International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-6, Issue-6)

Research Article | **June 2017**

Enhanced network security for IoT based Home Automation system

Vinay C Shekar, Sayeed Ur Rahman, SrinivasVishal Bhat DB, Abdul Mateen
Dept of Electronics and Communication Engineering,
SJBIT, Bangalore, India

Ranjitha A.S,
Assistant Professor,
SJBIT, Bangalore, India

Abstract: ***Advancement in automation technology has led to automation in many specific fields which has made life simpler and easier in all aspects. Where in the rise of Internet of Things (IoT) is taking advantage of the evolving automation technology, once such field in which the IoT is taking advantage of automation technology is Home Automation (HA).***

IoT for home automation is used in order to control home appliances such as lights, ovens, refrigerators, fans etc., In this project we present a home automation system with the help of Raspberry Pi added to which we provide enhanced network security to the home automation system with the open source tools Snort(Wireless Intrusion Detection System-IDS) and IpTables(Firewall).

Keywords—IoT, Home Automation, Raspberry Pi,Snort(IDS), IpTables(Firewall).

I. INTRODUCTION

Raspberry Pi(RPi) is a very powerful, small computer which is credit card sized. This computer uses ARM (Advanced RISC Machines) processor, the processor at the heart of the Raspberry Pi system is a Broadcom BCM2835 system on-chip (SoC) multimedia processor.

The Home Automation devices connected to Internet through the IoT are vulnerable to be controlled by an unauthorized user in layman terms it can be described that the Home Automation is vulnerable to be hacked, since the home appliances which cannot control themselves from being hacked there needs to be a method to restrict the unauthorized access.

II. EXISTINGSYSTEM

There has been a significant increase in home automation in recent years due to affordability and advancement in smart devices such as phones and tablets which allows vast connectivity. Research on IoT and implementation of home automation systems are getting more popular. Various wireless technologies are being used that can support some form of remote sensing, data transfer and control such as Wi-Fi, Bluetooth, cellular networks and RFID are embedded at various levels of intelligence in the home automation systems. There are various studies that have presented Bluetooth based home automation systems based on Android smart phones without the internet control. These devices are under physical connection to a Bluetooth controller module which is then accessed & controlled by the smart devices which have built-in Bluetooth connectivity. Due to limited Bluetooth range, operation can only be within that particular area. Radio frequency control of the home appliances through Bluetooth have some disadvantages hence it is not always feasible for the devices that are at far distance.

In order to overcome the disadvantages of Bluetooth, GSM and ZigBee based control and communication for home appliances has also been presented, where the devices are controller using the ZigBee Transceiver and it communicates with every appliance connected in the home automation system. GSM control operation is from mobile phone, where the control can be obtained by sending SMS, which is interpreted by the controller and then activates the required 'switch' to control the electrical appliance. This system also has disadvantage of connectivity, where the GSM connectivity is unavailable the system is invalid.

The above mentioned systems have made contributions significant enough to design and development IoT based home automation systems. The existing systems are mainly focused on switching and controlling electrical home appliances or connected devices rather than monitoring of home environment remotely. User friendly interface is expected from Home automation, so that the devices can be easily setup, monitored & controlled. Entire system should be swift enough to realize the true power of wireless technology and IoT. The system should also be of low cost so as to justify its use in the field of IoT based home automation.

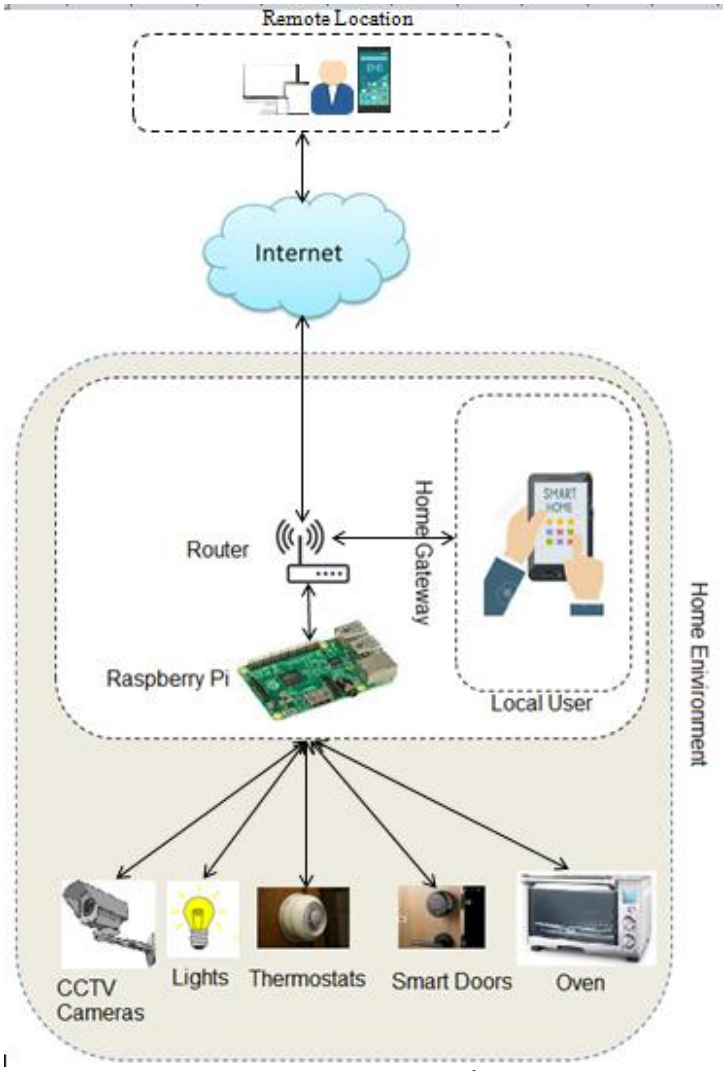

Fig 1: Existing system using Raspberry Pi

Fig 1 shows the existing system based on Raspberry Pi which uses internet in order to control the system remotely from anywhere in the world and can also be controlled within the Wi-Fi limits.
However there is a disadvantage of this system. Since this system can be controlled remotely from the internet the system is open for anyone over the internet and who can take over the access of Wi-Fi, in order to overcome these disadvantages we propose a system with enhanced security of the system from the Wi-Fi limits point of view as well as from the internet access point of view.

III. PROPOSED SYSTEM

Leveraging on the existing system of IoT based home automation using Raspberry Pi, proposed is a system which is secure both within the Wi-Fi limits as well as from the internet access perspective, in order to build a safe home automation system we implement firewall as well as intrusion detection system, Fig2 shows the block diagram of proposed safe home automation system.
Below figure shows the setup of the proposed system, where in we have leveraged on the existing system and added the firewall and the intrusion detection system, out of many variant of intrusion detection systems we have implemented the penetration based intrusion detection system which will detect any penetration towards the home automation system in the Wi-Fi limits, we have implemented the intrusion dectection system as well as the firewall in the Wi-Fi limits since the connection from the internet is secured due to the client used to connect from the internet. Similar to implementation of the intruion dectection system out of many variants of firewalls we have implemented the packet filtering firewall, which will filter the incoming traffic at the packet level.

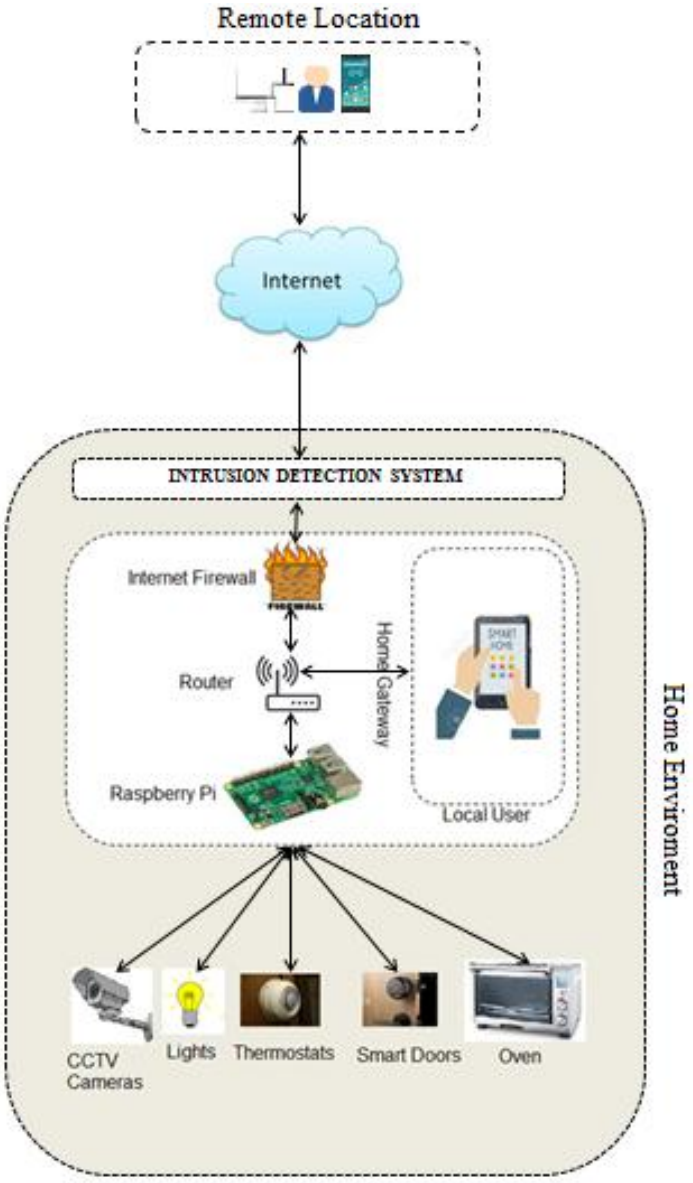

Fig 2: Safe HA system with enhanced security

IV. SETUP FOR WI-FILIMTS

The setup mainly consists of connecting all the electronic devices to Raspberry Pi's wherein the connection is from Raspberry Pi's GPIO (General Purpose Input Output) pins to relays which in turn are connected to electrical appliances. There are two possibilities of connecting the Raspberry Pi, first being connecting the Pi in headed mode which is connecting the monitor, keyboard and the mouse physically to the ports available on the board and the second method is to connect to the Pi in wireless mode also known as the headless mode. Since we are using Pi to build home automation system we opt for the headless mode where in the RPi is accessed in wireless configuration

Below are the steps followed in order to connect RPi in headless mode.

- There is an IP address assigned to the RPi from the router.
- To login into the RPi and tap into its functionalities in wireless configuration we use putty software as in Fig 3 which allows command line interfacing to the RPi, since it allows only command line interface we use a Graphical user interface (GUI) client known as VNC viewer in order to access the GUI.
- As mentioned above RPi is connected to relays which in turn are connected to the home appliances, connectivity illustration is as shown in the Fig 4, this is a prototype where in only low power devices are used to demonstrate the project and only a single bulb is used to connect to the 230V supply, we have used 4 channel relay in this prototype, we can increase the use of relay depending upon the electrical devices that are to be connected.

- In order to control the RPi with in the Wi-Fi limits we are using an open source tool kit for controlling RPi known as WebIOPi [12].
- WebIOPi can control, debug, and use your Pi's GPIO, sensors and converters from a web browser or any app WebIOPi is the perfect Swiss-knife to make connected things Developed and provided by Eric PTAK (trouch)
- Fig 5 illustrates WebIOPi's customized interface for control of devices, within the Wi-Fi limits.
- Cmd 1: sudo /etc/init.d/webiopi start
- Cmd 1 is the command to start WebIOPi service from the terminal console.

Fig 3: Putty Interface

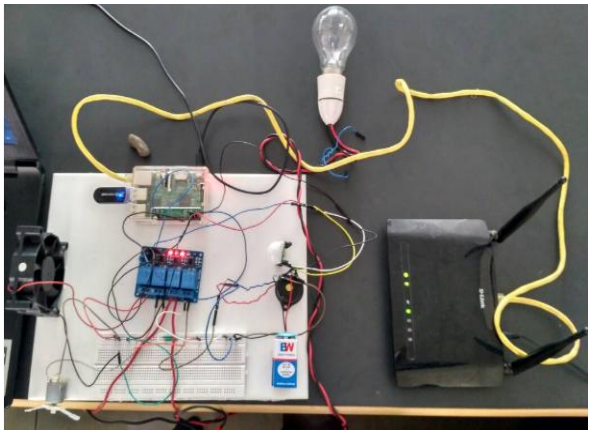

Fig 4: Prototype of the setup.

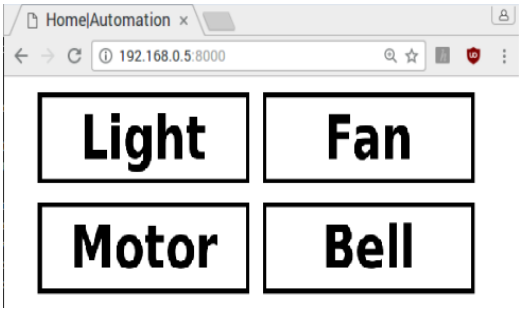

Fig 5: WebIOPi control in Wi-Fi limits

V. SETUP FOR INTERNET CONTROL

In order to connect to the HA system remotely from the internet we are using a service known as Weaved [13] now the service is changed to remot3.it[13].We setup this service while the device is connected to the internet, with the RPi connected to internet we interface the RPi to weaved's server [14].

Fig 7 shows the interface of weaved page when connected from the internet. Which gives us multiple options of controlling the RPi one such option is controlling the RPi using the WebIOPi. Here we have linked the WebIOPi and weaved to obtain the same ease of access as in the case when we are connected to the system in Wi-Fi limits.

Fig 7a shows the control of devices from the internet, when opted to connect, from the interface as shown in fig7 the program generates as unique link by entering the link in the browser we get the WebIOPi's interface same as we get for the Wi-Fi limits.

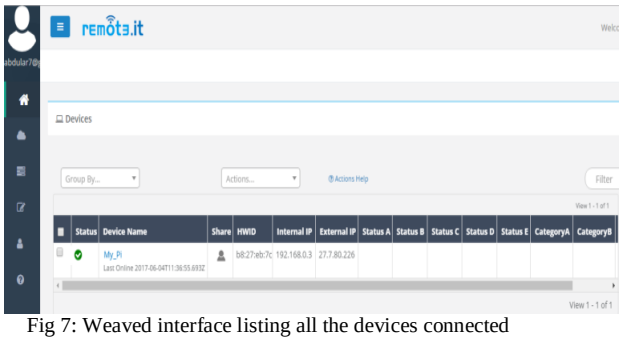

Fig 7: Weaved interface listing all the devices connected

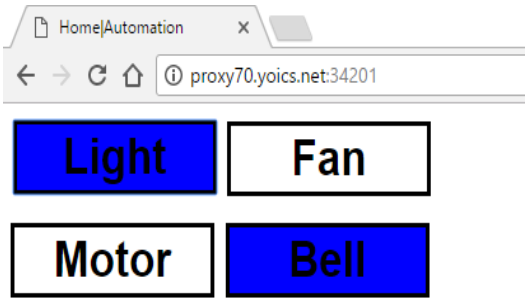

Fig 7a: Controlling the Devices from the internet

VI. SECURING HA IN WI-FI LIMITS

With the increase in home automation systems the security risks are also increasing, HA systems can be hacked and can be for many purposes such as either a zombie for DDOS attacks, monitor the activities of the persons at home etc.,
In order to overcome this security related issues we are implementing an IDS and a firewall which can monitor any illegitimate access of the home automation system using IDS as well as stop the illegitimate access.
We setup the IDS using open source application called as Snort and the firewall known as Iptables, the firewall used for stopping the unauthorized access, this firewall can be used either to block the access of the user based on its IP address or based on its MAC address since IP address can be dynamic we allow the access based on MAC address, firewall rule is created only to allow access to RPi from the predefined MAC address and request from all other devices are blocked implementing this method the request from all the users except the predefined MAC address is denied or dropped.
While the firewall is blocking the unauthorized access, IDS is implemented to detect such requests and notify the home owner about the possible attack on the home automation system, the attacks could be such as brute force attack which is an attack of trying to login to the system using different combinations of password

VII. SETTING UP FIREWALL AND IDS

The firewall and the IDS implemented are for the Wi-Fi limits.

1. Intrusion Detection System(IDS)

IDS is used in order to monitor the access, anytime there is an unauthorized activity observed the system generates an alert E-mail.
IDS used is an open source IDS named Snort, we setup the system by installing the IDS packages from the official website and define our rules, below figures show the IDS in action.

alert tcp $EXTERNAL_NET any -> $HOME_NET 22 (msg:"Incoming SSH connection!!"; flags:S; sid:10000; Priority:0;) is a rule which is written in the snort.conf file which monitors the traffic and **sudo snort -c snort.conf -i wlan0** is command to be issued in the terminal to start the snort to monitor traffic on wlan0 interface, traffic can also be monitored on Ethernet also wherein wlan0 needs to be replaced by eth0.
Once we have snort actively monitoring the traffic on port 22(which is used in headless connection), we need to watch the log files of snort where every activity will be logged, as defined in the rule every time an intrusion is detected "Priority:0" is generated and logged in the log file.
Hence in order to generate a automated email we use an open source log watcher program called as swatch, which monitors the log files and performs predefined actions(generates email in our case), as in snort we use a configuration file instead of rule.

watchfor /Priority: 0/
exec echo "There is intrusion detected at your home automation network" | mail –s "!!!!!!!Alert!!!!!!!"**@gmail.com.**
Is the action defined in the swatchrc file in order to generate an email.When the "Priority:0" event occurs the swatchrc file commands swatch program to generate an e-mail.
Swatch –config-file=/home/pi/.swatchrc –tail-file=/var/log/snort/alert
Is a command to be issued in terminal order to start watching the snort's log file.Fig8 shows example email received during the testing.

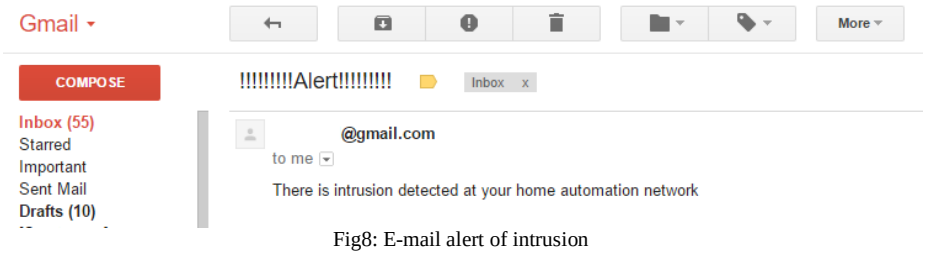

Fig8: E-mail alert of intrusion

2. Firewall

We setup penetration detection firewall in order to restrict the illegitimate access to home automation system.
We have setup a rule to allow traffic only from the MAC address E0:98:61:XX:XX:XX , request from any device other the predefined MAC addresses is blocked.
sudo iptables –A INPUT –p tcp –destination-port 22 –m mac --mac-source E0:98:61:XX:XX:XX –j ACCEPT is therulewritten in order to block all the requests from any MAC address except the MAC address E0:98:61:XX:XX:XX.
Note: All the commands mentioned "to be issued" are only for demonstration purpose in order to execute all the commands on system's startup we need to define all the commands in an startup file in the /etc directory of the operating system.

VIII.CONCLUSIONS

In this project we have leveraged on the existing raspberry pi based home automation system, where in we have improved the security aspect of the home automation system and have also narrowed down the vulnerabilities of the home automation system by adding the firewall and the intrusion detection system.
The added advantage of this project is that the firewall and the intrusion detection system used are open source, hence any user willing to leverage the presented work is free to modify the proposed system as per individual requirement.

ACKNOWLEDGEMENTS

We are extremely thankful of our guide Mrs. Ranjitha A.S who helped us doing the best in presenting the work we carried out, we are also thankful to college for providing the resources in order to test our work under various instances. Last but not the least we would like to thank International Journal of Emerging Research in Management and Technology (IJERMT) whole heartedly for giving us opportunity to publish the work carried out.

REFERENCES

[1] An Overview of Home Automation Systems Muhammad Asadullah, AhsanRaza Department of Electrical Engineering National University of Computer and Emerging Sciences Peshawar, Pakistan P136384@nu.edu.pk, P136399@nu.edu.pk

[2] Globally Accessible Machine Automation Using Raspberry Pi Based on Internet of Things V.Sandeep Department of Electronics and Communications National Institute of Technology PuducherryKaraikal, India vemulasandeep93@gmail.comK.LalithGopal, S.Naveen, A.Amudhan, L. S. Kumar Department of Electronics and Communications National Institute of Technology PuducherryKaraikal, India

[3] A Smart Home Automation Technique with Raspberry Pi using IoT Vamsikrishna Patchava1 , HariBabu Kandala2, , P Ravi Babu3 Department of ECE1 , Department ofEEE2 , Centre for Advanced Studies in Electronics Science & Technology3 RGUKT-Nuzvid1 , , MVSREC2, University of Hyderabad3 Andhra Pradesh1 , Hyderabad-Telangana2,3 vamsi.patchava@gmail.com1,kandhala.hari94@gmail.com2,perakalapudi@gmail.com3

[4] Internet of Things based Home Automation System Soumya S, MaliniChavali, Shuchi Gupta, NiharikaRao

[5] Raspberry Pi based Advanced Scheduled Home Automation System through E-mail Narender M Vijayalakshmi M Dept of ECE, Velammal Institute of Technology, Dept of ECE, Velammal Institute of Technology, Chennai, India Chennai,Indianarender.malishetty@gmail.com vijayalakshmi022@gmail.com

[6] REMOTE CONTROL OF APPLIANCES BASED ON RASPBERRY PI Dr.M.S.S.Rukmini Department of Electronics and Communication Engineering Vignan'sUniveristy, Vadlamudi, Guntur, India. mssrukmini@yahoo.co.in D.BalaGayathri Devi Department of Electronics and Communication Engineering Vignan'sUniveristy,Vadlamudi, Guntur, India. gayathridanaboina@gmail.com

[7] RPiDS: Raspberry Pi IDS A Fruitful Intrusion Detection System for IoT Alessandro Sforzin† and Mauro Conti University of Padua Via Trieste, 63, Padua, Italy alessandro.sforzin@neclab.eu, conti@math.unipd.it Felix G ´ omez M ´ armol and Jens-Matthias Bohli ´ NEC Laboratories Europe Kurfursten-Anlage, 36, Heidelberg, Germany ¨ {felix.gomez-marmol,jens-matthias.bohli}@neclab.eu

[8] The Optimization and implementation of iptables rules set on linux Lei-feiXuan Information Engineering Institue Hangzhou Vocational & Technical College Hangzhou,China4995738@qq.com Pei-fei Wu Information Engineering Institue Hangzhou Vocational & Technical College Hangzhou,Chinawupeifei8413@sina.com.cn
[9] Design and Evaluation of Wireless Home Automation Systems Manikandan J. Crucible of Research and Innovation (CORl) and Department of ECE, PES University, lOO-Feet Ring Road, BSK Stage III, Bangalore-560085, Karnataka, India E-mail: manikandanj@pes.edu
[10] Weaved Installation http://forum.weaved.com/t/how-to-get-started-with-remot3-it-for-pi/1029
[11] Configuring Email alert system in Raspbian https://www.howtoforge.com/tutorial/configure-postfix-to-use-gmail-as-a-mail-relay/
[12] http://webiopi.trouch.com/
[13] https://www.remot3.it/web/remot3-it-is-the-new-weaved.html
[14] http://forum.weaved.com/t/how-to-get-started-with-remot3-it-for-pi/1029

