NETWORK SECURITY FOR IOT DEVICES

BY

NAJMUL AMIN

ID: 161-15-7440

MEHEDI HASAN

ID: 161-15-7454

PRITOM CHAKRABORTY

ID: 161-15-7112

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Most. Hasna Hena

Senior Lecturer

Department of CSE

Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

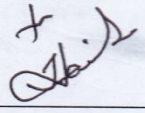
DHAKA, BANGLADESH

December 2019

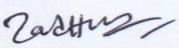
APPROVAL

This Project/internship titled **"Network security for IOT Devices"** submitted by Najmul Amin, Mehedi Hasan, Pritom Chakraborty. ID No: 161-15-7440,161-15-7454 161-15-7112, to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 07-12-2019.

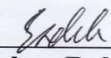
BOARD OF EXAMINERS



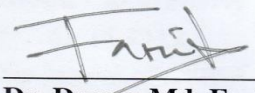
Dr. Syed Akhter Hossain — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Md. Zahid Hasan — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Sadekur Rahman — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Dewan Md. Farid — **External Examiner**
Associate Professor
Department of Computer Science and Engineering
United International University

DECLARATION

We hereby declare that this project has been done by us under the supervision of Most. **Hasna Hena,** Lecturer, Department of CSE, and Daffodil International University in Partial of the requirements for the Degree of Bachelor of Computer Science. We also declare that neither this project report nor any part of this project report has been submitted elsewhere of any Degree or Diploma.

Supervised by:

Most. Hasna Hena
Lecturer
Department of CSE
Daffodil International University

Submitted by:

Najmul Amin

Najmul Amin
ID: 161-15-7440
Department of CSE
Daffodil International University

Mehedi Hasan

Mehedi Hasan
ID: 161-15-7454
Department of CSE
Daffodil International University

Pritom Chakraborty.

Pritom Chakraborty
ID: 161-15-7112
Department of CSE
Daffodil International University

I

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to almighty God for his divine blessing makes us possible to complete the final year project successfully.

We have been taken efforts in this project. However, it would not have been possible without the kind support and help of many individuals. We would like to extend our sincere thanks to all of them. We really grateful and wish our profound our indebtedness to **Ms. Most. Hasna Hena**, Lecturer, Department of CSE, Daffodil International University, Dhaka. Deep Knowledge & keen interest in our supervisor field in the "**Network Security for IOT Devices**" to carry out this project. His endless patience, continual encouragement scholarly guidance, constant and energetics supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them at all stages have made it possible to complete this project.

We would like to express our heartiest gratitude to **Dr. Syed Akhter Hossain** Head, Department of CSE, for his kind help to finish our project and we would also like to admit with much appreciation the crucial role of the staff of Daffodil International University (DIU), who gave me permission to access all kinds of library materials and equipment to gain knowledge and to clear out our understandings. We have to appreciate the guidance given by the other supervisors and lecturers who has helped us to clear our understanding and created a concern and importance of completing the project report carefully with maintaining good knowledge and quality.

Finally, we would like to express our gratitude towards our parents & our supervisor Ms. **Most. Hasna Hena** for their kind cooperation and encouragement which helped us in the completion of this project.

ABSTRACT

Network security for IOT device is very tough. A security breach can put human life at risk, because hackers can get control of real-world objects. IoT devices collect huge amount of information about us like names, ages, addresses, phone numbers and even social media accounts information that's invaluable to hackers.

This Research Project titled “Network Security for IOT Devices” which can help to secure the IOT Devices in ‘Home Automation System’. In this paper we discussed different type of security issue related to IoT devices. There are different types of attack can be done in IoT devices such as csrf, file inclusion, xss, brute force, social engineering etc. The outcomes of this project is to improve the security and the performance of IoT devices. Therefore, we proposed a methodology based on testing approach that is able to effectively facilitate interactions of different stage of IoT device testing from technical point of view. These challenges are basically related to the IoT development pipeline, security, synchronization between on real-life environment and the adaptability imperatives of cutting edge IoT testing procedures.

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES **Pages**

CHAPTER-1

INTRODUCTION

1.1 **Introduction**

The networking, communication and connectivity used with internet enabled devices largely depend on the specific IOT application. Just like there are many different IOT applications, there are many different connectivity and communication options. Internet of things are nonstandard registering gadgets that interface remotely to a system and can transmit information. Network security for IOT devices is tough and risky. A security branch can put human life at risk, because hackers can get control of the real-world objects. IOT devices collected huge amounts of information about users like name, age, address, phone number and even social media accounts information that are valuable to hackers. Notwithstanding, Hackers aren't the main danger for Internet of things, security is another significant worry for IOT gadgets clients. For instance, companies that make and distribute consumer IOT devices could use those devices to obtain and sell users personal data.

Thus, in order to catch the step of evolving “IOT devices”, it is necessary to have a basic understanding of the concept of Network security for IOT devices. Nevertheless, the idea of security for IOT devices is still quite elusive and blurry for users. So, what exactly the Network security for IOT devices is? What are the key points to build a secured network for IOT devices? What are the benefits and usage in real life and work? Are there any security issues with it and how can we solve them? Gradually, the mysteries of network security for IOT devices will be uncovered in the thesis and presented in a methodical structure.

The following chapters will focus on analyzing the essence of Network security for IOT devices, explaining the implementation of network and IOT devices, introducing the typical utilization of it, finally illustrating the primary security issues and certain methods or schemes to solve them.

1.2 Motivation: Nowadays, the word “IOT devices” is become very increasingly popular in information technology. It is very common to hear about data stolen from IoT devices that are really harmful for users.

- It is estimated that there will be up to 21 billion connected devices to the internet within 2020. With the billions of IOT devices connected to the open network. How do we ensure these devices belong into secure network? The motivation behind this project is to improve the security of these IOT devices and ensure better privacy.
- In future we want to study and work more on information and network security for IOT devices
- There are many questions that arise as to whether IOT devices is secure enough?
- Our motive is trying to find the answer of this question.

1.3 Objective:

- The objective of this project is how to secure IOT devices and what challenges we will have to consider in the future. The paper will help you to understand the components of iot devices and which components are vulnerable and how to secure them [1].
- Also, to Study some research paper about information and network security and find some lacking areas in network security for IoT devices which needed to be improved.
- We will try to analyze and solve the problem.

1.4 Expected Outcome:

In this project we are expecting that we will find the common problems of IOT devices and find a way to solve them. After this project user can understand the difference between the secure network and unsecure network and users will be able to implement a secure network by using this technique. User can understand how to implement an IOT based home automation easily and securely with low cost. User can understand the different kinds of possible threat level for IOT devices. User can control the home automation appliance with mobile or web application interface.

1.5 Report Layout:

To complete this report, we add the layout. Layout is the process of add something in a short form or in a table to show the whole process in short time. We use layout because we want to show all of my work in a short form, so that the viewer can understand it clearly.

Chapter 1: This chapter is describing the introduction, objective, motivation, expected result of this project.

Chapter 2: This chapter is about the project background and the project overview. This chapter gives information about related work, scope of the problem and project challenges.

Chapter 3: This chapter is describing the research methodology of IOT devices.

Chapter 4: This chapter is discussing about out experiment result and discussion.

Chapter 5: This chapter is about summary, conclusion, recommendations and future study of this project.

CHAPTER- 2

BACKGROUND

2.1 Introduction:

This research project focuses on studying and analyzing the network security for IOT devices, which is still a developing technology with great convenience and portability for exchanging information over the Internet via different devices. We have done a satisfactory home automation system. We completed our Bachelor of Science in Computer Science and engineering; all previous knowledge needs to build up a Secured IOT device like Home automation system. In this research project we have created four level.

2.2 Related Works:

Before working out research project, we have studied some projects which is related with network security for IOT devices.

- Self-driving cars using IOT devices: IoT based device refers to the connection of multiple devices through the internet. Driverless cars utilize this property once change their algorithms supported user knowledge. These autonomous vehicles need a colossal amount of knowledge grouping and process. during this case, through IoT, the driverless automobile shares info concerning the road which has already been mapped out. This info includes the particular path, traffic, and the way to navigate around any obstacles. User can easily control this self-driving car from anywhere. All of this knowledge is shared between IoT connected cars and is uploaded wirelessly to a cloud system to be analyzed and place to use rising the automation [2].

- Virtual Assistant using IOT devices: There is a huge amount of user's interaction in their modern life appliance through Virtual assistant. Day by day increasing the number of ratios exponentially. User basically using Virtual assistant speech recognition landscape, the voice-activated home speakers like- Google Home, Amazon Echo, Apple Home Pod. Even large amount of the user interactions on the smartphones are occur through virtual personal assistants.

- Home automation System using IOT devices: Exponentially increasing the ratio of using IOT based home automation system. Users are more concerned about their security purpose. Using IOT devices in home automation system help to user efficiently control their house appliance. User can control securely this whole system without present their house.
- Healthcare care system using IOT devices: Now a days the healthcare system is in a very disappointment stage. IOT based healthcare system can change the whole system. With period of time observation, the condition of a patient in place by means of a sensible medical device connected to a smartphone app, connected devices will collect medical and alternative needed health data and use the information affiliation of the smartphone to transfer collected information to a medical Assistant. IoT will automatize patient care advancement with the assistance attention quality answer and alternative new technologies, and next-gen attention facilities. IoT in attention allows ability, machine-to-machine communication, data exchange, and information movement that creates attention service delivery effective.

2.3 Research Summary:

IOT devices are most usable devices in this current world. when are thinking about security related work, we want to make a secured home automation system? Which helps users easily maintain home automation system within secured network. So, we study some IOT devices related research paper and find some security issues that is harmful for users. We find out smart and secured home Automation System that is controlled by smartphone in case users no need to present at home.

2.4 Scope of problem:

IOT devices are increasing exponentially. By 2025 there will be 50 billion IOT devices. User may face lots of security problems by using unsecured IOT devices. Hacker or third-party can access into the unsecured system get a lot of data which is valuable to the hacker [3].

2.5 Challenges:

In Our modern life, security is the most challenging thing for IOT devices. At this time security threats are one of the most serious issues in modern life. Users use Normal security system in home automation system. Using normal home automation system users have risk getting cyber attacked by hackers. So, we try to solve some home automation system problems and make a project that is easy to use in home automation system [4].

When we try to solve, we have faced some challenges on our research project, they are given below.

- Insufficient Testing and updating
- Brute force against the default password
- Data security and privacy concerns
- Poor Encryption
- Phishing Attacks
- Small Scale attacks in IOT
- Untrusted communication

CHAPTER-3

RESEARCH METHODOLOGY

3.1 Introduction:

At this time, IOT is a new revolution of the internet. We also know that in this time, it is not possible to have a totally better secure network but it is possible and control to that, by means of periodic evaluations, appropriate methodologies establishing risks the better security levels. The Internet of Things is based on a global network structure and self-configuring nodes (things) interconnected in a dynamic. It represents the most pervasive computing scenario and disruptive technologies, enabling ubiquitous is generally characterized by issues regarding reliability, performance, security and privacy.[5]

3.2 Research Subject and Instrumentation:

To make a Home automation system we use there are various kinds of requirements to complete our Research project. Some of them are given below

- Node MCU.
- Raspberry Pi
- Breadboard
- Wires and Jumpers for connecting devices
- Battery
- LCD Display
- Servo
- DC motor
- Relay channel connects equipment.
- LED bulbs
- Using Hard paper for making House and
- Different types of Sensors

3.3 Research requirement collection and Analysis:

First level: In this first level we just use a simple get request. Most of the IOT devices people don't usually any kind of encryption or any kind of security method to prevent the hacker. We use a NodeMcu and create a server in NodeMcu.

When the NodeMcu starts an IP, address is automatically assigned to it. We use get request to function our home automation components.

Example: http://site.com/led=on

So, when we send a get request to the server it turns the led on or off.

This is the basic level. So, Hacker can just send the get request he can manipulate the devices.

Second level: In this level we used a login from to prevent the hacker to get access directly to the admin panel. if hackers want to access the admin panel, he has to login first.

In second level we did not use any encryption to encrypt the password. So, if the hackers are in the same network, he can trace the packet with packet tracer software like (Wireshark) and trace the data. then he can easily get the username and password. After login into the system Users send a get request. Every request sends a get request to control the home automation components. Hackers can access the user name and user password because of in this level password is not encrypted. So, hackers can easily access into the system and hacked the home automation system.

Third level: At this level we also use login form to login into the system. When user's login into the system it creates a session, without login into the system user can't access into the system. This level is similar to level two. But at this level we used encryption method to hide the password from hackers. If hackers and users are belonging under the same network hacker can traces users name and user encrypted password. After getting username and user password hacker can't access into the system. But using packet replying tool the same request hacker can gain access into the system and hacked the home automation system.

Fourth level: At this level We also use login form to login into the system. To hide the password, we also use encrypted password method. We used Raspberry pi in this level to

prevent level one, level two and level three hacking process. There are three methods that ensure IOT security of our home automation system. Some of them are given below:

- Cross-Site Request Forgery [Random token generator]
- Time-stamp on all request
- One-time password for each transaction

In level 4 to prevent the replying attack we use Cross-Site Request Forgery (CSRF) to generate a random token.

So, every time it generates a random token and even if the hacker gets the access, hacker can't login because the token expires every time the user logged in.

3.4 Block Diagram and Description:

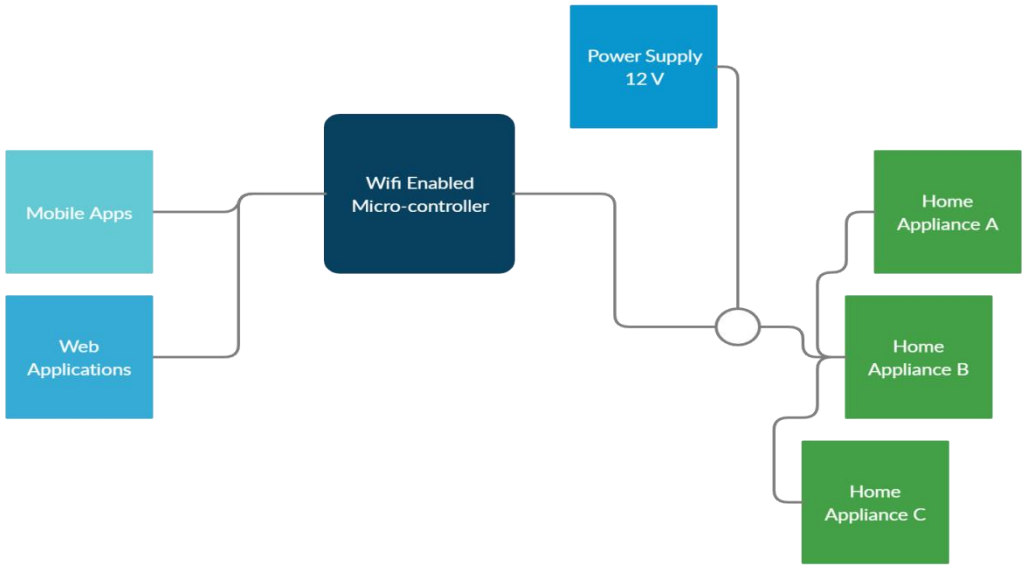


Fig 3.4.1 Block Diagram

Description:

In our project we used NodeMcu and Raspberry Pi as a microcontroller device. As both microcontrollers is connected through the internet so we can access this with mobile application and web application. For every home appliance we use 12v power supply to make them Powered. We can control the appliance by sending a post request or a get request based on the level of security.

As we have four levels of security system so we used for types of software implementation for this system.

For the first three levels we use NodeMcu and for the fourth level we used Raspberry Pi.

It's hard to use strong software implementation in NodeMcu so to implement better and secure system we used Raspberry Pi in our fourth level.

User can add more home appliances in this system like add extra led or fan or automated door lock etc.

3.5 Implementation Requirements:

To design a secured IOT devices home automation system, we use various kinds of elements.

3.5.1 NodeMcu ESP8266:

The internet of things has been trending field in the world are connected now more than ever. NodeMCU8266 is Wi-Fi enabled microcontroller. It can monitor and control things from anywhere in the world. Perfect for just about any IOT projects. The ESP8266 NodeMcu has a total of 17 GPIO pins broken out to the pin headers on the both sides of the board. These pins can be assigned to all sorts of peripheral duties, including

- ADC channel - A 10 bi ADC channel.
- UART interface - UART interface is used to load code seriously.
- PWM outputs - PWM pins for dimming LEDs or controlling motors.
- SPI,12c and 12S interface- SPI and 12C interface to hook up all sorts sensors and
- peripherals.
- 12S interfaces _ 12S interface help to add sound on projects.

The ESP8266 NodeMCU has total 30 pins that interface it to the outside. The connection are as follows:

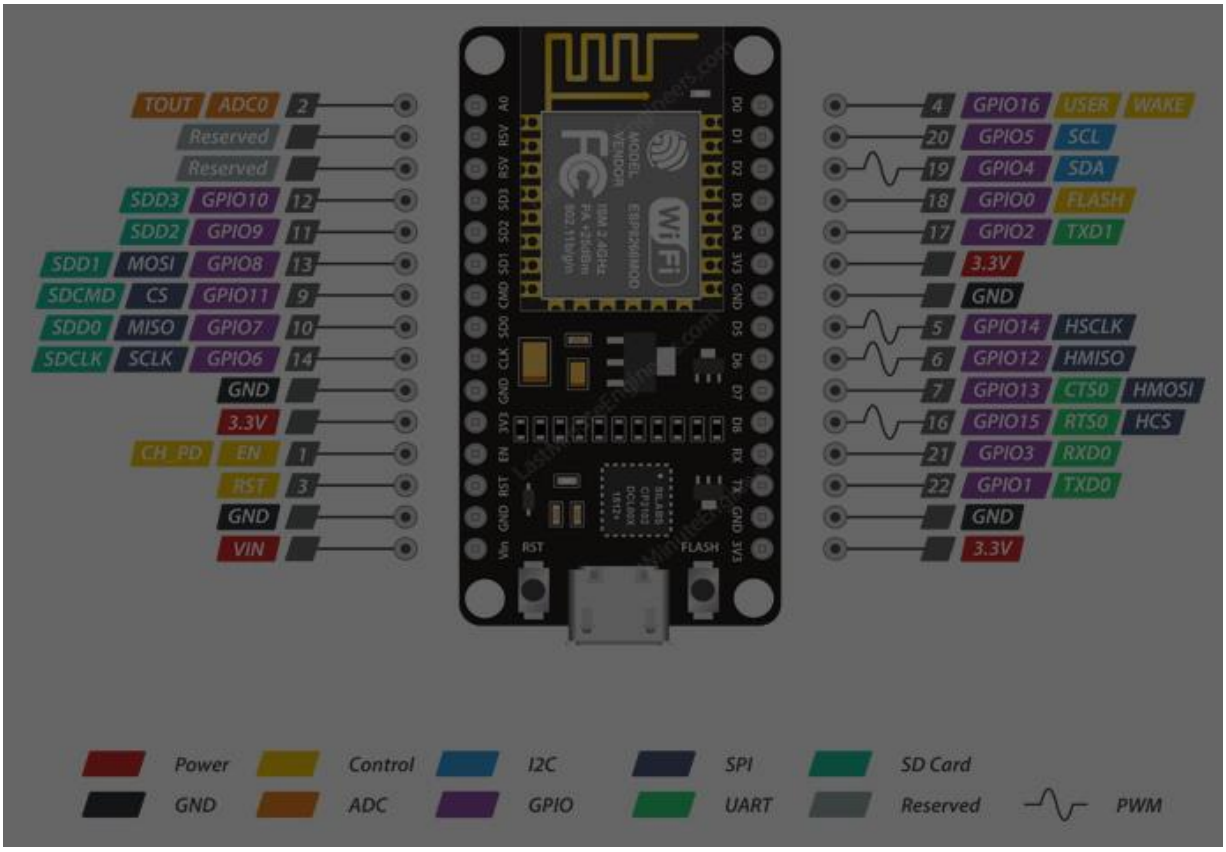


Fig 3.5.1: NodeMcu ESP8266

3.5.2 Raspberry Pi:

Raspberry Pi is the name of single-board computers. The Raspberry Pi is a very cheap computer that also provides a set of general-purpose input and output pins that allow to control electronic components for physical computing and explore the internet of things.

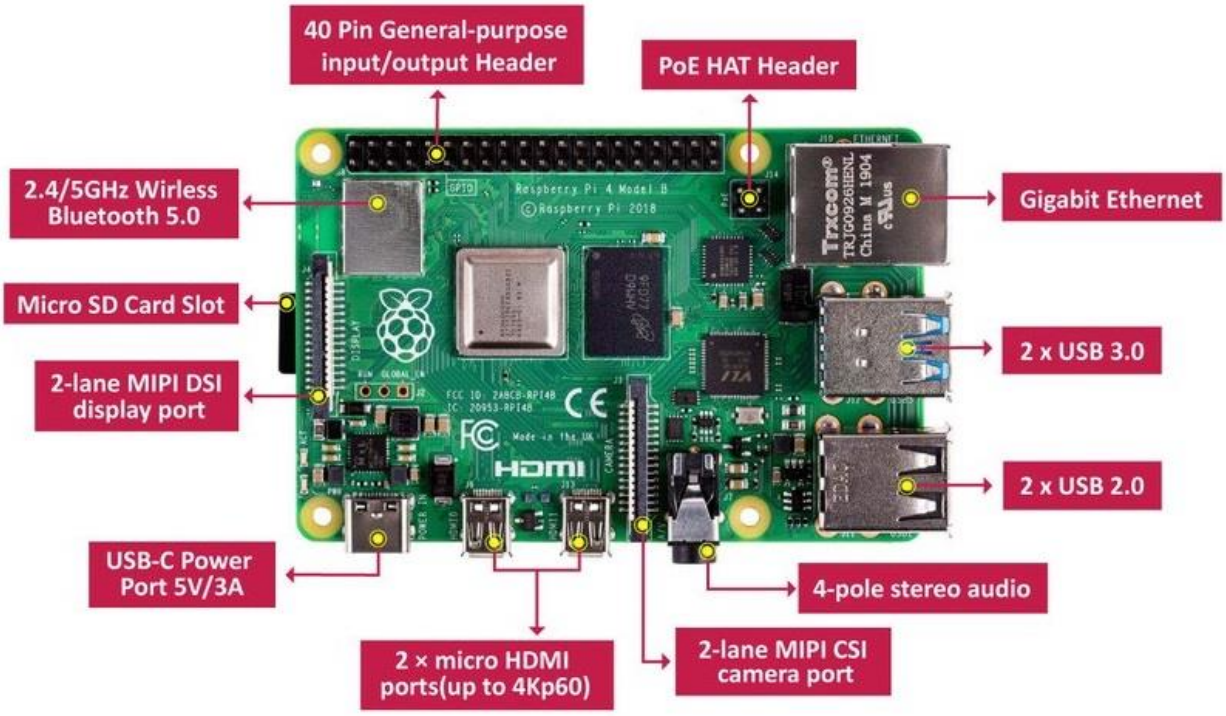


Fig 3.5.2 Raspberry Pi

3.5.3 Breadboards Connection:

Breadboards are the most fundamental and useful pieces when we use to build a new circuit. It is fast and easy when we use it is easy to prototype circuit with the help of breadboard is generally used to test circuit. A Breadboard is mentioned as it is used for temporary circuit for testing. A Breadboard consist of lots of holes where wires can easily be pushed in. It has many sockets in a 0.1 grid where holes are arranged in. The ICs are dot on the left where pushed inside across the gap. In the Breadboard, standard wires cannot be used as they get damages easily. Here is a diagram which shows how the holes of a breadboard are connected. The Top rows and the top bottom are connected horizontally as the black and the red denotes. The other rows are connected in a vertical manner which consist of five rows without the center of across any link.

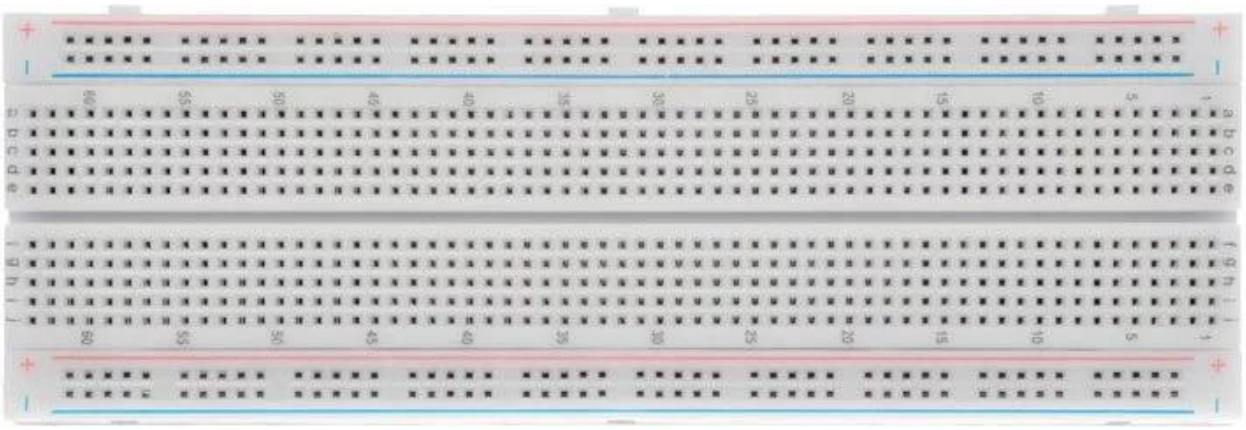


Fig 3.5.3 Breadboards

3.5.4 Wires and Jumpers:

Wires and Jumpers are simply wiring that have connector pins at each end, allowing to be used to connect two points to each other's without soldering.

Fig 3.5.4 Wires and Jumpers

3.5.5 Batteries:

The battery is an electrical device that storage energy and supplied to the system when it needed.

Fig 3.5.5 Batteries

3.5.6 LED:

An LED light is an electric light for use in light fixtures that produces light using one or more light-emitting diodes. LED light have a lifespan many times longer than other lights.

Fig 3.5.6 LED Lights

3.5.7 Servo:

A servomotor is a rotary actuator that allows for precise of angular or linear position, velocity and acceleration. It consists of a suitable motor coupled to a sensor for position feedback. It also requires a relatively sophisticated controller.

Fig 3.5.7 Servo

3.5.8 DC Motor:

A DC motor is any pf a class of rotary electrical machines that converts direct current electrical energy into mechanical energy

Fig 3.5.8 DC Motor

3.5.9 Relay:

A relay is an electrical Switch. It is utilized applications to turn on and a circuit by a low power flag or where a few circuits must be controlled by one flag.

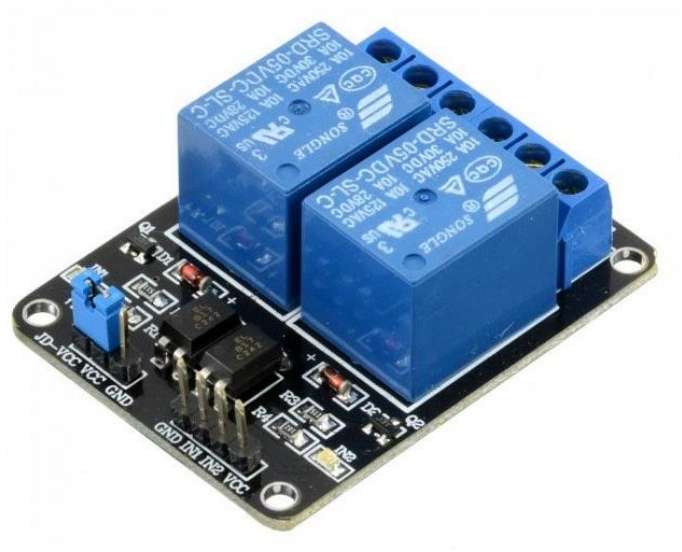


Fig 3.5.9 Relay

3.5.10 LCD Display:

LCD is a liquid crystal display to produce a visible image. For displaying input and output LCD display is more useful and very effective features include:

- Good color reproduction
- Very thin So use to set on project
- Lightweight
- Perfect sharpness at native resolution
- Excellent longevity
- No screen burn-in effect
- Do not flicker like CRT

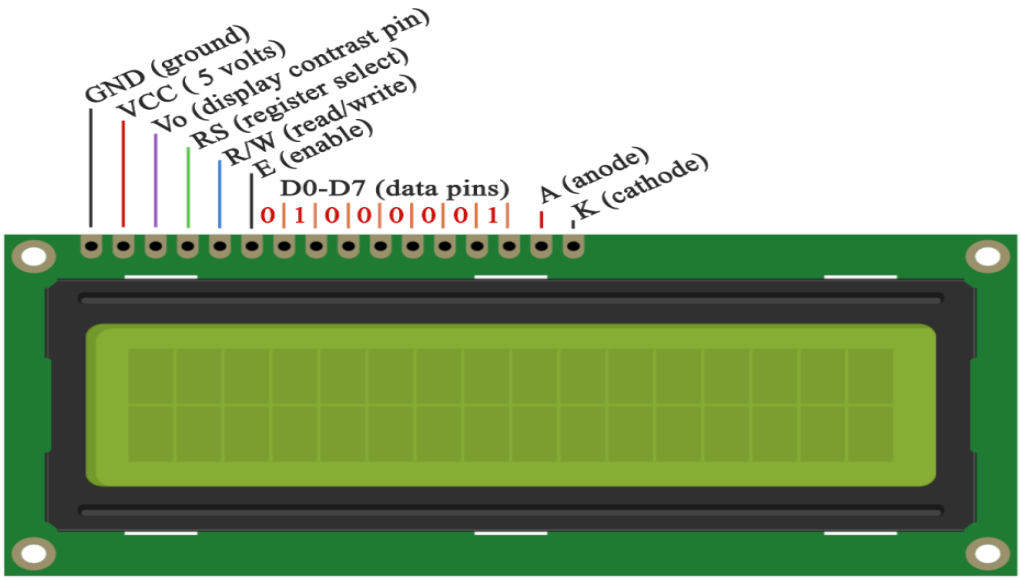


Fig 3.5.10 LCD Display

CHAPTER-4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Introduction:

Providing security for IOT devices is tough and risky. Every day new problems are appearing in IOT sectors and the authority trying to implement different protocol and layer to fix those problems. While we were working on our IOT project we faced few problems and we implemented different types of layer to solve them. We tried to analyze different types of attack that can cause the IOT devices to be hacked. example, brute force attack, social engineering attacks, DDOS attack, CSRF, different types of injection etc. we created a layer of four level of security and every next layer we solved the previous problems.[8]

4.2 Experimental Result:

We used four security Levels to determine our project output. In level 1 we used minimum number of security features. We did not used any kinds of security protection from any kinds of attack.

Fig 4.1.1 Home Automation System

In this level users can access into this system without any authentication system. Just visiting the IP address of the NodeMcu user can control the home automation components.
To scan the IP address, we can used different types of tools like Nmap, Arp-scan, Advance Ip Scanner etc.

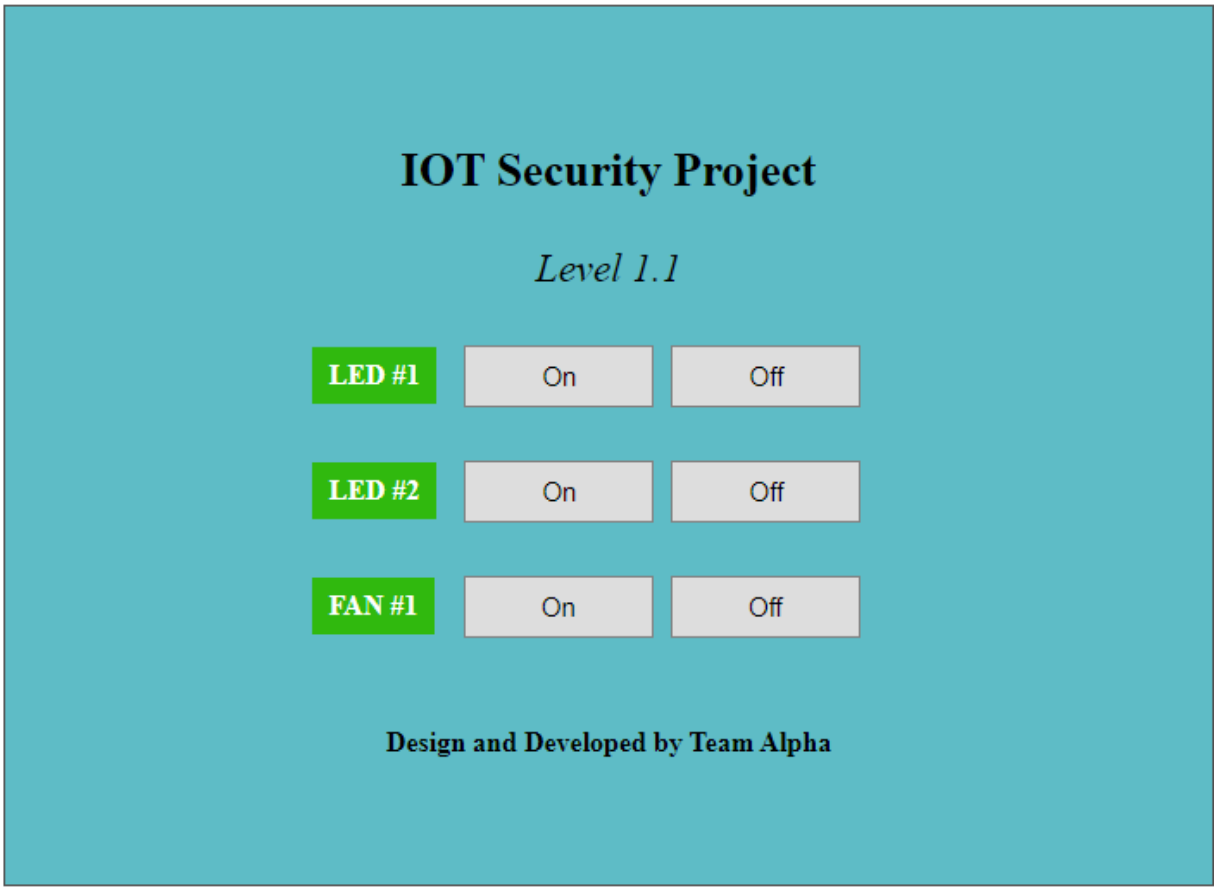


Fig 4.1.2 Level 1 Dashboard

Level 2: In level 2 we used a basic authentication system. Users have to login to access the Dashboard. But Hackers can still gain access into this system. First, we scan the IP address then we used Cisco Packet Tracer to Trace the Communication between the server and user. With this tools we can get the username and password.

Fig 4.2.1 Level 2 Login Page

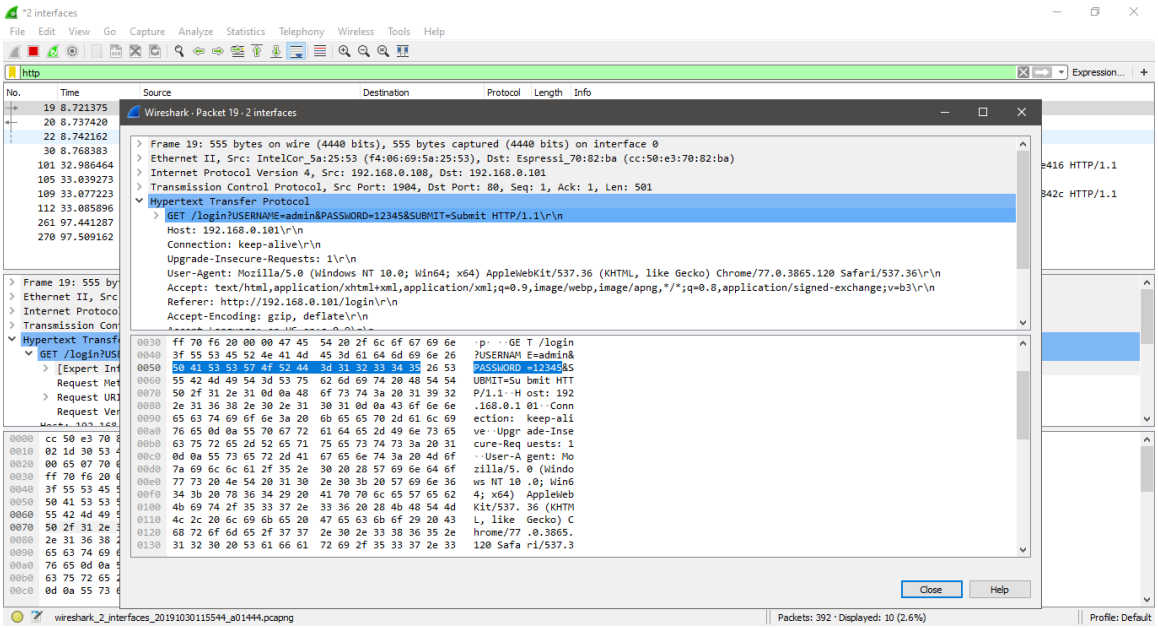


Fig 4.2.2 Level 2 Wireshark

After Login into the server user can access into the dashboard.

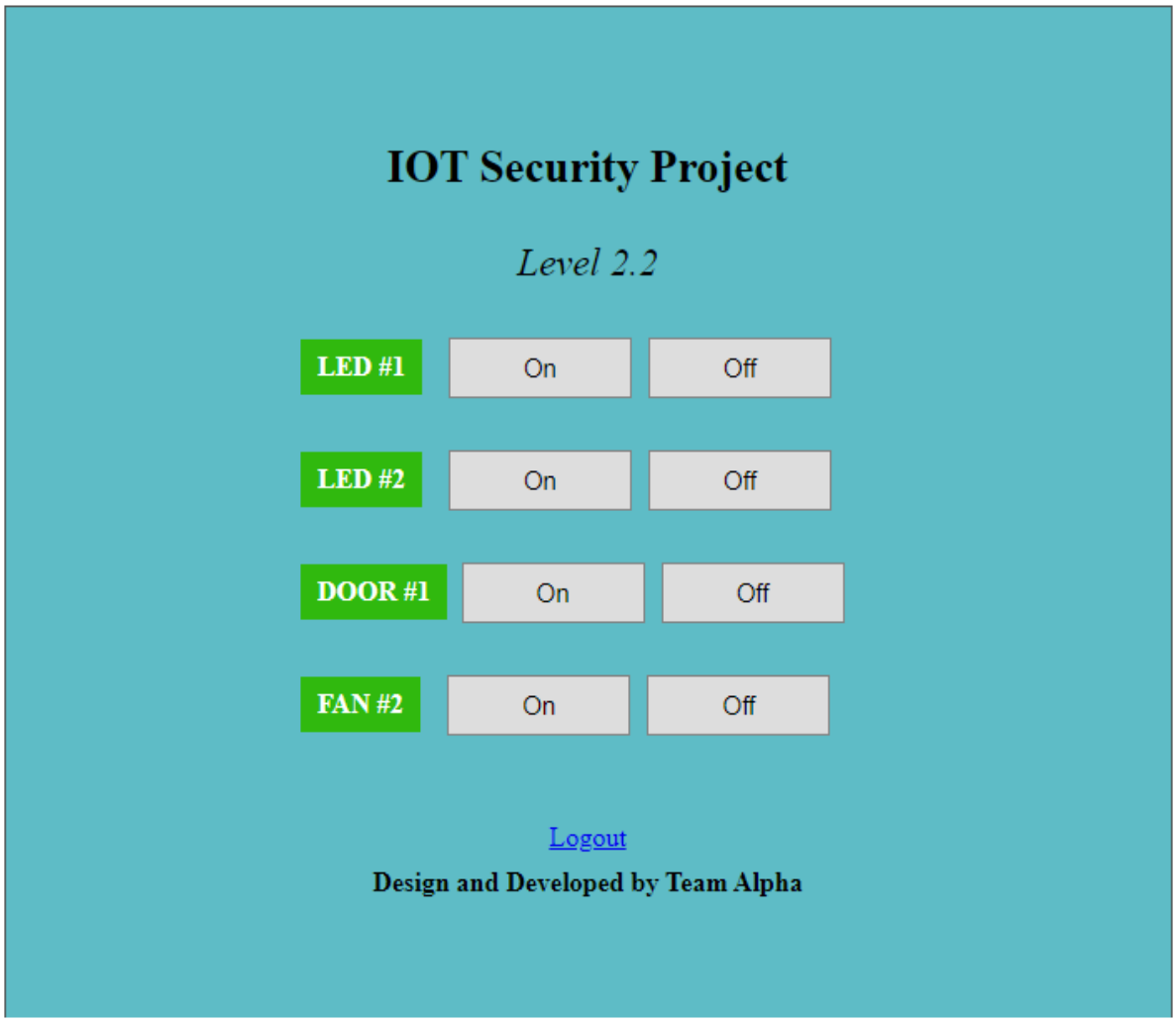


Fig 4.2.3 Level 2 Dashboard

Level 3: Level 3 and Level 2 both of them are similar but the main different between them is in Level 3 the password is encrypted. So even if the user gets the password, he can't login in to the dashboard.

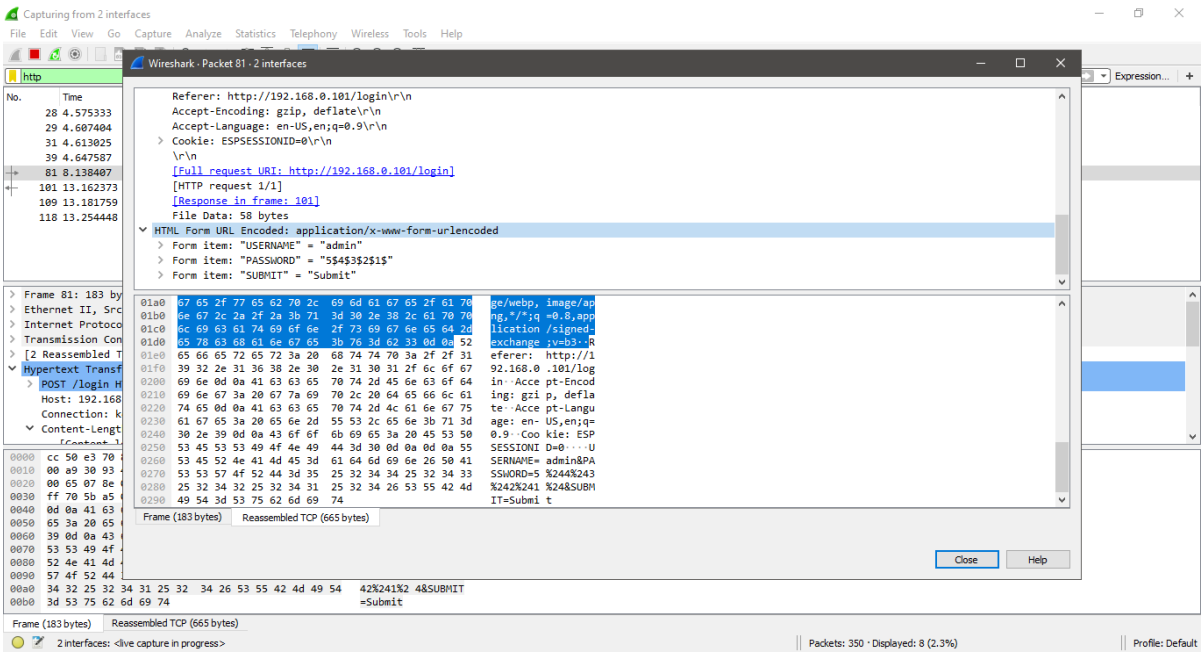


Fig 4.3.1 Encrypted Password

But we can still access the dashboard. By using Packet Replying Tools we can just reply the packet.

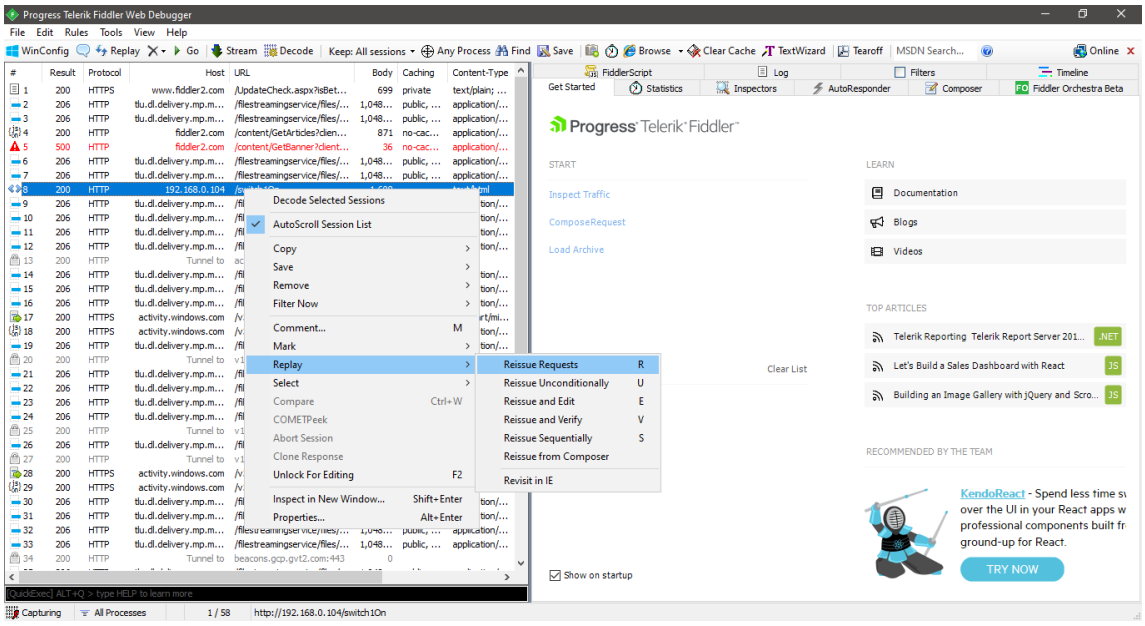


Fig 4.3.2 Packet Replying Tools

By replying the packet, we can still access the dashboard. We don't need to login or need to decrypt the password.

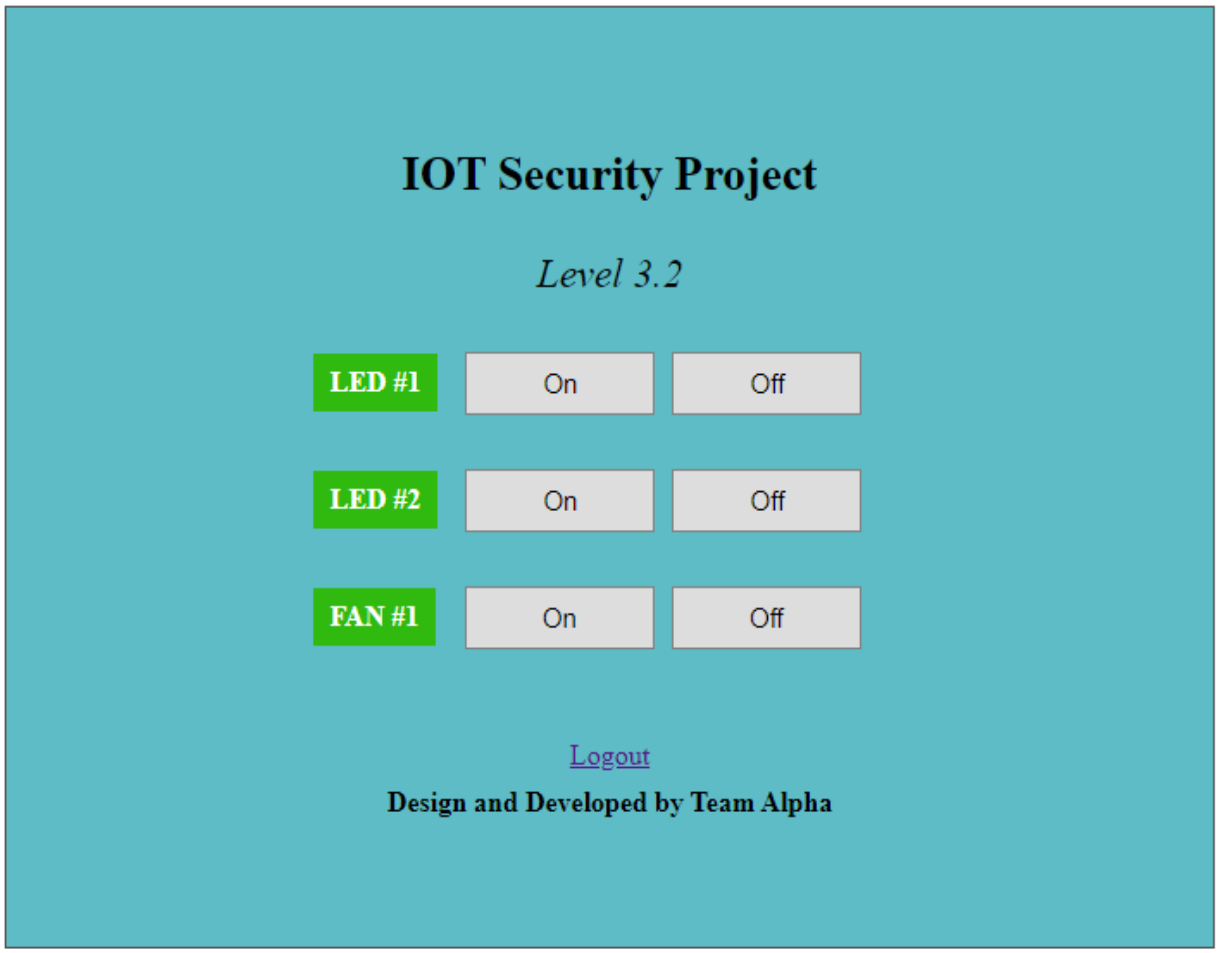


Fig 4.3.3 Level 3 Dashboard

Level 4: In Level 4, we make this system more secure. We used Raspberry Pi as our Sever and PHP as a server-side Language. This is our final version. We tried to prevent all kinds of security attacks. We used CSRF token generating method to prevent from packet replying attack. We used SSL to make the communication between the server and the user more secure.

4.3 Descriptive Analysis:

IoT sector is going to be the biggest concern for the security specialist. By 2025 there will be 50 billion IoT devices. With this number huge of devices, providing a security is going to be tough. Every year Internet Engineering Task Forces are improving the IoT structure to make it more feature able and secure. With extra features comes with new vulnerabilities. So every year the patterns of vulnerabilities are changing. There are several IoT standards and frameworks.

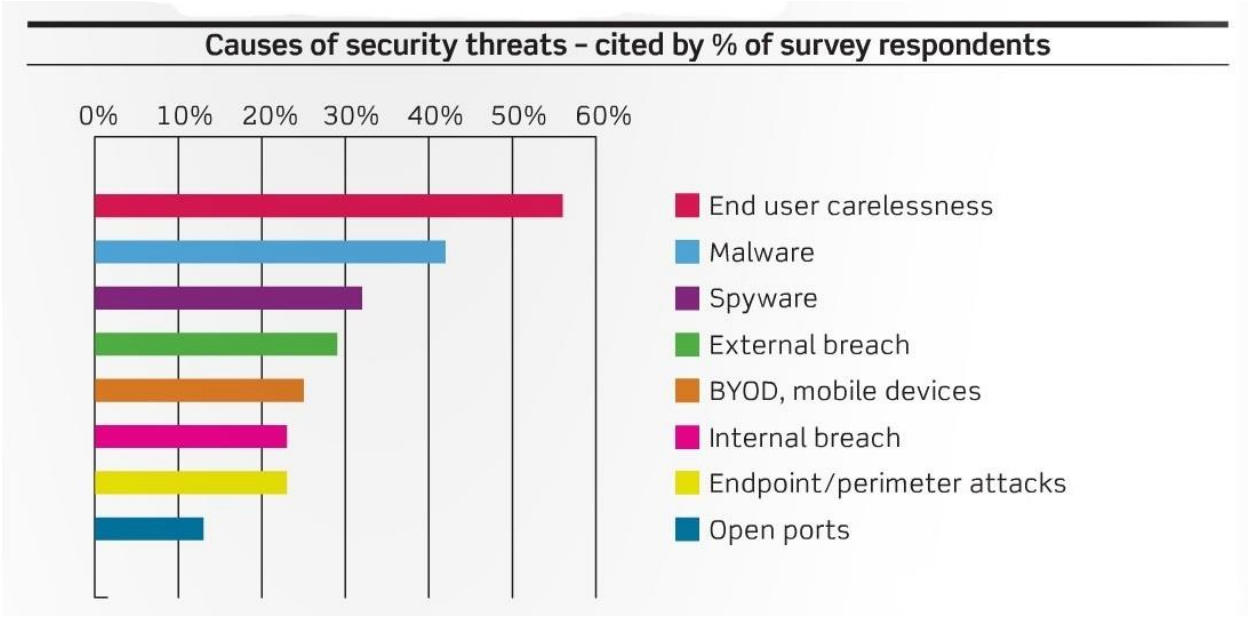


Fig 4.4.1 IoT Security Challenge

In this fig 4.3.3 we can see that almost 58% of the hacking causes due to end users carelessness. According to recent research from Kaspersky, it was known that during the first half of 2018, IoT Malware that was explicitly designed for IoT devices grew three-fold with over 1,20,000 modifications of malware. People thought that malware cannot be attacked in IoT devices. But that's turning out to be wrong.[9]

Spyware particularly become danger for IoT devices because it can run in background so it's hard to detect. With spyware hacker can track the user activity, exploit different kinds of vulnerabilities and send the data to cyber criminals.

4.4 Summary:

There are a lot of attacks can be done in IoT devices. To prevent this attacks both hardware and software must be updated. The most common Vulnerabilities are data theft, ransomware, xss, csrf, ssrf, different types of injection, file inclusion, Remote Code Execution etc. We used different authentication system to fix them.

CHAPTER-5

SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE OF THE STUDY

5.1 Summary of the Study:

We can finally conclude that there are lots of ways an IOT device can be attacked. By implementing a better combination of software and hardware we can prevent those attacks. IOT users have to be aware of the security flaws that can be harmful for the data and information

5.2 Conclusions:

This Network secured IOT based Home Automation system is made for low cost effort accessible. This secured Home Automation system is user friendly. User can control this system from anywhere. This secured IOT based Home Automation system is effectively flexible at any home or office space. This Home Automation tasted various occasions that it is effectively control. User can control this system through Mobile Application and Web Application. In Future, we will try to make it more user friendly, efficient and reliable for Users.

5.3 Recommendations:

To use a secure IOT devices user must use a secure networks, secure devices and secure operating system. User must use a strong password. Every request must be sent over using SSL protocol and must use a strong authentication system for accessing dashboard. User can also use a two-factor authentication system which will provide an extra layer of security.

5.4 Implication for Further Study:

We have tried to solve some network security issues for IOT Devices. These security issues we can implement more efficiently in future. We can add new features in this application such as SSL/TLS.TLS or SSL is a secure protocol that provides data security over internet.

Now it becames an standards for websites. TLS was proposed by the Internet Engineering Task Force (IETF) and published in 1999. The recent version is published in 2018 [7].

Firebase is a mobile and desktop application development platform. It provides a secure network communication system. It provides real time database, firebase storage, firebase hosting, firebase auth, machine learning kits etc.

Two factor authentication system is the best and easy way to make your application more secure. It is a method of confirming users' claimed identities by using a combination of two different factors.it can be confirmed by message authentication or by email authentication.

The graphical interface is a form of interface that allows user to interact with the devices or programs. we could make our applications interface looks better and easier to use.

Powerful Encryption is a way to make our application more secure. We could use stronger algorithm to make our application more secure [6].

REFERENCES

[1] Objectives of IoT based project available at,<<https://link.springer.com/article/10.1007/s11390-011-1189-5>>, last accessed on October 30, 2019.

[2] Related Works for IoT available at <<https://www.skyfilabs.com/blog/best-internet-of-things-iot-final-year-project-ideas-for-engineering-students>>, last accessed on October 30, 2019.

[3] Problem and Scope of IoT projects available at <<https://www.cmswire.com/cms/internet-of-things/7-bigproblems-with-the-internet-of-things-024571.php>> last accessed on October 30, 2019.

[4] Challenges of IoT available at << http://techgenix.com/internet-of-things-challenges>>, last accessed on October 30, 2019.

[5] Yehui Liu. Study on smart home system based on internet of things technology. In Informatics and Management Science IV, pages 73{81. Springer, 2013

[6] Miorandi, Daniele, Sabrina Sicari, Francesco De Pellegrini, and Imrich Chlamtac. "Internet of things: Vision, applications and research challenges." Adhoc networks 10, no. 7 (2012): 1497-1516

[7] Granjal, Jorge, Edmundo Monteiro, and Jorge Sá Silva. "Security for the internet of things: a survey of existing protocols and open research issues." IEEE Communications Surveys & Tutorials 17, no. 3 (2015): 1294-1312.

[8] Sicari, Sabrina, Alessandra Rizzardi, Luigi Alfredo Grieco, and Alberto Coen-Porisini. "Security, privacy and trust in Internet of Things: The road ahead." Computer networks 76 (2015): 146-164

[9] Musa G Samaila, Miguel Neto, Diogo AB Fernandes, Mario M Freire, and Pedro RM Inacio. Security challenges of the internet of things. In Beyond the Internet of Things, pages 53{82. Springer, 2017.

Turnitin Originality Report

Processed on: 30-Oct-2019 13:49 +06
ID: 1203417389
Word Count: 4060
Submitted: 1

NS_IOt By Hasna Hena

3% match (Internet from 29-Jul-2017)

Similarity Index	Similarity by Source	
22%	Internet Sources:	17%
	Publications:	1%
	Student Papers:	16%

http://publications.theseus.fi/bitstream/handle/10024/96535/Ou_Yang.pdf?sequence=1

3% match (Internet from 27-Jun-2019)
https://lastminuteengineers.com/esp8266-nodemcu-arduino-tutorial/

1% match (student papers from 11-Feb-2018)
Submitted to Daffodil International University on 2018-02-11

1% match (Internet from 23-Oct-2019)
https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

1% match (Internet from 29-Oct-2019)
https://www.peerbits.com/blog/internet-of-things-healthcare-applications-benefits-and-challenges.html

1% match (Internet from 24-May-2019)
https://dspace.iiuc.ac.bd/xmlui/bitstream/handle/88203/335/IIUC-EEE-Report-17.pdf?isAllowed=y&sequence=1

1% match (Internet from 12-Oct-2019)
https://www.iotforall.com/iot-and-autonomous-vehicles/

1% match (student papers from 08-May-2019)
Submitted to Universiti Teknikal Malaysia Melaka on 2019-05-08

1% match (Internet from 15-Mar-2019)
https://internetofthingsagenda.techtarget.com/definition/IoT-device

1% match (student papers from 23-Nov-2018)
Submitted to Auston Institute of Management and Technology on 2018-11-23

1% match (Internet from 26-Oct-2019)
http://www.dgs2.com/90950.html

1% match (student papers from 01-Sep-2019)