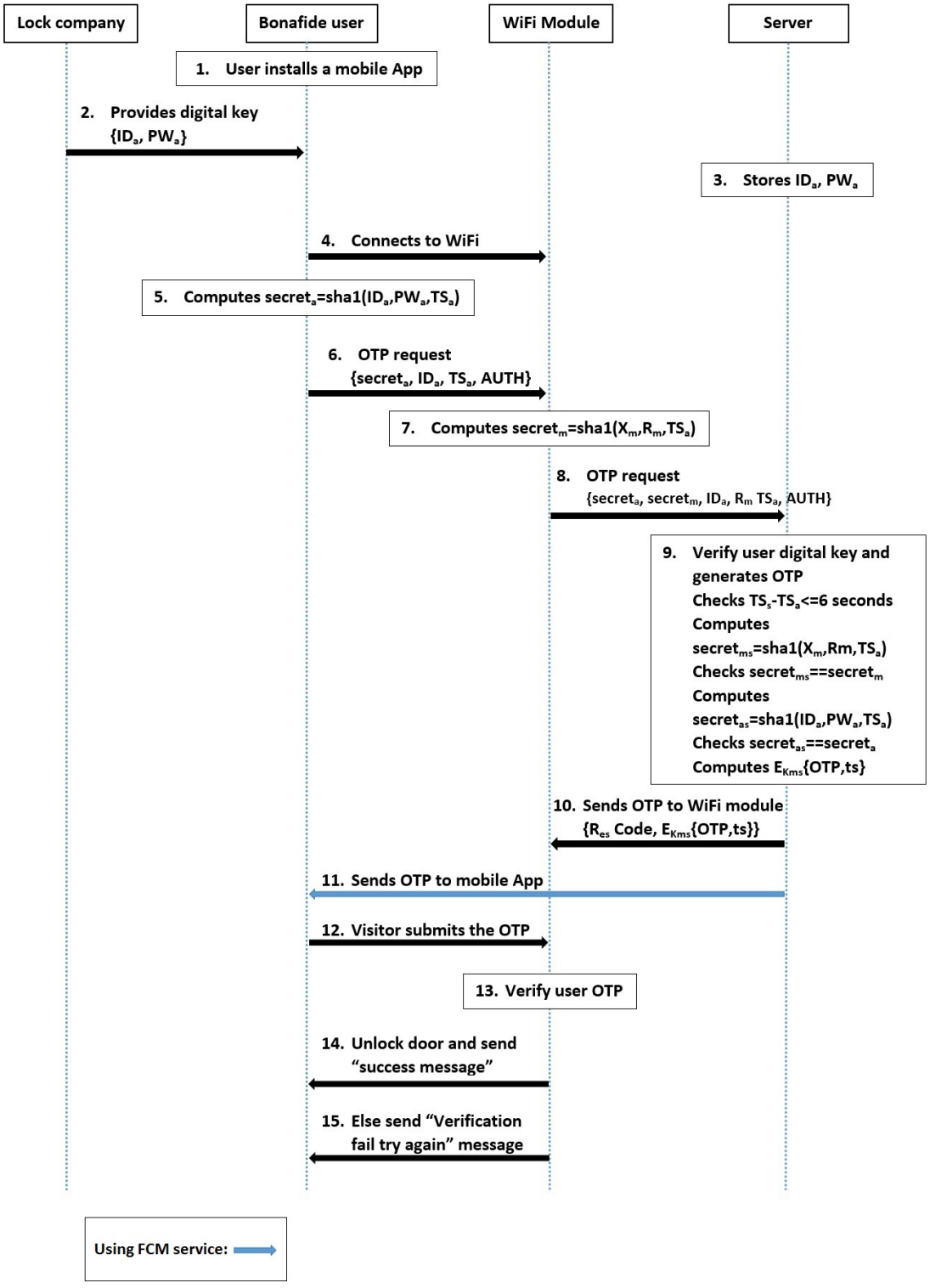


Figure 4.1: Sequence diagram with bonafide user digital key and OTP request handling.

7. Server sends OTP to visitor mobile App and WiFi module.

8. Visitor receives the OTP and uses mobile App to submit the OTP to the WiFi module.

9. The WiFi module now verifies the OTP with the OTP received from the server.
10. If the OTP matches then WiFi module unlocks the door and sends the success message to mobile App.
11. If the OTP match fail then it sends the fail message to user mobile App.

4.1.2 For Guest Visitor

Steps for the authentication of guest visitors and OTP request handling are as shown in figure 3.2 and explained briefly as follows:

1. The visitor request digital key using SMS/call from a family member.
2. The owner then verifies the authenticity of the visitor and request the digital key with the validity of a digital key from the server.
3. Server stores digital key with validity time for further validation of visitor for OTP request and also updates the corresponding shared secret in database for this row (As shown in step 5 of figure 4.2).
4. Server sends digital key, validity time to a visitor via mobile App. The application saves it and shows message that key updated.
5. App sends the SHA1 of the key, FCM token, Ra and timestamp to the server, which verifies updated user password and returns a success message. In case if this message not received by the visitor then visitor requests the digital key again.
6. The visitor connects to WiFi module access point.
7. Further steps are same as steps 4 to 11 of the user (as in section 4.1.1).

4.2 Functionality of the Server

A server is working on an Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips web server and a MariaDB database server [19]. Roles of the server are as follows:

- A server handles the user request to generates an OTP and also verifies it.
- It discards an OTP if OTP verification is successful.
- It sends an OTP generated to Mobile App using Firebase cloud messaging (FCM) service via a secure channel.
- It maintains an user identity, password and a secret stored at WiFi module.
- A Database at server maintains a time at which the request arrived and check for OTP timeout period.

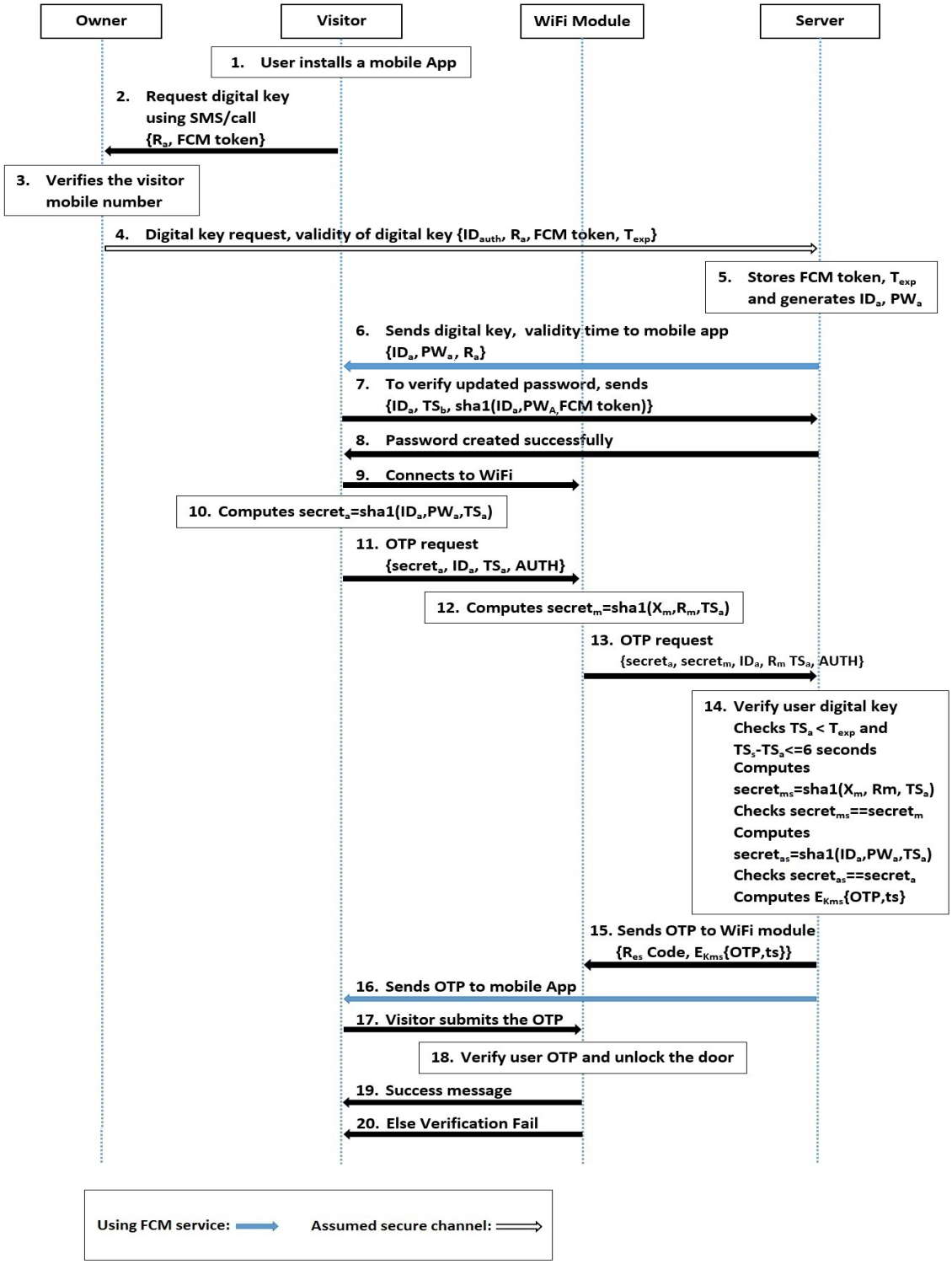


Figure 4.2: Sequence diagram with visitor digital key request and OTP request handling.

4.3 Functionality of the WiFi Module Attached with the Digital Lock

The D1 R1 is a WiFi capable ESP8266EX [13] based development module in the form of the common Arduino UNO board format. This module is compatible with

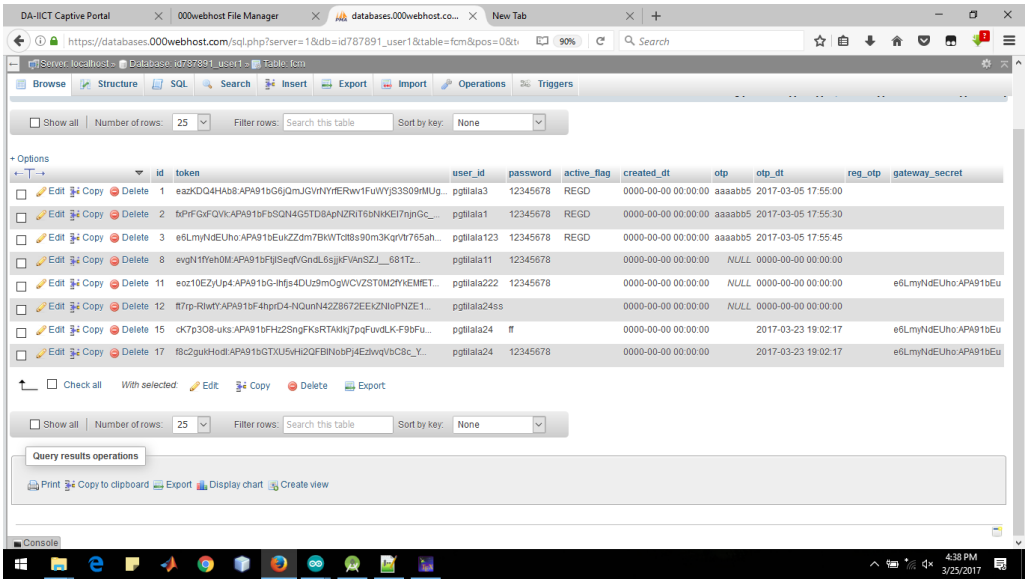


Figure 4.3: Database server user table

the Arduino IDE and with NodeMCU. This WiFi module is attached with a lock and runs HTTP server which accepts an OTP request and changes the status of lock with OTP verification. The WiFi module is connected to the Internet via a router at home. Smartphone connects to WiFi AP of WiFi module with the local IP address provided by WiFi module. The server running on the WiFi module cannot be accessed from outside the Local Area Network (LAN). So it ensures that user is at home and connected to local IP address.

- WiFi module handles the request by the user to unlock the door and sends that request to the server for authentication and the OTP generation purpose.
- WiFi module sends the hash of stored secret to insist that the request is coming from the WiFi module.
- It handles the response coming from the web-server and shows it on user smartphone.

4.4 Functionality of the Smartphone

A smartphone is installed with the android App that is enabled with the Firebase cloud messaging (FCM) service. Firebase cloud messaging (FCM) is a cross-platform messaging service with reliable delivery of messages at no cost. FCM architecture is shown in figure 4.4. The smartphone can connect to lock directly if the mobile has the Internet data plan to access the Internet and receives the push notifications. A user can also connect to a home router and get access to the Internet to receive notification.

- Android App receives the OTP generated by the server using FCM service as a push notification.
- This App has simple on-click GUI that requests and submits the OTP.

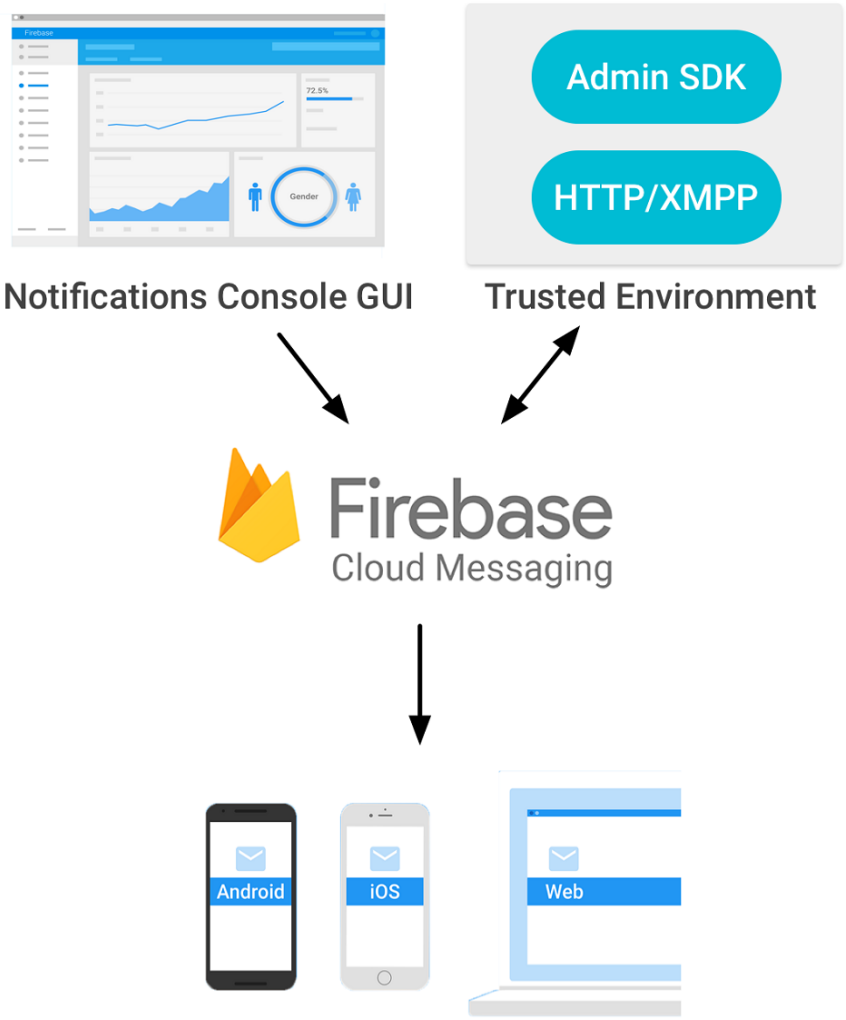


Figure 4.4: FCM Architecture [15]

4.5 Different Use Cases in Smart Lock Scenario

We have implemented the possible use-cases for smart lock scenario are as follows:

- Auto-lock the door if not opened after unlocking the door lock.
- Keeps door in open state after unlocking by visitor/user for some stipulated time period.
- User tries to lock the door in open state.
- If a malicious user tries to unlock through the spurious OTPs.
- If an intruder tries to smash the door and make a break in attempt.
- Valid user unlocks the door and enters the house.

Different factor used to make this functionalities works are as shown in the following table:

Table 4.1: Variables used to implement different functionalities

Parameters	Possible values/Description
Door status	Open/Close
Lock status	Lock/Unlock
Last open/close time	Timestamp
Last lock/unlock time	Timestamp
Flag opened	True if door opened once after unlock else false
Current time	Current timestamp from RTC
Door close threshold	Magnetic heading while door in proper close state
Wrong OTP counts	Maximum 3 times
Last wrong OTP time	Time when last wrong OTP submitted
Last OTP request time	Time when last successful OTP requested
Random number	To check that same user has made the OTP request and submission
User index	Returned from server on authentication of OTP request

4.5.1 Auto-lock the Door

As statistics shows that unlocked or open door is the reason behind the thirty percent of all burglaries. The condition for auto-lock is as shown in the table. If all this

Table 4.2: Conditions for auto lock

Parameters	Values
Door status	Close
Lock status	Unlock
Last open/close time	last close time > last open time
Current time−Last unlock time	$\geq$ 20 second
Flag opened	False

values satisfies then the lock status changed to lock, and last close time and last lock time gets update.

4.5.2 Keeps Door in Open State for a Long Time after Unlocking by Visitor/User.

The condition for this case is as follows:
This all conditions implies that the door is in open state from a long time. It sends the message to a user and all the family members of the house once. It also activates the buzzer such that it beeps every 5 minutes which makes a user aware of the open door.

Table 4.3: Conditions to check long open unlocked door

Parameters	Values
Door status	open
Lock status	unlock
Last close time == Last lock time	True
Current time − last open time	$\geq$ 120 second
last close time $\geq$last open time	True

4.5.3 User Tries to Lock the Door in Open State.

The user must ensure that door is properly closed before locking the door. So this can be ensured by verifying the door status. The door status is checked by comparing the current magnetometer reading and the value stored for door close threshold parameter. The response on App displays that "DOOR IS OPEN" if it is found to be open.

4.5.4 Three Wrong OTP Submission

The condition for the Three wrong OTP submission will be checked against the following parameters:

Table 4.4: Parameters to find consecutive three wrong OTP submission

Parameter	Possible values/Description
Wrong OTP counts	$\geq$ 3 times
Difference between two wrong OPTs	$\leq$ 20 seconds
Random number	To check that same user has made the OTP request and submission
User index	If same for 3 wrong consecutive OTPs

If the same user submits the wrong OTP three times, then the system sends an alert message to the family members.

4.5.5 Valid User Enters the House

In case if some user is already in the house and another user enters the house after completing the OTP verification process, then system rings the door bell. Even though, the house is empty i.e. no member is present, and any visitor enters, then also the door bell rings.

Table 4.5: Parameters for user authentication

Parameters	Values/Description
$\mathbf{T}_{exp}$	**Validity time of digital key**
FCM token	**Token provided by FCM server to uniquely identify mobile**
$\mathbf{ID}_{auth}$	**The identity of owner(authenticator)**
$\mathbf{ID}_a$	**The identity for each user stored in android device**
$\mathbf{PW}_a$	**The password for each user stored in android device**
$\mathbf{X}_{ms}$	**The shared secret between the WiFi module and server**
$\mathbf{K}_{ms}$	**The AES encryption key (shared by WiFi module and server)**
$\mathbf{TS}_a$	**Time stamp at android App**
$\mathbf{secret}_a$	**Hash(ID_a,PWD_A,ts_a) computed by android App**
$\mathbf{secret}_m$	**Hash(Xms,R_m,ts_a) computed by WiFi module**
$\mathbf{secret}_{as}$	**Hash(ID_a,PWD_A,ts_a) computed by server**
$\mathbf{secret}_{ms}$	**Hash(Xms,R_m,ts_a) computed by server**
Res_Code	**Response code by server(AUTHSUCCESS/AUTHFAIL)**

4.6 Security Aspect of the Usecase

4.6.1 User Authentication

The user authentication in this use case is through the identity and password. The user submits the hash of the identity, password, and the timestamp. Identity and password of the user are stored in the smartphone android App.
The following steps are involved in authentication:

- As shown in figure 4.2, in step 10 user/visitor clicks the OTP request button. The App gets current timestamp TS_a and computes $secret_a = sha1(ID_a, PW_a, TS_a)$ where identity ID_a and password PW_a are stored in android device. After that it sends $ID_a, secret_a, TS_a$, AUTH(type of request) to Wi-Fi module.

- Upon receiving the above request, the Wi-Fi module compares the current timestamp TS_c from RTC and TS_a. If $(TSc - TSa) \leq 3$ second then it generates random number R_m and computes $secret_m = sha1(X_{ms}, R_m, TS_a)$ where X_{ms} is shared secret between Wi-Fi module and Server. After that it sends the $ID_a, secret_m, secret_a, TS_a, R_m$ to the server. (As shown in step 11 of figure 4.2)

- As the server receives the above request, compares TSa with the current timestamp at server TSs. If $(TSs - TSa) \leq 6$ seconds and $TS_a \leq T_{exp}$ then computes the $secret_{ms} = sha1(X_{ms}, R_m, TS_a)$. If $secret_{ms} == secret_m$ implies that the request is coming from the Wi-Fi module. After that server computes the $secretas = sha1(ID_a, PW_a, TS_a)$ where ID_a, PW_a are stored on database at server. It compares it with the received $secret_a$ to check the authenticity of user. (As shown in step 12 of figure 4.2)

- The server then delivers a JSON string containing Res_Code, $\{OTP, ts\}_{Kms}$ (encrypted JSON array of OTP, ts by AES CBC with 128 bit key). The Res code is AUTH SUCCESS /AUTH FAIL. Also, it sends this OTP to user App using the FCM service. (As shown in step 13 ad 14 of figure 4.2)

- The WiFi module decrypt the encoded OTP, ts and then parse the JSON array and then use this OTP to verify the submitted OTP. (As shown in step 16 of figure 4.2)

4.6.2 Password Generation for Visitor

- Visitor request a new key, the App sends a FCM token, Random number (R_a) to the authenticator number using SMS. (While user installs App, FCM server sends FCM token to android App) (As shown in step 2 of figure 4.2)

- After receiving the request, Authenticator adds it's own identity and expiration time for the requested key. It sends a packet comprising of ID_a, R_a, FCM token, T_{exp} to server using secure channel. (As shown in step 3 ad 4 of figure 4.2)

- The server saves FCM token and T_{exp}, sends the packet with ID_a, PW_a, R_a to android App using the cloud messaging service. The App saves it and pops up the message that the key has been updated. (As shown in step 6 of figure 4.2)

- Now App sends the hash of the key, token and timestamp to the server which verifies updated user password and a return success message. (As shown in step 7 and 8 of figure 4.2)

Chapter 5

Implementation and Results

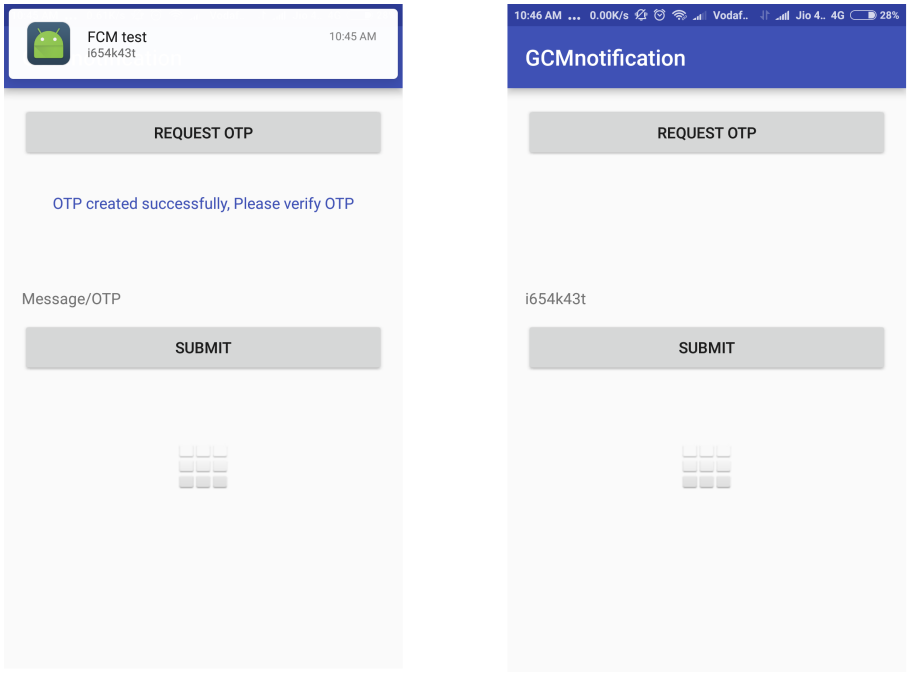
This chapter focuses on the experimental results and thereby obtained working system. It describes implementation results at each tier of system architecture as discussed in methodology earlier. With some basic features described as below:

- The android App automatically do all required computations on just a button click without entering the identity and password of the user.
- Server ensures that OTP request is coming from WiFi module by verifying a shared secret (between server and WiFi module).
- The OTP generated at the server is verified by the WiFi module for user authentication.

5.1 Android Application

An android App that runs the Firebase messaging service which checks for messaging-events received by the App. User clicks the "REQUEST OTP" button to get OTP. After this request, the server generates the OTP and sends it to user android App. The message event received as push notification by the Firebase messaging service is as shown in figure 5.1 (a) and also displays the message "OTP created successfully, Please verify OTP."

As shown in figure 5.1 (b), as the user clicks the push notification with OTP, the OTP is displayed into the text-box above the SUBMIT button.
User submits the OTP by using the SUBMIT button and in response, App will show the message "Verification Successful" in text-box below the button as shown in figure 5.2 (a) and timeout message "OTP verification timeout. Please generate new OTP" as shown in figure 5.2 (b).



(a) (b)

Figure 5.1: When OTP received by an android App (a)OTP received as push notification. (b)The OTP shows in text-box on clicking the notification.

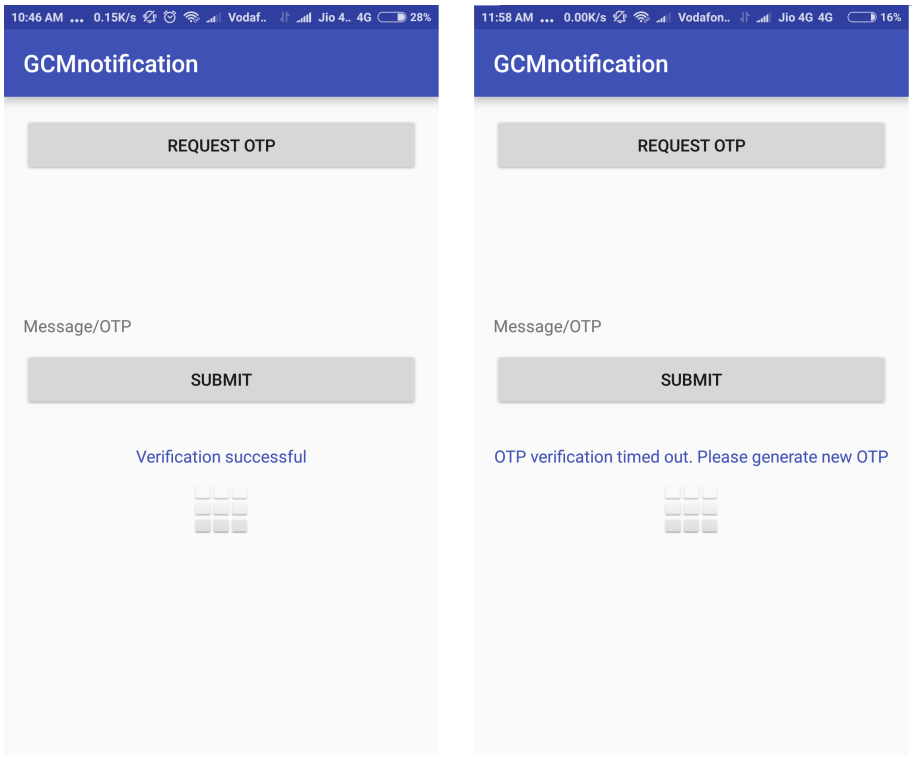


Figure 5.2: On OTP verification (a)On OTP verification success (b)on OTP verification timeout

5.2 WeMos D1 WiFi Module

WeMos D1 WiFi module runs HTTP server on local static IP address. First of all, a WiFi module connects to the home router and gets the IP address as shown in figure 5.3. Then it starts the server with “HTTP server started” message.

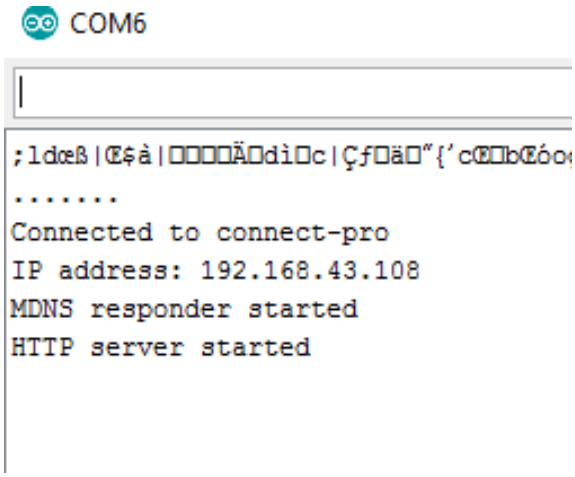


Figure 5.3: WiFi module setup

As shown in figure 5.4 WiFi module accepts the request by mobile App and checks whether the required arguments for that request are not missing or null. Therefore WiFi module requests the server to generate OTP and displays the response in the Arduino IDE serial monitor.

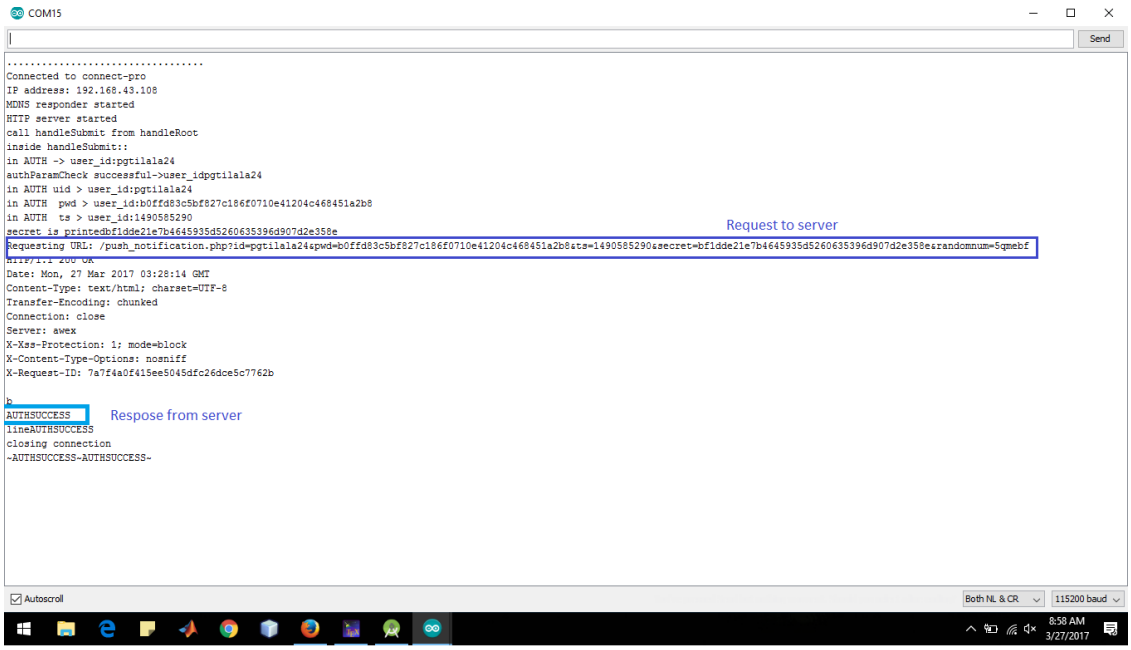


Figure 5.4: WiFi module handles the OTP request and response

5.3 Database Server

For experimental purpose database server is hosted at www.000webhost.com. The 000webhost is providing free hosting with limited resources that fulfills the requirement of our implementation. Database server stores the OTP and time of its generation. So, as shown in figure 5.5 the OTP field is blank and the otp_dt (OTP time) field is the time when the last OTP was generated.

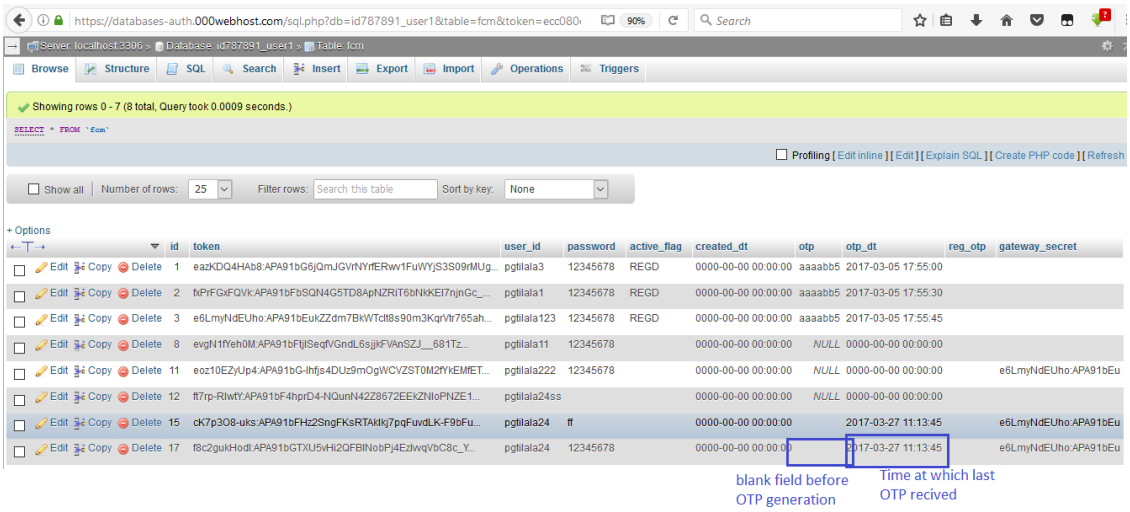


Figure 5.5: Database before OTP generation

After generation of OTP, the database is updated with new time and OTP as shown in figure 5.6.

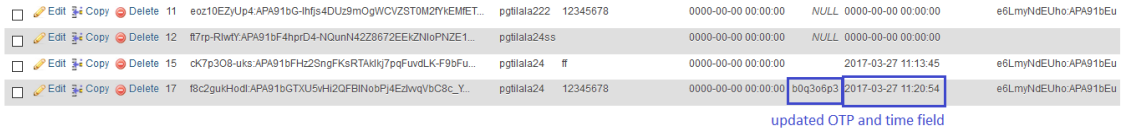


Figure 5.6: Database update with new OTP and time

On OTP submission, the server checks the OTP and time. If OTP submission time is less than stipulated time period (here, 2 minutes), then it verifies the received OTP with the stored one. On successful verification,database deletes OTP as shown in figure 5.7.

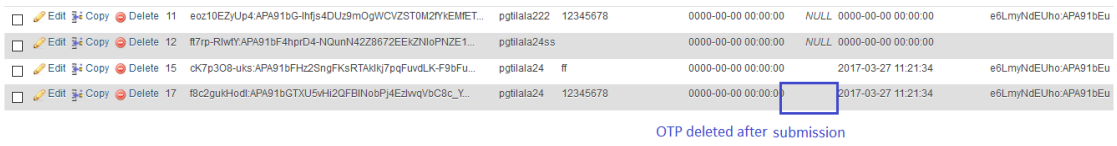


Figure 5.7: Database after submission of OTP

If a user submits the OTP after 2 minutes then OTP verification fails and the OTP and the value of otp_dt are not changed as shown in figure 5.8.

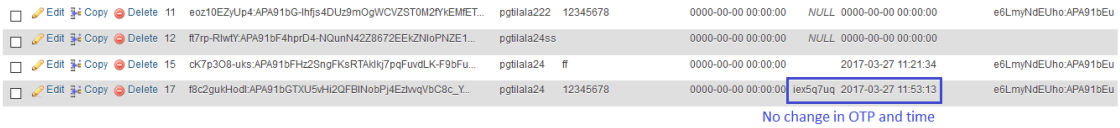


Figure 5.8: Database after OTP timeout

5.4 Use Case Implementation

5.4.1 Auto Lock

- It locks the door automatically if not opened within 60 seconds after unlocking the door as shown in figure 5.9.
- If the door is opened once then it will not auto lock.

Figure 5.9: Autolock after 60 seconds

- We have used a magnetometer to find the open door status after unlocking. If the door is opened once after unlocking then door does not lock automatically. In case if the door is in closed state after 60 seconds since the unlocking time, then this system locks the door. The automatic door locking happens only if last closing time equals last locking time and the time difference between last unlocking time and the current time reaches to 60 seconds.

5.4.2 Three Wrong OTP Submission

When three consecutive wrong OTPs are submitted by the user, he will get alert notification.

- It also restricts the user with OTP timeout of 2 minutes. The user needs to submit OTP within the 2 minutes. The WiFi module checks that OTP has

been generated in last 2 minutes if not, then it discards the OTP submission request.

- If any user submits the three wrong OTPs with the time difference between two OTP submission less than 20 seconds then only the system will deliver the alert message to the members of the house as shown in figure 5.10.

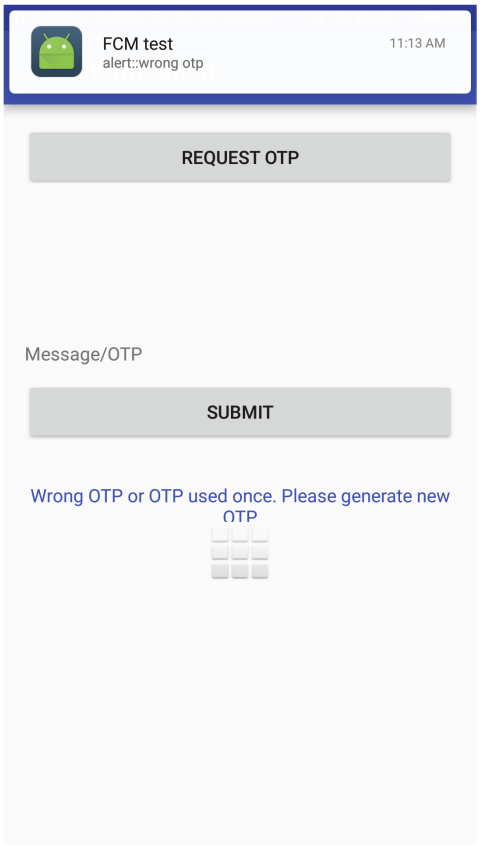


Figure 5.10: Alert notification after three wrong OTP

5.4.3 Door Open for Long Time after Unlocking

To alert the user, regarding the open state of the door for a long time after unlocking.

- If the difference between the last unlock time and last open time increases to 2 minutes then it sends the alert message to all house members and to the user who has opened the door last time as shown in figure 5.11.
- If the door is kept open for more than 2 minutes then buzzer attached to door lock will ring. This buzzer beeps every 5 minutes when the door is in opened and unlocked state.

Figure 5.11: Door in open state from 2 minutes after unlocking

5.4.4 Door Tapped by Burglar

If a burglar tries to smash the door hard, then the system sends an alert message to all family members as shown in figure 5.12.

- The tapping/smashing is detected using the accelerometer by detecting the continuous vibrations of the door.
- The buzzer beeps (security alarm) for long time in case of detection of such attempt to break-in the house.

5.4.5 Door Opened in Lock State and Try to Lock the Open Door

This alerts the user when door is opened by the intruder in locked state as shown in figure 5.13. The system also alerts the user of open door before locking. Response gets displayed that “DOOR IS OPEN” and beeps buzzer attached to lock as shown in figure 5.14.

Figure 5.12: Door tapping alert

5.5 User Authentication Security Implementation

Firstly, we implemented the OTP verification at server as shown in section 5.3. As shown in figure 5.15, the OTP and the timestamp in response are encrypted using AES standards. These values are then decrypted by the controller and used for OTP verification as shown in figure 5.15. The authentication code will get sent in plain text to show response for the authentication request.

5.6 Time and Memory Space Analysis

5.6.1 AES CBC Mode Time Analysis for Different Microcontrollers

The time taken by encryption and decryption process is negligible to be considered. Such less time ensures that implementing/using the AES would not make much difference in efficiency of the device from the time perspective. The analysis of the AES on Arduino Mega controller shows that it is easy to implement in such constrained devices [20]. As we have compared the three controllers for same AES library, the time taken by the Arduino uno and the Arduino Mega [21] is similar as both are using the 8-bit microcontroller with clock speed of 16MHz [22]. Whereas the WeMos D1 is embed with ESP8266 32-bit microcontroller having clock speed of 80MHz/160MHz.

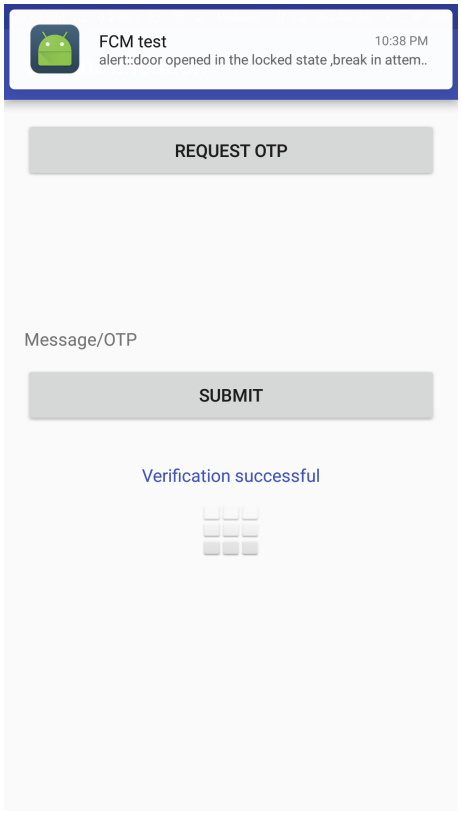


Figure 5.13: Door lock break alert

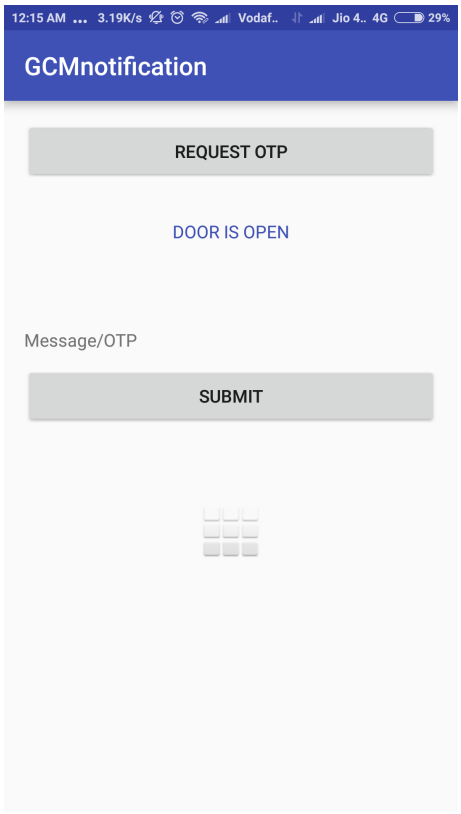


Figure 5.14: Lock door while it is open

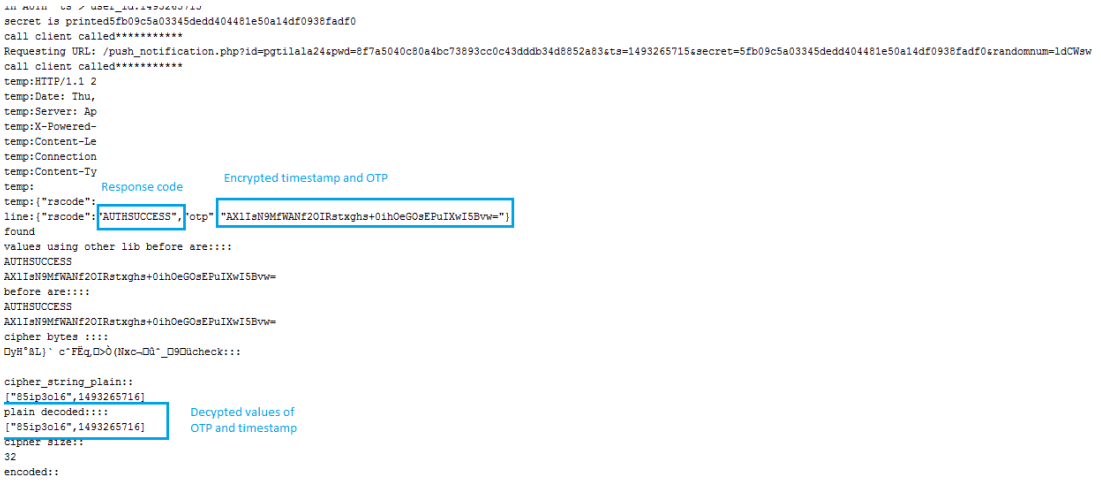


Figure 5.15: Encrypted response by server

Table 5.1: AES CBC time time analysis for the controllers

Controller	Key setup time	Encryption time	Decryption time
Arduino Uno(8-bit)	372 μs	611.2 μs	787 μs
Arduino Mega(8-bit)	370 μs	580 μs	770 μs
WeMos D1(32-bit)	71 μs	126.5 μs	178.1 μs

5.6.2 AES CBC Mode Memory Analysis on WeMos D1

There is enough memory space for additional functionalities after using AES encryption/decryption on WeMos D1 WiFi module. We have used the AES for encrypting the JSON array containing OTP and timestamp which is being send to the WiFi module from server in response to successful user authentication. As shown in figure 5.16, the WeMos D1 module has the 1 MB of flash memory space out of which 222 KB is used. So, remaining memory can be used for many other functionalities as we attached different devices to module using I^2C communication. This module does not have the E^2PROM in built, so we are saving the key for hash and encryption in the program sketch while installing. It is also feasible to use the external E^2PROM to store the permanent parameters.

Table 5.2: Memory usage for AES encryption and decryption on WeMos D1

Type of memory	Total space available	Space used	Space Remaining
Flash	1,044,464 bytes	227,345 bytes	817,119 bytes
SRAM	81,920 bytes	31,960 bytes	49,960 bytes

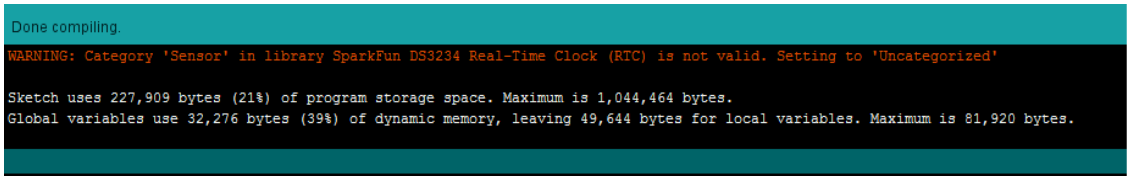


Figure 5.16: Memory space used by AES sketch

5.6.3 SHA1 Hash Time and Memory Analysis on WeMos D1

The average time to compute digest of sha1 on WeMos D1 device is 786.72μs. The memory scape used is as shown in figure 5.17. The time and space complexity do not add much delay to the system.

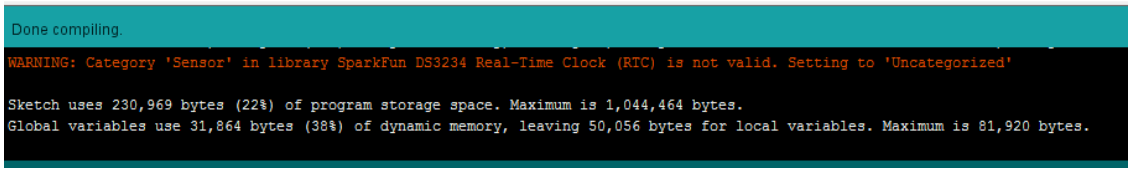


Figure 5.17: Memory space used by sha1 sketch

5.7 Time Taken for Different Request

The time taken by the system to unlock the door is sum of the time taken to generate OTP and submit it. This time is on an average about 5 seconds (assuming user submits the OTP instantaneously). The time taken by OTP submission request and round trip time to send the alert message is less than 1.2 seconds.

Table 5.3: Time taken for different request

Type of request	**Time in seconds**
RTT(Round Trip Time) OTP request-response	3.77
RTT OTP request-receive OTP on App	3.87
OTP submission	1.29
Request to server by WiFi module	3.06
Request to server by WiFi module(including processing time at WiFi module)	3.29
RTT to send an alert message	1.05

- Initially 50 percent of the RAM is initialized and other space used for storing the intermediate temporary results.
- As shown in figure 5.18, the memory space used by whole working code which includes code for reading the magnetometer, accelerometer, sending HTTP request, decrypting the AES encrypted data and sha1 computation is 27 percent of total flash memory available.

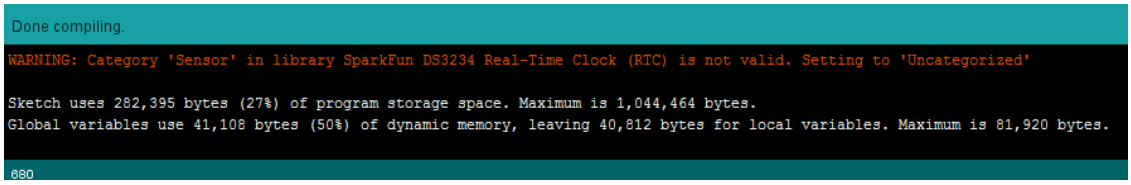


Figure 5.18: Memory space used by WiFi module sketch

Chapter 6

Conclusion and Future Work

We proposed a remote user authentication scheme for home access that uses WeMos D1 WiFi module with integrated sensors and an android App which makes system convenient to use. We ensured the security of the system with AES and the sha1 algorithm. We proposed a key generation for visitor to enter the house within predefined stipulated time period. We used Firebase cloud messaging service to deliver the alerts to the remote user of the smartphone App. This service removes the need to embed the GSM module for the same purpose. The prototype of the proposed system is experimented with lightweight accessories and found the proposed solution practical. The designed prototype can be extended for future work as follows:

- Such systems can also be implemented using more constrained aspects [12] of 6LOWPAN (IPv6 over Low power Wireless Personal Area Network), COAP (Constrained application protocol) and standard security of DTLS (Datagram transport layer security) for such real time application. IETF community is working toward a single security suite that is based on DTLS to provide security functionalities to the IoT devices. When every IoT devices are connected to the Internet, they must work on the same application (security) protocol to ensure interoperability.

Apart from the above mentioned point, different real time scenarios are required to be considered for the complete smart home access system. Such as:

- There could be cases where multiple users enters the premises while only one of them has the permission to enter (i.e., he has requested for the OTP).

  Another case could be considered when an user mistakenly presses the OTP request button multiple times within a short time. So, challenge is to take care of multiple requests from the same user, i.e., the first request of the user is in process and he tries for the second attempt.

  Also, multiple user requests within a short period of time could lead to long request queue at Wi-Fi module, it may not able to handle all. How to overcome such limitations of the Wi-Fi module? So, there is a need to analyze and overcome such limitations of each entity at each level of architecture.

From the security perspective of the use case, need to consider the ransomware attempt to lock guests out of their rooms by hijacking the central key management system (i.e., malware encrypts the victim's files and demands a ransom remittance to decrypt them). After such attack users couldn't use their key to enter their houses and also not possible to generate new keys [23].

References

[1] Mandela Quotes and Interesting information— South African History Online, Sahistory.org.za, 2017. [Online]. Available: http://www.sahistory.org.za/archive/mandela-quotes-and-interesting-information. [Accessed: 28 Mar 2017].

[2] Crime in India 2015 statistics. [Online]. Available: http://ncrb.gov.in/StatPublications/CII/CII2015/FILES/CrimeInIndia2015.pdf[Accessed: 11 Jul 2017].

[3] Crime in India 2015 compendium. [Online]. Available: http://ncrb.nic.in/StatPublications/CII/CII2015/FILES/Compendium-15.11.16.pdf. [Accessed: 11 Jul 2017].

[4] Use Cases for Authentication and Authorization in Constrained Environments, Tools.ietf.org, 2017. [Online]. Available: https://tools.ietf.org/html/draft-ietf-ace-usecases-10. [Accessed: 29 Mar 2017].

[5] Home Security Statistics, Safeguardtheworld.com, 2017. [Online]. Available: http://www.safeguardtheworld.com/statistics.html. [Accessed: 27 Mar 2017].

[6] I. K. Hwang and J. W. Baek, "Wireless access monitoring and control system based on digital door lock," in *IEEE Transactions on Consumer Electronics*, vol. 53, no. 4, Nov 2007.

[7] B. Yuksekkaya, A. A. Kayalar, M.B. Tosun, M.K. Ozcan and A. Z. Alkar, "A GSM, internet and speech controlled wireless interactive home automation system," in *IEEE Transactions on Consumer Electronics*, vol. 52, no. 3, pp. 837-843, Aug 2006.

[8] I. Kaur, "Microcontroller based home automation system with security," in *International Journal of Advanced Computer Science and Applications*, vol. 1, no. 6, pp. 60-65, Dec 2010.

[9] D. Husemann, "The smart card: don't leave home without it," in *IEEE Concurrency*, vol. 7, no. 2, pp. 24-27, Jun 1999.

[10] N.H. Ismail, Zarina Tukiran, N.N. Shamsuddin and E.I.S Saadon, "Android-based home door locks application via Bluetooth for disabled people," in *IEEE International Conference on Control System, Computing and Engineering*, pp. 227-231, Nov 2014.

[11] Y. T. Park, P. Sthapit, and J. Y. Pyun, "Smart digital door lock for the home automation," in *Proceedings of IEEE TENCON'09*, pp.16, Jan 2009.

[12] S. L. Keoh, S. S. Kumar and H. Tschofenig, "Securing the internet of things: A standardization perspective," in *IEEE Internet of Things Journal*, vol. 1, no. 3, pp. 265-275, May 2014.

[13] ESP8266, En.wikipedia.org, 2017. [online]. Available at: https://en.wikipedia.org/wiki/ESP8266 [Accessed 4 Mar 2017].

[14] D1, WEMOS Electronics, [Online]. Available: https://wiki.wemos.cc/ products:d1:d1. [Accessed: 03 Mar 2017].

[15] Firebase — App success made simple, Firebase, 2017. [Online]. Available: https://firebase.google.com/. [Accessed: 27- Mar- 2017].

[16] ADXL345, Analog Devices, 2009. [Online]. Available: https://www.sparkfun .com/datasheets/Sensors/Accelerometer/ADXL345.pdf. [Accessed: 04 Mar 2017].

[17] 3-Axis Digital Compass IC HMC5883L, Honeywell, 02 2013. [Online]. Available: https://cdn-shop.adafruit.com/datasheets/HMC5883L_3-Axis_Digital_Compass_IC.pdf. [Accessed: 05 Mar 2017].

[18] DS1307 64 x 8 Serial I^2C Real-Time Clock, Maxim Integrated, 2017. [Online]. Available: https://datasheets.maximintegrated.com/en/ds/DS1307.pdf

[19] About MariaDB, MariaDB Foundation , 2017. [Online]. Available: https:// mariadb.org/about/. [Accessed: 04 Mar 2017].

[20] P. Gupta, "Implementing security in a personal security device," Ph.D. dissertation, The University of California Los Angeles, 2013. [Online]. Available: https://pdfs.semanticscholar.org/314d/90321057a7d641071afb8cb68e3509933fca.pdf. [Accessed: 27 Feb 2017]

[21] Arduino Mega 2560, Arduino.cc, 2017. [Online]. Available: https://www.arduino.cc/en/Main/arduinoBoardMega2560. [Accessed: 27 Apr 2017].

[22] AES library, Utter.chaos.org.uk, 2017. [Online]. Available: http://utter .chaos.org.uk/ markt/AES-library.zip. [Accessed: 27 Apr 2017].

[23] A. Ghoshal, Hackers use ransomware to target hotel guests' door locks, The Next Web, 2017. [online]. Available at: https://thenextweb.com/security/2017/01/30/hackers-use-ransomware-to-lock-hotel-guests-in-their-rooms/ [Accessed 14 Feb 2017].