International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Smart Homes System Using Internet-of-Things: Issues, Solutions and Recent Research Directions

Mrs.Jyotsna P. Gabhane[1], Ms.Shradha Thakare[2], Ms.Monika Craig[3]

[123]*Assistant Professor,Department of Computer Technology,Priyadarshini College of Engineering,Maharashtra,India*

Abstract - *Smart home has evolved from exclusively referring to the centralized and semi-automated control of environmental systems whereas Internet-of-Things (IoT) is the expansion of internet services. Applications of IoT are increasing. Uses of new technologies in IoT environment are increasing rapidly. It has been already developed in Industrial Wireless Sensor Network (WSN). A smart home is also one of the applications of IoT. Rapid growth in technologies and improvements in architecture comes out many problems that how to manage and control the whole system, Security at the server, security in smart homes, etc. This paper presents the architecture of IoT. Smart homes are those where household devices/home appliances could monitor and control remotely. When these household devices in smart homes connect with the internet using proper network architecture and standard protocols, the whole system can be called as Smart Home in IoT environment or IoT based Smart Homes. Smart Homes ease out the home automation task. This paper presents not only the problems and challenges come in IoT and Smart homes system using IoT but also some solutions that would help to overcome on some problems and challenges.*

Key Words: *Internet of Things (IoT), Smart Home, Radio Frequency Identification RFID*

1 .INTRODUCTION

Internet has changed human's life by providing anytime, anywhere connectivity with anyone. As many advancement in technology has been come the sensors, processors, transmitters, receivers, etc. are now available in very cheap rate. Hence these all things can be used in our day to day life [4]. If anyone wants to expand the services of internet then Internet of Things can be said as the expansion of internet services [1]. Today's internet is now expanding towards Internet of Things (IoT).

1.1 Internet-of-Things: The internet where the existing network of internet to the computer systems will connect to the real world objects or things. Things may include any objects, home appliances, devices, vehicles, etc. And when these things connect to the internet in specific infrastructure via standard protocols then the whole system is said to be Internet of Things (IoT) [1-4].

1.2 Things: Things may be real or virtual, moving or steady but things will be active participants in the whole system. Things will communicate with each other, called as things-to-things communication. Things will also able to communicate or interact with human then it is called as things-to-human communication [4].

However the internet of things is not just deep vision for future. It is already here and is having an impact on more than just technological development. These things and communicating objects which used to communicate with the internet can configure themselves independently and can operate without human intervention [3]. Figure 1 shows the architecture of IoT [5].

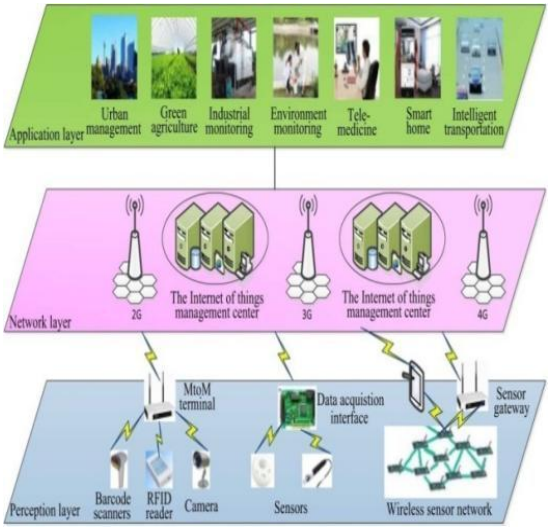

Fig. 1. Architecture of IoT [5]

1.3 Smart Home: A smart home is the home or that living environment having technology to allow all the household devices/home appliances to be controlled automatically and can be controlled remotely [8]. In Smart homes user can easily monitor and control all home devices/home appliances through internet. Home appliances connect in predefined proper network architecture and using standard protocols. Basic idea for Smart Homes using IoT is shown in figure 2 [2].

The whole system can be divided into two parts: in one part consist all the home devices and switch modules and RF transmitter receiver and in second part include all the interface device, processor, data collector, GPRS module that will communicate with the internet.

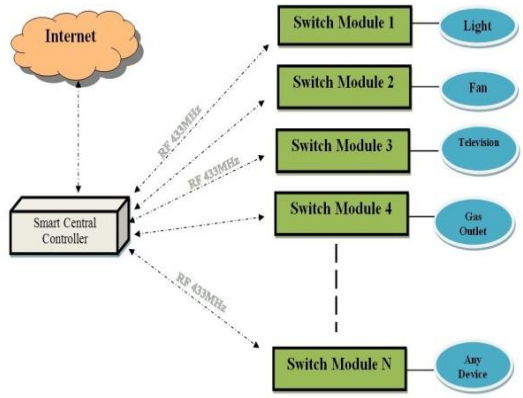

Fig. 2. Basic idea for Smart Home System using IoT [2]

In this paper for consideration only four households devices: Light, Fan, Television, Gas outlet are shown. But in reality user can connects number of devices. These all household devices will connect to the switch modules. Switch module may contain any type of module which changes its state as it received signal. Switch module connected to the device in such a way that when it change the state, the state of household device connects to it will also change [2] [4] [8] [14]. Relays can be used as a switch module. It is an electromagnetic device or normally called as relay switch. It isolates two circuits electrically and connects them magnetically. In basic relay there are three contactors which are normally open (NO), normally closed (NC), and common (COM). COM is normally connected to the NC. At normal condition when household devices is not in working mode then relay is on NO state. When it gets signal then it changes the state to NC and the device will get on working state [9]. Switch modules will connect to the smart central controller through RF transceiver. Each switch module will has one transceiver or one transceiver can also be connects to all switch modules. Each switch module and device will be identified by assigning a unique identity to them. One RF transceiver will connects at the smart central controller. RF modules communicate between themselves at 433MHz. 433MHZ spectrum is specially made for the RF communication [2] [4]. Smart central controller will act as interface device between household devices and internet server. Smart central controller will not be a single device. It will be the set of devices like microcontroller, CPLD processor, RF transceiver, GPRS or Zigbee module, etc. Microcontroller can be used as a main controller and for data processing. Data acquisition can be easily done by microcontroller hence it can be act as interface device [5] [8].

2. RELATED WORK AND METHODOLOGIES USED

Layered architecture of the IoT-based Smart Home System is described by Kang Bing et al., in [8]. The smart home system is divided into three layers: application layer, network layer, and sensing layer. Starting from the bottom, sensing layer is responsible for data collection from all the home appliances and it sends data to the middle layer that is network layer. Network layer uses internet for sending data to the upper most application layer which has different applications on different level for different purposes. For data collection and data processing at the sensing layer it used microprocessor SAMSUNG S3C2440A which is a type of ARM microcontroller [8]. To transfer the collected data to the network layer it uses Zigbee module which is based on IEEE 802.15.4 wireless standard [7-8].

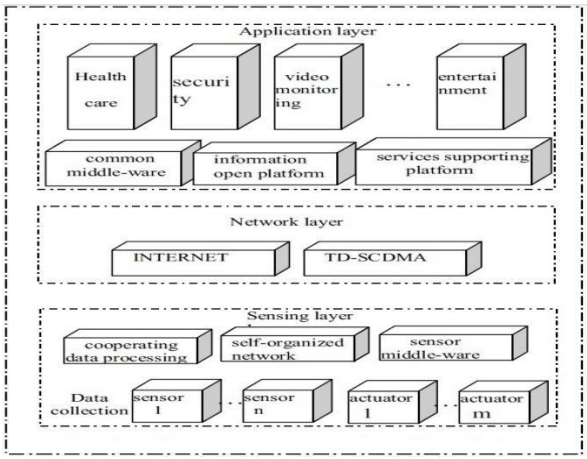

Fig. 3: Layered architecture of the IoT-based Smart Home System [8]

A reconfigurable smart sensor interface device that integrates data collection, data processing, wired and wireless transmission together is already design for industrial Wireless Sensor Network (WSN) in IoT environment using CPLD by Qingping Chi et al., [5].

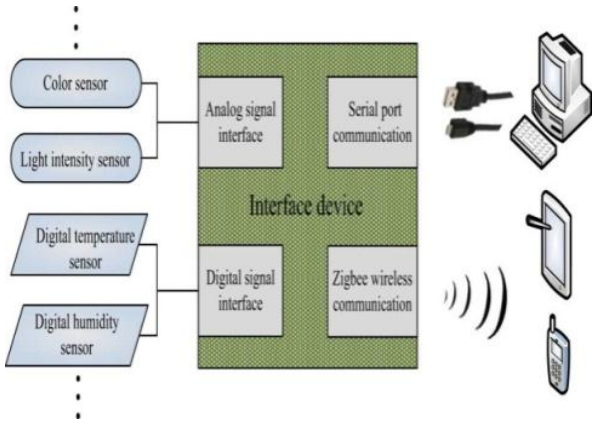

Fig. 4. Reconfigurable Smart Sensor Interface for Industrial WSN [5]

For industrial wireless sensor network in IoT environment the problem is regarding with the data acquisition of multi sensor nodes. If microcontroller is used as the interface device it performs a task by way of

interrupt, which makes these multisensor acquisition interfaces not really parallel in collecting multisensor data though microcontroller has the advantages of low cost and low power consumption. CPLD is a complex programmable logic device. Both microcontroller and CPLD are near about same. But both have their advantages and disadvantages. CPLD/FPGA is used in industrial wireless sensor network. FPGA is a field programmable gate array which has unique hardware logic control; it has real time performance and synchronicity [5]. CPLD/FPGA has more demand because of its advantages over microcontrollers. It is mostly used in wireless sensor network as interface device. CPLD/FPGA can acquire multisensor data in parallel and improves real time performance of the system [5]. Hardware block diagram of CPLD is shown below [5].

The smart home control system uses a smart central controller to set up a radio frequency 433MHz wireless sensor and actuator network (WSAN). Radio frequency modules, switch modules, control modules, etc. have been designed to control directly all kinds of appliances by Ming Wang et al., and Sarita Agrawal et al. The smart system holds the functions of appliance monitor, control and management, home security, energy statistics and analysis [2] [4]. RF identification used by Gaurav Tripathi et al., Ming Wang et al., and Sarita Agrawal et al., in [1] [2] [4] is very useful for security purpose. This technology assigns a unique identity to each household device. So, that, each device can be uniquely identified. Range of the RF can be increased or decreased. It is easy to deploy and has low deployment cost. RFID tags take low power to operate and tags can be active or passive [1] [2].

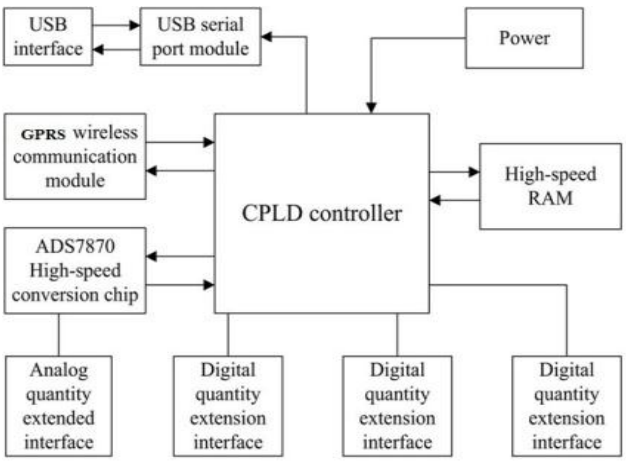

Fig. 5. Hardware block diagram of CPLD [5]

A FPGA based Grid Friendly Appliance (GFA) controller has been already designed by Yu-Qing Bao and Yang Li in [10]. FPGA chips are used to make the GFA controller. GFA has an advantage of used of FPGA chips that it can be used for real time applications [10].

To manage secure and efficient communication between human being and machines is very difficult for smart homes. Tongtong Li, Jian Ren, And Xiaochen Tang gave the architecture and design of Secure Access Gateway (SAG) for home area network [11] which serves as the interface between remote users and managed devices [11].

Lucio Ciabattoni, Gionata Cimini, Massimo Grisostomi, Gianluca Ippoliti and Sauro Longhi have given an interoperability framework which is realized with the software LabVIEW and integrates a real and a virtual environment to enable vertical solutions in different and multi-functional (energy, security, comfort) domotic applications [12]. They have been provided the complete home automation architecture together with details about the implementation of the virtual environment in [12]. Scheme of the developed interoperable Real/Virtual framework is shown in figure below.

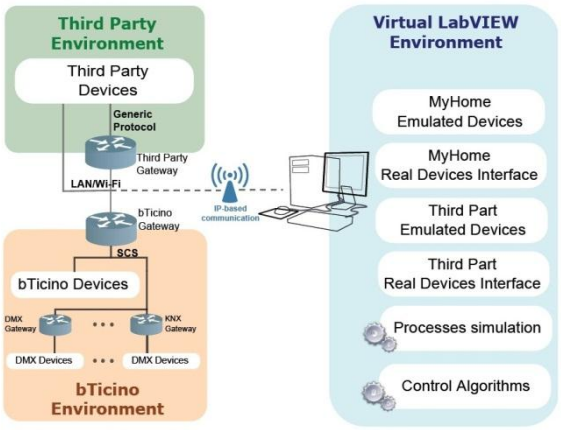

Fig. 6. Scheme of the Developed Interoperable Real/Virtual Framework

For wireless sensor network there are several nodes connected to the internet, hence the problem of security comes. The main problem in this type of network is how to establish the initial session key between the wireless sensor nodes and how to control the center. For the problem of security and issue A lightweight key establishment protocol for the smart home energy management system is proposed in [13] by Yue Li.

M. Al-Qutayri, H. Barada, S. Al-Mehairi, and J. Nuaimi have been also made the system for control and to monitor home appliances using simple PIC Microcontroller and GSM modem in [15]. The system gives the successful output. They use mobile network to monitor and control house hold devices [15].

Basim Hafidh, Hussein AL Osman,Juan Sebastian Arteagafalconi,Haiwai Dong, presents the simple Internet of Things enabler (SITE), a smart home solution thatallows users to specify and centrally control Internet of Things smart objects. Unlike most existing systems,SITE supports

End-User Development. Hence, it defines a simple language for the specification of controlrules for smart objects. It also provides a user interface to graphically illustrate the data received from smartobjects[17].

Every device that connects to the internet needs IP address [3]. People are still working on IPv4 which has very low address space. As number of users increasing people need to move towards IPv6 which offers large address space. Vittorio Miori et al., has proposed an interesting approach of DomoNet, Which is a 'ecosystem" software created to overcome the issues of compatibility with pre-existing systems of smart home, lack of interoperability in smart home system which is due to the fact that current market practice effectively binds consumers to proprietary technologies, thereby forcing them to purchase only devices conforming to a specific manufacturer's system to enjoy full interoperability. DomoNet has been coded using Java language and open source libraries and tools IPv6 and DomoNet link together and work together [3].

For better performance of system and to provide better services by the system network should have the capability of self-organization [6]. Arjun P. Athreya et al., has proposed five key components of self-organization which are as follows [6]:

- Neighbor discovery
- Medium access control
- Local connectivity and path establishment
- Service recovery management

3. PROBLEMS AND CHALLENGES

There are many problems, issues and key challenges could be come in the Smart Home system. As the applications of IoT are increasing rapidly it is difficult to handle all the applications in IoT environment. It comes out problems that how to manage and control these various increasing applications. The whole system could not be more comfortable, secure if these increasing applications not controlled efficiently and conveniently [2]. Security is less on the server side as no special method for authentication is used. This could leads to the insecure system. An attacker can get access to victims home and he would break the whole Smart home system. Connectivity is also the problem could occur [4]. It also comes into challenge that how to achieve connectivity at any place any time [4]. For communication towards internet 3G services are used [8]. But it could have signal problem hence it will not connected every time. The functioning of the smart home system in IoT environment should be done in real time. RF identification is used at 433MHz [1] [2] [4]. It may cause the problem of interference.

Many key challenges have discussed by Dhananjay Singh et al., and Sarita Agrawal et al., in [1] [4].

3.1 Standards: Standardization is very essential for IoT environment as it is expanding globally. Challenges are comes related which standard should be used, which will provide secure medium, how it will make system more reliable.

3.2 Identification: Identification is required for each device so that each device can identify uniquely.

3.3 Privacy: The user's data should be confidential. Connection should be done with providing privacy.

3.4 Authentication: Authentication is must to secure Smart Home system from an attacker. Server has to give access only authentic users.

3.5 Security: The system should able to take appropriate actions on security threats. And system should be able to reconfigure by itself after attacks.

3.6 Integration: The main challenge with IoT is to integrate applications in IoT environment.

3.7 Coordination: Coordination is required between the globally connected objects, humans, programs, process, etc.

3.8 Data Storage: As applications of IoT are increasing, the amount of data getting collected is huge. The challenge is where to storage the huge data. Huge database can solve this problem. Artificial intelligence algorithms must be applied to extract meaning data from redundant data.

3.9 Network Self-Organization: Network structure should be created in such a way that every device connected to it could self-organize them. Actually it is network which should be able to self-organize.

4. CONCLUSIONS

Internet of Things has many applications in different areas. IoT has been already designed for industrial WSN. It has been developed for Smart Homes System. This paper presents the architecture of IoT and architecture of Smart Homes using IoT. There are some problems found in IoT and Smart Homes. New technologies could help to minimize some of them. This paper presents the problems and challenges that could come. New technologies and methodologies which are already used to improve applications of IoT have been discussed in this paper. CPLD controllers, zigbee modules, RF modules are currently in used for IoT.

5 .POSSIBLE RESEARCH DIRECTION

IoT environment and Smart Home System has very low security at the server side. Designing of secure system can be the part of future work. Kerberos technology can be used to make the environment more secure at server side. Artificial intelligence algorithms can be made in future for making easier data extraction process from redundant data. A cloud platform can give revolutionary and potential solutions.

REFERENCES

[1] Gaurav Tripathi, Dhananjay Singh, and Antonio J. Jara, "A survey of Internet-of-Things: Future Vision, Architecture, Challenges and Service", IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 287-292

[2] Ming Wang, Guiqing Zhang, Chenghui Zhang, Jianbin Zhang, and Chengdong Li, "An IoT-based Appliance Control System for Smart Homes", Fourth International Conference on Intelligent Control and Information Processing (ICICIP) June 9 – 11, 2013, pp. 744-747

[3] Vittorio Miori, and Dario Russo, "Domotic evolution towards the IoT", 28th International Conference on Advanced Information Networking and Applications Workshops, 2014, pp. 809-814

[4] Sarita Agrawal, and Manik Lal Das, "Internet of Things – A Paradigm Shift of Future Internet Applications", International Conference on Current Trends in Technology, December, 2011

[5] Qingping Chi, Hairong Yan, Chuan Zhang, Zhibo Pang, and Li Da Xu, "A Reconfigurable Smart Sensor Interface for Industrial WSN in IoT Environment", IEEE Transactions on Industrial Informatics, vol. 10, no. 2, May 2014

[6] Arjun P. Athreya, and Patrick Tague, "Network Self-Organization in the Internet of Things", IEEE International Workshop of Internet-of-Things Networking and Control (IoT-NC), 2013, pp. 25-33

[7] Moataz Soliman, Tobi Abiodun, Tarek Hamouda, Jiehan Zhou, and Chung-Horng Lung, "Smart Home: Integrating Internet of Things with Web Services and Cloud Computing", IEEE International Conference on Cloud Computing Technology and Science, 2013, pp. 317-320

[8] Kang Bing, Liu Fu, Yun Zhuo, and Liang Yanlei, "Design of an Internet of Things-based Smart Home System", The 2nd International Conference on Intelligent Control and Information Processing, July 2011, pp. 921-924

[9] Vladimir Gurevich, "Electric Relays Principles and Applications", Taylor and Francis Group, 2006, pp. 1-52

[10] Yu-Qing Bao and Yang Li, "FPGA-Based Design of Grid Friendly Appliance Controller", IEEE Transactions On Smart Grid, Vol. 5, No. 2, March 2014, pp. 924-931

[11] Tongtong Li, Jian Ren, and Xiaochen Tang, "Secure Wireless Monitoring And Control Systems For Smart Grid And Smart Home", IEEE Wireless Communications, June 2012, pp. 66-73

[12] Lucio Ciabattoni, Gionata Cimini, Massimo Grisostomi, Gianluca Ippoliti and Sauro Longhi, "An Interoperable Framework for Home Automation Design, Testing and Control", 22nd Mediterranean Conference on Control and Automation (MED) University of Palermo, June 16-19, 2014, pp. 1049-1054

[13] Yue Li, "Design of A Key Establishment Protocol for Smart Home Energy Management System", Fifth International Conference on Computational Intelligence, Communication Systems and Networks, 2013, pp. 88-93

[14] Chao-Lin Wu, Yi-Show Tseng, and Li-Chen Fu, "Spatio-Temporal Feature Enhanced Semi-supervised Adaptation for Activity Recognition in IoT-based Context-aware Smart Homes", IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, 2013, pp. 460-467

[15] M. Al-Qutayri, H. Barada, S. Al-Mehairi, and J. Nuaimi, "A Framework for an End-to-End Secure Wireless Smart Home System", IEEE International Systems Conference Montreal, Canada, April 7-10, 2008

[16] M. R. Alam, M. B. I. Reaz, and M. A. M. Ali, "A review of smart homes–Past, present, and future," IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.,vol. 42, no. 6, pp. 1190–1203, Nov. 2012.

[17] Basim Hafidh, Hussein AL Osman, (Member, IEEE),Juan Sebastian Arteagafalconi, (Senior Member, IEEE),Haiwai Dong, (Senior Member, IEEE),Abdulmotaleb El Saddik, (Fellow, IEEE," SITE: The Simple Internet of Things Enabler for Smart Homes",IEEE Access Year: 2017, Volume: 5 Pages: 2034 - 2049, DOI: 10.1109/ACCESS.2017.2653079IEEE Journals & Magazines