International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

An Overview of Internet of Things

Miss. Gauri D. Amane

[1]*UG Student, Department of Computer Science Engineering,*

Shivaji University, NMCE, Peth (India)

ABSTRACT

Internet-of-Things envisions a future in which digital and physical entities can be linked, by means of appropriate information and communication technologies, to enable a whole new class of applications and services. Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years.This article reports on the current state of research on the Internet of Things by examining the literature, identifying current trends, describing challenges that threaten IoT diffusion, presenting open research questions and future direction.

Keywords :Internet of Things (IoT),Radio Frequency Identification (RFID), Internet Protocol (IP) etc.

I.INTRODUCTION

The IOT concept was coined by a member of the Radio Frequency Identification (RFID) development community in 1999, and it has recently become more relevant to the practical world largely because of the growth of mobile devices, embedded and ubiquitous communication, cloud computing and data analytics.

Imagine a world where billions of objects can sense, communicate and share information, all interconnected over public or private Internet Protocol (IP) networks. These interconnected objects have data regularly collected, analyzed and used to initiate action, providing a wealth of intelligence for planning, management and decision making. This is the world of the Internet of Things (IOT). Internet of things common definition is defining as: Internet of things (IOT) is a network of physical objects. The internet is not only a network of computers, but it has evolved into a network of device of all type and sizes , vehicles, smart phones, home appliances, toys, cameras, medical instruments and industrial systems, animals, people, buildings, all connected ,all communicating & sharing information based on stipulated protocols in order to achieve smart reorganizations, positioning, tracing, safe & control & even personal real time online monitoring , online upgrade, process control & administration. We define IOT into three categories as below: Internet of things is an internet of three things: (1). People to people, (2) People to machine /things, (3) Things /machine to things /machine, Interacting through internet. Internet of Things Vision: Internet of Things (IoT) is a concept and a paradigm that considers pervasive presence in the environment of a variety of things/objects that through wireless and wired connections and unique addressing schemes are able to interact with each other and cooperate with other things/objects to create new applications/services and reach common goals. In this context the research and development challenges to create a smart world are enormous. A world where the real, digital and the virtual are converging to create smart environments that make energy, transport, cities and many other areas more intelligent.

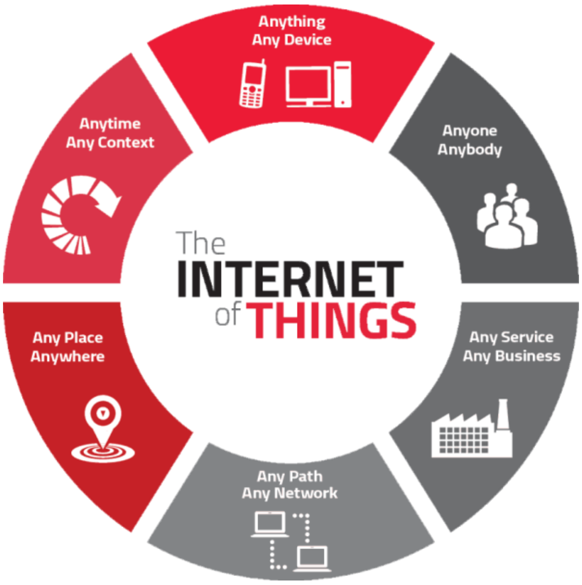

Figure 1. Internet of Things.

The next wave in the era of computing will be outside the realm of the traditional desktop. In the Internet of Things (IoT) paradigm, many of the objects that surround us will be on the network in one form or another. Radio Frequency Identification (RFID) and sensor network technologies will rise to meet this new challenge, in which information and communication systems are invisibly embedded in the environment around us. This results in the generation of enormous amounts of data which have to be stored, processed and presented in a seamless, efficient, and easily interpretable form. This model will consist of services that are commodities and delivered in a manner similar to traditional commodities. Cloud computing can provide the virtual infrastructure for such utility computing which integrates monitoring devices, storage devices, analytics tools, visualization platforms and client delivery. The cost based model that Cloud computing offers will enable end-to-end service provisioning for businesses and users to access applications on demand from anywhere. [4]

II.LITERATURE REVIEW

[1] John A. Stankovic,In this paper author describes the research directions towards Internet of Things and future vision for IoT. New research problems arise due to the large scale of devices, the connection of the physical and cyber worlds, the openness of the systems of systems, and continuing problems of privacy and security. It is hoped that there is more cooperation between the research communities in order to solve the myriad of problems sooner as well as to avoid re-inventing the wheel when a particular community solves a problem. [1]

[2] PoojaKanase et al., In this paper they have proposed a system which include combination of sensor technology and Internet of Things(IoT).Using this system one can control switch of the electricity and monitor level of the saline bottle from distant position. In this project smart hospital using Internet of Things (IoT) has been successfully designed. This project is highly energy efficient as it uses arduino board having microcontroller (Atmega Atmel 328PU) which having low power utilization. It also uses MQTT networking protocol which is a light weight protocol and helps in power saving. [2]

III.INTERNET OF THINGS COMMUNICATION MODELS

From an operational perspective, it is useful to think about how IoT devices connect and communicate in terms of their technical communication models. In March 2015, the Internet Architecture Board (IAB) released a guiding architectural document for networking of smart objects (RFC 7452),39 which outlines a framework of four common communication models used by IoT devices. The discussion below presents this framework and explains key characteristics of each model in the framework.

1.1 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,40 Z-Wave,41 or ZigBee42 to establish direct device-to-device communications, as shown in Figure,

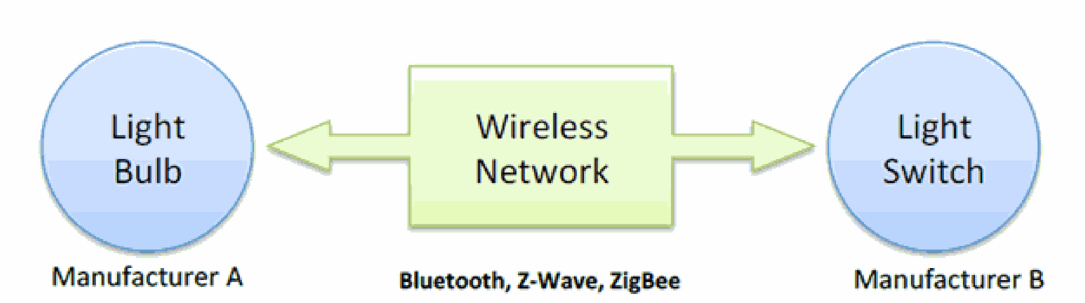

Figure 2. Device-to-device communication model diagram.

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.

1.2 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

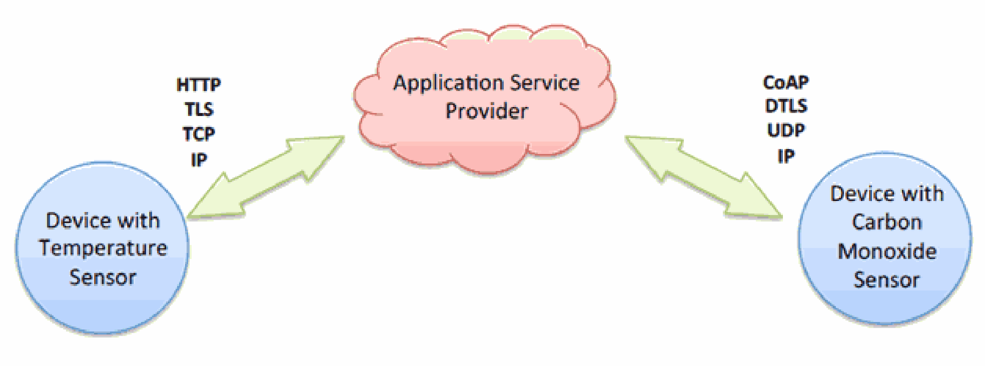

Figure 3. Device-to-cloud communication model diagram.

This communication model is employed by some popular consumer IoT devices like the Nest Labs Learning Thermostat and the Samsung SmartTV. 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 smartphone 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, thedevice-to-cloud model adds value to the end user by extending the capabilities of the device beyond its native features.

1.3 Device-to-Gateway Model

In the device-to-gateway model, or more typically, 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.

Several forms of this model are found in consumer devices. In many cases, the local gateway device is a smartphone running an app to communicate with a device and relay data to a cloud service. This is often themodel 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 smartphone app software to serve as an intermediary gateway to connect the fitness device to the cloud. The model is shown in Figure,

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, February 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

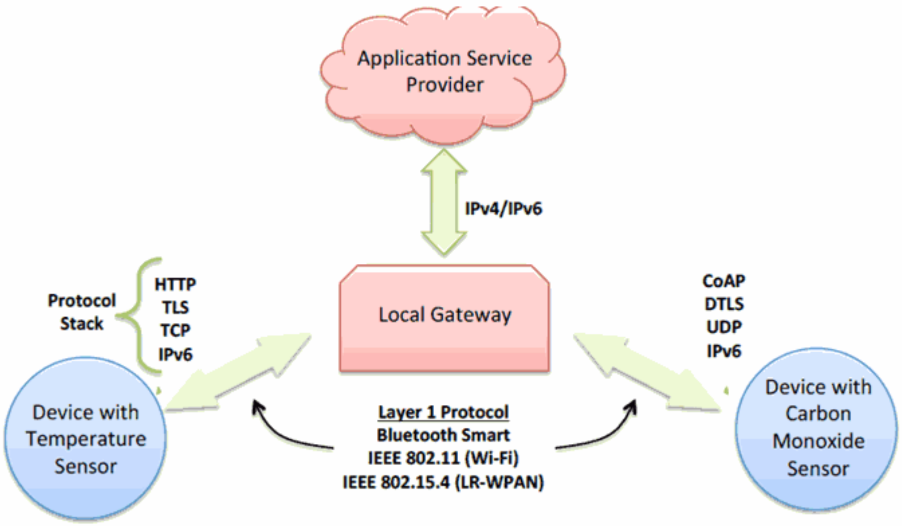

Figure 4. Device-to-gateway communication model diagram.

The other 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 interoperability gap between devices themselves. For example, the SmartThings hub is a stand-alone gateway device that has Z-Wave and Zigbee transceivers installed to communicate with both families of devices.47 It then connects to the SmartThings cloud service, allowing the user to gain access to the devices using a smartphone app and an Internet connection.

1.4 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. Thisarchitecture supports "the [user's] desire for granting access to the uploaded sensor data to third parties".50 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''.51 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. Often in the single device-to-cloud model, the data each IoT sensor or system produces sits in a stand-alone data silo. 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 datasharing architectures allow 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 approach52 or cloud applications programmer interfaces (APIs) are needed to achieve interoperability of smart device data hosted in the cloud.53 A graphical representation of this design is shown in Figure,

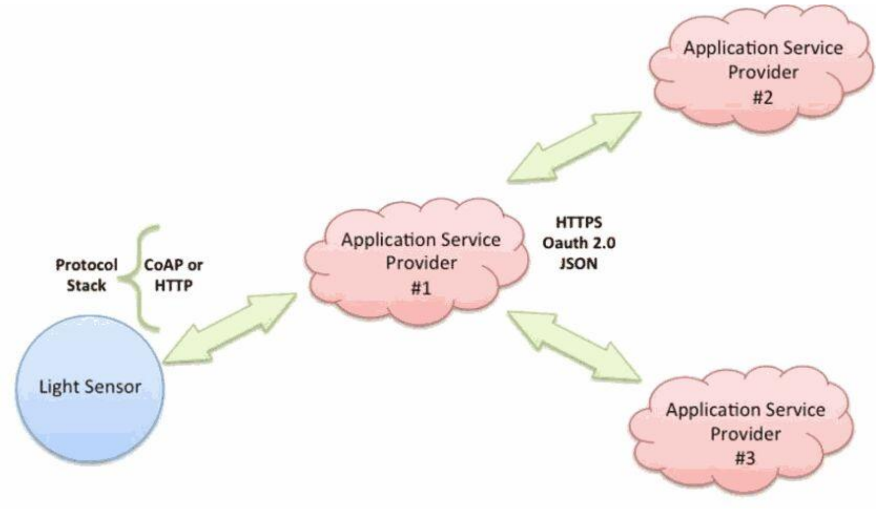

Figure 5. Back-end data sharing model diagram.

The four basic communication models demonstrate the underlying design strategies used to allow IoT devices to communicate. Aside from some technical considerations, the use of these models is largely influenced by the open versus proprietary nature of the IoT devices being networked. And in the case of the device-to-gateway model, its primary feature is its ability to overcome proprietary device restrictions in connecting IoT devices. This means that device interoperability and open standards are key considerations in the design and development of internetworked IoT systems.

IV.CHARACTERISTICS

The fundamental characteristics of the IoT are as follows:

- **Interconnectivity:** With regard to the IoT, anything can be interconnected with the global information and communication infrastructure.

- **Things-related services:** The IoT is capable of providing thing-related services within the constraints of things, such as privacy protection and semantic consistency between physical things and their associated virtual things. In order to provide thing-related services within the constraints of things, both the technologies in physical world and information world will change.

- **Heterogeneity:** The devices in the IoT are heterogeneous as based on different hardware platforms and networks. They can interact with other devices or service platforms through different networks.

- **Dynamic changes:** The state of devices change dynamically, e.g., sleeping and waking up, connected and/or disconnected as well as the context of devices including location and speed. Moreover, the number of devices can change dynamically.

- **Enormous scale:** The number of devices that need to be managed and that communicate with each other will be at least an order of magnitude larger than the devices connected to the current Internet.

- **Safety:** As we gain benefits from the IoT, we must not forget about safety. As both the creators and recipients of the IoT, we must design for safety. This includes the safety of our personal data and the safety of our physical well-being. Securing the endpoints, the networks, and the data moving across all of it means creating a security paradigm that will scale.

- **Connectivity:** Connectivity enables network accessibility and compatibility. Accessibility is getting on a network while compatibility provides the common ability to consume and produce data.

- Even more critical will be the management of the data generated and their interpretation for application purposes. This relates to semantics of data, as well as efficient data handling. [4]

V.ADVANTAGES

5.1 Data

The more the information the easier it is to make the right decision.Knowing what to get from the grocery while you are out without having to check on your own, not only saves time but is convenient as well.

5.2 Tracking:

The computers keep a track both on the quality and the viability of things at home. Knowing the expiration date of a product before one consumes them improves safety and quality of life. Also, you will never run out of anything when you need it at the last movement.

5.3 Time:

The amount of time saved in monitoring and the number of trips done otherwise would be tremendous for money. The financial aspect is the best advantage. This technology could replace humans who are change of monitoring and maintaining supplies.

VI.DISADVANTAGES

6.1Compatibility

As of now, there is no standard for tagging and monitoring with sensors. A uniform concept like USB or Bluetooth is required which should not be that difficult to do.

6.2Complexity

There are several opportunities for failure with complex systems. For example, both you and your spouse may receive messages that the milk is over and both of you may end up buying the same. That lives you with double the quantity required. Or there is a software bug causing the printer to order ink multiple times when I requires a single cartridge.

6.3Privacy or Security

Privacy is a big issue with IOT. All the data must be encrypted so that data about your financial status or how much milk you consume isn't common knowledge at the workplace or with your friends.

6.4Safety

There is a chance that the software can be hacked and your personal information misused. The possibilities are endless. Your prescription being change or your account details being hacked could put you at risk. Hence, all the safety risks become the consumer's responsibility.

VII.APPLICATIONS

This system is designed for a shopping complex mall but it can be also used in various organizations like educational Notice board system or at Railway station, Bus stand and Air-port to display the information and notification. In mall it is also used to control the humidity and temperature of mall via central AC by using temperature sensor. In Industrial organization it can be also used. E-display system may be used to display Emergency message in Hospitals. Some areas where IoT frequently used,

Smart Cities

To make the city as a smart city to engage with the data exhaust produced from your city and neighborhood.

- Monitoring of parking areas availability in the city.
- Monitoring of vibrations and material conditions in buildings, bridges and historical monuments.
- Detect Android devices, iPhone and in general any device which works with Bluetooth interfaces or WiFi.
- Measurement of the energy radiated by cell stations and and Wi-Fi routers.
- Monitoring of vehicles and pedestrian levels to optimize driving and walking routes.

• Detection of rubbish levels in containers to optimize the trash collection routes. Intelligent Highways with warning messages and diversions according to climate conditions and unexpected events like accidents or traffic jams.

Security & Emergencies

- Perimeter Access Control: Detection and control of people in non-authorized and restricted.
- Liquid Presence: Liquid detection in data centers, sensitive building grounds and warehouses to prevent breakdowns and corrosion.
- Radiation Levels: In nuclear power stations surroundings distributed measurement of radiation levels to generate leakage alerts.
- Explosive and Hazardous Gases: Detection of gas leakages and levels in industrial environments, surroundings of chemical factories and inside mines.

Smart Agriculture

- Wine Quality Enhancing: Monitoring soil moisture and trunk diameter in vineyards to control the amount of sugar in grapes and grapevine health.
- Green Houses: Control micro-climate conditions to maximize the production of fruits and vegetables and its quality.
- Golf Courses: Selective irrigation in dry zones to reduce the water resources required in the green.
- Meteorological Station Network: Study of weather conditions in fields to forecast ice formation, rain, drought, snow or wind changes.
- Compost: Control of humidity and temperature levels in alfalfa, hay, straw, etc. to prevent fungus and other microbial contaminants.

Domestic & Home Automation

In home by using the iot system remotely monitor and manage our home appliances and cut down on your monthly bills and resource usage.

- Energy and Water Use: Energy and water supply consumption monitoring to obtain advice on how to save cost and resources.
- Remote Control Appliances: Switching on and off remotely appliances to avoid accidents and save energy.
- Intrusion Detection Systems:Detection of windows and doors openings and violations to prevent intruders.
- Art and Goods Preservation: Monitoring of conditions inside museums and art warehouses.

Medical Field

- All Detection: Assistance for elderly or disabled people living independent.
- Medical Fridges: Monitoring and Control of conditions inside freezers storing medicines, vaccines, and organic elements.
- Sportsmen Care: Vital signs monitoring in high performance centers and fields.

- Patients Surveillance: Monitoring of conditions of patients inside hospitals and in old people's home.
- Ultraviolet Radiation: Measurement of UV sun rays to warn people not to be exposed in certain hours.

Industrial Control

- Machine to Machine Applications: Machine auto-diagnosis the problem and control.
- Indoor Air Quality: Monitoring of oxygen levels and toxic gas inside chemical plants to ensure workers and goods safety.
- Temperature Monitoring: Monitor the temperature inside the industry.
- Ozone Presence: In food factories monitoring of ozone levels during the drying meat process.
- Vehicle Auto-diagnosis: Information collection from Can Bus to send real time alarms to emergencies or provide advice to drivers. [3]

VIII.CONCLUSION

Internet of Things is a new revolution of the Internet & it is a key research topic for researcher in embedded, computer science & information technology area due to its very diverse area of application & heterogeneous mixture of various communications and embedded technology in its architecture. [4]

IX.FUTURE SCOPE

- The Industrial Internet of Things has been indicated primarily as a way to improve operational efficiency. But in today's environment, companies can also gain more profit by seeing it as a tool for finding growth in unexpected opportunities.
- The IoT-enabled transformation has developed massively in the last couple of years and will continue to do so. In the near future, we were supposed to have a home full of Internet-enabled devices that would cater our every need. Experts estimate that more than 50 billion smart devices will be a part of IoT by 2020. IoT becomes an integral part of our lives and makes our lives moresophisticated than ever before.

REFERENCES

[1] John A. Stankovic, "Research Directions for the Internet of Things".
[2] PoojaKanase, SnehaGaikwad, "Smart Hospitals Using Internet of Things(IoT)", International Research Journal of Engineering and Technology (IRJET), Volume: 03, Issue: 03, Mar-2016.
[3]Vandana Sharma, Ravi Tiwari, "International Journal of Science, Engineering and Technology Research (IJSETR)", Volume 5, Issue 2, February 2016.
[4] Keyur K Patel, Sunil M Patel, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", May 2016.