Home Automation Implementation Challenges

Renu Sharma

Asst. Professor,DAV College, Amritsar
Renusharma1978@yahoo.com

---***---

Abstract:- Smart Home is a network of smart devices (IoT enabled) to provide ease in modern living. IoT enabled devices means, devices that can be connected through internet. Involvement with internet provides flexibility to work or communicate or control devices from anywhere. Communication among varied devices arises many challenges. In this paper issues are discussed regarding adoption of IoT devices in smart homes and various solutions given in literature is categorized.

Key-words: Smart Home, IoT .

Introduction

Smart Home is a network comprising of many devices that can communicate with each other or with outer world through internet. This communication enables a person to watch and manage a home remotely. Internet of things or IoT means having devices linked through internet to exchange their information and to create results helpful for mankind. Next era of computing will not be based on desktops but will be of IoT devices.[1]. IoT is most significant electronic revolution after internet[2]. According to Gartner number of IoT enabled devices will be 26 billion by 2020. If we list area of applications of IoT, list is expanding day by day to various diverse fields. Some area of applications is:

- Smart Homes
- Remote Health care monitoring
- Smart cities
- Education
- Smart Transport
- Smart Agriculture
- Business
- Energy
- Disaster detection etc.....

Components for Home Automation

IoT is mainly based on:[3]

- Sensors
- Middleware
- Cloud computing
- Internet

A. Sensors

They are used to detect and react to certain type of input. The base of IoT is various types of sensors. Constraints of sensors are: low energy, constrained computation and small memory. Because of these constraints a system involving sensors are difficult to design.

B. Middleware

In smart home, sensors do have different architectures and working based upon different protocols. So to make communication between sensors and home automation system, mediators are required and they are called middleware. They are used to interoperate various devices.

C. Cloud computing

To have an IoT based application, cloud is required. Due to constrained resources of sensors, all the computation required cannot be done in these devices, so cloud is necessary in many applications.

D. Internet

To join different sensors and cloud, Internet is required. In any IoT based application, sensors have very less amount of power, so they cannot afford to be on network all the time. Generally PANs are used and connectivity to internet is provided when required.

Advantages of Home Automation

Smart home concept is mainly to raise level of luxury. But it has given many added advantages other than luxury. Some of the benefits of Smart Homes are:

- Remote monitoring
- Assisted living for elderly. [4]
- Energy efficiency [5]
- Comfort etc.

Challenges in Home Automation

Although smart home market is having many possibilities for user as well as for market. But many technical as well as social hazards are there in the implementation.[6].In development of smart home applications, many challenges are there. Some of them are:[7]

- Interoperability and integration[8]
- Security[8]
- Privacy [9]
- Data storage
- Constrained resources
- Data Analysis

Interoperability and integration

Smart home, idea is mostly based upon sensors. Sensors do have varied architectures. To integrate them is a major challenge. Smart home industry lacks in standardization or in other words so many standards are there. Every company has adopted different standards. While integrating these devices many technological issues got arise. So there is a requirement of one standard model for development of IoT devices. To ease in the integration of new devices. For example if we have employed a home automation system and we want to change a device due to lack of unique standardization it might be possible there will be a need of updating our home automation system.

Security

Security is the major challenge for IoT devices. As in many intelligent cars there is major possibility of intrusion using server of the company. IoT is based upon network and network is vulnerable to threats. As in home automation system main identity of user is RFID card. Copy of that card is possible. If a person is having GPRS all its travelling pattern can be monitored and that can create major security issues. If we study health monitoring, intruder can create major blunders. In all sensitive areas, IoT is quite helpful but its implementation is really important to be focused on security.

Privacy

Privacy is also a major concern. If somebody is using smart environment, an intruder can study all his/her patterns just by analyzing data of sensors. And that information can be used for criminal activities. GPRS, wearable devices[9] and other sensors used in home can easily tell about daily routine of somebody. So privacy is also one of the major issues in implementation of IoT.

Data Storage

In any smart environment huge data is produced. To store that huge data traditional data storing techniques cannot be used or we can say they are not capable enough to store. To overcome this challenge we need data storing techniques capable to work on high volume and high velocity data.

Constrained Resources

In IoT devices, main components are sensors. These sensors are really constrained as far as processing power , battery life and memory is concerned. To overcome these constraints are also a big challenge.

Data Analysis

Using IoT sensors, huge amount of data will be generated. It is a challenge to process such a large amount of data. To process huge data timely, efficient algorithms are required. Existing data mining tools are to be updated.

Conclusion

Smart home is a part of today. But many challenges are still there in the implementation of home automation. Solution in these areas can be attained and many solutions are being purposed by many researchers but still there is a scope for a solution with lesser hazards. As far as integration and interoperability is concerned there should be some solution on which any devices can be used as plug and play. Security and Privacy is a major research area. All devices of home automation are constrained in terms of resources. So all areas can be explored.

References

[1] G. Jayavardhana, R. Buyya, S. Marusic and M. Palaniswami.,"Internet of Things(IoT): a vision, architectural elements and future directions " , Journal of Future Generation Computer Systems, Vol. 29, Issue 2, pp. 1645-1660, September 2013.

[2] A.H. Ngu, .M. Gutierrez, V. Metsis, S. Nepal and Q. Z. Sheng ., " IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE Internet of Things journal, vol 4, issue 1, pp. 1-20, February 2017.

[3] I. Lee , K. Lee," The Internet of Things (IoT): Applications, investments, and challenges for enterprises", Business Horizons, volume 58, issue 4, pp. 431-440 , july-august 2015.

[4] S. J. Daraby,"Smart technology in the home : time for more clarity", Building Research & Information, Vol. 46, Issue 1, pp. 140-147, March 2017.

[5] C. Wilson, T.Hargreaves and R. Hauxwell-Baldwin," Benefits and Risks of smart home technologies", Energy Policy, Vol. 103,pp. 72-83, April 2017.

[6] D. Raggett, " The Web of Things: Challenges and Opportunities," IEEE Computer, vol. 48, Issue 5,pp. 26-32, May 2015.

[7] M. Elkhodr, S. Shahrestani and H. Cheung., "The internet of things: new interoperability, management and security challenges", International Journal of Network Security & Its Applications, Vol. 8, No. 2, March 2016.

[8] S. Notra, M. Siddiqi, H. H. Gharakheili, V. Sivaraman and R. Boreli, "An experimental study of security and privacy risks with emerging house-hold appliances", In Proc. IEEE Conference on Communications and Network Security, 2014, pp. 79-84.

[9] J. A. Martin,"10 things you need to know about the security risks of wearables", para. 4, March 24, 2017.[online]. Available: https://www.cio.com/article/3185946/wearable-technology/10-things-you-need-to-know-about-the-security-risks-of-wearables.html.