Internet of Things

[1]Iqra Zain, [2]Abu Rehan, [3]Javed Ashraf
[1]Research Scholar, [2]Lecturer, [3]Assistant Professor
Department of Electronics and Communication Engineering,
Alfalah University ,Dhauj , Faridabad Haryana,121004, India

***Abstract* - This paper provides an overview of Internet of Things (IoT), it discusses the vision, the challenges, possible usage scenarios and technological building blocks of the "Internet of Things". In particular, we consider its definition, communication models and challenges. The IoT is enabled by the latest development in RIFD,smart sensors, communication technologies and Internet protocols. The current revolution in Internet, mobile, and machine-to-machine (M2M) technologies can be seen as first phase of the IoT. In coming years IoT is expected to deliver technologies to enable new applications by connecting physical objects together in support of intelligent decision making. The paper concludes with a discussion of social and governance issues that are likely to arise as the vision of the Internet of Things becomes a reality**.

***Keywords* - Internet of Things, RFID, smart objects, wireless sensor networks.**

I. DEFINITION

The Internet of Things is a rising topic of technical, social, and economic significance. The Internet of Things (IoT) describes the revolution already under way that is seeing a growing number of internet enabled devices that can network and communicate with each other and with other web-enabled gadgets.
IoT is simply the network of interconnected things/devices which are embedded with sensors, software, network connectivity and necessary electronics that enables them to collect and exchange data making them responsive.More than a concept Internet of Things is essentially an architectural framework which allows integration and data exchange between the physical world and computer systems over existing network infrastructure.
The Internet of Things (IoT) refers to the ever-growing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems

We organize this paper into three main sections:

- **What is the Internet of Things?**, which provides an overview of its origins, definitions, and technical connectivity models;
- **What issues are raised by the Internet of Things?**, which provides an introduction and discussion of concerns that have been raised about IoT, and;
- **For Further Information,** which provides additional information and pointers to efforts around the world addressing IoT issues.

***What is the Internet of Things?* Origins, Drivers, and Applications**

The term **"Internet of Things" (IoT) was first used in 1999 by British technology pioneer Kevin Ashton** to describe a system in which objects in the physical world could be connected to the Internet by sensors.Ashton coined the term to illustrate the power of connecting Radio-Frequency Identification (RFID) tags used in corporate supply chains to the Internet in order to count and track goods without the need for human intervention. Today, the Internet of Things has become a popular term for describing scenarios in which Internet connectivity and computing capability extend to a variety of objects, devices, sensors, and everyday items.
While the term "Internet of Things" is relatively new, the concept of combining computers and networks to monitor and control devices has been around for decades. By the late 1970s, for example, systems for remotely monitoring meters on the electrical grid via telephone lines were already in commercial use.14 In the 1990s, advances in wireless technology allowed "machine–to–machine" (M2M) enterprise and industrial solutions for equipment monitoring and operation to become widespread. Many of these early M2M solutions, however, were based on closed purpose–built networks and proprietary or industry–specific standards,15 rather than on Internet Protocol (IP)–based networks and Internet standards.
Using IP to connect devices other than computers to the Internet is not a new idea. The first Internet "device"—an IP–enabled toaster that could be turned on and off over the Internet—was featured at an Internet conference in 1990.16 Over the next several years, other "things" were IP–enabled, including a soda machine17 at Carnegie Mellon University in the US and a coffee pot18 in the Trojan Room at the University ofCambridge in the UK (which remained Internet–connected until 2001). From these whimsical beginnings, a robust field of research and development into "smart object networking"19 helped create the foundation for today's Internet of Things.

If the idea of connecting objects to each other and to the Internet is not new, it is reasonable to ask, "Why is the Internet of Things a newly popular topic today?

From a broad perspective, the confluence of several technology and market trends20 is making it possible to interconnect more and smaller devices cheaply and easily:

- *Ubiquitous Connectivity*—Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable''.
- *Widespread adoption of IP–based networking*— IP has become the dominant global standard for networking, providing 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 law21 continues to deliver greater computing power at lower price points and lower power consumption.22
- *Miniaturization*— Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects.23 Coupled with greater computing economics,this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.
- *Advances in Data Analytics*— 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 leverages 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.

The Web-based experience is largely characterized by the active engagement of users downloading and generating content through computers and smartphones. If the growth projections about IoT become reality, we may see a shift towards more passive Internet interaction by users with objects such as car components, home appliances and self-monitoring devices; these devices send and receive data on the user's behalf, with little human intervention or even awareness.

IoT may force a shift in thinking if the most common interaction with the Internet -- and the data derived and exchanged from that interaction -- comes from passive engagement with connected objects in the broader environment.The potential realization of this outcome – a "hyperconnected world" -- is a testament to the general-purpose nature of the Internet architecture, which does not place inherent limitations on the applications or services that can make use of the technology.32

II. Internet of Things Communications Models

Device-to-Device Communications

The device-to-device communication model represents two or more devices that directly connect and communicate between one another, rather than through an intermediary application server. These devices communicate over many types of networks, including IP networks or the Internet. Often, however these devices use protocols like Bluetooth, Z-Wave, or ZigBee to establish direct device-to-devicecommunications, as shown in Figure 1.

Figure 1: Example of device-to-device communication model.

These device-to-device networks allow devices that adhere to a particular communication protocol to communicate and exchange messages to achieve their function. 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. Residential IoT devices like light bulbs, light switches, thermostats, and door locks normally send small amounts of information to each other (e.g. a door lock status message or turn on light command) in a home automation scenario. From the user's point of view, this often means that underlying device-to-device communication protocols are not compatible, forcing the user to select a family of devices that employ a common protocol.

Device-to-Cloud Communications

In a device-to-cloud 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 frequently takes advantage of existing communications mechanisms like traditional wired Ethernet or Wi-Fi connections to establish a connection between the device and the IP network, which ultimately connects to the cloud service. This is shown in Figure 2

Fig 2: Example Of Device to Cloud Communication Model

This communication model is employed by some popular consumer IoT devices like the Nest Labs *Learning Thermostat* and the Samsung *Smart TV*. In the case of the Nest *Learning Thermostat*, the device transmits data to a cloud database where the data can be used to analyze home energy consumption.Further, this cloud connection enables the user to obtain remote access to their thermostat via a smart phone or Web interface, and it also supports software updates to the thermostat. Similarly 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. In these cases, the device-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.

Device-to-Gateway Model

In the device-to-gateway model, also called, the device-to-application-layer gateway (ALG) model, the IoT device connects through an ALG service as a conduit to reach a cloud service. In simpler terms, this means that there is application software operating on a local gateway device, which acts as an intermediary between the device and the cloud service and provides security and other functionality such as data or protocol translation.

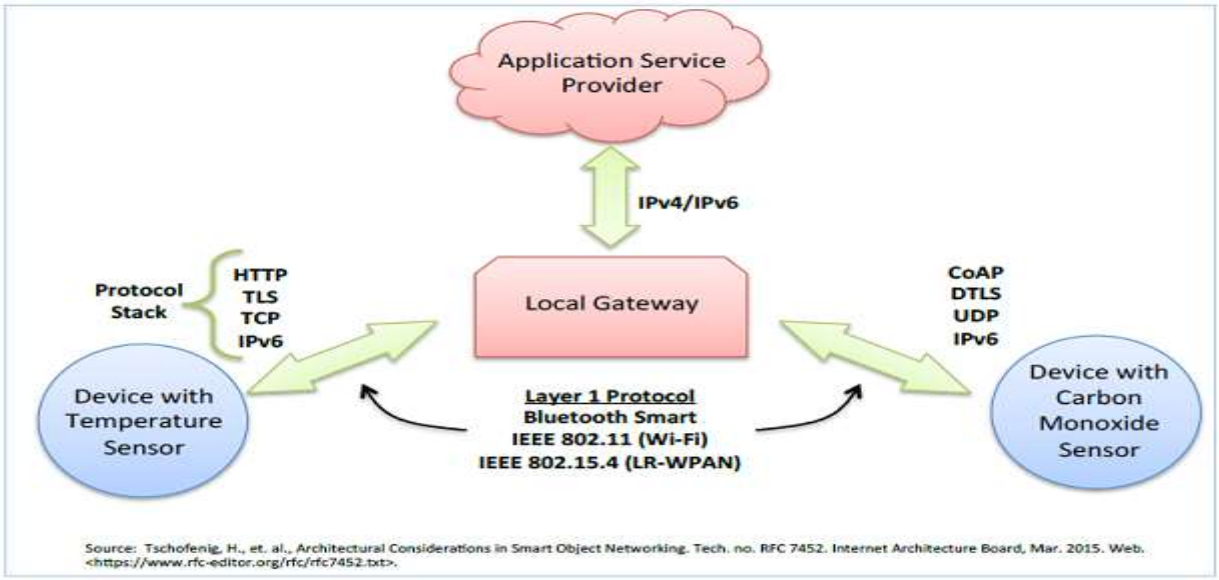

Figure 3:Example of Device to Gateway Model

Several variations of this model are found in consumer devices. In many cases, the local gateway device is a smart phone running an app to communicate with a device and relay data to a cloud service. Many a times, this model employed with popular consumer items like personal fitness trackers.These devices do not have the native ability to connect directly to a cloud service, so they frequently rely on smart phone app software to serve as an intermediary gateway to connect the fitness device to the cloud.

Another form of this device-to-gateway model is the emergence of "hub" devices in home automation applications. These are devices that serve as a local gateway between individual IoT devices and a cloud service, but they can also bridge the inter-operability gap between devices themselves. For example, the Smart Things hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices. It then connects to the Smart Things cloud service, allowing the user to gain access to the devices using a smart phone app and an Internet connection.

From a technical perspective, the IETF Journal article explains the benefit of the device-to-gateway approach:

This communication model is used in situations where the smart objects require inter operability with non-IP (Internet protocol) devices. Sometimes this approach is taken for integrating *IPv6*-only devices, which means a gateway is necessary for legacy *IPv4*-only devices and services.

In other words, this communications model is frequently used to integrate new smart devices into a legacy system with devices that are not natively inter-operable with them. A downside of this approach is that the necessary development of the application-layer gateway software and system adds complexity and cost to the overall system.

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. This architecture supports "the (user's) desire for granting access to the uploaded sensor data to third parties".

This approach is an extension of the single device-to-cloud communication model, which can lead to data silos where "IoT devices upload data only to a single application service provider''. A back-end sharing architecture allows the data collected from single IoT device data streams to be aggregated and analyzed.For example, a corporate user in charge of an office complex would be 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. Effective back-end data sharing architecture allows users to move their data when they switch between IoT services, breaking down traditional data silo barriers.

The back-end data-sharing model suggests a federated cloud services approach or cloud applications programmer interfaces (APIs) are needed to achieve inter operability of smart device data hosted in the cloud. A graphical representation of this design is shown in Figure 4

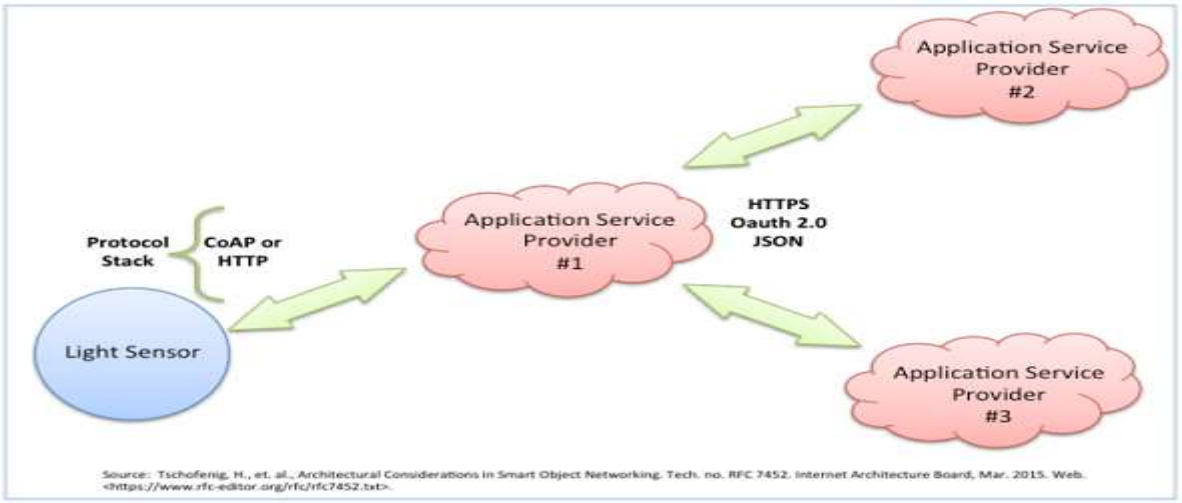

Fig 4:Example of Back-End Data-Sharing Model

IPv6 and the Internet of Things

As the Internet of Things continues to grow, devices that require true end-to-end Internet connectivity will not be able to rely on IPv4, the protocol most Internet services use today. They will need a new enabling technology: IPv6

IPv6 is necessary because the Internet is running out of original IPv4 addresses. While IPv4 can support 4.3 billion devices connected to the Internet, IPv6 with 2 to the 128th power addresses, is for all practical purposes inexhaustible. This represents about 340 trillion,trillion, trillion addresses, which more than satisfies the demand of the estimated 100 billion IoT devices going into service in the coming decades.

What issues are raised by the Internet of Things?

It would be impossible to cover the broad scope of issues surrounding the Internet of Things in a single paper. Below, however, we tried to provide an overview of three topics frequently discussed in relation to IoT. These include: security; privacy; interoperability and standards.

The IoT Security Challenge

The loss of security and privacy in communications and services, with personal data is becoming available and unwanted communication becoming rampant.The overall problem is further aggravated by the diversification of the Internet with new types of devices and heterogeneous networks.

Solution:

ID-management for things (security, authentication, privacy)

Basically each object should not be able to authenticate during the short time because the hundreds of objects may request the approval at the same time. Therefore, group authentication and authorization methods are required.

Internet of Things Privacy Consideration

IoT often refers to a large network of sensor-enabled devices designed to collect data about their environment, which frequently includes data related to people.In other situations, the user might not be aware that an IoT device is collecting data about the individual and potentially sharing it with third parties. This type of data collection is becoming more prevalent in consumer devices like smart televisions and video game devices. These kinds of products have voice recognition or vision features that continuously listen to conversations or watch for activity in a room and selectively transmit that data to a cloud service for processing, which sometimes includes a third party. A person might be in the presence of these kinds of devices without knowing their conversation or activities are being monitored and their data captured.

IoT *Inter-operability*

In the traditional Internet, interoperability is the most basic core value; the first requirement of Internet connectivity is that "connected" systems be able to "talk the same language" of protocols and encodings.

In a fully interoperable environment, any IoT device would be able to connect to any other device or system and exchange information as desired. In practicality, interoperability is more complex. Interoperability among IoT devices and systems happens in varying degrees at different layers within the communications protocol stack between the devices.The standardization and adoption of protocols that specify these communication details, including where it is optimal to have standards, are at the heart of the interoperability discussion for IoT.

III. REFERENCES

[1] ITU-T Internet Reports, "Internet of Things," (November 2005)
[2] Zouganeli E., Svinnset, I.E, "Connected objects and the Internet of things-a paradigm shift," Photonics in Switching,(September 2009)
[3] Harald Sundmaeker, Patrick Guilemin, Peter Friess, Sylvie Woelffle, "Vision and challenges for realizing the Internet of Things," (March 2010).
[4] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A survey," Computer Networks, Volume 54, Issue 15, pp.2787-2805,(October 2010).
[5]Shelby, Zach, and Carsten Bormann. *6LoWPAN: The wireless embedded Internet*. Vol. 43. John Wiley & Sons, (2011).
[6]Tim Kellogg, "Why HTTP won't work for IoT," (January 15, 2014)
[7]Transformation to a Next Generation IoT Denise Denson-Hanson on (Dec 21, 2015)