International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Security Issues in Home Automation

Vandana C. P, Taffazul Imam, Shubham Dubey

Department of Information Science Engineering, New Horizon College of Engineering, Bangalore, Karnataka, India

ABSTRACT

In this modern world all the operations are done via smart manner without manual interruptions and hard activities. This system concentrates two major portions, one is like controlling the smart devices based on wireless manner and provides access rights to its users to operate the load according to that. Security is a major factor for this kind of API enabled devices as limited resources are available for these heterogeneous devices. Authentication Manager and Access Control Manager is used to provide security for these API enabled devices. Authentication manager generates an access control token to verify the user and the Access control manager is to handle the right of users and restrict access to resources.

Keywords: IOT, Home Automation, API enabled devices, Security.

I. INTRODUCTION

The term "Internet of things" in [1] defined as a large number of embedded devices employ a communication service offered by Internet protocol. Many of the devices called as small object and not directly operated by humans.

IOT also called as interconnecting embedded devices via the internet enabling them to send or receive data.

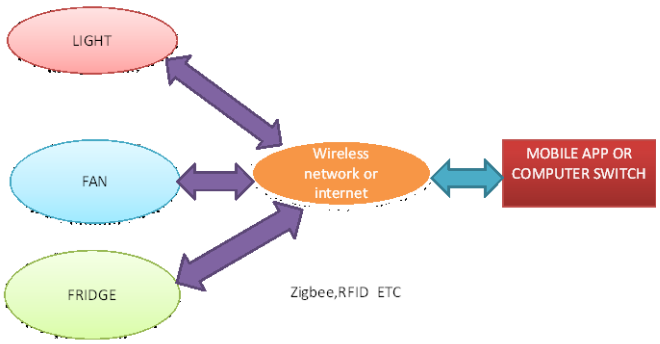

Fig shows that devices are connected via internet .

Home automation or smart home is the application of IOT which is used control home appliances via internet. we can control or access devices either through one or more computer or mobile based application on mobile.

Some of the application of home automation is the automatic operation of water sprinkling, heating and air conditioning, window coverings, security systems, lighting, and food preparation appliances. We can access and control remotely

II. METHODS AND MATERIAL

Architecture of IoT:

Architecture of IoT is divided into three domains [2] sensing domain, network domain, application domain. The sensing domain plays an important role in IOT. It allows to interact and communicate among themselves and with existed or evolving communication infrastructure. Sensing domain consist of many smart thing and is to realize information collection of physical targets by means of technology such as wireless sensor network (WSN), RFID, barcodes and ZigBee.

Network domain build on existing network or evolving communication network such as PSTN, 2G, 3G, LTE and satellite. The main feature of network domain is transfer data from sensing domain to remote domain.
Application domain responsible for data processing and service providing. Data from transmission layer is

controlled by management system and then various service will be provided to user.

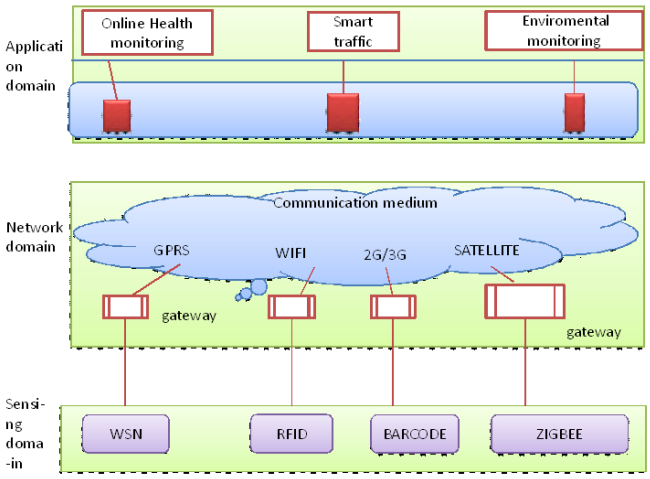

Figure 1. IOT Architecture

Protocols being used in home automation are:

1. C-BUS: C-Bus is a communications protocol based on a seven layer OSI model for home and building automation that can handle cable lengths up to 1000 meter using Cat.5 cable, which has a data rate of 3500bits/sec.
2. Universal Powerline Bus: it is a 2-way communications technology which enables control products to utilize existing powerlines for both residential and commercial applications, which has a data rate of 480 bits/sec.
3. ZigBee: it has a data rate of 20 000 – 250 000 bit/s.
4. Z-WAVE: it is a low-power RF communications technology that is primarily designed for home automation products. Frequencies used are 908.42 MHz North America; other countries use sub-1 GHz, usually data rate of 100 000 bit/s.
5. EnOcean: low power wireless protocol for energy harvesting and low power devices.
6. xAP: open protocol.
7. BACnet: used for building automation, designed by committee ASHRAE.
8. KNX: It is Standardized by internationally (ISO/IEC), Canada (CSA-ISO), Europe (CENELEC/CEN), China (GB/T. Bitrates of 9600 bits/sec).
9. Thread: it is based on 6LowPAN with a networking protocol that is IPv6 addressable, and it's aimed at the home automation environment.
10. SCS: It is Proprietary by bTicino. The upper protocol is OpenWebNet.
11. xPL: Transmits commands and status within a LAN. Some systems, such as the Squeezebox audio player are directly controlled through an Ethernet connection. Others require a computer to bridge the xPL messages to the equipment's hardware interface such as RS-232. It has a bit rate of >10000000 bit/s.

2. Security issues in home automation

Connected to home makes our life more lot easier and convenient but it may have several issues related to connectivity. Connected to the internet allows the intruder to hack into our computers this means they can control our home appliance without being aware.

Privacy and security are the main issues when we talk about home automation. Securing smart devices is an important issue vendor must face. The true challenge is how to offer security in such a way that does not affect the overall user experience and also in a cost-effective manner.

When we use cloud tech to store the data, data is vulnerable, and hackable protecting data in the cloud is measure issues in today's era.

Security measures in smart home alarm that detects if the window is broken and locker is broken. We can develop an app that detects any unauthorized access to home security, or unencrypted channel.

When we use cloud tech to store the data, data is vulnerable and incapable of protecting data in the cloud is the major issue in today’s era.

Security measures in smart home alarm that detects that, if the window is broken and locker is broken. We can develop an app that detects any unauthorized access to home security, or unencrypted channel.

- OAuth: An open Standard for Authorization which provides one more layer of authorization. But the major drawback of OAuth protocol implementation is that the OAuth token could be stolen and can manipulate the app. Data can also be misused.
- API access control: Set of function, routines, protocols and the tools used to build Software applications. API provides an access control for the functionality for an application based on certain rules and policy and also which access is to be permitted.

- The issue with this access control is, it has an Unrestricted Communication ability which makes this vulnerable. Apps can be used to send SMS to any numbers through the SmartThings which provides these apps to leak sensitive information via the Smart Things.

3. Existing Home Automation System

➢ GSM based home automation System:

- In [3], proposed model is based on GSM. It has three means the home: the GSM network, the Internet and through speech.
- GSM is used when there is not a proper internet connection.
- Server side uses the AT commands in [4], which are instructions used to have control in the modem. AT is an abbreviation of Attention. Each command line starts with "AT" or "at."
- The mobile interface is developed using J2ME, and the server side consists of 4 engines running the web server, the database, main control program.
- The GSM system is controlled using SMS and can send confirmation messages.
- Dynamic time wrapping algorithm is utilized for the speech processing. Since Voice activation is found to be very impractical. So, as a much more stable alternative, a wireless unit the user carries within the home is used to activate the voice input.
- The Application node has four parts- the transmitter, receiver, I/O device and a microcontroller.
- GSM is used due to its high availability, coverage, and security and control of home appliances are done through SMS codes.

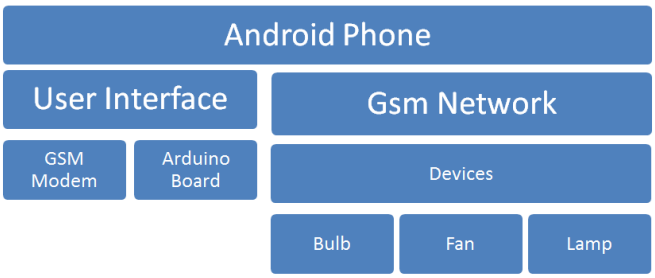

Figure 1: GSM based System

➢ Bluetooth Based Home Automation:

- It uses the cell phone and Bluetooth technology [5]. It is secured and low cost.
- An Arduino Bluetooth board is used for the Bluetooth technology. The user interface in [6] the cell phone is provided using python program.
- The Bluetooth board and relays of the I/O ports are used to interact with the devices to be controlled.
- The system is password protected for ensuring security and to safeguard the misuse of the system.
- The range is 10 to 100 meters with 2.4GHz bandwidth and 3Mbps speed.
- The drawback of this system is that it takes a long time to discover and access.

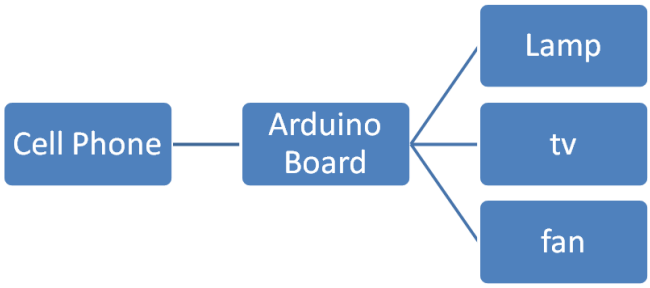

Figure 2: Bluetooth based System

➢ Phone based automation

- It consists of facilities such as a system controller [7], house-wide wiring and a common interface that provides the system for the smart home.
- The primary function of the remote controller is to regulate the power supplied to devices at the particular location.
- In this automation telephone lines being used for transmitting the commands. It can be implemented using infrared signal and AC power line carrier technology. Also, we can implement using DTMF transceiver mapped with solid state to control power supply
- It consists of three components [8], first is DTMF receiver and ring detector. Second is IO interface unit and third is PC which does the online operation. PC detects the line of control and authenticates the user.

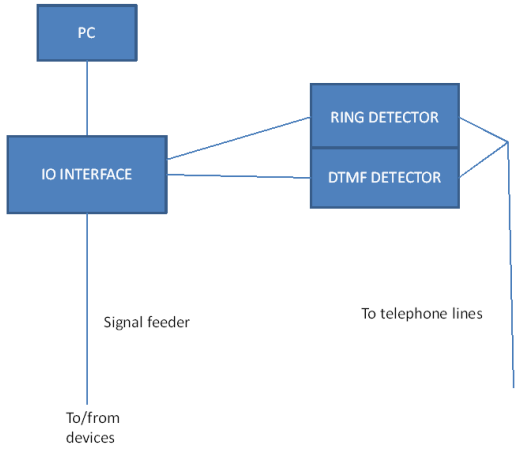

Figure 3: phone based automation

➢ ZigBee based Home Automation:

- It is a Wireless Communication Technology [9] to be used in the home automation and uses voice recognition technique and PIC microcontroller.
- A Mike is used for the voice command, and the voice is stored and processed.
- The commands are transmitted via ZigBee to Receiver using the PIC microcontroller which has one more PIC microcontroller to process the command. Relays are used to control the appliances.
- The drawback of this system is that the communication medium has the low range which prevents remote access from distant locations.

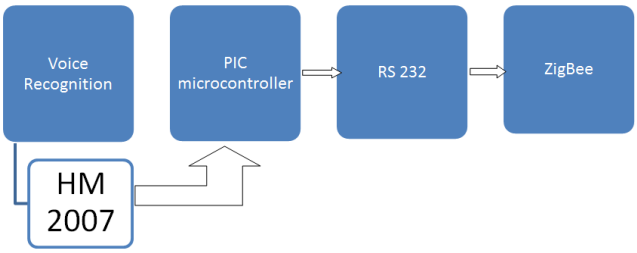

Figure 4: ZigBee Based System

III. RESULTS AND DISCUSSION

➢ ***Proposed architecture***

- In [10], The proposed framework enforces on security challenges. Moreover, the device can be removed or attached dynamically at a time, to achieve the dynamic environment in the building security manager is consider as trusted third party.
- To ensure efficiency and scalability, the security manager is split into authentication manager and access control manager.
- Authentication manager generates an access control token to verify the user. To achieve authentication method, the idea of confidence level is introduced. After the device receives the request from the user, the device forces the access control manager to evaluate the received request .it handle the request based on the access control policies.
- The primary function of access control manager is to handle the right of users and restrict access to resources.

I. Authentication Manager:

Credentials information is sent by users as the request parameter [11]. Auth, Authentication method and strength, the confidence level is optional parameters may also send by users.

Users are verified by the authentication method. The confidence level is introduced in our framework as the smart building environment is dynamic. Different critical levels for APIs are introduced in the smart building environment. Users are verified with an authentication manager; the high confidence level is required for high critical level APIs.

II. Access Control Manager:

A request is sent directly to resources via a verified user [12]. Access token expiration and existence are checked when the resources receive an invocation from the user. Access tokens are evaluated at the resource side by the access control manager.

Authentication method, confidence level, and permission, which included in the access token. Authorization of the requesting user is evaluated by the access control manager.

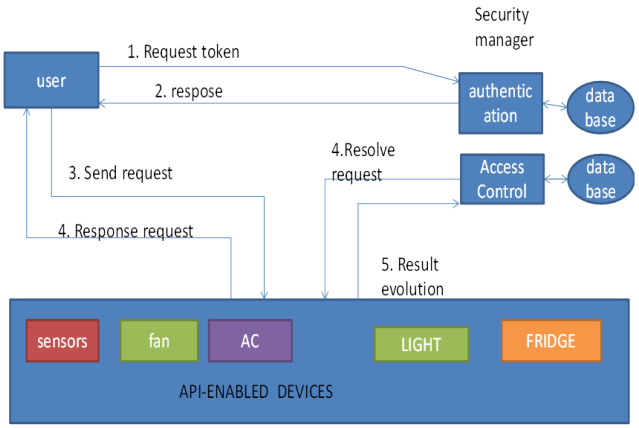

Figure 5: Proposed Architecture

IV.CONCLUSION

In this paper, we have proposed the Security issues in the home automation which include the Authorization and the access control. The Existing systems used in the home Automation have been briefly explained in this paper.

V. REFERENCES

[1]. Hao chen, Xuegin jia,Heng LI ,IOT Gateway : "A brief introduction of Iot gateway :IET International Conference on Communication Technology and Application (ICCTA 2011

[2]. Qian zhu, Ruicong wang, Qichen, Yan Liu and Weijun Quin, IOT Gateway: bridgeing wireless sensor network into internet of things ,2010 IEEE/IFIP international conference on embeded and ubiquitous computing.

[3]. Baris Yuksekkaya, A. Alper Kayalar, M. Bilgehan Tosun, M. Kaan Ozcan, and Ali Ziya Alkar "A GSM, Internet and Speech Controlled Wireless Interactive Home Automation System", 2006, IEEE Transactions on Consumer Electronics, Vol. 52(3), pp. 837 - 843.

[4]. Rozita Teymourzadeh, Salah Addin Ahmed, Kok Wai Chan and Mok Vee Hoong, "Smart GSM Based Home Automation System", 2013, IEEE Conference on Systems, Process & Control, Kuala Lumpur, Malaysia.

[5]. R.Piyare,M.Tazil, " Bluetooth Based Home Automation System Using Cell Phone", 2011, IEEE 15th international Symposium on Consumer Electronics, Singapore, pp. 192 - 195.

[6]. Home Automation System via Bluetooth Home Network", 2003, SICE Annual Conference, Fukui, Vol. 3, pp. 2824 - 2829.

[7]. H. Brooke Stauffer "Smart Enabling System for Home automation", 1991, IEEE Transactions on Consumer Electronics, Vol. 37(2), pp. 29-35.

[8]. Eddie M C Wong, "A Phone Based Remote Controller for Home and Office Automation", 1994, IEEE Transactions on Consumer Electronics, Vol. 40(1), pp. 28-34.

[9]. V. Sathya Narayanan, S. Gayathri, "Design of Wireless Home Automation and security system using PIC Microcontroller", 2013, International Journal of Computer Applications in Engineering Sciences, Vol. 3 (Special Issue), pp. 135- 140.

[10]. C. Lee, L. Zappaterra, K. Choi, and H.-A. Choi, "Securing smart home: Technologies, security challenges, and security requirements," in Communications and Network Security (CNS), 2014 IEEE Conference on. IEEE, 2014, pp. 67–72.

[11]. An OAuth based Authentication Mechanism for IoT Networks Shamini Emerson, Young-Kyu Choi, Dong-Yeop Hwang, Kang-Seok Kim and Ki-Hyung Kim* Department of Computer Engineering, Ajou University San5, Woncheon-dong, Yeongtong-gu, Suwon 443-749, South Korea {shamini, chmj0320, bc8c, kangskim, kkim86}@ajou.ac.kr

[12]. Access Control Framework for API-Enabled Devices in Smart Buildings, Syafril Bandara1, Takeshi Yashiro2, Noboru Koshizuka1, 2, and Ken Sakamura1, 2 Interfaculty Initiative in Information Studies, The University of Tokyo, Tokyo, Japan 2YRP Ubiquitous Networking Laboratory, Tokyo, Japan.