THINK INDIA JOURNAL

ISSN:0971-1260
Vol-22-Issue-34-December -2019

Comprehensive Study of Internet of Things- Requirements and Key Research Challenges

Dushyant Kumar Singh[1], Himani Jerath[2*]

1 HOD, Embedded System,Lovely Professional University, Phagwara, Punjab

2 Assistant Professor, Embedded System,Lovely Professional University, Phagwara, Punjab

dushyant.kumar@lpu.co.in, himani.22788@lpu.co.in

Abstract

Today internet is easily accessible to most of the population of world. And with the increase in accessibility of the internet and advancement in the technology, Internet of Things (IoT) has emerged as one of the hot research topics with infinite opportunities and is penetrating in all applications areas like consumer electronics, health care, industrial automation, smart homes, public administration, mobile healthcare, smart grids, intelligent energy management, traffic management and many others. But as with the other technologies, IoT also comes with its own design challenges and security issues. This review paper presents the various requirements for IoTsystem and architectures, research challenges in IoT and security issues connected with IoT.

Keywords— Internet of Things(IoT), IoT architecture, IoT Design, IoT Security

I. INTRODUCTION

With the IoT the form of the communication has been revolutionized. The generic form of communication is either human to human or human to machine but IoT has given rise to machine to machine (M2M) communication giving great future to internet [1]. The first application of IoT was developed in 1982 as modified coke machine enabling it to report about the drinks contained and their temperature. The machine was connected to internet for the purpose of reporting about drinks contained and its temperature. Thereafter in 1991, ubiquitous computing concept to IoT was given by Mark Weiser. In 1999, Bill Joy discussed about Device to Device communication and Kevin Ashton gave the term Internet of Things (IoT) in the same year [1].

IoT is interconnected network of everyday object which may also be considered as self-configuring wireless network of objects. It allows the everyday objects, embedded with electronics, to be sensed and controlled remotely through network. By connecting the numbers of objects to internet makes it dynamic global network with ability of self-configuration [2]. In [3] IoT has been viewed in three paradigms - internet oriented (middleware), things oriented (sensors), and semantic oriented (knowledge) [4]. The IoT covers the various aspect of extending the internet in to the physical world with the deployment of various distributed devices having embedded identification. IoT gives the concept of linking the digital entities with the physical on through suitable information and communication technology, thus giving a whole new area of applications.

ISSN:0971-1260
Vol-22-Issue-34-December -2019

The idea being the IoT device is to exchange the valuable information between uniquely identifiable real world devices equipped with leading technology like Wireless Sensor Network (WSN and Radio-Frequency Identification (RFID) which is to be processed for decision making [1]. IoT is to integrate the physical devices with cyber physical infrastructure by embedding the electronics in to the everyday objects and making them 'smart''. In this context IoT may be refer to I) a global network connecting the smart objects through extended internet technologies. II) set of technologies need to support such vision III) opening the new opportunities in market and business with the different applications and services exploiting such technologies[4].

The IoT in the near future will make it possible that everyday object will be equipped with microcontrollers; transceivers for communication and required protocol making them enable to communicate with each other and also with the users. This will make the internet more immersive and pervasive. The heterogeneous application fields of IoT such as applications areas like consumer electronics, health care, industrial automation, smart homes, public administration, mobile healthcare, smart grids, and intelligent energy management make it a daunting challenge to identify a solution capable of satisfying the requirement of all possible applications. This sometimes leads to propagation of different or sometimes incompatible solution of practical implementation of IoT systems [5].

The present review on IoT presents the implementation requirement for IoT systems in section 2. Looking into the various heterogeneous application areas, it is always challenging to design a common solution for the IoT applications, which leads to various design challenges and security issues associated with IoT which are presented in section 3 under Key Research Challenges in IoT. Section 4 concludes the finding of the paper.

II. REQUIREMENT FOR IOT IMPLEMENTATION

The basic and key feature of IoT is embedding of computing and communication features into everyday objects. An IoT system should be fulfilling the following requirements:

A. **Scalability:** In 2013about 9 billion interconnected devices were there andby 2020 it is expected to rise by 24 billion devices [3]. It is perception that every device has its own virtual representation and with that many devices interconnected through IoT infrastructure, scalability is desired in IoT architecture for future new IoT applications [6].

B. **Interoperatability:** IoT consists of the heterogeneous application areas and IoT objects may communicate from various service networks. Therefore in order to empower the IoT devices to communicate from various networks too all types of IoT application, interoperability is desired [6].

C. **Identification:**In IoT each object need to be identified specifically. The object may be identified as individual or as belonging to a class like object is pen without the details of what type of pen. This may be achieved by means of RFID tags or any suitable method, but identification of object is desired [2].

D. **Sensing/Actuation:** Sensing and actuation is desired to interface the IoT device with physical world. Device can be interfaced with physical environment through passively thus performing sensing or actively hence performing action[2].

E. **Resource Control and Management:**The various devices participating in IoT application must be remotely operating as this will help in controlling the device remotely when operator is not

ISSN:0971-1260
Vol-22-Issue-34-December -2019

present at site. Along with this constraint of resource redundancy may affect the IoT application and is required to balance the load for proper resource utilization[6].

F. **Energy Efficiency:**The life time is the most important for smart objects, moreover the energy consumption of networks is also increasing day by day with the increase in data rate and are, hence energy efficiency and green technology of the IoT enabled devices is desired[6][7].

G. **Quality of Service(SoC):** Quality of Service is also an import anent requirement of IoT architecture. QoS isnonfunctional facility factor which can be obtained by organizing the service provided and retrieval. For instance, Real Time Systems imposes requirement of high precedence for particular performance and it is desired that only compulsory information to be retrieved in response to the addressed request [6].

H. **Security:** Security is the most important aspect for IoTobjects which may lead to physical damage and data as the information is to be transferred and processed in hostile environment[6][7].

III. KEY RESEARCH CHALLENGES IN IOT

The future of the IoT faces many challenges and needs deliberation by the expert to address these challenges. Some of the key research challenges in IoT are listed below:

A. Computing, communication and identification:

IoT is envisioned as development of the technique to transform a device to smart device and making them capable for communication, computing and identification. The process of distributing computation in order to reduce communication overhead is called as in-network processing or computing [4]. The existence of interconnected links between the objects in IoT need research consideration with existing tools, methods [8]. There are many possible solution proposed like RF front end activation pattern i.e. sleep period, integrating energy harvesting from several sources for sensors like solar, piezocrystals and others [4]. IoT is very heterogeneous network with variety of devices from various application areas. Thus complicates the process of communication amounts the IoT nodes resulting in fraud ant, delayed communication [9][10]. IoT also suffers from the challenge of identity management which requires the unique identity for the all the physical devices. The current technology deploys is short range RF identifiers. As the IoT includes very large number nodes which are expected to increase in the coming future and further research is needed in the identification for IoT node to operate in a dynamic heterogeneous network[4][8][7]. The IPv4 protocol uses only 4 - byte address so new addressing policies is needed in which IPv6 may be strong contender [8]. Ultimately there is need of an IoT architecture that can support low power, low cost and yet fully functional network and devices that too compatible with well-established communication technologies and standards,, addressing of the huge number of the devices connected to IoT [4][8]

B. Network Technology:

The IoT consists of connecting the devices from various networks in which user happens to be human, machines. WSN happens to be the dominant network technology in IoT [8][5]. With the

ISSN:0971-1260
Vol-22-Issue-34-December -2019

large number of device connected to IoT infrastructure, it is going to face many challenges like providing service to the different types of IoT connected devices. Thus there is a requirement of scaling up the IoT architecture in order to handle the large number of devices [15]. Interoperability of IoT devices amongst the various service providers is also important. The technical challenges in interoperability are standards, protocols, semantics challenges is to ensure that every node in IoT architecture is trustworthy for processing and handling the data and pragmatic challenges are design a strategy for realization of ability in IoT system to observe the intention of participating elements [15].Protocol forms the backbone for data tunnel between IoT node and outer world. Many energy efficient MAC protocols are proposed like TDMA (collision free), FDMA(collision free with additional circuitry), TCP/IP, Ipv4 and IPv6 for node addressing but none of them are suitable as more 'things' available in IoT[5]. Research focus is needed on exploitation of networks for IoT, scalability of network infrastructure, interoperability of networks, identifying the new protocols to handle the network traffic with more devices added, adaptability to heterogeneous networks environment[5][8][15].

C. **Greening of IoT:**

The network nodes in IoT need or expected to be independent, battery operated and life span is most important in smart objects participating in IoT application. Energy consumption increases with the computational capabilities and high rate transmission of data. In near future IoT will lead to significant increase in the energy consumption, thus there emerges the need and research for energy efficient sensing and green energy to make the network devices more energy efficient [[5]13][15].

D. Security:

In IoT security of the embedded devices along with the data is the major issue and challenge. As of embedded system, security is not at all new but as more and more devices is connected potential threat to security scales up [14]. In IoT as all the devices are connected to each other and IoT architecture is complex because of heterogeneity in IoT applications which provided the attackers platform to invade the system[10][15]. IoT architecture suffers from numerous device or network based security issues like object safety and security, data confidentiality, unauthorized access, network security and security due to diversity in the IoT applications[1][5][6][8][9][11][12][13].

E. Diversity:

IoT is a heterogeneous network and almost every application nowadays intends to use IoT network. As a result market is being flooded with IoT devices with fewer safety checks and it has been observed that more than 90% of the devices suffer from firmware security vulnerability. The challenge is that it is difficult to design a common security system for such diverse IoT devices [9].

F. Object safely and security:

IoT objects may spread over large geographical area in which they can be easily accesses by the attackers. So they need to be protected against the physical damage and logical attack by the malicious entities [12][13].

ISSN:0971-1260
Vol-22-Issue-34-December -2019

G. Data confidentiality and unauthorized access:

Data confidentiality and unauthorized access represents the fundamental security issues in IoT architecture. It includes defining the access control and object authentication process. Data confidentiality seems more relevant in business context, as data confidentiality may be important to protect the competitiveness and market values [1].

Also in IoT devices sensors provides the data for processing and it is required to have proper encryption technique for data transmitted to maintain data integrity. The threat associated with the may be more logically represented in the figure below [9]:

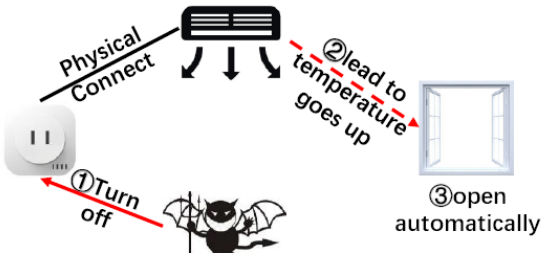

Figure 1: Block Diagram showing an IoT system

Many access control has been proposed to ensure authentication widely used is Role Based Access System (RBAS)[1]. The main advantage of RBAC is that the access rights can be changed based on the role assigned to the user. RFID is the main authorization technology and with more and more devices being integrated in IoT, RFID lacks in proper authentication mechanism[6][13].

H. **Network and Routing Information Security:**

In IoT data from large number of sensors travels over the diverse network through wired or wireless links using various routing protocols like TCP/IP. The network should be able to handle the data and provide the security against the external interference or monitoring[6]. Routing information attacks mainly focus on routing protocols of IoT, which may lead to extended source path and end to end delay in transmission. This lead to requirement of secure network protocols to establish secure link among IoT devices and provide quality services [13].

IV. CONCLUSION

In the last few years IoT has emerged as hot research and application area. The concept behind the IoT is to embed the intelligence to the object so that they can communicate autonomously and can exchange information. IoT is transitions human - human communication to human to machine and machine to machine communication. This paper presents the major requirements for the implementation of IoT system and finally addresses the various research and implementation challenges faced by the IoT technology. Deployment of IoT solution could be hard and will bring more serious security problems and other challenges. This creates the new era of research in which efforts and focus of the researchers is desired to solve the presented issues by IoT. In addition to challenges offered, IoT will be significantly benefitting persons, professionals and economics in the near future.

ISSN:0971-1260
Vol-22-Issue-34-December -2019

REFERENCES

[1] Farooq,M.U.Waseem,M. Mazhar,S. Khairi,A. and Kamal,T,"A Review on Internet of Things (IoT)", International Journal of Computer Applications,Vol.113 No.1,PP:1-7, 2015.

[2] Monika, and R. Sharma, "Research paper on Internet of things" .International Journal in Multidisciplinary and Academic Research, Vol. -6, No. 3, PP:1-7, 2017

[3] Gubbi,J.Buyya,R.Marusic,S. and Palaniswami,M, "Internet of Things (IoT): A vision, architectural elements, and future directions", Future Generation Computer Systems,Vol. 29, PP: 1645-1660, 2013.

[4] Mirondi,D.Sicari,S.Pellegrini,F.D. and Chlamtac,I, "Internet of things: vision, application and research challenges", Adhoc Networks,Vol:10, PP:1497-1516, 2012.

[5] Zanella,A. and Vangelista,L, "Internet of Things for Smart Cities", IEEE Internet of Things Journal, Vol:1, PP:22-32, 2014.

[6] Burhanuddin ,M.A. Mohammed,A.A.Ismail,R. and Basiron,H, "Internet of Things Architecture: Current Challenges and Future Direction of Research",International Journal of Applied Engineering Research, Vol:12, No.21, PP:11055-11061, 2017.

[7] Kahan R, Khan S.U, Zaheer R and Khan S, "Future Internet: The Internet of Things Architecture, PossibleApplications and Key Challenges", In: 10th International Conference on Frontiers of Information Technology, Islamabad: IEEE Xplore, PP: 257-260, 2012.

[8] Ray P.P, "A survey on Internet of Things architectures", Journal of King Saud University – Computer and Information Sciences, 30, PP:291-319, 2018.

[9] Khalid A, "Internet of Thing Architecture and Research Agenda", International Journal of Computer Science and Mobile Computing, Vol. 5 No. 3, PP: 351-356, 2016.

[10] Jindal F, Jamar R and Churi P, "Future and Challenges of Internet of Things", International Journal of Computer Science & Information Technology, Vol. 10, No.2, PP: 13-25, 2018.

[11] Lin J, Yu W, Zhang N, Yang X, Zhang H and Zaho W. "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications", IEEE Internet of Things Journal, Vol. 4, No. 5, PP: 1-17, 2017.

[12] Zhou W, Zhang Y, and Liu P, "The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved", IEEE Internet of Things Journal, Vol. 6, No. 2, PP: 1606-1616.

[13] Suo H, Wan J, Zou C, and Liu J, "Security in the Internet of Things: A Review", In: International Conference on Computer Science and Electronics Engineering, Hangzhou: IEEE Xplore,Vol. 3, PP: 648-651, 2012.

[14] Babar S, Stango A, Prasad N, Sen J, and Prasad. R, "Proposed Embedded Security Framework for Internet of Things (IoT)", In: 2nd International Conference on Wireless Communication, Vehicular-Technology, Information Theory and Aerospace and Electronics System Technology(Wireless VITAE), Chennai:IEEE Xplore, 2011.

[15] Ukil A, Sen J. and Koilakonda S, "Embedded Security for Internet of Things", In: 2nd National Conference on Emerging Trends and Applications in Computer Science, Shillong:IEEE Xplore, 2011.

ISSN:0971-1260
Vol-22-Issue-34-December -2019