CHAPTER 1

INTRODUCTION

CHAPTER 1: INTRODUCTION

The emergence of smart devices has boosted the concept of connecting everyday objects via the existing networks. The drastic increase of connected devices has outreached the boundaries of the conventional networks, resulting the renaissance of the web as the third wave "Internet of Things (IoT)". IoT is rapidly growing network of heterogeneous devices and objects, which are uniquely addressable within the network and capable of identifying and sharing information with or without human interaction. The concept of Home Automation was a topic of interest in the Academic arena since the late 1970s, with time and advancement of technology people's expectations about Home Automation and how they should access their home has dramatically changed. The affordability and popularity of electronic devices and internet were contributing factors to this change.

The modern Home Automation System is a delicate balance of Ubiquitous Computing Devices and Wireless Sensor/Actor Networks. The added expectations and Convenience of Access' has brought new security challenges to the Home Automation front. Various researchers showed that, there are vulnerabilities in many commonly used devices and technologies in Home Automation. In this sense, learning and recognizing human behavior has emerged as a relevant issue, and, concurrently, the analysis of the human–machine interaction and the definition of the appropriate ways to communicate with a smart home as intuitively and naturally as possible has become crucial. With respect to this, gesture interpretation represents an appealing, as well as valid, alternative to other more conventional contact-based or video-based modalities.

In particular, the specialized literature reports on studies that refers to context-aware multimodal interfaces based on video and audio inputs, static hand pose and dynamic hand gesture visual recognition glove-based sensing, or marker-based motion capture systems. These technologies have pioneered the research in the field but show

some limitations for a seamless employment in a smart home: They require a dedicated and often expensive environment; they frequently need a complex setup that involves calibration procedures and may be strongly affected by environmental nuisances (e.g. light changes).

Security of human property is one of the paramount challenges facing any nation or any corporate organization. Also, ensuring safety and confidentiality electrical appliances is quite essential to prevent unauthorized access. The design and construction of user fingerprinting with device fingerprinting system provides a sure way of ensuring this security and safety for human property. Unique Bio-identification with integrated device fingerprint system provide high security door access system that can be used to open and close objects in IOT such as door in smart home.

There are certain situations which are very annoying like when a person locks himself out of his house or office or he leaves his key inside or sometimes when a thief just breaks the lock and steals everything. These kinds of situations always trouble people who use manual door lock with keys. Although in some places people use smart cards, there might arise a situation when someone loses the card or keeps the card inside. Then in other scenarios there are caretakers for locking houses or offices and keeping the keys safe. But then again there are times when a person in charge of the keys might not be available or has gone to some emergency routine, which can cause unwanted delay for people who need the key straightaway. These are some of the hassles that people might face when using keys or smart cards. That is when our system, fingerprint based lock system comes into play. Our design is implemented to provide better securities as users don’t need to remember passwords and don’t need any sort of keys or cards that often get lost. If someone’s fingerprint is authorized in the system he would not face any sort of delays to enter a room.

Fingerprint recognition is one of the most secure systems because fingerprint of one person never matches with the others. Therefore unauthorized access can be restricted by designing a lock that stores the fingerprints of one or more authorized users and unlock the system when a match is found. Bio-metrics authorization proves to be one of the best traits because the skin on our palms and soles exhibits a flow like pattern of ridges on each fingertip which is unique and immutable. This makes fingerprint a unique identification for everyone. The popularity and reliability on fingerprint scanner can be easily guessed from its use in recent hand-held devices like mobile phones and laptops.

Device fingerprinting is the collection of information which gives the remote computing devices for the purpose of identification. Fingerprints can be used to identify individual users or devices even when cookies are turned off. Objectives of the work is to successfully identify a device accessing the home over the internet using Device Fingerprinting. The second objective is to identify authorized user even when there are changes in location, browser or other browser specific features.

CHAPTER 2

PROBLEM STATEMENT

CHAPTER 2: PROBLEM STATEMENT

Home Automation System uses the technology of Internet of Things for monitoring and controlling of the electrical and electronic appliances at home from any remote location. Implementation of a low cost, flexible home automation system is presented. It enhances the use of wireless communication which provides the user with remote control of various electronic and electrical appliances. A smart home automation based on device fingerprinting improves the security. Device fingerprinting is used for fighting fraud on websites. The device fingerprint along with user fingerprint based security enables the verification of user as well as the device used to access the home. This significantly improves home security when they are accessed over the internet.

CHAPTER 3

LITERATUTE SURVEY

CHAPTER 3: LITERATUTE SURVEY

1]Arun Cyril Jose, Reza Malekian, "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home",DOI 10.1109/ACCESS.2016.2606478, IEEE Access.

The paper explains the importance of accessing modern smart homes over the internet, and highlights various security issues associated with it. The work explains the evolution of Device Fingerprinting concept over time, and discusses various pitfalls in existing device fingerprinting approaches. This paper propose a two stage verification process for smart homes, using Device Fingerprints and User fingerprints, which verifies the user device as well as the user accessing the home over the internet.

2]Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit, "Design and Implementation of a Fingerprint Based Lock System for Shared Access", North South University, Dhaka - 1229 {jayasree.baidya, trina.saha, ryad.moyashir.

Security has always been a major concern for the households and the office environment, and for this concern various approaches are in place to address the problem. Most of the major door lock security systems have several loopholes which could be broken down to gain access to the desired places, and it creates a concern for a secure lifestyle and proper working environment. Additionally, terrorism and unauthorized access to places have become a major issue now-a-days, and there is a need for a secure system to prevent unauthorized access especially in shared access environment. With this consideration, a design and prototype of a biometric fingerprint based door lock system has been presented in this paper. Biometric systems such as fingerprint provide tools to enforce reliable logs of system transactions and protect an individual's right to privacy.

3] Murad Khan, BhagyaNathali Silva, Kijun Han"Internet of Things based Energy Aware Smart Home Control System",DOI 10.1109/ACCESS.2016.2621752, IEEE Access.

They propose a smart home control system using a coordinator based ZigBee networking (CoZNET). The working of the proposed system is three fold, 1) smart interference control system controls the interference caused due to the co-existence of IEEE 802.11x based wireless local area networks (WLAN) and Wireless Sensor Networks (WSN), 2) smart energy control system is developed to integrate sunlight with light source and optimizes the energy consumption of the household appliances by controlling the unnecessary energy demands, and 3) smart management control system to efficiently control the operating time of the electronic appliances.

4]AthiraSankar, Lakshmi S, "A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home", International Research Journal of Engineering and Technology (IRJET) ,Volume: 04 Issue: 04 | Apr -2017.

Home automation involves automatic control of household features, activity and appliances. A home with an automatic control system is known as smart home. Automation system helps one's home to promote security, comfort and convenience. This paper is a survey on home automation by integrating device fingerprinting. This paper explains the importance of accessing modern smart home over the internet and highlights various security issues with it.

5] Shrikrishna Jogdand1, Mahesh Karanjkar, "Implementation of Automated Door Accessing System with Face Design and Recognition" , International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Most doors are controlled by persons with the use of keys, security cards, password or pattern to open the door. The aim of this paper is to help users for improvement of the door security of sensitive locations by using face detection and recognition. Face is a complex multidimensional structure and needs good computing techniques for detection and recognition. This paper is comprised mainly of three subsystems: namely face detection, face recognition and automatic door access control. Face detection is the process of detecting the region of face in an image. The face is detected by using the viola jones method and face recognition is implemented by using the Principal Component Analysis (PCA).

CHAPTER 4

REQUIREMENTS SPECIFICATIONS

CHAPTER 4: REQUIREMENTS SPECIFICATIONS

4.1 SOFTWARE REQUIREMENTS

4.1.1 Python

Python is a high level, interpreted, interactive and object oriented scripting language. Python is designed to be highly readable. It uses English keywords frequently where as other languages use punctuation, and it has fewer syntactical constructions than other languages. Python is interpreted. Python is processed at runtime by the interpreter. Do not need to compile your program before executing it

Python Features:

Python's features include: Easy-to-learn Python has few keywords, simple structure, and a clearly defined syntax. This allows the student to pick up the language quickly. Python2 is Easy-to-read: Python code is more clearly defined and visible to the eyes. Easy-to-maintain: Python's source code is fairly easy-to maintain. A broad standard library.

Python is a widely used high-level programming language for general-purpose programming, created by Guido van Rossum and first released in 1991. An interpreted language, Python has a design philosophy which emphasizes code readability (notably using whitespace indentation to delimit code blocks rather than curly braces or keywords), and a syntax which allows programmers to express concepts in fewer lines of code than possible in languages such as C++ or Java. The language provides constructs intended to enable writing clear programs on both a small and large scale.

Python features a dynamic type system and automatic memory management and supports multiple programming paradigms, including object-oriented, imperative, functional programming, and procedural styles. It has a large and comprehensive library.

Python interpreters are available for many operating systems, allowing Python code to run on a wide variety of systems. C Python, the reference implementation of Python, is open source software and has a community-based development model, as do nearly all of its variant implementations. C Python is managed by the non-profit Python Software.

4.1.2 PHP

It is a server-side scripting language designed primarily for web development but also used as a general-purpose programming language. The PHP reference implementation is now produced by The PHP Development Team. PHP originally stood for Personal Home Page, but it now stands for the recursive acronym PHP: Hypertext Preprocessor.PHP code may be embedded into HTML code, or it can be used in combination with various web template systems, web content management systems and web frameworks. PHP code is usually processed by a PHP interpreter implemented as a module in the web server or as a Common Gateway Interface (CGI) executable. The web server combines the results of the interpreted and executed PHP code, which may be any type of data, including images, with the generated webpage. PHP code may also be executed with a command-line interface (CLI) and can be used to implement standalone graphical applications.

4.1.3 Apache tomcat:

Apache Tomcat is used to deploy your Java Servlets and JSPs. So in your Java project you can build your WAR (short for Web ARchive) file, and just drop it in the deploy directory in Tomcat. So basically Apacheis an HTTP Server, serving HTTP. Tomcat is a Servlet and JSP Server serving Java technologies. Apache Tomcat, often referred to as Tomcat Server, is an open-source Java Servlet Container developed by the Apache Software Foundation (ASF). Tomcat implements several Java EE specifications including Java Servlet, JavaServer Pages(JSP), Java EL, and WebSocket, and provides a "pure Java" HTTP web server environment in which Java code can run.Tomcat is developed and maintained by an open community of

developers under the auspices of the Apache Software Foundation, released under the Apache License 2.0 license, and is open-source software.

4.1.4 Mysql

MySQL is an open source relational database management system (RDBMS) based on Structured Query Language (SQL). MySQL runs on virtually all platforms, including Linux, UNIX, and Windows. Although it can be used in a wide range of applications, MySQL is most often associated with web-based applications and online publishing and is an important component of an open source enterprise stack called LAMP. LAMP is a Web development platform that uses Linux as the operating system, Apache as the Web server, MySQL as the relational database management system and PHP as the object-oriented scripting language. (Sometimes Perl or Python is used instead of PHP.) MySQL, which was originally conceived by the Swedish company MySQL AB, was acquired by Sun Microsystems in 2008 and then by Oracle when it bought Sun in 2010. Developers can still use MySQL under the GNU General Public License (GPL), but enterprises must obtain a commercial license from Oracle. MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons.

4.2 HARDWARE REQUIREMENTS

4.2.1 RASPBERRY PI

Raspberry Pi is a credit-card-sized single board computer developed in the UK by Raspberry Pi foundation with the intention of stimulating the teaching of basic computer science in schools. It has two models; Model A has 25 6Mb RAM, one USB port and no network connection. Model B has 5 12Mb RAM, 2 USB ports and an Ethernet port. It has a Broadcom BCM2835 system on a chip which includes an ARMl176JZF -S 700 MHz processor, Video Core IV GPU, and an SD card. The GPU is capable of Blu-ray quality

playback, using H.264 at 40MBits/s. It has a fast 3D core accessed using the supplied OpenGL ES2.0 and Open VG libraries. The chip specifically provides HDMI and there is no VGA support.

The foundation provides Debian and Arch Linux ARM distributions and also Python as the main programming language, with the support for BBC BASIC, C and Perl, detailed description of Raspberry Pi board has been given in Fig. 3(Raspberry Pi user guide). Python was chosen as the main programming language, as it is generally accepted to be both easy to learn and a fully fledged, programming language suitable for real world applications.

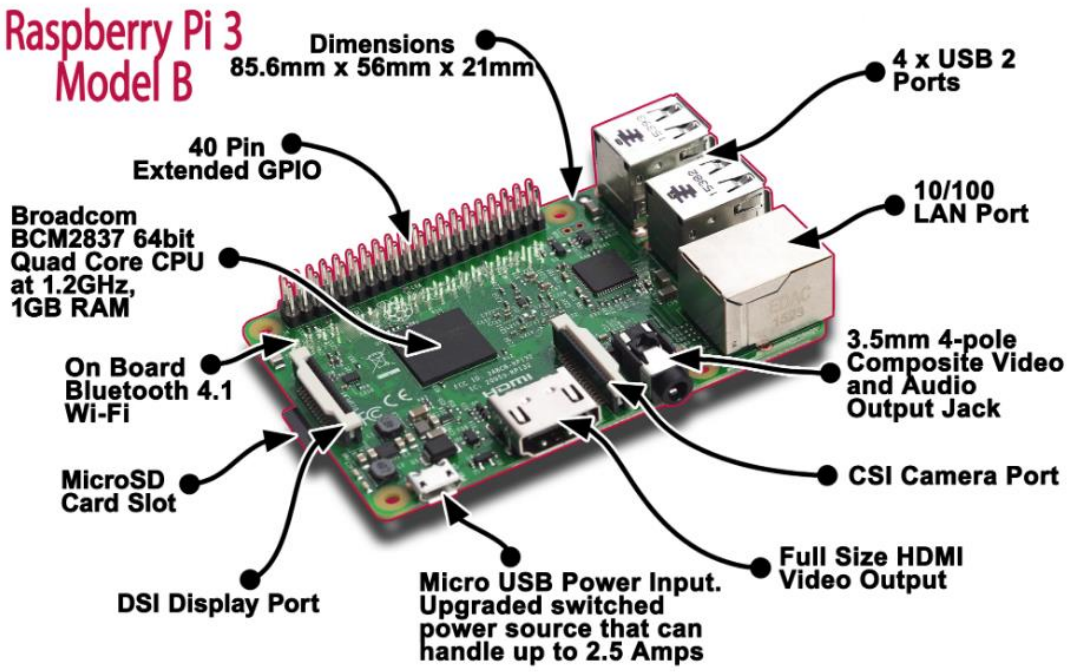


Figure 3.1 Raspberry pi module B

GPIO

The Raspberry Pi 3 features the same 40-pin general-purpose input-output (GPIO) header as all the Pis going back to the Model B+ and Model A+. Any existing GPIO

hardware will work without modification; the only change is a switch to which UART is exposed on the GPIO's pins, but that's handled internally by the operating system.

USB chip

The Raspberry Pi 3 shares the same SMSC LAN9514 chip as its predecessor, the Raspberry Pi 2, adding 10/100 Ethernet connectivity and four USB channels to the board. As before, the SMSC chip connects to the SoC via a single USB channel, acting as a USB-to-Ethernet adaptor and USB hub.

Antenna

There's no need to connect an external antenna to the Raspberry Pi 3. Its radios are connected to this chip antenna soldered directly to the board, in order to keep the size of the device to a minimum. Despite its diminutive stature, this antenna should be more than capable of picking up wireless LAN and Bluetooth signals – even through wall.

4.2.2 FINGERPRINT SENSOR MODULE

Figure 4.2.2: Finger print sensor module

This is a fingerprint sensor module with TTL UART interface for direct connections to microcontroller UART or to PC through MAX232 / USB-Serial adapter. The user can store the finger print data in the module and can configure it in 1:1 or 1: N mode for identifying the person. The FP module can directly interface with 3v3 or 5v Microcontroller. A level converter (like MAX232) is required for interfacing with PC serial port. Optical biometric fingerprint reader with great features and can be embedded into a variety of end products, such as: access control, attendance, safety deposit box, car door locks.

Features

- Integrated image collecting and algorithm chip together, ALL-in-One
- Fingerprint reader can conduct secondary development, can be embedded into a variety of end products
- Low power consumption, low cost, small size, excellent performance
- Professional optical technology, precise module manufacturing techniques
- Good image processing capabilities, can successfully capture image up to resolution 500 dpi

Specifications

- Fingerprint sensor type: Optical.
- Sensor Life: 100 million times.
- Static indicators: 15KVBacklight: bright green.
- Interface: USB1.1/UART(TTL logical level).
- RS232 communication baud rate: 4800BPS~115200BPS changeable.
- Dimension: 55*32*21.5mm.
- Image Capture Surface 15—18(mm).
- Verification Speed: 0.3 sec.
- Scanning Speed: 0.5 sec.
- Character file size: 256 bytes.
- Template size: 512 bytes.

- Storage capacity: 250.
- Security level: 5 (1,2,3,4,5(highest)).
- False Acceptance Rate (FAR) :0.0001%.
- False Rejection Rate (FRR): 0.1%.
- Resolution 500 DPI.
- Voltage :3.6-6.0 VDC.
- Working current: Typical 90 mA, Peak 150mA.
- Operating Environment Temperature: -20 to 45° centigrade.

CHAPTER 5

SYSTEM DESIGN

CHAPTER 5: SYSTEM DESIGN

5.1 UML DIAGRAMS

5.1.1 USE CASE DIAGRAM

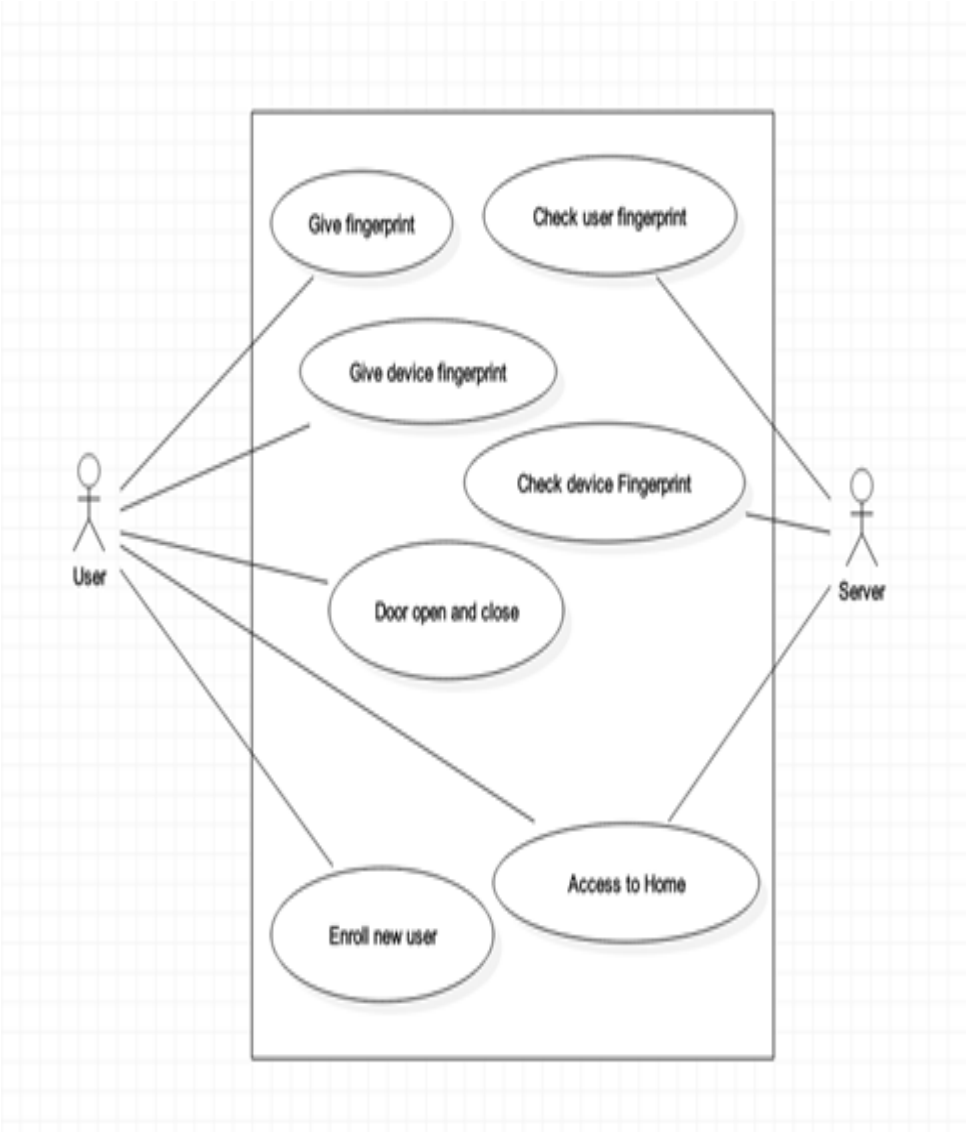


Figure 5.1.1: USE CASE Diagram

5.1.2 CLASS DIAGRAM

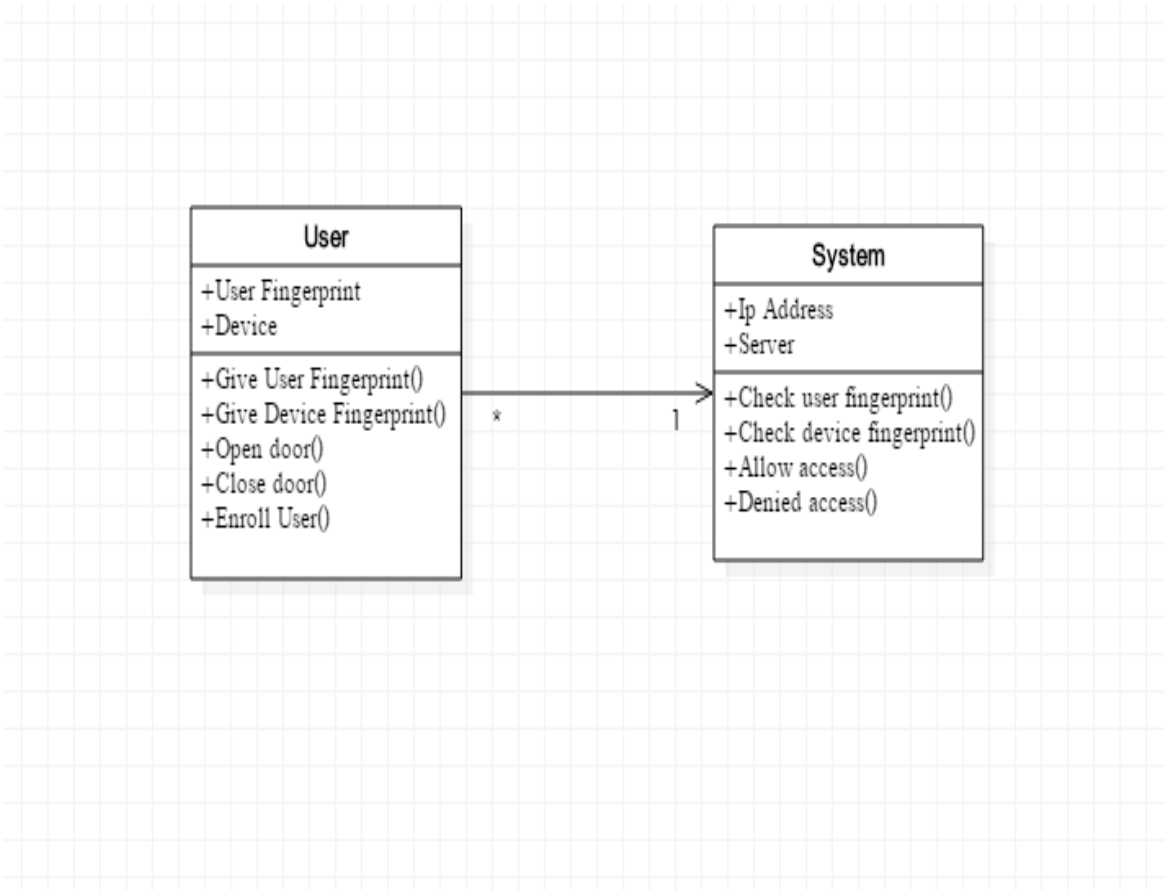


Figure 5.1.2: Class Diagram

5.1.3 SEQUENCE DIAGRAM

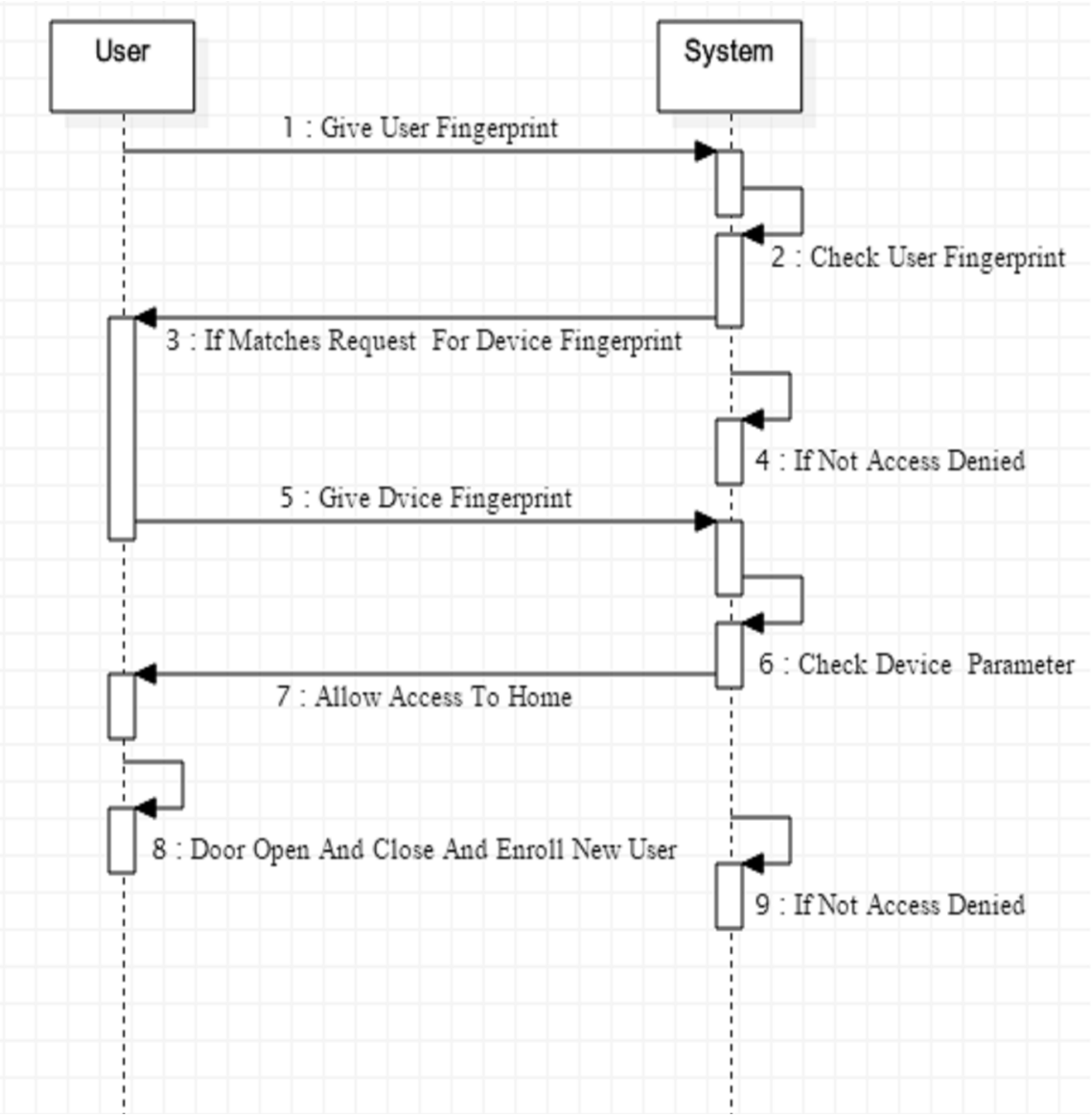


Figure 5.1.3: Sequence diagram

5.1.4 ACTIVITY DIAGRAM

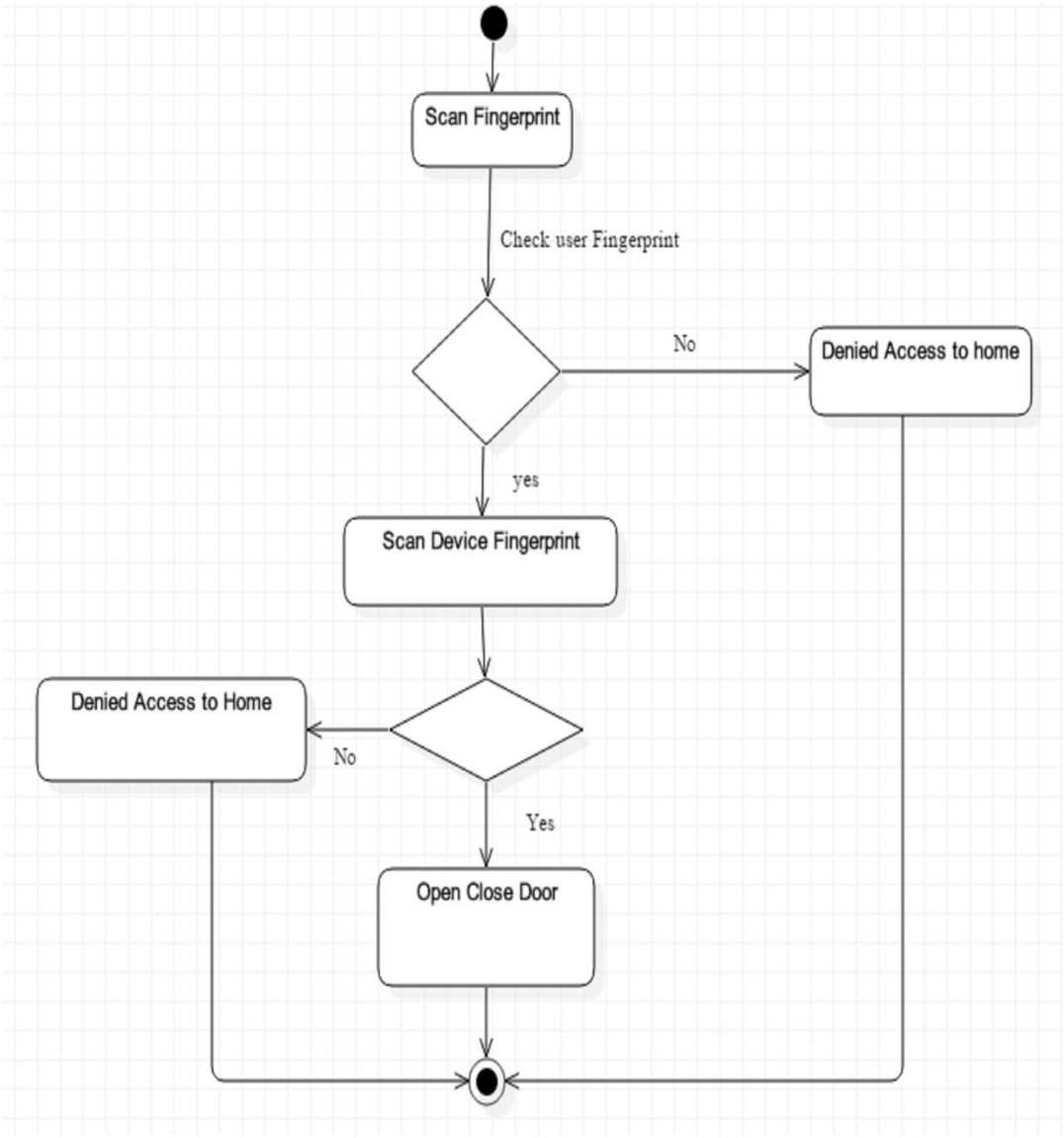


Figure 5.1.4: Activity diagram

5.1.5 DEPLOYMENT DIAGRAM

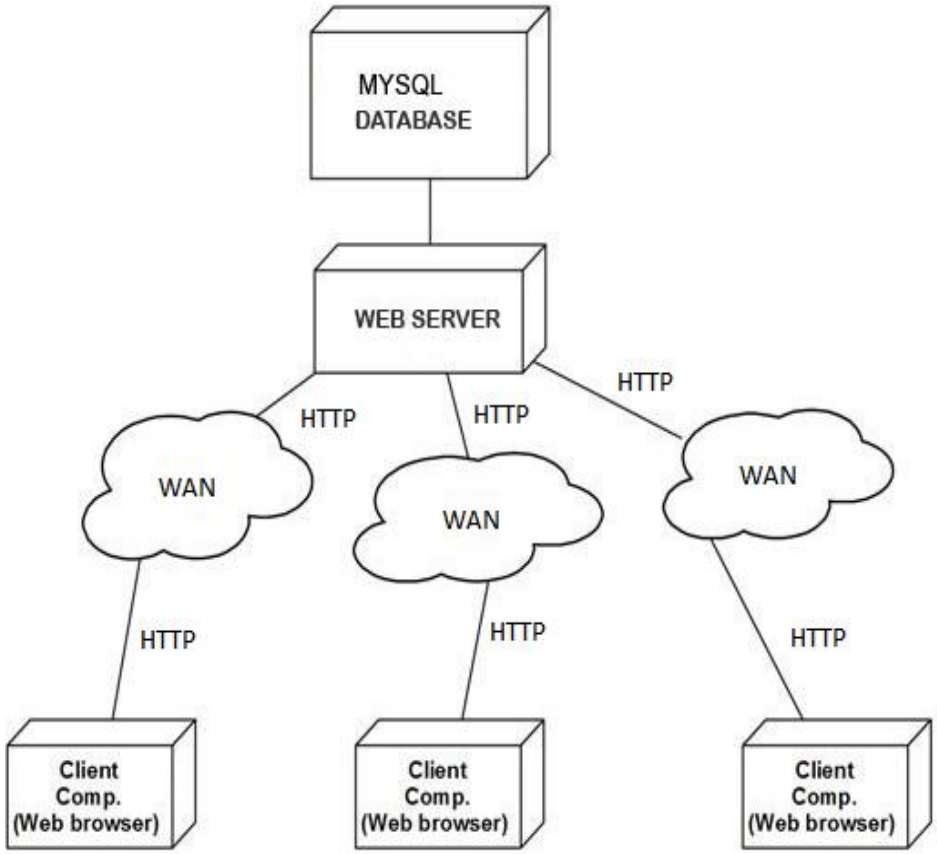


Figure 5.1.5: Deployment Diagram

CHAPTER 6

IMPLEMENTATION

CHAPTER 6: IMPLEMENTATION

6.1 ARCHITECTURE

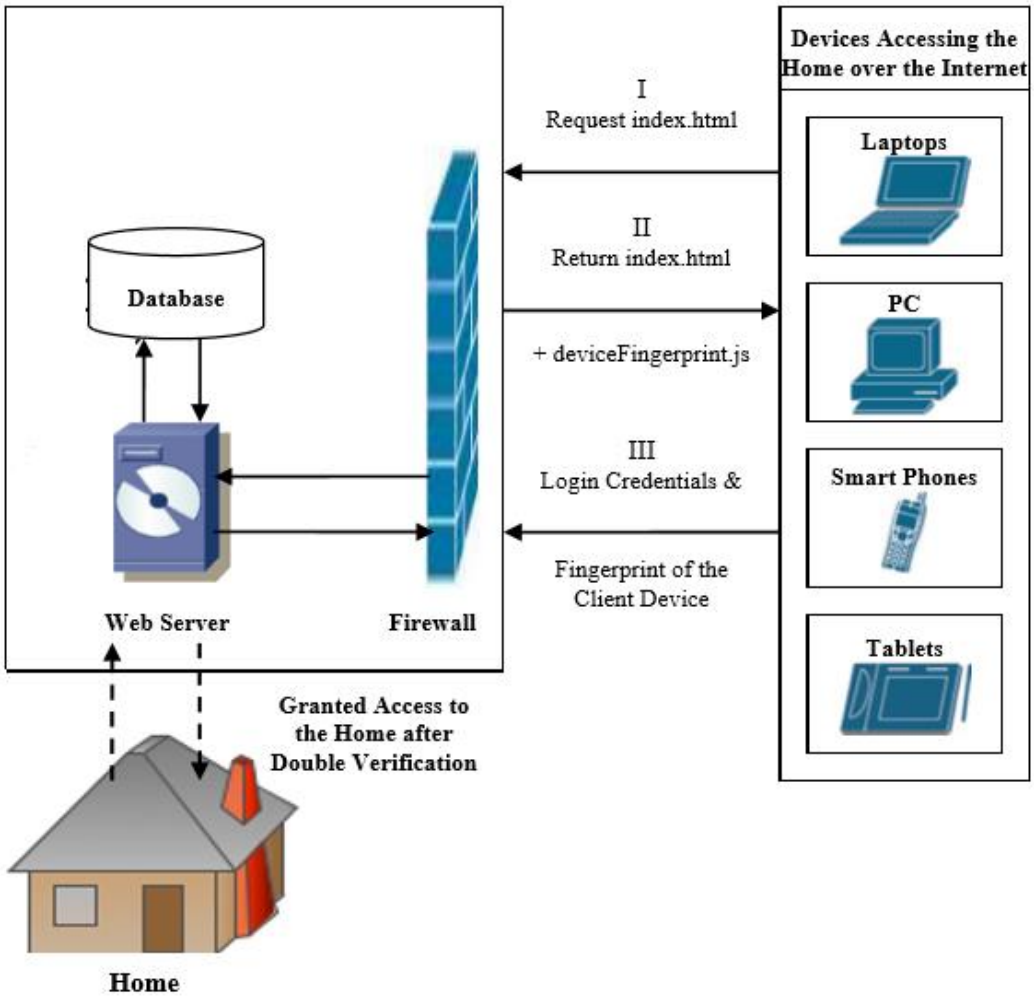


Figure 6.1: Architectural design

6.1.1 User Fingerprinting Process

User fingerprint process is the very first verification process in our implementation. There are various fingerprint modules are available. Optical scanners are the common types of fingerprint scanners that use an LED light to illuminate the finger. The sensor detects and creates the fingerprint image by determining the light and dark areas created by the fingerprint ridges. The scanning process starts when the individual

places his finger on the glass plate that is known as a touch surface. In our implementation fingerprint module is placed at the door for verification of user.

6.1.2 Device Fingerprinting Process

The Fig4.1 shows the Device Fingerprinting process in the proposed system. When a user wishes to access the home over the internet, he requests the login page from the server, the server then returns the login page along with the fingerprint java script. The user provides the user fingerprints along with the fingerprint of the device he is using. The user fingerprints are verified, if the verification is passed, then the gathered device fingerprint is analyzed to see if there are enough device fingerprinting parameters available to provide a comprehensive fingerprint of the user device.

6.2 DATA FLOW DIAGRAM

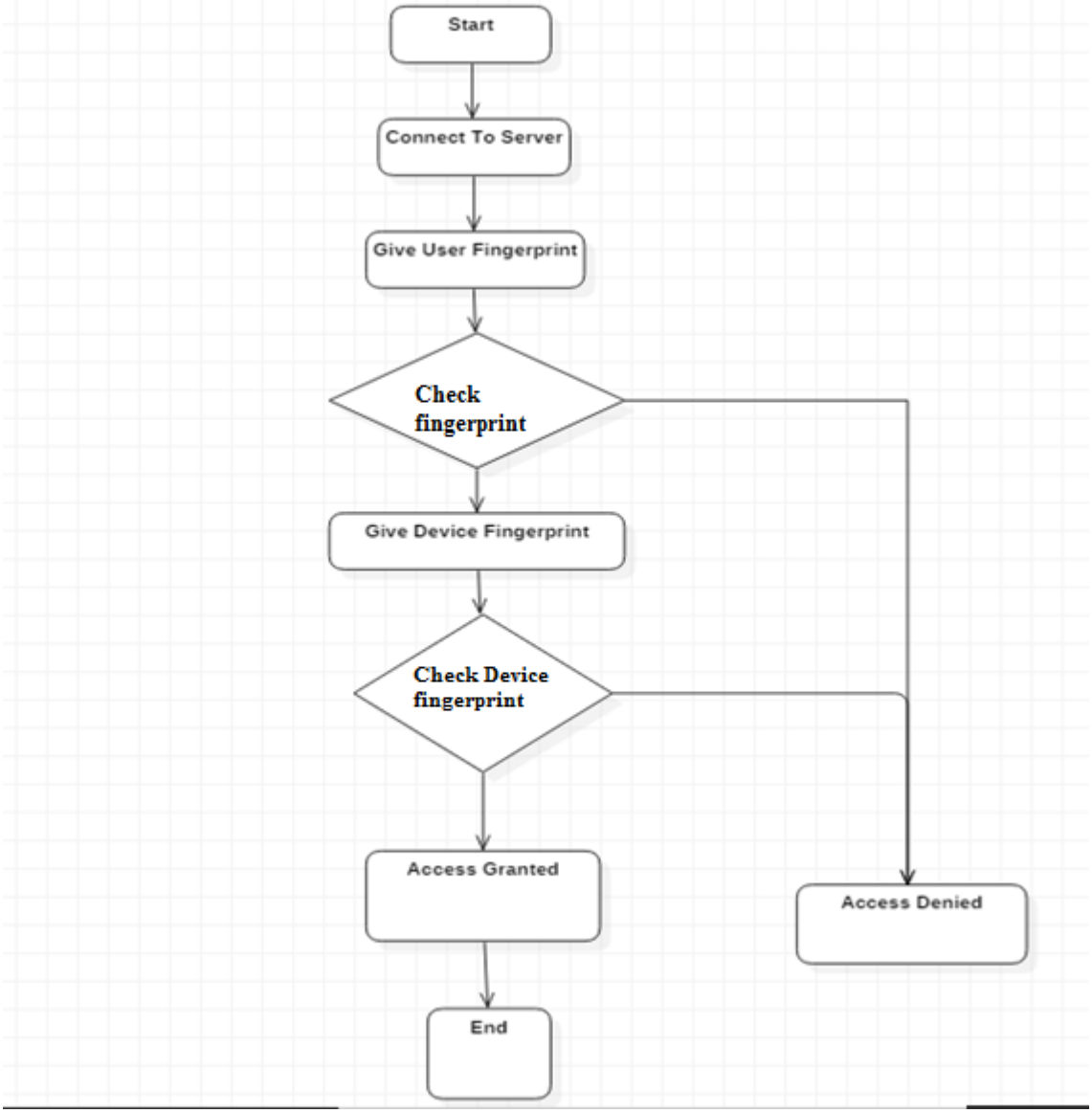


Figure 6.2: Design Workflow

6.3 POWER SUPPLY DESIGN

The basic step in the designing of any system is to design the power supply required for that system. The steps involved in the designing of the power supply are as follows:

1) Determine the total current that the system sinks from the supply.

2) Determine the voltage rating required for the different components.

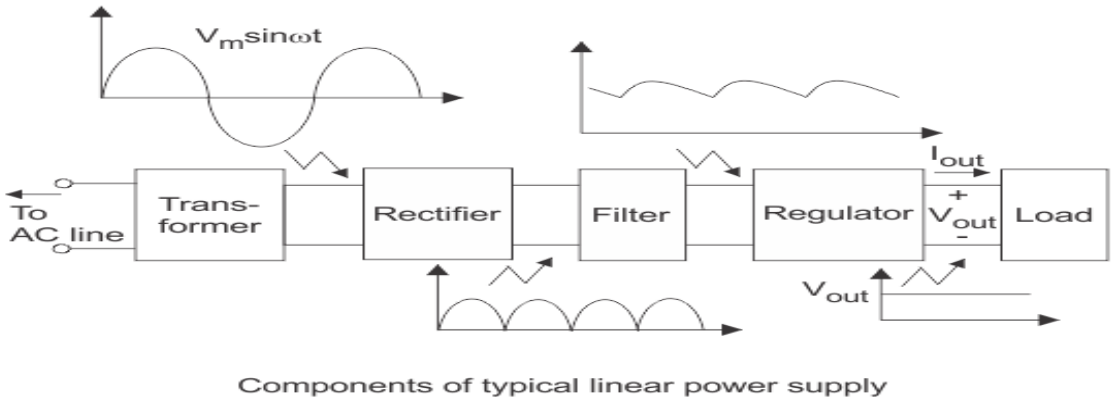


Figure 6.3: Power Supply Design

Power supply unit consists of the following units:

a) Step down transformer
b) Rectifier unit
c) Input filter
d) Regulator unit
e) Output filter

Step Down Transformer

The instrument transformer for power supply in this project is to convert AC from 230V to required low level such as 5V AC. This transformer apart from stepping down AC voltage gives isolation between power source and power supply circuitries.

Rectifier Unit

In a power supply unit, rectification is normally achieved by a solid state diode. Diode contains two electrodes called the anode and the cathode. A diode has the property that will let electron flow easily in one direction. As a result when AC is applied to a diode, electrons only flow when the anode is positive and cathode is negative. Reversing the polarity of voltage applied to a diode will not permit electron flow. The various method of rectifying AC to DC or half wave, full wave and bridge rectifications. This project employs a full wave bridge rectifier which is most commonly used in industries. A bridge structure of four diodes is commonly used in power supply units to achieve full wave rectification when AC voltage is applied to the primary winding of power transformer. It is stepped down to 5V AC across the secondary winding of the transformer. Normally one alteration of the input voltage will cause the polarities to reverse. Opposite end of the transformer will therefore, always be 180 degrees out of phase with each other.

Filter Unit

After pulsating DC has been produced by our rectifier, it must be filtered in or for it to be usable in a power supply. Filtering involves the ripple frequency. The power supply unit employed in this project used 7805 voltage regulator (for positive output voltages) and a 7905 regulator (for negative output voltages). Resistors R1 and R2 maintain line load regulation. The Capacitors C2 and C4 act as high frequency suppressors.

Regulator Unit

Regulator regulates the o/p voltage constant depends on upon the regulator. The 78XX series of voltage regulator are intended to provide a fixed voltage for use with a variety of different circuits. They are available in a range of different voltages as shown below and, although only the positive variety is considered here, there is a complimentary range of negative regulators that are essentially identical. The voltage regulators are capable of providing currents of up to 1.5A with adequate heat-sinking and internal protection circuitry makes them almost indestructible. In other configurations and with extra components, these regulators can be employed as variable voltage sources or constant current sources crystal, so oscillator circuits incorporating them became known as crystal oscillators, but other piezoelectric materials including polycrystalline ceramics are used in similar circuits.

CHAPTER 7

RESULT

CHAPTER 7:RESULT

The following system give a secure connection and reduction of various security issues during access. Hence two way verification - user fingerprint and device fingerprinting. compare to other biometric sensors by using optical fingerprint sensor help in better performance, easy to access, reliability with no harm. Trust built up in user as including to biometric fingerprinting device printing is used . chances of failure of the system is nearly zero. Availability of hardware leads gives good availability. By user fingerprint and device fingerprinting access is granted and motor runs with door operation. Basic requirements and overall all security issues is solve resulting in great accuracy.

CHAPTER 8

CONCLUSION

CHAPTER 8: CONCLUSION

The novel architecture for low cost and flexible home control and monitoring system using Android based Smart phone is proposed and implemented. The proposed architecture utilizes restful based Web services as an interoperable application layer for communicating between the remote user and the home devices. Any Android based Smart phone with built in support for Wi-Fi can be used to access and control the devices at home. When a Wi-Fi connection is not available, mobile cellular networks such as 3G or 4G can be used to access the system. Also high security will be provided.

CHAPTER 9

FUTURE WORK

CHAPTER 9:FUTURE WORK

Device Fingerprint can be further extend to whitelist and blacklist, where the client should be verified by some other more direct method in order to assure legitimacy. A simple and safe method would be make contact with the client using a phone call to the registered mobile number of the client and verify it is him trying to login to his home.

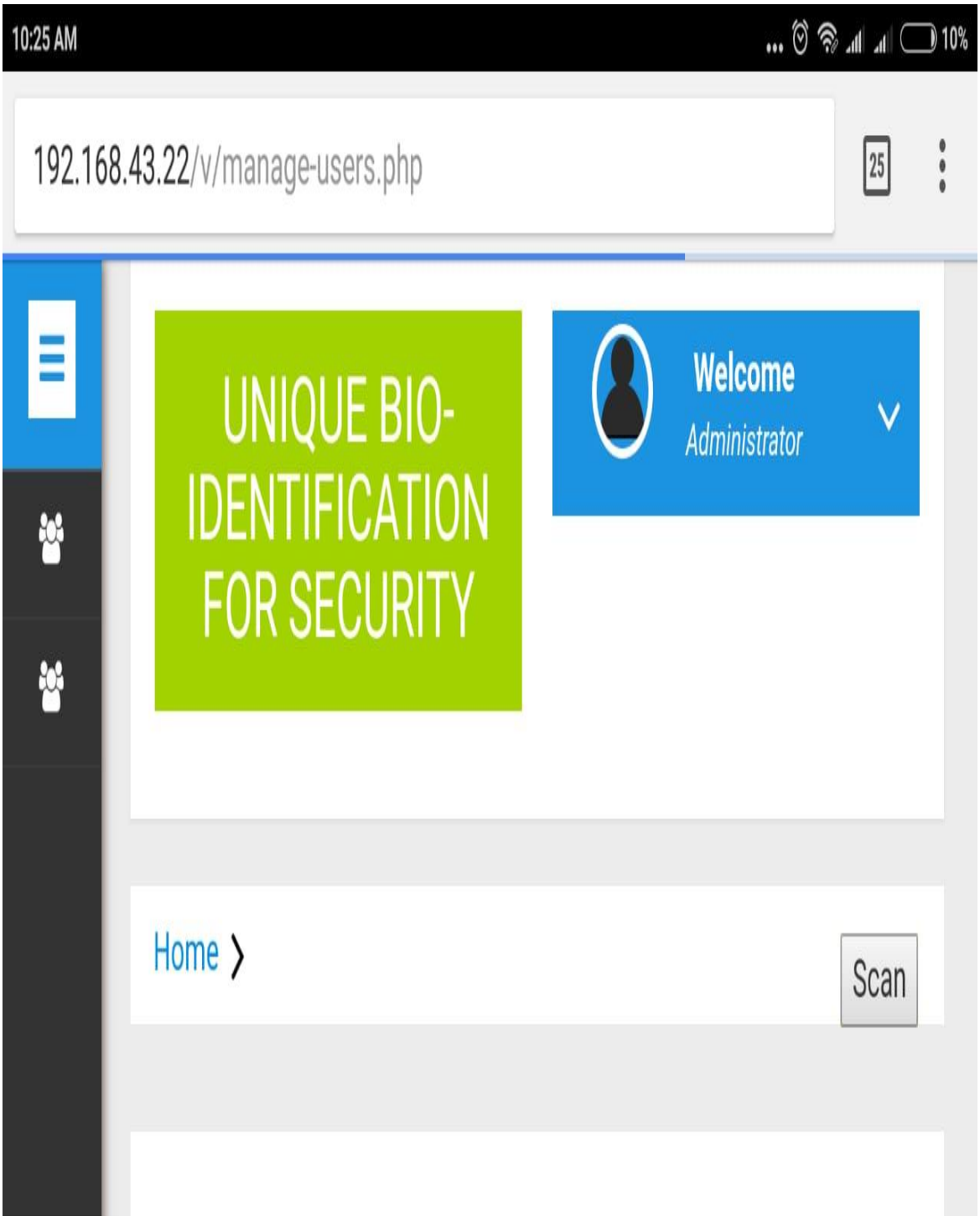
Another alternative is, the server generates a One Time Password (OTP) and sent it to the legitimate user‘s registered mobile number via Short Message Service (SMS), which the user enters in the website and thus the legitimacy of the user is verified.

Future works will focus on creating a wireless network between the home server and the home devices using WIF and implementation of voice commands for controlling the application via voice.

CHAPTER 10

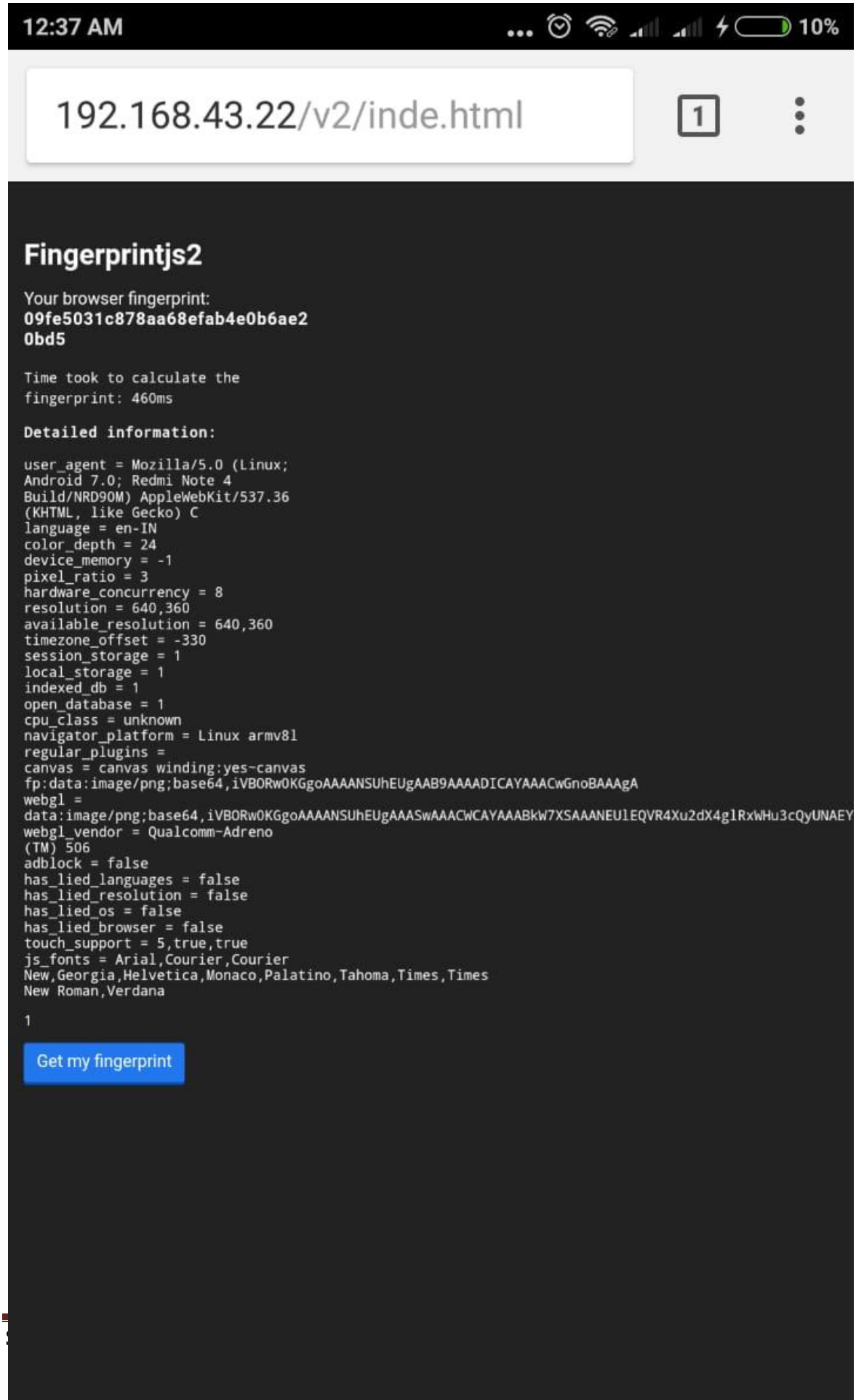
SYSTEM EXECUTION

CHAPTER 10:EXECUTION




10:46 AM
78%
192.168.43.22/v/inde.html
64
Fingerprintjs2
Your browser fingerprint:
Get my fingerprint


12:34 AM
8%
192.168.43.22/v2/manage-users6.php
2
UNIQUE BIO-IDENTIFICATION FOR SECURITY
Welcome
Administrator
Home
Enroll
Motor on
Motor off


12:37 AM
10%
192.168.43.22/v2/inde.html
1
Fingerprintjs2
Your browser fingerprint:
09fe5031c878aa68efab4e0b6ae20bd5
Time took to calculate the fingerprint: 460ms
Detailed information:
user_agent = Mozilla/5.0 (Linux; Android 7.0; Redmi Note 4 Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) C
language = en-IN
color_depth = 24
device_memory = -1
pixel_ratio = 3
hardware_concurrency = 8
resolution = 640,360
available_resolution = 640,360
timezone_offset = -330
session_storage = 1
local_storage = 1
indexed_db = 1
open_database = 1
cpu_class = unknown
navigator_platform = Linux armv8l
regular_plugins =
canvas = canvas winding:yes~canvas
fp:
webgl =

webgl_vendor = Qualcomm~Adreno
(TM) 506
adblock = false
has_lied_languages = false
has_lied_resolution = false
has_lied_os = false
has_lied_browser = false
touch_support = 5,true,true
js_fonts = Arial,Courier,Courier New,Georgia,Helvetica,Monaco,Palatino,Tahoma,Times,Times New Roman,Verdana
1
Get my fingerprint

REFERENCES

1]Arun Cyril Jose, Reza Malekian, "Improving Home Automation Security; Integrating Device Fingerprinting into Smart Home",DOI 10.1109/ACCESS.2016.2606478, IEEE Access

2]AthiraSankar, Lakshmi S, "A Survey On Improving Home Automation Security by Integrating Device Fingerprinting Into Smart Home", International Research Journal of Engineering and Technology (IRJET) ,Volume: 04 Issue: 04 | Apr -2017.

3] Murad Khan, BhagyaNathali Silva, Kijun Han"Internet of Things based Energy Aware Smart Home Control System",DOI 10.1109/ACCESS.2016.2621752, IEEE Access.

4]Jayasree Baidya, Trina Saha, Ryad Moyashir, Rajesh Palit, "Design and Implementation of a Fingerprint Based Lock System for Shared Access", North South University, Dhaka - 1229 {jayasree.baidya, trina.saha, ryad.moyashir.

5] Arun Cyril Jose1 and Reza Malekian2 "Smart Home Automation Security: A Literature Review", University of Pretoria / Private bag X20, Pretoria, South Africa- 1229 Received June 4, 2015; Revised June 2 9 , 2015; Accepted July 2 4, 2015; Published August 31, 2015.

6] https://www.raspberrypi.org/.

7] https://www.stewright.me/.