International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072

Internet of Things- Remote Desktop & Wireless Hibernation

Amrit Solanki[1], Sanket Ramesh Kamble[2], Bhavin Patel[3], Amol K Kadam[4]

[1234]*B.tech Computer Engineering*

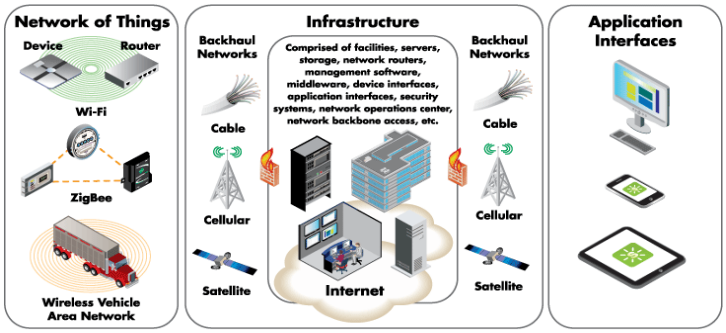
Abstract **-** The Internet of Things (IoT), contains many technologies together from connected houses and metropolitans to connected cars and roads, roads to devices that track user's data collected from connected devices. Some mention ten trillion Internet-connected devices by 2030 and define mobile phones as the eyes and ears of the applications connecting all of those connected things. Multiple devices can communicate over a public, private internet protocol network in 2010, the number of everyday devices connected to the Internet was around 50 billion. Cities, cars, Public safety, house automation and Environmental Protection has been given the high intention for future protection by IoT Ecosystem. For the transparency in governmental work, many countries and governments have included the concept of IoT in the offices including Asia, Europe, America etc. Many organizations have taken a step towards the development of IoT, the devices which are connected to the Internet and possess some useful data that can be used take active decisions are connected each other with LAN, RFID (Radio Frequency Identification), ZigBee, Bluetooth or other means. The connected devices can be readable, recognizable, locatable, portable etc. These 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. Due Internet of things hospital management have become less complicated and very much effective, we can track patient's heartbeats, sugar level, blood pressure level using less complicated devices and we can decide suitable vaccine and operation procedure much more easily.
Internet of Things is a new revolutionary idea that use to connect devices and expand the network by connecting active devices with each other using some secure communication between each other such as Radio Frequency Identification(RFID), ZigBee, WLAN etc. RFID is more secure by means of connecting devices. IT provides a platform to active devices to share useful information, and it makes everyone to connect each other anywhere, anytime.

Introduction

In September 1985, Peter T. Lewis delivered a speech at a U.S. Federal Communications Commission (FCC) about the concept of Internet of Things.
The Internet of Things is the internetworking of physical devices and other items which are synchronized in sensors, electronics that have the aim to collect and exchange data. IoT allows devices to be controlled from remote locations that expand the existing network which improve the availability, accuracy, benefit. Until the year 2020, it is expected that there will be almost 50 billion active IoT devices.

In IoT sense, Things can be referred as active devices such as heartbeat measuring devices on an athlete, biochip transponders on animals, vehicles with sensors for damage protection, blood analysis for soldiers, firefighters, police, fire, and smoke detection sensors for home and offices. In legal scholar's view Things is an unceasing mixture of hardware, software, data, and service. Current examples include Home automation which can have automatic temperature control, smoke and fire detection system, electric power optimization, and another example can be Sixth Sense technology by Pranav Mistry, August smart lock, automatic car tracking adapter.

2. Enabling technologies for IoT



There are many technologies that enable IoT. Followings are some of the wireless technologies:

Short-range wireless

1. Light-Fidelity (Li-Fi) – This is wireless technology is similar to Wi-Fi but it requires actual line of sight.
2. Near-field communication (NFC) – NFC devices have range up to 4cm. Enables devices which having same NFC technology.
3. Radio-frequency identification (RFID) – It uses electromagnetic fields to read data from other devices, data is stored in RFID tags.
4. Bluetooth low energy (BLE) – This technology creates Personal Area Network in the form of Piconet and Scatternet. Bluetooth devices have ranged from 10 m to 100 m.

Medium-range wireless

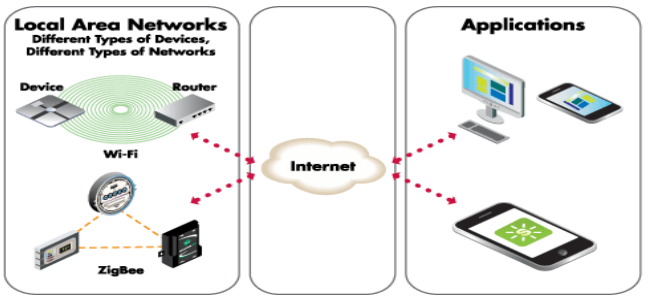
1. HaLow – It extends the Wi-Fi into 900 MHz, provides low power connectivity to sensors, actuators, wearables and other devices.
2. LTE-Advanced – It provides extended network to the existing LTE network of mobile phones with

larger area coverage, higher throughput and low latency.

Long-range wireless

1. Low-power wide-area networking (LPWAN) – These wireless networks are designed to provide communication at the low data rate, low power and reduced cost for transmission.
2. Very small aperture terminal (VSAT) – It is used to provide narrowband data such as transactions using a credit card, RFID, SCADA. VSATs are transportable and provides data rates from 4kbps to 16mbps.

3. Working of IoT



Three main components in Internet of Things:

- The things or active devices
- The network used for the communication
- The system that uses data flowing from connected devices

Sensors & Sensor Technology –
They will fetch the information from smart vehicles, smoke detection from home automation, location, from weather conditions, Train maintenance.

IoT Gateways –
It bridges the gap between an internal network of sensor nodes with the Internet or World Wide Web. They collect the data from the sensor nodes and transmit to the Internet.

IoT gateways are the gateways for the devices with whom we want to interact.

Cloud/Server Infrastructure & Big Data –
The job of the Big Data analytics engine is to store and process the data transmitted through IoT gateway. This data is used to take active decisions which make our general devices smart.

End-user Mobile apps –
The end user control and monitor the active devices from a remote location using the mobile app. These apps provide a user interface to push the information on handheld devices.

IPv6 –
The IP address is the main backbone of the IoT system. It provides a vast number of addresses than the previous version which is useful in IoT system billions of devices are interconnected within the system.

4. The Advantages of IoT

Automation and Control
Without human interaction, the machines are communicating with each other which results in faster communication and timely output. Due to physical devices are connected and digitally and centrally there is a large amount of automation in the working.

Monitor
Monitoring is the second advantage of IoT. More useful information is added for instance if you know how much of ink is remaining in the printer then you can decide when to buy ink.

Saves Money
Saving money is the biggest advantage of IoT. Internet of Things is widely accepted when there is the cost of equipment is less than the amount of money saved. For example, if you know how much of electricity we are spending on the particular appliances then we can decide how to save electricity, which results in saving money.

Saves Time
We get the faster and accurate information from the machine to machine interaction.

For example, if you know there is an accident occurred on the road on which you are driving then you can take divergence in advance to avoid delay and inconvenience and this results in saving the time.

5. The Advantages of IoT

Complexity
IoT is a connection of lot of devices together which causes complexity while resolving any issue. Bugs and defects can cause lot of inconvenience, power failure can also be cause lot of inconvenience.

Compatibility
As the devices which are interconnected can be from different manufacturers and vendors which lead to complexity while connecting devices with each other. There are various international standards issues such as GSM (Global System for Mobile communication) is widely accepted in Europe and Asia but in America, it is not widely accepted which causes confusion and compatibility issues.

Safety/Privacy/Security
The Internet is a playground to the notorious hackers which can be harmful to the users of IoT as there is sensitive information is flowing through the system. As home appliances, road safety equipment, public sector devices are connected to the internet, a lot of data is available on the internet. For example, a hacker changes your prescription list and ordered wrong medicine then it can be disastrous.

Conclusion

The Internet of Things is a good concept in order to provide better services, safety, production, minimizing cost. There should be global standards in order to avoid confusion and complexity. As the "Things" are connected to the Internet, there should be proper safety such as Antivirus, Firewall etc and this will lead to a better world. Anyone can misuse the data such as workers, hackers, intruders but handling these issues with proper care and safety Internet of Things will become a huge success. And nowadays many governments and individuals, companies are coming together for the development of Internet of Things.

References

1. Cutting edge: IT's guide to edge data centres
2. www.prezi.com
3. www.wikipedia.com
4. de.slideshare.net
5. http://www.oemsensors.com
6. http://www.digitaltrends.com
7. http://techzulu.com
8. http://www.inc.com
9. LinkedIn: Bhaskara Reddy Sannapureddy
10. BizDev & Strategy