IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 3, March 2016

IOT-An Overview

Anupama Kaushik

Assistant Professor, Department of IT, Maharaja Surajmal Institute of Technology, Delhi, India

Abstract: The Internet of Things (IOT) refers to the environment where network connectivity and computing capability extends to objects, sensors and everyday items not normally considered computers. These items are then capable to generate, exchange and consume data with minimal human intervention. This paper gives an overview of Internet of Things (IOT).

Keywords: Internet of Things (IOT);

I. INTRODUCTION

The Internet of Things (IOT) is an emerging topic which includes the entire world. This technology includes a wide spectrum of networked products, systems, and sensors, which take advantage of advancements in computing power, electronics miniaturization, and network interconnections to offer new capabilities not previously possible. It is going to transform many aspects of the way we live. For consumers, new IoT products like Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the "smart home'', offering more security and energy efficiency[1].Other personal IoT devices like wearable fitness and health monitoring devices and network enabled medical devices are transforming the way healthcare services are delivered. This technology promises to be beneficial for people with disabilities and the elderly, enabling improved levels of independence and quality of life at a reasonable cost [1].

So, now the question is "What will be the platform that support such an environment?". The answer is "Internet should become utility now".

IoT will not be seen as individual systems, but as a critical, integrated infrastructure upon which many applications and services can run.

K. Rose in 2015 [1] gave reasons that why IOT is possible. It is possible due to :

- Ubiquitous Connectivity: Now-a-days the connectivity is everywhere due to low cost and high speed pervasive networks.
- Widespread adoption of IP–based networking: IP has been widely used and it has become a global standard for networking. It provides a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively.
- Computing Economics: Driven by industry investment in research, development, and manufacturing, Moore's law continues to deliver greater computing power at lower price points and lower power consumption. According to Gordon Moore, the number of transistors per square inch on integrated circuits doubles roughly every two years, allowing more processing power to be placed into smaller chips over time.
- Miniaturization: Due to advances in manufacturing, cutting-edge computing and communications technology is incorporated into very small objects. With greater computing power there is an advancement of small and inexpensive sensor devices, which drive many IoT applications.
- Advances in Data Analytics: Due to new algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.
- Rise of Cloud Computing: Cloud computing, which provides remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.

So, the IoT is the convergence of a variety of computing and connectivity trends that have been evolving for many decades.

The paper is organised as follows: Section II describes IOT communication model; Section III describes IOT in research and Section IV provides the conclusion.

II. IOT COMMUNICATION MODEL

In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452),[2] which outlines a framework of four common communication models used by IoT devices.

1. Device to Device Communications:

In this, two or more devices can directly connect and communicate with each other rather than through intermediate application server. They can communicate using different types of networks and they use protocols like Bluetooth [3], Z-wave [4] or Zig Bee [5] to establish direct device-to-device. This communication model is commonly used in applications like home automation systems, which typically use small data packets of information to communicate between devices with relatively low data rate requirements. But this device-to-device communication approach illustrates many of the interoperability challenges.

DOI 10.17148/IJARCCE.2016.53264

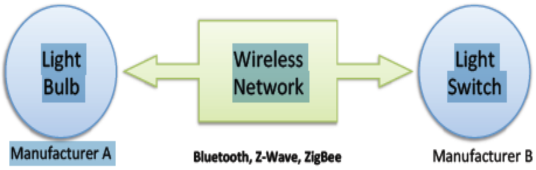

Fig.1. Device-to-Device Communication Model.

2. Device to Cloud Communications :
In this communication model, the IoT device connects directly to an Internet cloud service like an application service provider to exchange data and control message traffic. This approach uses existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which connects it to the cloud service. This communication model is employed by some popular consumer IoT devices like Samsung *SmartTV* [6] . With the Samsung *SmartTV* technology, the television uses an Internet connection to transmit user viewing information to Samsung for analysis and to enable the interactive voice recognition features of the TV.

Here again, interoperability challenges can arise when attempting to integrate devices made by different manufacturers. But this model adds value to the end user demands as the capability of the product is extended beyond its features.

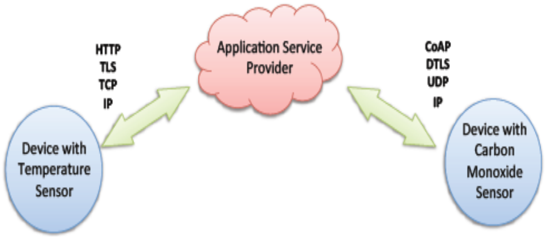
HTTP
TLS
TCP
IP
Application Service Provider
CoAP
DTLS
UDP
IP
Device with Temperature Sensor
Device with Carbon Monoxide Sensor

Fig.2. Device-to-Cloud Communication Model.

3. Device to Gateway Model :
In this model the IoT device connects to application-layer gateway which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation. This model is found in many consumer devices. For example, items like personal fitness trackers do not have the ability to connect directly to a cloud service, so they frequently rely on smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

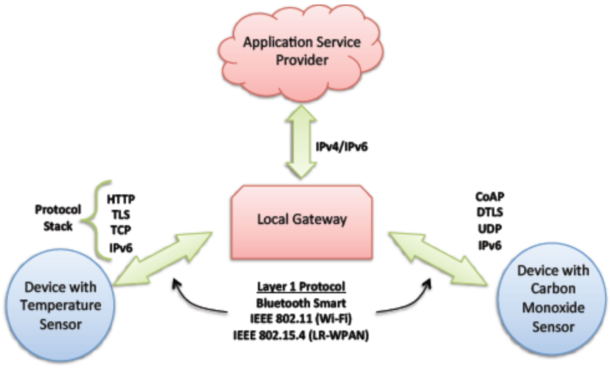

Fig.3. Device-to-Gateway Communication Model

4. Back End Data Sharing Model :
The back-end data-sharing model refers to a communication architecture that enables users to export and analyze smart object data from a cloud service in combination with data from other sources. In this the user allows the third parties to access the uploaded sensor data. This approach is an extension of the single device-to-cloud communication model.

For example, if a corporate user in charge of an office complex is interested in consolidating and analyzing the energy consumption and utilities data produced by all the IoT sensors and Internet-enabled utility systems on the premises. An effective back-end data sharing architecture would allow the company to easily access and analyze the data in the cloud produced by the whole spectrum of devices in the building. Also, this kind of architecture facilitates data portability needs.

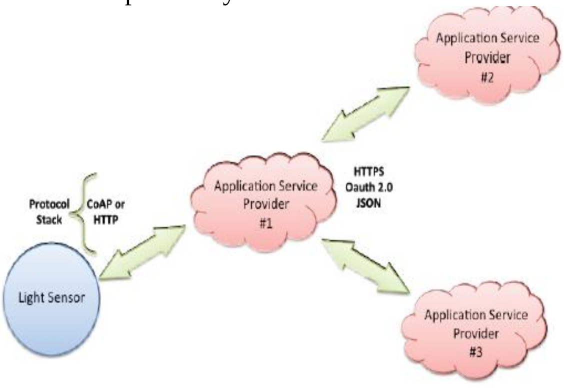
Application Service Provider #2
Protocol Stack
CoAP or HTTP
Application Service Provider #1
HTTPS
Oauth 2.0
JSON
Light Sensor
Application Service Provider #3

Fig.4. Back End Data Sharing Model

III.IOT IN RESEARCH

A vast amount of research is to be done if we really want IOT to be a reality.

John A. Stankovic [7] in 2014 highlighted 8 major areas where the researchers can focuss. They are :

1. Massive Scaling : As trillions of things will be on Internet, what are the various protocols to be used, what standards are to be followed, what will be the architectural model that can support the heterogeneity of various devices and all these devices will be emitting large amount of data so how to collect, use and store this data.
2. Architecture and Dependencies: The architecture which is to be used must allow easy connectivity and control. All the objects must be able to interact with multiple applications and across different platforms. So, research is required in detecting and resolving dependencies across applications.
3. Creating Knowledge and Big Data: As a vast amount of data is generated with IOT so it is required that this data must be converted into useful information. Various data mining techniques should be used and the main challenge will lie in extracting useful data from the noisy data and developing new inference techniques.
4. Robustness: In IOT deployments, it is required for the devices to know their locations, have synchronized clocks, know their neighbor devices when cooperating,

and have a coherent set of parameter settings. However, over time, these conditions can deteriorate. Due to differences in clock time can lead to application failures. So the research question arises here is for how long an IOT system will work. Here mainly the researchers should focus on creating a robust IOT system that will work in noisy, faulty and non-deterministic realities of the physical world.

5. Openness: Previously, the devices having sensor based information operate within those devices only. But with IOT the devices must be talking to eachother. So this requires openness to achieve these benefits. New communications interfaces will be required to enable efficient information exchange across diverse systems but it will cause difficulty with security and privacy.
6. Security: IOT has to deal with lot of security issues. IOT devices are prone to security attacks as these devices have the physical accessibility to sensors, actuators, and objects, and there is openness of the systems and most devices communicate wirelessly. So, the IoT applications must be able to continue to operate satisfactorily in the presence of, and to recover effectively from, security attacks. It needs to detect the attack, diagnose the attack, and deploy countermeasures and repairs.
7. Privacy: As there is lot of interactions involved in IoT . It may create many opportunities to violate privacy. So to tackle this privacy problem privacy policies for each domain must be specified. An IoT paradigm must be designed in order to allow the users to express requests for data access and the policies. These requests must be evaluated against the policies in order to decide if they should be granted or denied.
8. Humans in the Loop: As many IOT applications involve humans their role cannot be neglected. These IOT applications can model the daily activities of a human being. For example the home health care can improve medical conditions of the elderly and keep them safe. So, Human in-the-loop systems offer exciting opportunities to a broad range of applications.

IV. CONCLUSION

In future IOT is going to become a reality. It will change our life style. But there are many challenges to face related to the deployment, growth, implementation, and use of this technology. The Internet of Things involves a complex and evolving set of technological, social, and policy considerations across a diverse set of stakeholders. But it will be a boon for us in future.

ACKNOWLEDGEMENT

Most of the material in this paper is taken from previous authors [1] and [7].

REFERENCES

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

[2] Tschofenig, H., et. al., Architectural Considerations in Smart Object Networking. Tech. no. RFC 7452. Internet Architecture Board, Mar. 2015. Web. https://www.rfc-editor.org/rfc/rfc7452.txt

[3] http://www.bluetooth.com

[4] http://www.z-wave.com

[5] http://www.zigbee.org

[6] "Samsung Privacy Policy--SmartTV Supplement." Samsung Corp. Web.29Sept2015.http://www.samsung.com/sg/info/privacy/smarttv.html

[7] John A. Stankovic, "Research Directions for the Internet of Things" IEEE Internet of Things Journal, Vol.1, No.1, pp. 3-9

DOI 10.17148/IJARCCE.2016.53264