Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

Secure Home Automation

Hemant Saini[1], Sohan Thakur[2], Uttam Shukla[3], Shubham Mane[4] , Prof. Nilesh Korade[5]

[1,2,3,4,5]*Department Of Computer Engineering, Pimpri Chinchwad College of Engineering & Research, Ravet*

Abstract —Home Automation is becoming more and more popular day by day due to its numerous advantages like managing all of your home devices from one place, Energy efficiency, convenience and comfort. The main drawback of Home Automation is that it is vulnerable to cyber-attacks like DDOS, Mac Flooding etc. In this project we are implementing various security techniques such that putting firewall and IDS at server side and securing website/android application at client side.

Keywords- home automation, raspberry pi, security, 10WASP, DDOS Attacks

I. INTRODUCTION

With the increase in consumption of energy and population, there is a grave need to conserve energy in every way possible. The inability to access and control the appliances from remote locations is one of the major reasons for energy loss. A web or an android application is used by the users to give instructions to these systems. This system can make use of a host of communication methods such as Wi-Fi. Different controlling devices and configurations can be found in existing systems. Such systems have been found already in many places for a wide variety of applications. We are attempting to build a system to control home appliances securely via wireless medium and provide user interface like android application and websites.

II. PROBLEM STATEMENT

To implement a prototype for controlling home appliances remotely via android application and a website, which will be access by authenticate user. Also covering better security measures for user with respect to all perspective as compare to traditional system.

III. LITERATURE REVIEW

1. Title: - Securing Smart Home: Technologies, Security Challenges, and Security Requirements
Author: - Changmin Lee, Luca Zappaterra, Kwanghee Choiy, and Hyeong-Ah Choi
Year: - 2014

Proposed work: - In this paper the security challenges and threats to the existing solutions suited for smart homes are examined in detail with the objective of fostering the development of practical solutions to secure the smart homes.

2. Title: - Secure remote access to home automation networks
Author: - Khusvinder Gill, Shuang-Hua Yang, Wan-Liang Wang
Year: - 2012

Proposed work: - In this paper we examine the security issues raised by the anywhere and anytime accessible home environment. The existing approaches for addressing these security challenges and their weaknesses are reviewed. This study concludes with the proposal, implementation and evaluation of an improved approach for providing remote access security for the home environment.

3. Title: - Securing Fog Computing for Internet of Things Applications: Challenges and Solutions
Author: - Jianbing Ni, Kuan Zhang, Xiaodong Lin, Xuemin (Sherman) Shen
Year: - 2017

Proposed work: - In this survey, we review the architecture and features of fog computing and study critical roles of fog nodes, including real-time services, transient storage, data dissemination and decentralized computation. We also examine fog-assisted IoT applications based on different roles of fog nodes. Then, we present security and privacy threats towards IoT applications and discuss the security and privacy requirements in fog computing.

4. Title: - A Threat-Model for Building and Home Automation
Author: - Dominik Meyer, Jan Haase, Marcel Eckert, and Bernd Klauer

Year: - 2016

Proposed work: - This work presents an abstract model of a building automation system and some attack trees which simplify threat identification. Attack trees are common in secure software development and secure system deployment. An example smart home deployment is evaluated using the proposed model and attack trees to show the feasibility.

5. Title: - Web Application Security Vulnerabilities Detection Approaches: a Systematic Mapping Study
Author: - Sajjad Rafique, Mamoona Humayun, Bushra Hamid, Ansar Abbas, Muhammad Akhtar, Kamil Iqbal
Year: - 2015
Proposed work: - In this paper, we aimed at providing a description of mapping study for synthesizing the reported empirical research in the area of web applications security vulnerabilities detection approaches. The proposed solutions are mapped against: (1) the software development stages for which the solution has been proposed and (2) the web application vulnerabilities mapping according to OWASP Top 10 security vulnerabilities.

6. Title: - IoT based smart security and home automation system
Author: - Ravi Kishor Kodali, Vishal Jain, Lakshmi Boppana
Year: - 2016
Proposed work: - This IoT project focuses on building a smart wireless home security system which sends alerts to the owner by using Internet in case of any trespass and raises an alarm optionally. Besides, the same can also be utilized for home automation by making use of the same set of sensors. The leverage obtained by prefering this system over the similar kinds of existing systems is that the alerts and the status sent by the wifi connected microcontroller managed system can be received by the user on his phone from any distance irrespective of whether his mobile phone is connected to the internet

IV. SYSTEM ARCHITECTURE

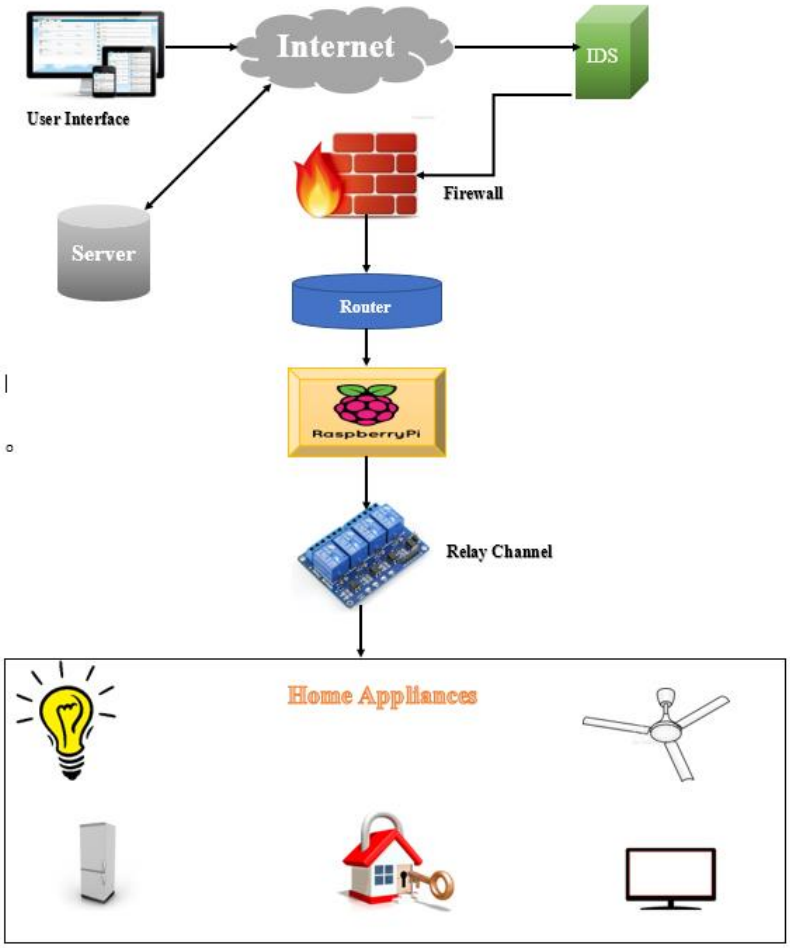
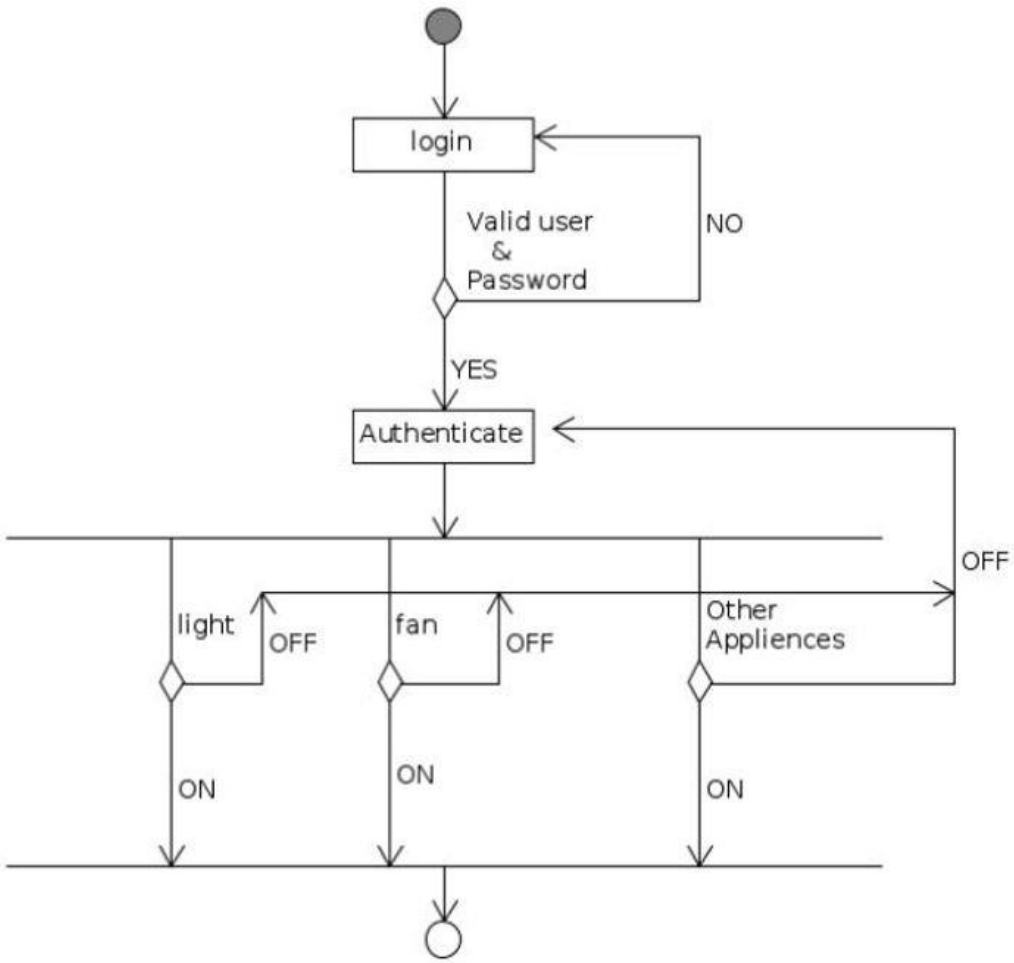


Figure 1: System Architecture

V. ARCHITECTURE EXPLANATION

After the user logs in, the server checks whether the user is authenticated or not. If yes, the control is given to the system and the user can access the various services through the Raspberry Pi. Further, the IDS and Firewall will provide additional layers of security. The power strip and relays are connected to power strip. The relays are connected to the GPIO pins of the raspberry pi. All devices are connected to a common network. Smartphone, Raspberry pi are connected to the common network router is used to create a common network.

VI. ACTIVITY DIAGRAM



VII. MODULES

- GUI
- Security
- Server

- GUI: This is the Graphical User Interface that users can interact with easily. The GUI includes – the website and the mobile app.

- Security: This includes the Intrusion Detection System and a secure Firewall. Further, the website is being tested for injection attacks based on the 10 OWASP references.

- Server: We are hosting the website on the Raspberry Pi.

VIII. CONCLUSION

Our system will assure that by implementing testing methods like 10 OWASP and Networking Monitoring tools, it is not vulnerable to cyber-attacks. The Raspberry pi acts as a server, analyses the data and activates the GPIO (General Purpose Input Output) Pins. The GPIO Pins are connected to the relays switch which activated the required home appliances. In this way, automation process is carried out.

IX. REFERENCES

[1] Changmin Lee, Luca Zappaterra, Kwanghee Choiy, and Hyeong-Ah Choi, "Securing Smart Home: Technologies, Security Challenges, and Security Requirements." tech.rep.2014.

[2] Khusvinder Gill, Shuang-Hua Yang,Wan-LiangWang, "Secure remote access to home automation networks" tech.rep.2012

[3] Jianbing Ni, Kuan Zhang, Xiaodong Lin, Xuemin (Sherman) Shen," Securing Fog Computing for Internet of Things Applications: Challenges and Solutions" tech.rep.2017

[4] Dominik Meyer, Jan Haase, Marcel Eckert, and Bernd Klauer, "A Threat- Model for Building and Home Automation" tech.rep. 2016

[5] Sajjad Rafique, Mamoona Humayun, Bushra Hamid, Ansar Abbas, Muhammad Akhtar, Kamil Iqbal, "Web Application Security Vulnerabilities Detection Approaches: a Systematic Mapping Study" tech.rep.2015

[6] Ravi Kishor Kodali, Vishal Jain, Lakshmi Boppana "IoT based smart security and home automation system" tech.rep.2016