Challenges and Risk to Implement IOT in Smart Homes: An Indian Perspective

Rakesh Roshan
Assistant Professor
Institute of Technology & Science,
Ghaziabad

Abhay Kr. Ray
Assistant Professor
Institute of Technology & Science,
Ghaziabad

ABSTRACT

The concept of Internet of Things requires the seamlessly connectivity of millions of heterogeneous devices. In today's world, Implementation of IoT in Smart Homes is one of the major applications of Internet of Things. In this paper, we will discuss the different challenges and risk to implement IoT in Smart Homes of India. An Indian perspective is taken, because India is in very first stage for implementing the Smart Homes. This paper explains many challenges in Indian scenario like availability of Internet, Cost of devices, device maintenance issue etc. and proposes a framework of smart homes is also discussed here.

Keywords

Smart homes, IOT, Wireless protocols

1. INTRODUCTION

The digital space and recent technology development in the world and smart home technology are creating their importance in the today's market place. Smart homes have highly developed systems beyond the basic functionality like automatic door openers, light control system to provide many tangible benefits in terms energy efficiency. IP-enabled cameras, security alarms, object motion sensors, and connected door locks provide better home safety and security. Taking view of this kind of automations in the smart homes it require a such revolutionary technology which provides anytime seamless connection among the sensors of different home appliances is internet of Things (IOT)[1].

According to Zanella et al [6], The IoT shall be able to integrate transparently and seamlessly a large number of different heterogeneous devices, while providing open access to selected subsets of data for the development of a large scale of digital services. To build a general architecture of IoT for smart cities are very complex because of the extremely large variety of devices, link layer technologies, protocols and services that are involved in such a system.

IoT is often associated with home automation and empowered the house hold devices by the integration of sensors, transmitters and receivers which helps the application to collect, consolidate, analyze and take the design in an efficient manner for instance if a smart air conditioning system make a co-relation between the temperature inside the home and outside the home in different months weekly or fortnightly then it can smartly manage its internal setting of cooling or heating which may save energy.

The government of India has planned to develop 100 smart cities in the country, and allocated Rs. 3305 Cr. in the current year(2016-17) budget which may boost the fast expansion of application of IoT in order to develop the smart cities. Smart cities not only deals with Smart parking, smart transport system, better tele-care, smart safety and security systems , smart power grids, smart urban lighting, smart waste management, smart city maintenance. Intelligent water management but also deals with smart homes. But in India there are so many challenges and risk to implement IOT in smart homes.

In Year 2015 , Government of India planed to create a market place of 15 billion US Dollar for Internet of Things in upcoming five years. However, IoT has not a major publicity and it has to create any major buzz in India. subdued to a large extent. Department of Electronics and Information Technology , Government of India announced a draft about the IOT Policy document with following objectives.

a. To create a market place of 15 billion US Dollar for Internet of Things in upcoming five years means by 2020.It has been assumed that India would have a share of 5-6% of global IoT industry.

b. To develop the skill set or capability building in human resources for IOT and its related technology specific for Indian or international markets.

c. To undertake capacity development (Human & Technology) for IoT specific skill-sets for domestic and international markets.

d. To start Research & development for all the supporting technologies of the IOT.

Smart homes now day's using the IoT to automate its many subsystems like smart lighting system, Smart Thermostat controller or HVAC, Entertainment ,Smart home care, Smart Security and access control system, Smart Kitchen, Smoke Alarms ,Pet feeding, Washers ,Refrigerators. There are many benefits to use these systems in smart homes as given below.

- Money saving: smart home provides opportunity to consume less energy and cut expenses on their utility bills. In the long duration, smart home can also provide a good return on investment by increasing its worth and making it easier to sell.
- Enhance Safety: Smart devices can assist to protect family members both young and old by providing monitoring mechanisms on kid's activity and assistance requirements of old family members.
- Prevent Damage: One of the primary objectives of smart home is that homeowner can monitor his home while he is away. This creates feeling of good security even if a glass breaks, the oven is left on, or any adverse condition will be alerted and can promptly respond to the situation.
- Convenience Enhancement: ease of living and a customized living space are important. The smart home can remind homeowners when they are

running low on household products, and smart doors and security systems can give peace of mind to the homeowners.

2. PROPOSED FRAMEWORK FOR SMART HOMES

The resources required for the Smart Homes are:

1. WiFi
2. Sensors
3. Internet
4. Mobile application for remote access

From the above resources, Smart Homes can be implemented successfully. The tentative framework for the Smart Homes will like in Fig 1.

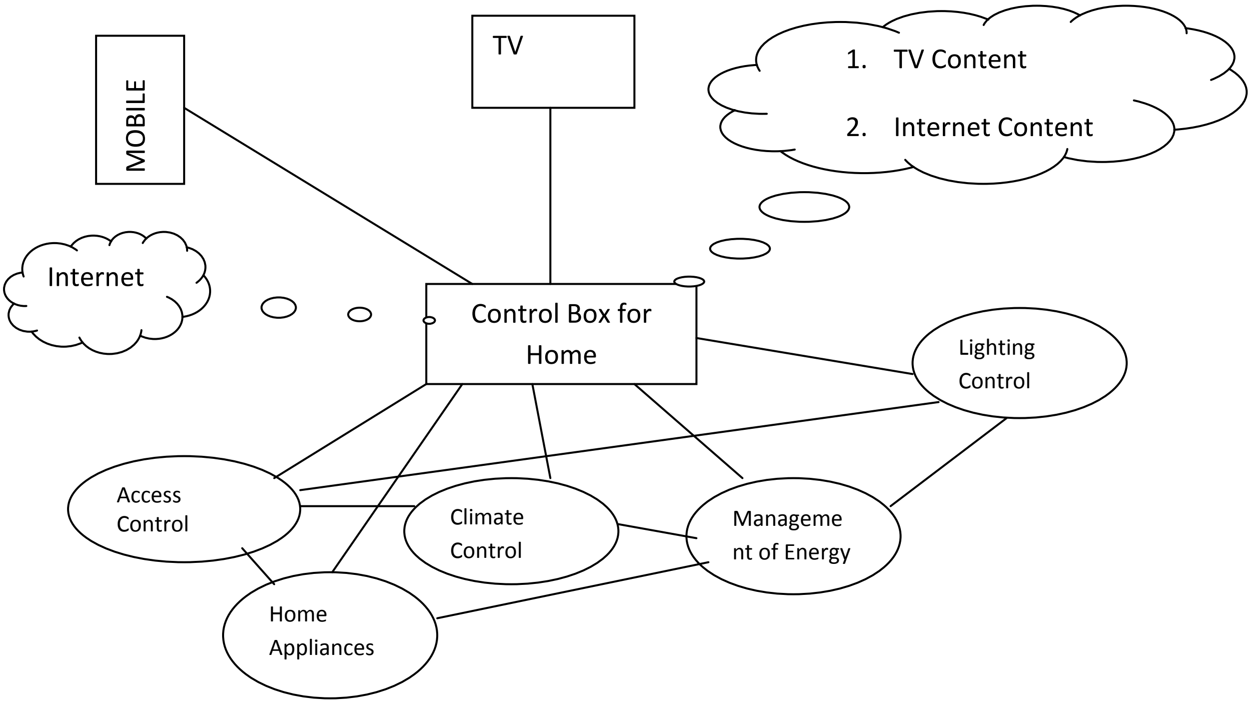

Fig 1: Proposed Framework of Smart Homes

The central part of Smart Home Framework is a Control Box(CB), a (virtual) device that can be implemented on a Set-Top Box , Gateway, built into a Television set or any other electronic device, When this CB will connected to the internet then, every device of the home can be access by the mobile from any part of the world. This CB also works like a network address translation (NAT)[3].

Control Box has several of functionalities like processing of services, Configuration management, Analysis of Services and Discovery of devices.

2.1 Processing of Services

It is a package of web service modules that allow home users to configure their IoT Device and enabling the IoT devices search. In addition to device discovery, use the IOT control system and the response notification to devices also is part of the layer functionalities. The discovery of services later served a pivotal role in ensuring IoT devices in the Smart home environment dependence are constant throughout the period of use.

2.2 Configuration Management

This ensures that a Configuration resource [3] of IoT devices is available for all entities in the smart home environment. So, that It includes an API that allows resource extraction when registered to the Smart home network. Details like endpoint, device identification, and configuration resources are stored in a database component configured. It also allows the integration of legacy devices intelligently ensures the implementation of the joint family and the environment Actions federated manner. Such integration Legacy device dependencies hold When heterogeneous devices in the smart home Environment. When the details of the integration and Device registration, deregistration steps are Described in [4].

2.3 Analysis of Services

It collects the data from Internet of Things(IoT) using different sensors. Sensor Markup Language (SenML) is used to collect data from sensors. This provides a mechanism to encode the data receive by sensors and other parameter of Inter of Things(IoT) devices as a payload of Hyper Text Transfer Protocol (HTTP). This simplifies the data of heterogeneous IoT devices and execution of tasks. The modules contains inference engine, pre defined rules that applied to registered IoT devices in house

2.4 Discovery of devices

It is a important aspect of the framework given in figure. This functionality allows the consumers discover the managed IoT devices of smart home, their strength, attributes and URIs. This module can be also used by the configuration management module.

3. MAJOR CHALLENGES IN INDIA

There are so many basic problems and challenges of Indian IoT consumers that is why IoT adoption in India would be very slow. Some of these IoT adoptions challenges are Lake of Standardization data security issues, data storage and ownership issues, return on investment, power supply problems etc , these are really not unique to India. Apart from these challenges, IoT in India would consider with a some other challenges are as given below.

- **Internet availability:** Even today Internet connectivity, Internet connection reliability and availability of required connection bandwidth are still a major challenge in India. For a smart homeowner or a IoT consumer adoption – this can a remain a most important challenge.
- **Cost of IoT enabled systems and devices for smart homes** : Indians consumers in respect of any technology are very selective in terms of investment on convenience and technology Even some products such as smart wearable fitness bands are yet to take off in India, and price is a major factor .
- **Lack of vendor activity**: Global vendors are generally or by mistaken assume that Indian consumers are not ready for advance devices or product. This is very much obvious in case of adoption of smart home technology and IoT space, with rarely any kind of vendor activity today. This led to low level of awareness of IoT Systems or smart home appliances among the Indian consumers.
- **Overall infrastructure challenges:** Not only the internet but the supporting infrastructure such as Smart power grids, Smart drainage/ sanitation System, Smart Water Supply etc, which are indistinguishable part of a smart home and these are far from being ready to use in India.
- **Lack of skilled resource in India:** IOT adoption is also constrained by the unavailability of skilled workforce for implementation of nationwide IoT enabled smart systems. According to the report of Labor Bureau Report of 2014 the skilled workforce in India is only two percent of total population , which is much lower when compared to some other developing nations. So there is need to introduce some educational programmes that helps the workforce to learn these technology and meet the requirements in order to support the growing ecosystem.

4. RISK FACTORS

IoT Products associated with smart homes can vulnerable, for instance a report of time of India, 28 Nov 2015 Pune india researchers of Kaspersky Lab have discovered serious threats to the smart home .A coffeemaker machine that exposes the Wi-Fi password of homeowner to third party , a baby video monitor equipment that can be accessed and controlled by a malicious third-party, and a smart phone-controlled smart home security system that can be fools with a magnet. There are always some security control risks will exist in smart homes regarding the Data Protection, End point protection, Trust & Safety, Physical Security, Security monitoring and analysis ,Identification and access management, Regulatory compliance. Some basic risk of smart homes is as given below.

- Hackers Attacks
- Data ownership risk
- Single point of Failure

4.1 Hackers Attacks

Hackers attacks are not new in the digital world, however, the hackers attack in the smart home may cause of a huge loss of security and safety of the homeowner as well as vendor too. There are many threats that's may cause of data loss and data hacking are counterfeiting ,denial of services ,eavesdropping ,buffer overloading ,malicious modifications ,password based attacks ,man in the middle attack ,phishing etc. There are some steps which a homeowner must follow to **ensure your home remains out of the reach of hackers**.

- **A case of need v/s security:** Do a house owner really need to have remote access to his house? Does the owner need webcams inside the house, or just an intercom at the door? If owner is worried about intruders, presence sensors work very well as part of an integrated alarm system, no webcams needed.
- **Avoid to open unnecessary Ports of devices:** Another way to keep smart home private is to ensure that a home don't have any ports opened in its router. If owner does decide to have remote access to his home then always make use of virtual private network (VPN) rather than opening ports in your router.
- **Use of trusted vendor's tools :-** Always use of trusted vendor's tools, applications and devices for smart home automation by which a homeowner can restrict which parts of the web interface can be accessed remotely. So owner could have some features such as a holiday mode accessible – which doesn't allow cameras to be accessed outside of the local area network (LAN).

4.2 Data ownership risk

According to the Intel's security survey 2015, most users consider biometrics as the most trustworthy and simple authentication and security solution. Half of respondents named fingerprints as the best option, 46% also opted for voice recognition and 42 percent for eye scans. But still a big question arrived regarding the data ownership whether it should store on local server to get the advantage of locality reference of data or store on a trusted vendor's server to get more security. In both cases there is chance of data hacking. There is no full-proof mechanism to restrict data hacking. Therefore owner has to subscribe a good server security system if he store the sensitive data on his local server or he has to use virtual private network in case he is using the remote server of vendor.

4.3 Single Point Failure

A security system based on the centralized controlled system for data store, application processing or application storage, and then there will always a risk of a point of failure. Even decentralized control systems still have the problem that the cable or power supply is a single point of failure, and this is the downside to control. It's not all doom and gloom though, as there are many sensible ways to get around this. One of the best solutions is the use of an uninterruptible power supply (USP) so that in the event of a power cut your system still runs. A smart home could has an additional Mini-server as a backup, arrangement of certain emergency lighting circuits on conventionally wired circuits, and owner can ensure there is always an SD card with the applications saved on site. So in case of application fault a live install take place from the vendor side.

5. CONCLUSIONS

In the paper we discussed and explained about smart homes, application of Internet of Things in smart homes, major challenges and risk to implement smart homes by using IoT in Indian prospective, and also proposed a simple framework to implement smart home. In a nutshell, paper presents challenges and risk that already exists in India which must taken care by government, service providers and venders to make better market place of IoT and smart homes in India. The paper also presents a framework of Smart Home using Internet of Things (IoT) and its different components like home access control energy management control, climate control etc these systems must be IoT enabled and connected to a central control box store and analyze the data to take effective designs and send notifications and essential information to the home owner. In Indian prospective smart homes have many risk challenges and issues as mentioned in this paper and these must be taken care by government of India or government of states, service providers and compliance governing bodies for the successful implementation of smart homes.

6. REFERENCES

[1]. L. Atzori, A. Iera, and G. Morabito, “The internet of things: A survey,” Comput. Netw., vol. 54, no. 15, pp. 2787–2805, 2010.

[2]. Jin, J; Gubbi. J; marusic, s.; Palaniswami, M. “ An Information Framework for creating a smart City Through Internet of Things.” IEEE Inter of Things Journal, 2014, Vol 1, Issue 2, pp. 112-121.

[3]. Rajabzadeh, A; Manashty, A.R.; Jahromi, Z.F. “ A generic model for smart house remote control systems with software and hardware simulators.” 5th Conference on Information and Knowledge Technology (IKT), Shiraz, 28-30 May 2013, pp. 262-267.

[4]. Datta, S.K.; Bonnet, C.; Nikaein, N., "An IoT gateway centric architecture to provide novel M2M services," Internet of Things (WFIoT), 2014 IEEE World Forum on, pp.514,519, 6-8 March 2014.

[5]. How the Next Evolution of the Internet is Changing Everything https://www.cisco.com/web/about /ac79/ docs/innov/IoT_IBSG_0411FINAL.pdf

[6]. Zanella. A.; Bui, N.; Castellani, A.; Vangelista, L.; Zorzi, M.; “Internet of Things for Smart Cities.” IEEE Internet of Things Journal, 2014, Vil 1, Issue 1, pp.22-32

[7]. Suciu, G.; Vulpe, A, “ Cloud Computing and Internet of Things for Smart City Deployments. ” In Int. conf. Challenges of the Knowledge Society (CKS) 2013, Romania, 17-18 may 2013, pp 1409-1416.

[8]. Navarro, C.; Roca-Riu, M.; Furio, S.; Estrada, M. “ Designing new models for energy efficiency in urban freight transport for smart cities and its application to the Spanish case.” In 9th Int. Conf. on City Logistics, Tenerife, Canary Islands , Spain, 17-19 June 2015, pp 314-324.

[9]. Wolff, A.; Kortuem, G.; Cavero, J. “Towards smart city education.” 2015 sustainable Internet and ICT for Sustainability (SustainIT), Madrid, 14-15 April 2015, pp, 1-3.

[10]. Sanseverino, E.R.; Scaccianoce, G.; Vaccaro, V.; Zizzo, G.; Pennisi, S. “ Smart City and public lighting.” 2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC), Rome , 10-13 June 2015, pp. 665-670.