International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 8 113 – 116

Internet of Things: Definition, Applications, Issues and Future Prospective

Srishti Sharma
Research Scholar, Computer Engineering Department,
LDRP-ITR,
Gandhinagar, India
srishtis1258@gmail.com

Dr. Hiren B. Patel
HOD, Computer Engineering Department,
LDRP-ITR,
Gandhinagar, India
hod_ce@ldrp.ac.in

Abstract—Internet of Things (IoT) is the extension of Internet into the physical environment around us; by the embodiment of electronics into the everyday physical objects that we tend to use. This makes the digital and physical entities linked by the means of appropriate communication technologies. Penetration of these everyday objects into the web strengthens the goal of offering a whole new set of services to the users, showing them the amalgamation of varied devices, versatile data and various technologies as one common operating picture, using IoT. With the IoT advancements in various sectors, more number of devices are being digitally augmented leading to the discovery of newer issues and challenges that are faced due to these 3 Vs; varied devices, versatile data and various technologies. This survey focuses on identification of such issues and challenges in IoT; suggesting some clues for future research.

Keywords—*Internet of Things; Definition of IoT; Embedded Sytem vs. IoT; Applications of IoT; Issues & Challenges in IoT; Future Prospective of IoT*

*****

I. INTRODUCTION

Internet of Things (IoT) is dense network of connected physical things that are easily accessible through internet. The "things" in IoT are objects that have an IP address associated with them and have the ability to sense and transfer data over a network without human intervention. The embedded technology in the objects helps them interact with each other and with the physical environment around.

Industries in the utilities, oil & gas, insurance, manufacturing, transportation, infrastructure and retail sectors are all reaping the benefits of IoT by making more informed decisions, aided by the torrent of and transactional data at their disposal.

IoT is most of the time confused with being embedded system.

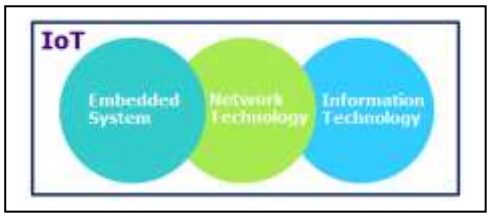

Fig. 1.1 IoT vs. Embedded System

Simply explaining, IoT is an amalgamation of Embedded Technology (ET), Network Technology (NT) and Information Technology (IT). Taking the example of a "Smart air conditioning unit"; It is tempting to have your room be cool enough by the time you reach home from your workplace so when you leave from your office, you can remotely switch ON the air conditioning unit of your home using your mobile (another "Thing" connected to the internet). Technically, with internet, you can control your air conditioner system from any part of the world as long as both the air conditioner and your mobile are connected using the "Internet". An extension to this concept is: your mobile phone will command your home air conditioner that you are leaving the office (it can detect your GPS co-ordinates and decide you are are on the move) and depending on the temperature, the air conditioner will be switched ON by your mobile phone itself, and the mobile will simply notify you that the air conditioner is ON.

For this purpose, your air conditioner is made smart by embedding within it, a temperature sensor collecting temperature data and a wifi module that would send the data to the cloud (internet). This forms the Embedded System. The ecosystem formed by wifi and the cloud is called Network Technology. The mobile phone will have an application running in it that will receive the data. Depending on the received data, the app (in turn the mobile) will switch ON the air conditioner depending on user's GPS co-ordinates. The mobile app infrastructure is Information Technology [6].

IoT application can help industries reduce cost with refined process efficiency, maximize utilization and productivity. With improved tracking of devices using sensors and connectivity, the industries can benefit from real-time insights and analytics, which would help them, make better decisions. The growth of data, processes and things on the internet would make such connections more relevant and important, creating more opportunities for people, businesses and industries.

The rest of the paper has been divided into five sections. The applications of IoT in various fields have been listed and explained in the section two. Section three describes the issues and challenges that are currently being faced in IoT while the futures prospective have been mentioned in the section five.

II. APPLICATIONS

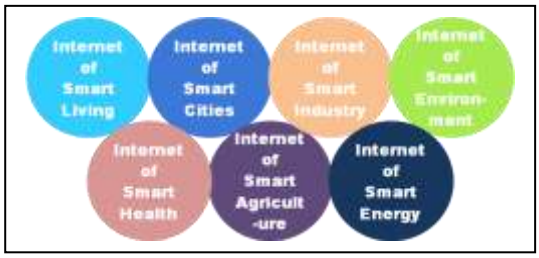

Fig. 2.1 Applications of IoT [2]

A. *Internet of Smart Living (IoSL)*

Remote controlled Appliances: Home appliances such as air conditioner, refrigerator, television, washing machine can all be controlled using panels on the App running on your mobile phones using IoT.

Safety Monitoring: Cameras and home alarm systems can be used for detection of an unusual activity at home.

Intrusion detection system: Detection of windows or doors being opened for intrusion detection.

Energy and Water use: Water and energy consumption monitoring to reduce usage and cost.

B. *Internet of Smart Cities (IoSC)*

Structural Health: Monitoring of the structural health, vibrations and material condition for buildings, bridges and historic monuments.

Lightning: Weather adaptive street lights.

Transportation: Warning messages for diversions, climatic conditions and traffic conditions.

Smart Parking: Monitoring of parking spaces at public places; nearest parking space available.

Waste Management: Indicates the trash level in the trash boxes; optimizing the trash collection route.

C. *Internet of Smart Industry (IoSI)*

Explosives and Hazardous gases: Detection of toxic gas leakage at chemical factories or in the surrounding.

Maintenance and Repair: Early prediction on machine or instrument malfunction; maintenance can thus be scheduled timely.

D. *Internet of Smart Environment (IoSE)*

Air pollution monitoring: Monitoring the amount of CO_2 in the air.

Forest fire detection: Detection of combustive gases in forest area.

River Floods: Monitoring of water level and variations in it in the river.

Protecting wildlife: Locating and tracking of animals for their safety.

E. *Internet of Smart Health (IoSH)*

Patient Surveillance: Monitoring the condition of patients in hospitals or at home.

Medical Fridges: Monitoring conditions inside a refrigerator used for storing vaccines, medicines.

Physical Activity Monitoring: Monitoring heart rate level, breathing and large motion caused by tossing and turning during sleep.

F. *Internet of Smart Agriculture (IoSA)*

Green House: Recreation and maintenance of micro climate conditions to increase production of crops.

Compost: Monitoring of temperature and humidity inside the compost.

Offspring care: Control of growing conditions of the offspring in animal farms.

G. *Internet of Smart Energy (IoSEn)*

Smart Grid: Energy consumption monitoring and management.

Wind Turbines/Power houses: Monitoring and analyzing the flow of control from the wind turbines and power houses.

III. ISSUES IN IOT

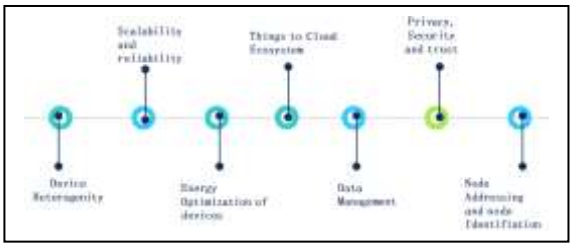

Fig. 3.1 Issues in IoT

A. *Device Heterogenity*

There are varied devices with varied capabilities being used in the IoT applications. Different devices have different computational and communication capabilities. This level of heterogeneity needs to managed at both architectural and protocol level.

B. *Energy Optimization*

Energy is the main constraint for the battery charged devices used in IoT (mostly sensors). The energy spent by them in commutations and communication must be minimized as much possible at electronics level as well as at the protocols level.

C. *Data Management*

The huge amount of data generated continuously by the IoT devices needs to be analyzed properly and be turned into useful format for interoperability between various applications. Standard, well defined formats must be decided for the data so as to make the data generated by different devices; stored at different servers; supplied to different applications interpretable and easy to use.

D. *Node Identification and Addressing*

With increasing number of devices in IoT, the node addressing mechanism should be sufficient enough to provide unique addresses to each of the devices in IoT. Also, for node discovery, service discovery, and access control; node identification mechanisms need to be dealt with.

E. *Things to Cloud Ecosystem*

The wireless technology used for communication of the data from the devices to the cloud needs to be secure, efficient, provide Low-latency and higher throughput; as per the application's need. This ecosystem should be protected from the attackers who could try manipulating or misusing the data.

F. *Scalability and reliability*

The addressing mechanism, interconnections, information management and service provisioning mechanisms should support the increasing number of devices allowing them to scale well within the system. Node failure needs to be detected and handled without interruption in the service.

G. *Security, Privacy and Trust*

IoT is vulnerable to attack since the devices spend most of the time unattended and hence can physically be damaged and communication is wireless which enables eavesdropping. Implementation of complex security scheme is not possible due to energy constraints. Authorization, access control, digital forgetting, proxy attack are all the possible security threats in IoT Application.

IV. CURRENT RESEARCH

A. *Energy Optimization*

1. Power consumption aware medium access protocols

According to [4], there are two types of protocols that are used for medium access. The comparison table between the two types has been given as table 1.

TABLE I. POWER CONSUMPTION AWARE MEDIUM ACCESS PROTOCOLS [4]

Name	Scheme	Advantage	Disadvantage	Example
Schedule Based protocols	Use TDMA or FDMA with TDMA	Avoids collision, idle listening and overhearing	They need clock synchronization mechanism	Latency MAC Application driven and energy efficient communication protocol
Contention based protocols	Use CSMA/ CA	Relax the clock synchronization requirement	Wastage of energy in idle listening	Nano MAC Protocol Adaptive Energy Efficient MAC Protocol

2. Integration of several sources of ***energy harvesting*** into sensors

Piezoelectric, thermoelectric and radio waves can be used for recharging the devices.

B. *Node Addressing*

According to [3], the current mechanism used for node addressing is the 6LoWPAN protocol. This protocol is an enhanced version of IPv6 protocol which uses 128 bits addressing. The RFID tags made use in the IoT applications are 64-98 bit tags. Henceforth, there is an agent required to convert these 64-98 bits into 128 bits address for a device. The "agent" suggested in [3] gets the first 64 bits of the 128 bits address from the RFID address of the tag attached to the device and the rest of the 64 bits are from the network gateway used. But there needs to be a better mechanism devised for RFID tags with more than 64 bits address.

C. *Node Identification*

According to [1], there are two techniques that can be used for node identification. They are:

Using RFID Tags
Advantage: cheaper
Disadvantage: requires possibility for the reader to access the global database where information is stored

Providing description within the object itself
Advantage: no database lookup needed
Disadvantage: more electronics required in the device

D. *Access Control - Security*

According to [5], there are three types of access control mechanism practiced till date. The comparison between the three mechanisms has been given in table 2.

TABLE II. ACCESS CONTROL MECHANISMS [5]

Method	Characteristics	Advantages	Disadvantages
Role based access control (RBAC)	Resources are granted access to on the basis of the role of user	Adding access rights to users is easy	Doesn't support least privilege access System wide update is difficult to be managed Fine grained access control if required, leads to role explosion
Attribute based access control (ABAC)	Resources are granted access to on the basis of attributes of the user	Attributes such as time and location can also be considered while authenticating	Doesn't support least privilege access System wide update is difficult to manage
Capability based access control (CapBAC)	Resources are granted access to by the resource owner	Supports least privilege access to resources	No privilege delegation

E. *Things to Cloud Ecosystem*

To secure the things to cloud ecosystem from all kinds of attacks, [7] suggests use of BitBox.
The **BitBox** is designed to connect with all your exiting IOT devices. The **BitBox** securely collects data from your IOT device and back them up with an encrypted code.
It transfers data to cloud with each data encrypted individually. This data on the **BitBox** can only be accessed by only the primary user. Any unauthorized user that tries to access this data we have to decrypt each data one by one.

V. Future Prospective

As described in [4], the schedule based protocols as well as the contention based protocols have a certain drawbacks that need to be overcome. There can be Hybrid protocols developed extracting the advantages and suppressing the disadvantages of both theses type of protocols. Such Hybrid protocols can be scalable, adaptable to changes in network size, node density and topology. There can be mechanisms developed for recycling the energies within the nodes. Node addressing described in [3] can be further worked upon by developing a new "agent"/mechanism for conversion of the RFID bits to IPv6 address. The node identification mechanisms described in [1] can be combined into a hybrid mechanism for node identification; leaving behind the drawbacks and keeping the advantages of both RFID tags and object description mechanisms. The access control methods defined in [5] do not have a privilege delegation mechanism supported within them. A new access control mechanism can be developed providing privilege delegation by enhancing CapBAC access control method.

VI. Conclusion

IoT has become the next big leap in the field of Computer Science. The seamless merger of real and virtual world, through these massive deployments of IoT devices has opened up new directions for research and business both. An attempt to understand the huge potential of IoT, major issues to be tracked and working on these issues, devising new technical solutions shall help turning these research visions into reality.

REFERENCES

[1] Daniele Miorandi, Sabrina Sicari, Francesco De Pellegrini, Imrich Chlamtac, Internet of Things: Vision, applications and research challenges, Ad Hoc Networks 10 (2012) 1497-1516

[2] Keyur K Patel, Sunil M Patel, Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges, International Journal of Engineering Science and Computing, May 2016

[3] Luigi Atzori, Antonio lera, Giacomo Morabito, The Internet of Things: A Survey, Computer Networks 54 (2010) 2787-2805

[4] Adebayo Segun, Akinwunmi A.O, OguntiE.O, A survey of Medium Access Control Protocols in Wireless Sensor Network, International journal of computer applications ,Volume 116 – No. 22 – April 2015

[5] S. Sicari, A. Rizzardi, L.A Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, Computer Networks 76 (2015) 146-164

[6] https://www.quora.com/What-is-the-difference-between-embedded-systems-and-IOT

[7] http://trendebook.com/bitbox-internet-of-things-security/

[8] .http://www.intopalo.com/blog/2015-05-25-access-control-for-internet-of-things/

[9] http://searchsecurity.techtarget.com/definition/principle-of-least-privilege-POLP

[10] http://www.webfarmr.eu/2011/05/coarse-grained-vs-fine-grained-access-control-part-i/