Efficient Security for IOT environment

Ashwin Prabhu[1], Sagar S Desai[2], Smt.S. Kuzhalvai Mozhi[3]

[1,2] *Student,*
[3]*Associate Professor in the Department of Information Science & Engineering, NIE, Mysuru.*

---***---

Abstract - *The new research on the smart home system helps in the increase of the commercialization day by day. The design of a security protocol for the Internet Of Things, and implementation of this corresponding security protocol on the embedded makes the Smart home products becomes more and more simple and safe to use for consumers. So, This paper introduces, protocol will cover the integrity of messages and authentication of each client by providing an efficient mechanism for various electronic appliances connected to this implemented device. Thus secure communication will be implemented on embedded devices.*

Key Words: **Smarthome, IOT, commercialization, integrity, authentication.**

1.INTRODUCTION

From the past few years, we have seen many companies developing the smart home system devices. With the help of IOT, many manufacturers use internet to connect with the various devices. As the consumers who purchase it will not only help them to use it efficiently, but also provides them various ways to use the devices with the help of Internet. Thus , creating opportunities for more direct integration between the physical world and computer-based systems, and resulting in improved efficiency, accuracy and economic benefit.

IOT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications. In this paper we concentrates on the design of a security protocol for the IOT, and the implementation of this corresponding security protocol on the Sensible Things platform. It is a common platform for communication between sensors and actuators on a global scale, and enables a widespread proliferation of IOT services. This secure communication provides a more efficient information transmission mechanism between user and device.

2. RELATED WORKS

Although many protocols for the Internet have been put forward, it is still not enough to meet the increasingly complex requirements from applications. Many of them are not efficient enough to adapt the device diversity and timely communication environment. Nowadays, network connects people, data, processes and things, standardized ultra-low power devices with wireless technologies, including Wi-Fi, RFID (Radio Frequency Identification). As time passes, powerful embedded devices such as smart phones and tablets will occupy the great part of the IOT. The different devices not only bring kinds of applications, but also many problems, especially in terms of privacy and security issues[2].It is easy to discover that how easy it is to physically attack these embedded devices, as most of the time these components are unattended. The second problem is that many devices use wireless communication, which makes it easier to eavesdrop the messages.Another issue that should be pointed out is their limited hardware resources and energy.

3.SECURITY PROTOCOL

The core of the P2P security system for the Internet of Things is the security protocol. This protocol is the base of all systems' communication and authentication[3]. There are two main parts in this security protocol:

3.1.Registration

3.2.Communication

The structure and design of this protocol mainly focus on high security, high efficiency and low cost.

3.1 Registration Process

[6]In this stage the registration process is carried out between the recently joined client and the Authority Node (AN).

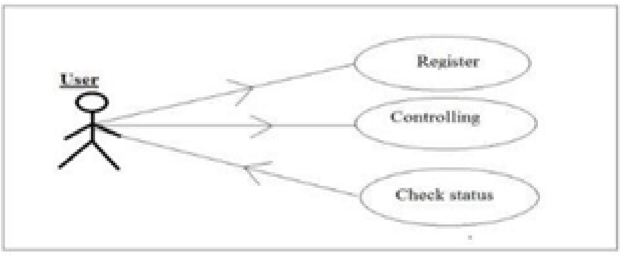

Fig 1: shows the actions performed by the user.

User is going to interact with the Authority by registering.

After the registration user can control the devices and check the status of devices that are connected to the IOT sever. There are six type of messages transmitted during the first registration process.

Client to AN: SSL connection request message, which is to enhance the security of the following registration transaction

Client to AN: registration request message

AN to client: Registration reply message

Client to AN: certificate signing request message AN to client: certificate signing response message Client to AN: certificate receiving message. The detail of these messages could be seen from below, without the first SSL connection request message..

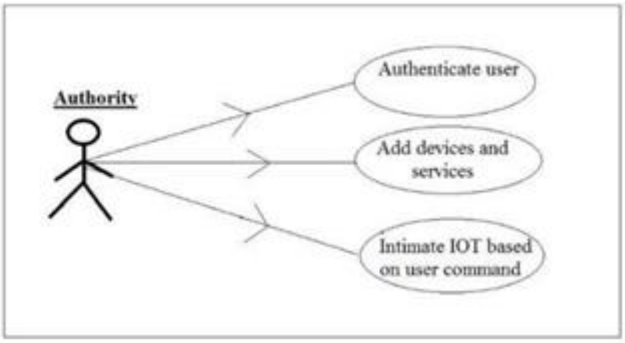

Fig 2: Shows the action performed by the Authority.

Authority will authenticates the user who is going to get Registered and Provides the list of services available. Based on the user command sends Information to IOT server[4].

3.2 Communication

Communication process is based on the first process. There are at most five types of message, including certificate exchange request message, certificate exchange reply message, session key exchange request message, session key exchange reply message and secure message. Most of the time, only secure message is used for information transmission. To test the efficiency of the secure communication, two nodes in the Local Area Network (LAN) are established. Two nodes running on two computers are set up along with an android mobile. Using the internet of things, the android app can control some electronic devices.

4.DESIGN

In this section the fig 3 shows how the user will get access to the electronic devices that are connected to IOT server. At the being user will send a registration request to the admin. The registration request will contains the user name, e-mail ID, mobile IMEI number. Then the admin will approve the request and provides the list of available services.

Now the admin will authenticate the user, when user logged into control the devices. After the successful login process, the commands from the user were send to the IOT server[5]. IOT server will perform the actions based on the commands sent by user. The status of the electronic devices after the actions performed by the IOT server will send back to the user.

5.IMPLEMENTATION

User will control the electronic devices from an android app. Where the details of the user are stored in the cloud infrastructure by the admin. User can also control device from outside the home remotely. For the Authentication process SHA(secure hash algorithm) algorithm is used .

Once the user get logged in successfully, user sends the command to the admin to control the devices. Then admin will generate the session key for both user and Raspberry pi. The command is send to the Raspberry pi by admin. Raspberry pi will generate the OTP using symmetric key algorithm. The OTP is encrypted and sent to the user. Now user will decrypt the OTP with help of same session key. The decrypted OTP will send back to Raspberry pi. Now the Raspberry pi will check received OTP with sent OTP. If both the OTPs are same then a secured connection is established between user and Raspberry pi for the certain period.[7] Now the user has to control the device within that period or else the connection will get disconnected, then the user has to repeat the entire process once again. The status of the action performed by the Raspberry pi will send back to both user and admin. The admin will store the details of the status for future use.

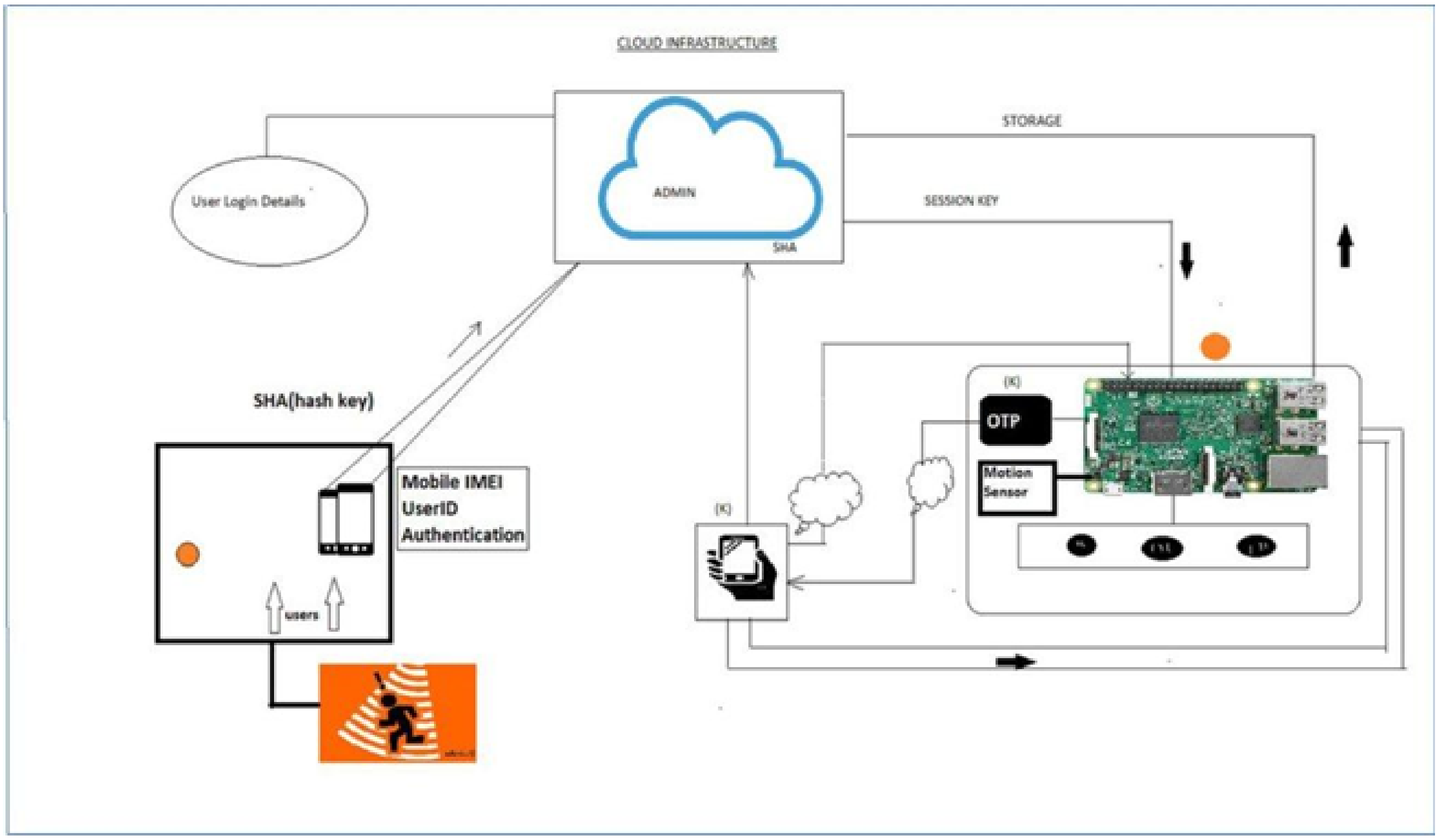

Fig 4: Flow Diagram

6.ADVANTAGES:

1. Authenticates the user to provide security.
2. Allows the user to control the switches efficiently.
3. Provides an android application through which the user can control the switches.
4. No other person other than the registered user can control the switches.

7. CONCLUSION:

In this project, the main purpose of the device is to provide simple configuration for the consumers and helps them to use it at most anytime anywhere. Since the device is useful for conservation of energy, it will be very much beneficial for the society and for the organization who use it.

Basically this device provides the security for the user in order to access various electrical appliances that are connected to the device efficiently.

8.REFERENCES

[1] Xu Xiaohui School of computer, Wuhan University School of economics and management, “Study on Security Problems and Key Technologies of The Internet of Things” Wuhan University Wuhan, China. 2013.

[2] Atzori, Luigi; Iera, Antonio; Morabito, Giacomo, “The Internet of Things: A survey” Computer Networks, 2010, Vol.54 (15), pp.2787-2805 [Peer Reviewed Journal]

[3] Gan, Gang ; Lu, Zeyong ; Jiang, Jun, “Internet of Things Security Analysis” 2011 International Conference on Internet Technology and Applications, Aug. 2011, pp.1-4

[4]Zou, Caifeng, Lu, Zeyong, Morabito, Giacomo, “Access control for IOT devices home automation, of computer science and electronic engineering, jan 2014

[5] Freddy K Santoso, and Nicholas C H VunSchool, “Securing IOT for Smart Home System” of Computer Engineering, Nanyang Technological University, Singapore. 2015.

[6]..https://www.google.co.in/search?q=images+of+registration&tbm=isch&tbo=u&source=univ&sa=X&ved=0ahUKEwj3gs3BucnTAhUJRo8KHaWjDmQQsAQIIQ&biw=1366&bih=638#tbm=isch&q=images+of+registration+process&imgrc=V3KO3I_VZ7kwwM

[7].http://technozed.com/wp-content/uploads/2016/03/GE-Home-Automation-Products.jpg