Analysis on IoT Challenges, Opportunities, Applications and Communication Models

Narasimha Swamy S[1], Shantharam Nayak[2], Vijayalakshmi M N[3]

[1,3]Department of Master of Computer Applications, R V College of Engineering, Bengaluru, India
[2]Department of Information Science and Engineering, R V College of Engineering, Bengaluru, India

Abstract— *Internet of Things (IoT) is a novel communication standard and it is researcher's preferred topic, which integrates heterogeneous systems seamlessly. Designing a universal architecture for IoT is a challenging task due to the integration of wide variety of the devices. The main objective of this paper is to provide comprehensive knowledge on challenges, applications, Security issues, and different communication models of IoT. This paper also focuses on the marketing trends of IoT with respect to variety of application with the end users. This motivates the researchers to contribute more productive work in this field by analyzing various parameters.*

Keywords— IoT, Security, Sensors Networks, Cloud computing, RFID.

I. INTRODUCTION

The number of devices that are connecting to the internet is increasing exponentially day by day. This leads to new communication standard in internet know as Internet of things (IoT). The typical idea behind IoT includes smart devices like refrigerators, street lights, washing machine, air conditioners, cars and etc., these are equipped with sensors and Radio Frequency Identification (RFID) tags [1].Cutting-edge communication practices like cloud computing, Wi-Fi and Wimax are used as communication medium between the IoT and smart devices [2][3].

IoT is an integration of wide variety of smart devices, and influencing human routine towards, e-health, e-learning, remote monitoring, surveillances. Similarly, IoT plays a key role in industries such as automation and intelligent industrial manufacturing, smart logistics, smart transportation and many [4].

The public, industries and government are the important stakeholders of IoT. At this stage, IoT requires promotional policies to build a new network models. The aim of IoT is 'Value Up' the data and 'Cost Down' models.

II. UNDERSTANDING IoT

It is easy to understand architecture of IoT. The figure1 illustrate the layered structure of an IoT. The Architecture of the IoT comprises of three important layers perception layer, network layer and application layer. The perception layer allows recognizing and accumulating data from the smart devices. The data broadcast from source to destination is done by transport layer using the communication standards like Wi-Fi, Wimax, GPRS and Zigbee technologies.

Application Layer
Transport/Network Layer
Perception Layer

Fig .1: Three Layered Architecture of IoT

The topmost layer in IoT is application layer, where large number of applications runs. IoT includes three different stages:

1. The device accumulates data from other devices. This stage also includes identification of devices and addressing the devices.
2. An IoT application accumulates data and analyses the data for further consolidation.
3. Decision making technique may accomplish with the help of analytical engines and big data. Once Decision making technique is completed the data is transmitted to the server.

III. PILLARS OF IoT

The Fig.2 illustrate the pillars of IoT

<table>
<tr><td colspan="3">Internet of Things Policy</td></tr>
<tr><td colspan="3">Standards</td></tr>
<tr><td>R & D and Innovation</td><td>Capacity Building and Incubation</td><td>Demonstration Centres</td></tr>
</table>

Fig. 2: Pillars of IoT

R&D and Innovation

R&D in IoT needs more fund to develop specific social application through call for proposal. Identify core members of IoT in R&D and start developing the open source projects using cloud and collaborative R&D.

conduct the tests to integrate hardware to hardware (H to H) and hardware to software (H to S).

Capacity building and Incubation

This includes implementing IoT test-bed suit for homogeneous and heterogeneous devices. This enables academic and research community to get benefit by doing the experiments and to improve the knowledge of IoT software and hardware infrastructure. This helps scientific community to enhance their knowledge about IoT. This encourages individual students to do research and to enhance the IoT technology by conducting training and workshops.

Exhibition centre

Demonstration centers are required to develop the domain specific applications such as industrial monitoring, smart cities, agriculture, healthcare, smart homes, forest and wild life, natural disasters, automotive, safety and security etc. This helps to get into the real time application from theoretical concepts.

IV. CHALLENGES IN IoT

Architecture: The wide varieties of applications from state full to stateless from resource constrained to resource freedom and from simulation to real time applications are the part of IoT. These may be infeasible to have a standard architecture for IoT applications, example, Sensor based identification architecture is different from RFID based identification [5].

Routing: Routing of information plays very important role in delivering the information to the destination irrespective of the network.

1. Positioning of nodes in IoT is challenging task because of changing topology, mobility, nodes may be attach or detach to various networks [5].
2. Different Networking Standards are the major task in routing of information in IoT. IoT uses different communication standards such as Zigbee, Wimax and Wi-Fi etc. The working principles of each and every technology are different and they use diverse protocol stacks [5].
3. Maintaining the Network Connectivity is a major challenge because of limited battery power and mobile nodes. Whenever node failure occurs and mobile node detached from the network the topology has to be reconstructed [5].

Fault Tolerance: The faults may occur due to environmental factors, deployment mechanisms or energy constraints devices. These may affect the overall performance of the network. So there is a necessity of some mechanism, which should be adopted in the routing protocols to handle such unexpected events [5].

Security: The goals of the network and information security are to achieve confidentiality, integrity and availability of information. This can be achieved using cryptographic algorithms but care should be taken while implementing the cryptographic algorithms for IoT because cryptographic algorithms include more calculations, since IoT comprises of resource constraint devices [5]. RFID tag information security, wireless communications information security, network transmission of information security, privacy, and information processing security are the unknown dangers in IoT [6].

V. APPLICATIONS OF IoT [1] [7] [8]

Committees for European Nano Electronics (CEN), Committee for European Electro technical Standardization (CENELEC), (ETSI) are the three European bodies playing the vital role in developing the standards for the IoT applications. The concept of IoT can be easily adaptable. Some of the applications of the IoT are:

Vehicle Traffic Control: In Traffic control application vehicles like cars, bus, trains, roads and street lights are equipped with the sensors and RFID tags to share traffic information.

Smart homes and offices: IoT play a vibrant role in smart homes and offices by controlling the room temperature and room lightning by scheduling it remotely.

Smart Cities: One can use the IoT in smart cities to minimize the parking problems and monitoring the physical condition of the building and bridges.

Health care: Health care sector is also a part of IoT. In this application sensor monitors the condition of the patient and forward the gathered information to the concerned doctor.

Energy: IoT is used to monitor and manage usage of the non-renewable resources like gas, coal, petrol and etc.

Environment: IoT also helps in managing the natural disasters like earthquakes, floods, volcanic eruptions and etc.

VI. MARKETING TRENDS

Unexpectedly, US National Intelligence Council (NIC) included IoT in the list of six ‘‘Disruptive Civil Technologies” by US national power [4] [9]. NIC forecasts that “By 2025 daily use things like furniture, food packages, important paper documents, and more are equipped with the internodes”. It focuses on forthcoming opportunities [4] [9].

IoT is the promising technology in future because it can be adopted easily with the existing technologies. Markets and Markets predicted that the size of the IoT in

manufacturing field grows to USD 13.49 Billion by 2020 from USD 4.11 Billion in 2015, at a compound annual growth rate (CAGR) of 26.9%. IoT is the solution for the manufacturing and other industries because, which increases the Functional efficiency of the industries. The IoT becomes very popular and successful for, efficient usage of sensors over enhanced automation and the hardware and connecting devices are available for low cost [4].

Recently TechSci released a study report called "India Internet of Things (IoT) Market Opportunities & Forecast, 2020", according to study report IoT market in India projected to progress at a CAGR more than 28% during 2015 - 2020.

Real-time security, monitoring and analytics are part of the IoT manufacturing industry which enhances the operational effectiveness. The biggest share of IoT is taken by the manufacturing industry to management the data during 2015 and it was predicted that IoT dominates the market in future. Radio Frequency Identification (RFID) leads the connectivity technology in IoT manufacturing industry. This development is due to reduction in the cost of connectivity devices and hardware across North America, Europe and Asia-Pacific (APAC) regions. Near Field Communication (NFC) is one of the evolving technologies in wireless communication, which can be used to communicate among the nodes in short-range.

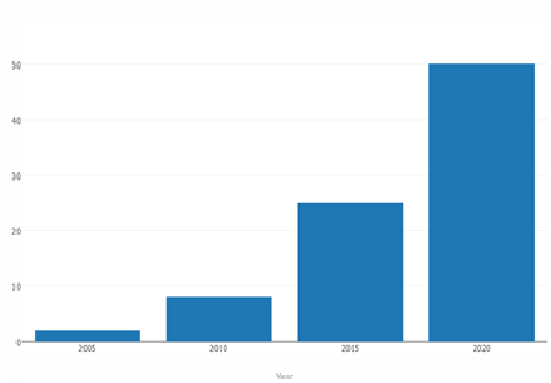

Fig .3: Number of People connected using IoT

Communication Models in IoT [10]

Internet Architecture Board (IAB) in March 2015 released an architectural document for IoT, which includes four communication models used by IoT. The key characteristics of the communication models details are presented in below discussion.

Device to Device Communication

In this model two or more smart devices communicate directly among one another, rather than communicating through an intermediate application server. This communication model uses the Bluetooth, Z-Wave, or Zigbee as communication media.

The applications like home automation systems and health care systems uses the device to device communication model. The home automation application includes tiny data packets to communicate between devices. Small IoT devices like tube lights, street lights, washing machines, and air conditioners normally exchange the smaller amount of information.

Device to device communication models are not well-suited with the communication protocols; the communicating devices should use the same type of the protocols. For example, Bluetooth family smart devices are not natively compatible with the Zigbee family of devices [10]. The Fig. 4 gives the idea behind the device to device communication model.

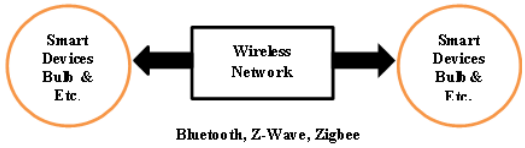

Fig. 4: Device to Device Communication Model

Device-to-Cloud Communication

In this communication paradigm the IoT smart devices exchange the data and control the flow of traffic by directly connecting to the cloud. The concept behind the device-to-cloud communication model is illustrated in the Fig. 5.

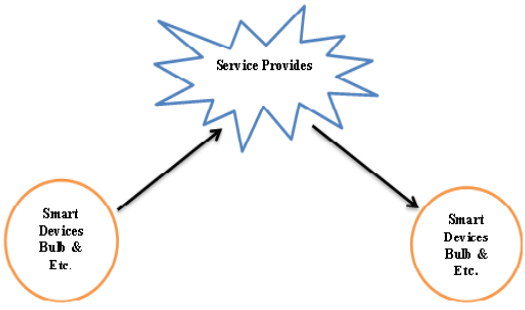

Fig. 5: Device-to-Cloud Communication Model

Ethernet or Wi-Fi is the most commonly used communication standards used by the device-to-cloud communication model in order to establish connection between the cloud service and the smart device.

This technology was adopted by Samsung Smart TV's. The smart TV's uses the internet technology in order to send the user viewing interest information for analysis.

Device-to-Gateway Model (AGLM) [10]

Device-to-gateway model is also recognized as the Device-to-application-layer gateway model. In this model

a local gateway acts as an intermediate between smart devices and the gateway is loaded with the application software.

In this model a local gateway device runs application software and it acts as an intermediate between the smart device and cloud service. The local gateway device provides the functionalities like security and data/ protocol translation. This model is used in the smart cities, smart homes and etc. [10].The Fig. 6 gives the more knowledge on device-to-gateway model.

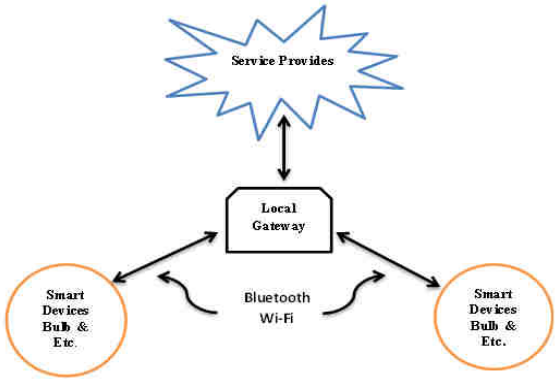

Fig. 6: Device-to-Gateway Model

Back-End Data-Sharing Model [10]

This communication architecture enables users to transfer and scrutinize smart device data from a cloud service in grouping with data from additional sources. This architecture enables "third parties to access the uploaded sensor data". Back-end data-sharing model was derived from single device-to-cloud communication model, in this model "The data can be uploaded by IoT smart devices to a single application service provider''. This model also enables aggregation of data and analysis of data. The Fig. 7 gives the knowledge on back-end data-sharing model.

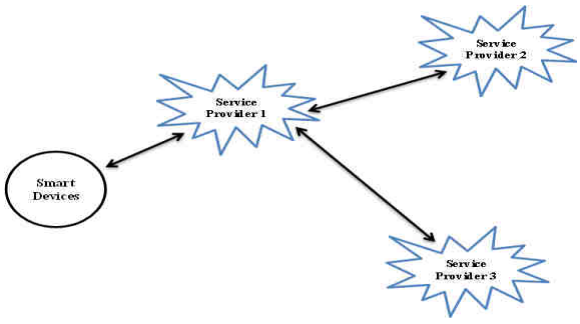

Fig. 7: Back-End Data-Sharing Model [10]

VII. CONCLUSION

Internet of Things has gained lots of impact in recent trends; this impact may be due to the trends in wireless communication and embedded devices connected over internet. The review presented here focused on studying the basic necessary aspects in IoT. This review may be useful for researcher interested in contributing in the field of IoT. This paper highlighted the architectural concepts, challenges, and real time applications in IoT. A glimpse of marketing trends of IoT and the most commonly used communication models are also discussed in this review.

REFERENCES

[1] Samia Allaoua Chelloug, Energy- Efficient Content-Based Routing in Internet of Things, Networks and Communication Systems Department, College of Computer and Information Sciences, Princess Nourah Bint Abdul Rahman University, Riyadh, KSA, Journal of Computer and Communications, Dec-2015, 3, 9-20.

[2] Souza, A.M.C. and Amazonas, J.R.A. (2015) A New Internet of Things Architecture with Cross - Layer Communication. Proceedings of the 7th International Conference on Emerging Networks and Systems Intelligence Emerging 2015, Nice, 19-24 July 2015, 1-6.

[3] Michael, M.P. (2007) Architectural Solutions for Mobile RFID Services on Internet of Things.

[4] Atzori, L., Iera, A. and Morabito, G. (2010) The Internet of Things: A Survey. Computer Networks, 54, 2787-2805.http://dx.doi.org/10.1016/j.comnet.2010. 05.010

[5] Amol Dhumane and Dr. Rajesh Prasad, Routing Challenges in Internet of Things, CSI Communications, January 2015.

[6] Chen Qiang, Guangri Quan, Bai Yu and Liu Yang, Research on Security Issues of the Internet of Things, International Journal of Future Generation Communication and Networking, Vol.6, No.6(2013), pp.1-10, http://dx.doi.org/10.14257/ijfgcn.2013.6.6.01.

[7] Jia, X., Feng, Q., Fan, T., and Lei, Q. (2012) RFID Technology and Its Applications in Internet of Things (IoT).2012 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), Yichang, 21-23 April 2012, 1282-1285.http://dx.doi.org/10.1109/CECNet. 2012.62015 08.

[8] Kopetz, H. (1997), Real-Time Systems: Design Principles for Distributed Embedded Applications. Real-Time Systems Series, Springer, New York.

[9] National Intelligence Council, Disruptive Civil Technologies – Six Technologies with Potential Impacts on US Interests Out to 2025 – Conference Report CR 2008-07, April 2008, http://www.dni.gov/nic/NIC_home.html.

[10] https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.