International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.8, Issue.5, May 2020 E-ISSN: 2347-2693

Information Delivery in Smart Home Automation Through Security Technique

Suraj Rasal[1*], Srijan[2], Vaibhav Kundu[3], Linika Labdhi [4]

[1,2,3,4]Dept. of Computer Engineering, Bharati Vidyapeeth (Deemed to be) University College of Engineering, Pune, India

**Corresponding Author: surasal@bvucoep.edu.in*

DOI: https://doi.org/10.26438/ijcse/v8i5.105109 | Available online at: www.ijcseonline.org

Received: 09/May/2020, Accepted: 18/May/2020, Published: 31/May/2020

Abstract **-** This project's motive is to construct a home automation system that uses any mobile device or any electric gadget to control the various home appliances. Smart home automation is very modern and developing field when it uses modern technologies such as Internet of Things (IoT). There are many existing smart home automation systems which includes automatic lights switch on and off, controlling the speed of fan, motion sensors, noise detectors, etc. Most of the electronic appliances which are included in the smart home appliances can be used or manipulated by any user which directly breaches the security of this system. This research mainly deals with the security of the appliances and better performance of the devices installed within the smart home.

Keywords **-** Wi-Fi, HTTP, POST, GET, Raspberry Pi, Smart Home Automation, Security, Hashing, Encryption, Security

I. INTRODUCTION

We are living in a modern era of Internet of Things (IoT), where almost every electronic appliance surrounding us are interconnected by a network and is controlled by a single device. This paradigm enables vast amounts of data to be stored, processed, and used in an appropriate interpretable form without any intervention of human. The emerging technologies and applications of IoT also focuses on the concept of "smart home automation." IoT-enabled smart house equipment enables for a smart home to be more intelligent, automatic, remote controllable, interconnected and most importantly secured.

A smart home generally makes a traditional home more automated and human friendly. Smart home can be defined as using common or interconnected communication devices to integrate with a variety of services at home, assuring economic, security, comfortable and more automated operation of the home [1]. Hence smart home services are used to handle environmental applications or systems like lighting and heating. These days as a result of technological development, the smart home applications monitor individual user activities and the internal environment at home comprising of fans, lights, motion sensors, gas leak detectors, etc. Moreover, an automated smart home provides services that fulfill the demands and necessities of the user.

The below Figure 1 is a basic block diagram where a single mobile application is used to control several devices at the same time which are interconnected among each other and is controlled via Wi-Fi network.

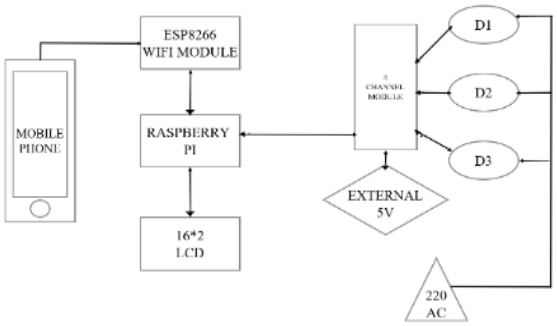

Fig 1: Architecture of Model

The mobile application is basically connected to raspberry pi using the Wi-Fi module which is already enabled in the raspberry pi microcontroller. This raspberry pi can also be connected to any kind of LCD module which manly shows the output or the status of connectivity of the whole circuit. This raspberry pi is then connected to a relay module which helps to communicate information and controlling of more than single devices or appliances at a single point of time. An external battery or power supply is provided to this relay module which helps in controlling and charging of this relay module so that it can effectively control all the devices in the smart home network. The devices namely D1, D2, D3 can be any devices such as light, fans or sensors which are to be operated using this single mobile application.

The upcoming sections of this research paper provides a detailed research methodology and comparison between different protocols to be used in order to complete the project. The later section is described over the main points which include the actual research methodology

used to fulfil the requirements of the project. The last part of the paper is quite crucial as it describes over the topic of security measures taken to secure the project from intruders or hackers in order to achieve complete privacy and safety to the project.

II. EXISTING RESEARCH WORK

In case of smart home automation system, the most important concept is of proper data flow and efficient controlling of the devices present in the entire network. The main research is all about this flow of information within the network using various protocols so that there is minimum amount of data loss and hindrances in the communication within the network.

The main protocol used for communication within this network is HTTP which provides faster and effective flow of communication within the network.

III. HTTP METHODS

The HTTP methods mainly comprises a major portion of the uniform interface constraint and provides the user with the action counterpart to the noun-based resource. HTTP methods provide various functions or namely actions which help in connecting with the world wide web and establishing any kind of connection within the network [2]. HTTP methods help in faster and effective communication with special features which are different methods to interact online which are namely POST, GET, PUT, PATCH, DELETE, etc. Our main primary focus will be on the GET and POST commands as those are the most important functions to establish a connection within a network and communicate through that network.

A. GET METHOD

The HTTP GET method is mainly used to send the data to the main server. In case of the JSP application, the GET method of the form type of application carries the form data and sends to the Java Bean, Servlet or any type of the server-side component which uses the form data carried by the GET method. Whenever we use the GET method to carry data for sending data to the server-side component, it is displayed in the URL as the value of all the form is handled and controlled individually and separately [3]. Only limited amount of data can be sent using the GET method because the data is sent in the form of header and in case of header only a stipulated or limited data can be sent.

GET method mainly requests the data from a specified source in order to establish or build a connection within a network. The requests made by the GET command can be bookmarked and is quite efficient as all the HTTP methods do not provide the ability of bookmaking the commands. GET commands are idempotent which implies that the next request will not be granted or will be ignored until the first request is delivered or executed appropriately. Various other properties of the GET command are:

i. The GET command mainly remains present in the browser history which helps in reuse of this command quite easily.
ii. The GET command can be easily bookmarked.
iii. The GET command can be easily cached.
iv. The GET command should be avoided when dealing with sensitive data as the requests made by the GET command are directly displayed over the URL bar.
v. The GET command should mainly be used while retrieving any kind of data.
vi. The GET command has many kinds of length restrictions.

B. POST METHOD

The HTTP POST method is also used for the same purpose to send information to the server-side component but this method is a more reliable and secured way of sending information than compared to the GET method. The POST method sends the information as a whole different or a separate type of message. When the data to be sent is sensitive for example if the data comprises of any kind of passwords, birth date or any private information then it should be always hidden and protected at every point during the whole communication within the network. In such type of communication, the POST method is used which helps in hiding the data or the hiding the content of the information over the header level. The POST method helps in maintaining the security and is used the most while sending the data over the network and hence the GET method should mainly be used while retrieving the data as it does not provide the feature of hiding the data. The data loss during the transmission of information is very minimum in case of the POST method and helps in maintaining the effectivity and efficient communication within the network. The POST commands do not use any kind of headers for the transmission of data and hence there is no limit in sending the data over the network and hence there is no restrictions in the limit or size of data while the communication within the network. Various other properties of the POST command are:

i. The POST commands cannot be bookmarked and hence the reuse of this command is less.
ii. POST requests have no restrictions of the size or the length of data as they do not use headers to send the information.
iii. AS the POST request are used for hiding the data and maintain the security concerns these requests can never be cached.
iv. These POST requests will never retain in browser history as they are not sent over the browser and is used for hiding the data therefore, they are never saved in the brow\ser history.
v. POST requests are mainly used for securing or hiding the sensitive data during the transmission of data within the network.

C. DIFFERENCES BETWEEN GET AND POST METHOD

Table 1

PARAMTERS	GET	POST
HISTORY	Parameters always remain in the browser history as they are a sub part of the URL	Parameters of no types are saved in the browser history
BOOKMARK	GET methods can be bookmarked	POST methods cannot be bookmarked
RESUBMIT BEHAVIOUR	GET methods can be re executed but may not be resubmitted	The browser alerts the user if the data is needed to be resubmitted
HACKED	Easier to hack ass the data is available over the URL	Difficult to hack as the data is not visible to the user
CACHED	GET methods can be cached	POST methods cannot be cached
USABILITY	GET methods should not be used while transmitting sensitive information	POST methods should be used while transmitting sensitive information
SIZE	Only a limited amount of data can be sent in a single time	No restrictions in the size or length of data
RESTRICTIONS ON DATA TYPE	There are restrictions as only ASCII characters are allowed	There are no restrictions as binary data is also allowed
VISIBILITY	GET methods are visible to everybody as they are displayed over the URL	POST methods are not visible to everybody as they are not displayed on the URL.

IV. RESARCH METHODOLOGY

This research on smart home automation consists of a very important module which is the raspberry pi. The raspberry pi is the main micro controller through which all the essential operations and the controlling of the devices are carried out. Another important part of this home automation system are the devices which are needed to be controlled and automated using a single mobile application. These devices are needed to perform in sync without any technical hindrances. Also, the main focus on this research is about the security of this system from the invasion of foreign users and maintaining the efficiency of the whole system.

A. RASPBERRY PI

The Raspberry Pi is a very low-cost microcontroller, credit-card sized computer that can be easily connected to a computer monitor, laptop or TV, and uses a standard keyboard and mouse. Raspberry pi despite being very small in size it is fully capable for all kinds of computing techniques, and to support programming such as Python and Scratch [4]. It's capable of doing almost every task which you'd expect a desktop computer or a laptop to do. Raspberry pi being a microcontroller it provides numerous modules within itself consisting of its own memory, CPU, and most importantly the Wi-Fi module which helps in establishing the connectivity of the system with online network and makes information flow feasible and provides better control over the connected devices.

The Raspberry pi generally comes in two types of models, which are namely model A and model B. The main difference between the two types of model is all about the USB port. Model A board consumes very less power as compared to model B and it also does not include an Ethernet port. On the other hand, the model B board includes an Ethernet port and was specifically designed in China. The Raspberry pi comes with whole big set of open source technologies and features, i.e. communication, controlling devices and multimedia web technologies. The Raspberry Pi 3 Model B is the latest and advanced type of Raspberry pi model. It supports advanced Wi-Fi range and is also known as the third generation Raspberry Pi. This model replaced the old Raspberry Pi 2 Model B in the year 2016. The following are the specifications of the latest model of Raspberry Pi model are:

i. It provides Quad Core 1.2GHz Broadcom BCM2837 64bit type of CPU
ii. Its memory extends up to 1 GB RAM
iii. The latest model of Raspberry Pi consists of special kind of BCM43438 wireless LAN and advanced Bluetooth Low Energy (BLE) on board
iv. It supports a whopping 100 Base Ethernet
v. Unlike the other models of Raspberry Pi, this latest version provides a full-size HDMI port
vi. This model also consists of 4 USB 2 ports
vii. The most highlighting feature includes of 4 pole stereo output and a composite video output
viii. It also consists of a CSI camera port for connecting and interacting with a Raspberry Pi camera
ix. It also has a micro SD port for loading the operating system and storing data into the database
x. This model is also upgraded and switched Micro USB power source high up to 2.5A

B. CONTROLLING DEVICES

These are the main devices in the smart home automation system which are to be controlled by a single application or a single user. These devices are mainly connected to a relay driver which is indeed connected with a Raspberry Pi. The devices used in the system are mainly motion sensors which will switch ON the lights

only when the sensors will sense any movement or any kind of activity by any individual. This kind of device or automated system is very important as it saves the electricity to a huge extent. The next very new and effective device or system included is auto drip irrigation wherein there are several ultra-sonic sensors placed in the soil which will detect the soil moisture and as per the requirement it would start ON the irrigation process if the moisture of the soil calculated is low[5]. This helps in saving a lot of water resource and is very important for almost every smart home to have this technology. When the user is not at home this type of technology proves all its worth as the soil and plants gets its proper nutrition and also there is no wastage of water resulting in sustainable environment. The next device used in this home automation system is that of pest control and is detected as there are sensors which will detect the movement of specific pests around the corners of the wall and then will alert the user or the individual about the need of pest control activity. Pest control can be handled in a quite effective manner if such automated techniques are installed within the smart home automation system. Also, a very latest technology which is not present in many home automation systems which is smart trolleys. As per the gestures of any individual the smart trolleys will come towards or go away from the user. These trolleys are purely gesture controlled and are very effective when aged people want to move some heavy basket or trolleys as per their convenience. The concept of machine learning and artificial intelligence is used in order to enable the gesture controlling technique and can be proved as very effective and modern concept in any smart home automation technique. The smart trolleys will have cameras and sensor installed within them which will detect the gestures of the user and will function accordingly.

C. SECURITY

Maintaining proper security levels in case of a smart home automation system is very essential as due to lack of security any foreign user can easily misuse this technology and can perform malicious activities. Misusing a smart home kind of technology is quite easy as there is often only a single point of area through which all the automated devices are controlled and therefore intervening such applications becomes quite easy for the hackers. Now to maintain security there are very few techniques in case of smart home system. Our research is mainly focused on this topic of providing accurate an appropriate security to this whole automated system. The link or the main URL which is used by the raspberry pi to link with the mobile application and the main controlled device should be encoded as the hackers or the malicious users try to attack these links to breach the system. This technique of encoding the link is very modern and hardly used in case of kind of smart home systems [6]. To encode this link or the main URL we need to use proper encryption algorithm which will suitably encode this link and will keep it hidden from the hackers and the security of the system will remain absolutely intact. The special kind of encryption algorithm used in this type of encoding should be very powerful and difficult to decode. Hence, we need to use encoding with the help of hashing functions which provide a very unique property which is only one-way encoding. This means that the link which is sent in the form of hash functions which can never be decrypted at the receiver's end. Such type of encoding is a very secured way to protect the automated system. The best suitable technique would be by using the SHA – 256 or SHA – 512 algorithms which have proved to be very powerful in the recent times.

D. SHA ENCODING ALGORITHM

Secure Hash Algorithms (SHA) are a very popular sub part of the family of cryptographic hash functions and was published by very famous National Institute of Standards and Technology (NITS). The family of SHA mainly comprises of four types of algorithms namely SHA-0, SHA-1, SHA-2 and SHA-3 [7]. The original version is SHA-0 which was a 160-bit hash function but it had a few weaknesses and it didn't prove to be very successful. Later in 1995, SHA-1 was designed specially to correct alleged weaknesses of SHA-0 algorithm. SHA-1 is the most widely used of the existing SHA hash functions. It is employed in several widely used applications and protocols including Secure Socket Layer (SSL) security

V. PROPOSED SYSTEM

The proposed system and modules are equipped with automation technologies along with SHA encryption algorithm. The research contribution provided by us helps in reducing numerous hacks and providing security to the whole system and increases the effectiveness of the project. There are many existing systems which facilitates with the same automation technology but they lack in system security at some point. For reference, we could take various smart Bluetooth speakers from leading companies like Google and Amazon, there exist security and privacy issues since number of users can connect to same device and therefore concurrent usage leads to lack of personalization. Therefore, in this system the SHA algorithm ensure that only legitimate user can operate and security of user and data is ensured.

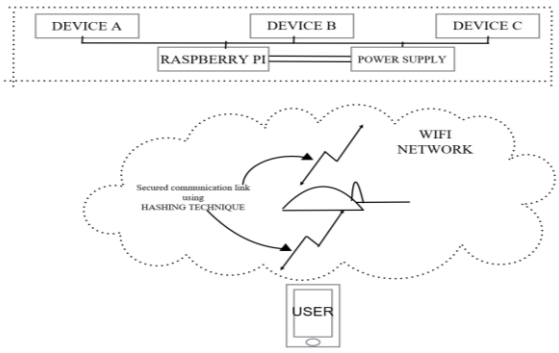

Fig 2: Encryption Architecture

VI. CONCLUSION

The proposed model of smart home automation overcomes maximum of the security challenges making the overall project a lot more effective and user friendly. Such an automated and secure system is quite challenging in in the current future. The use of this model in future can limit the major intrusions and attacks from the outside hackers and can be proved to be very effective. The proposed encryption architecture ensures the completeness of the security part in the project.

REFERENCES

[1] en.wikipedia.org," *home_automation*"
[2] w3schools," *http_methods.ref*"
[3] tutorialspoint.com, "*php_get_post*"
[4]watelectronics.com,"*know-all-about-raspberry-pi-board-technology"*
[5] smarthome.com," *products-you-should-know-about*"
[6] iconlabs.com," *security-smart-home*"
[7] en.wikipedia.org," *Secure_Hash_Algoithms*"

