International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 10
ISSN: 2454-4248
113 – 116

Internet of Things: Introduction, Issues and Challenges

Pradnya A. Vikhar
Department of Computer Engineering
KCES's College of engineering & Information Technology
Jalgaon (MH), India
pradnyav123@gmail.com

Abstract—In recent years, internet of Things (IoT) and its relevant technologies have been gaining more interest of researchers from academic world, industry, and government. As the concept of IoT are quite different from what the Internet today can offer, several pioneering techniques have been gradually urbanized and incorporated into IoT. This term is referred to as the Future Internet of Things (FIoT). The most crucial issue of it is how to extract "data" and transfer them into "knowledge" from sensing layer to application layer. This paper includes an overview of IoT and FIoT. Further there is a discussion on key issues in the area of IoT and the technical challenges of this field.

Keywords-*Internet of Things (IoT), Future Internet of Things (FIoT), Wireless communications*

*****

I. BACKGROUND

Very soon the things around us, the things that we are seeing around, are going to work on the internet. They all are going to be interconnected. So the 'I' in IoT is a global network which connects various computers and computing devices[1][2].

Thus with IoT the scope of internet is expanded beyond computing and computer devices. It is going to interconnect the physical objects around us form lights, fans, air-conditioners to toothbrush, refrigerators, microwave. It not only connects the objects at our home but also use to connect the object at remote places which are internet connected.

II. INTRODUCTION

The Internet of Things (IoT) refers to the use of brightly connected devices and systems to influence data assemble by embedded sensors and actuators in equipment and other physical stuff. IoT is expected to broaden rapidly over the upcoming years and this meeting will allow running free a new breadth of soldiers that improve the quality of life of consumers and productivity of enterprises, unlocking an aperture that the GSMA refers to as the 'Connected Life'[1][2]. For consumers, the IoT has budding to get across solutions that dramatically improve energy efficiency, sanctuary, health, education and many other aspects of daily life. For enterprises, IoT can strengthen solutions that pick up decision-making and productivity in industrialized, retail, agriculture and other sectors.

Machine-to-Machine (M2M) solutions is a division of the IoT which is already use wireless networks to attach devices to each other and the Internet, with minimal direct human attachment, to transport services that meet the needs of a wide series of industries. In 2013, M2M relations accounted for 2.8% of universal mobile connections (195 million), demonstrating that the sector is still at a relatively early stage in its development. An improvement of M2M, the IoT represents the organization of numerous vendors' machines, devices and appliances connected to the Internet from side to side multiple networks. While the prospective shock of the IoT is substantial, a concerted effort is required to budge beyond this early stage. In order to optimize the expansion of the market, an ordinary understanding of the distinct natural history of the opportunity is necessary.

Till date, mobile operators have identified the following key distinctive features:

1. The Internet of Things can facilitate the next wave of life attractive armed forces across several essential sectors of the economy.
2. Meeting the requirements of customers may have need of global distribution models and dependable global services.
3. The Internet of Things presents a chance for new profitable models to sustain mass global consumption.
4. The greater part of revenue will come up from the condition of value-added services and mobile operators are structure new capabilities to facilitate these new service areas.
5. Device and request behavior will leave new and varying demands on mobile.

A. Connectivity in IoT

In terms of the connectivity, 'I' means the internet of computer analogously i.e. LAN, WAN, Node, Gateway and Proxy.

Fig.1 : Connectivity terminology

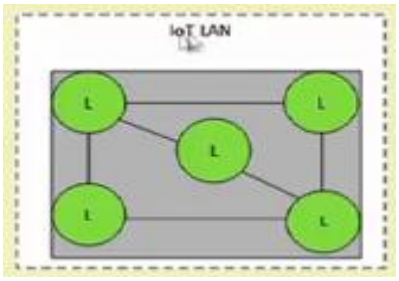
IoT LAN is very similar to IoT, the inernet LAN. It is for short range communiation may be building wide or campus wide. IoT WAN is basically internetworking of two different LANs. Inteconnecting of two different LANs, connecting different various segments organizationally or geographically wide. These can be connected to the internet IoT node which may consists of different nodes inside a LAN or may be WAN. Gateway is something like a router, typically beyong the LAN and connecting to WAN. Thus there are several

 ISSN: 2454-4248
113 – 116

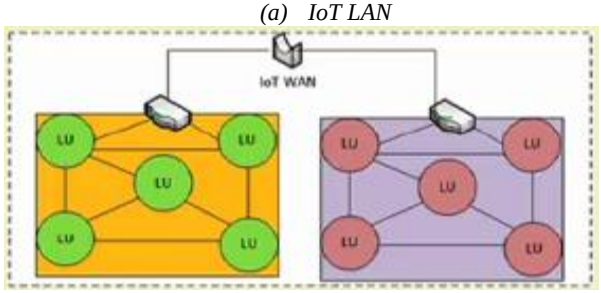
LANs connected to each other through individual Gateways ans Proxys, in a WAN.

B. IoT Network Configurations

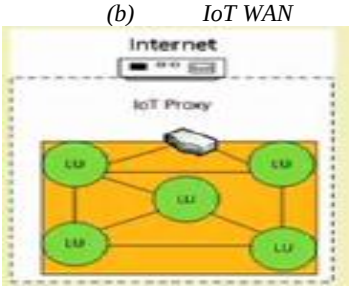
Following figure shows various network configuration of IoT. In the first figure, IoT LAN has its own IoT devices and these devices has its own local address. It might happen that a particular address might be unique to this LAN, but may be reused in another LAN.



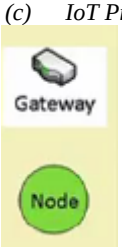
(a) IoT LAN



(b) IoT WAN



(c) IoT Proxy



(d) IoT Gateway

Figure2: Network Configurations in IoT

III. KEY ISSUES IN AREA OF IOT

Most urgent challenges and questions in the area of IoT are divided into five key areas. They are security; privacy; interoperability and standards; legal, regulatory, and rights; and emerging economies and increase [2][3][4].

- **Security:** Users can only trust, when IoT devices and related data services becomes more secure from vulnerabilities, particularly as this knowledge become more pervasive and integrated into our daily lives. Though safety considerations are not novel in the context of in order technology, the attributes of many IoT implementations present new and exclusive security challenges. The fundamental main concern in IoT products and services are addressing these challenges and ensuring safekeeping. The result of poorly secured IoT devices and services may leads to an entry points for cyber attack and it can expose user data to theft by leaving data streams inadequately restricted.

  The interconnected nature of IoT devices means that if every device is poorly secured then it is connected online potentially that affects the security and hardiness of the Internet globally. This challenge can be enlarged by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments. As a matter of principle, developers and users of IoT devices and systems have a collective responsibility to ensure they do not expose users and the Internet itself to potential harm. Thus, a collaborative approach to achieve security requires developing effective and appropriate solutions to IoT security challenges which will well suited to the scale and complexity of the issues.
- **Privacy:** The full latent of the Internet of Things is based on strategies that respect personal privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unchain unbelievable and single value to IoT users, but anxiety about privacy and potential troubles might hold back full adoption of the Internet of Things. The meaning of it is, privacy rights and respect for user privacy expectations are essential to ensuring user trust and confidence in the Internet, connected devices, and related services. Indeed, the IoT is redefining the debate about privacy issues, as many implementations can dramatically change the ways private data is collected, analyzed, used, and sheltered. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to pick out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not intractable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices crossways a broad spectrum of expectations, while still fostering innovation in new technology and services.
- **Interoperability / Standards:** An uneven environment of proprietary IoT technical implementations will slow down value for users and industry. While full interoperability across products and services is not always possible or essential, the purchasers may be uncertain to buy IoT products and services, if they find integration inflexibility, high ownership complication, and concern over vendor lock-in.

  Further, poor designed and configured IoT devices connected to and having the broader Internet, may shows negative results for the networking resources. Properly use of appropriate standards, reference models, and best practices will help to control the proliferation of devices that may act in disrupted ways to the Internet. The use of generic, open, and widely available standards as basic building blocks for IoT devices and services (such as the Internet Protocol) will support greater user profits, novelty, and financial chances.

- **Legal, Regulatory and Rights:** The use of IoT devices generates not only many new regulatory and legal questions but also enlarged existing legal issues around the Internet. The questions are broad in span, and the rapid rate of change in IoT technology often improves the capability of the associated policy, legal, and regulatory structures to adapt. When IoT devices collect data about people in one jurisdiction and transmit it to another jurisdiction with different data protection laws for processing it will generate set of issues surrounds cross border data flows. Further, data collected by IoT devices is sometimes vulnerable to misuse, potentially causing biased outcomes for some users. Other legal issues with IoT devices include the conflict between law enforcement supervision and civil rights; data preservation and demolition policies; and legal responsibility for accidental uses, security breaches or privacy lapses. While the legal and regulatory challenges are broad and complex in scope, acquiring the guiding Internet Society principles of promoting a user's ability to connect, speak, innovate, share, choose, and trust are core considerations for evolving IoT laws and regulations that enable user rights.
- **Emerging Economy and Development Issues:** The Internet of Things holds important guarantee for delivering social and economic benefits to emerging and developing economies. This includes areas such as sustainable agriculture, water quality and use, healthcare, industrialization, and environmental management, among others. As such, IoT holds promise as a tool in achieving the United Nations Sustainable Development Goals. The broad scope of IoT challenges will not be exclusive to industrialized countries; developing regions also will need to respond to realize the possible profit of IoT. In addition, the exclusive needs and challenges of implementation in less-developed regions will need to be addressed, including infrastructure readiness, market and investment incentives, technical skill requirements, and policy resources.

.

IV. TECHNOLOGICAL CHALLENGES

While the possible applications and scenarios require to very interesting, the demands placed on the underlying technology are significant. Moving ahead from the Internet of computers to the remote and somewhat unclear goal of an IoT is something that must be done one step at a time. In addition to the expectation that the technology must be available at low cost if a numerous objects are actually need to be equipped [1][5][6]. The many other challenges are as follows:

- **Scalability:** An Internet of Things potentially has a larger overall scope than the conventional Internet of computers. But then again, things cooperate mainly within a local environment. Basic functionality such as communication and service discovery therefore need to function equally efficiently in both small scale and large-scale environments.
- **Arrive and operate:** Smart everyday objects should not be perceived as computers that require their users to configure and adapt them to particular situations. Mobile things, which are often only sporadically used, need to establish connections spontaneously, and organize and configure themselves to suit their particular environment.
- **Interoperability:** As the world of physical things is tremendously varied, in an Internet of Things each type of smart object is likely to have different information, processing and communication capabilities. Various smart objects would depend on many different conditions such as the energy available and the required communications bandwidth. However, to avail communication and cooperation, general practices and standards are required. That is important with regard to thing addresses. These should conform to standardized schemes if at all possible, along the lines of the IP standard used in the conventional Internet domain.
- **Discovery:** In such vibrant environments, appropriate services describing their functionality for things must be automatically identified. Depending on it, users can receive information about product and can use search engines which helps to find things or provide information about an object's state.
- **Software complexity**: while the software systems in elegant objects will have to function with minimal resources, as in predictable embedded systems, a more general software infrastructure will be needed on the network. On background servers in order to manage the smart objects and provide services to support them.
- **Data volumes:** While some application includes short, uncommon communication, like sensor networks, logistics and large-scale "real-world awareness" scenarios, will require huge volumes of data on central network nodes or servers.
- **Data interpretation:** To support the users of smart things, it will require interpreting the local context determined by sensors more accurately. For service providers to profit from the unrelated data that will be generated, it would need to be able to draw some general outcomes from the interpreted sensor data. However, producing useful information from raw sensor data that can activate further action is by no means a trivial undertaking.
- **Security and personal privacy:** For the security and protection aspects of the Internet with which all familiar communications confidentiality, the authenticity and trustworthiness of communication partners, and message integrity, are important in an Internet of Things. It might want to provide things only selective access to certain services, or prevent them from communicating with other things at certain times or in an uncontrolled manner. The business transactions involving smart objects would need to be protected from competitors' prying eyes.
- **Fault tolerance:** The world of IoT is much more energetic and mobile than the world of computers, with concern to change quickly and in surprising ways. But it would still want to rely on things functioning properly. Structuring an Internet of Things in a robust and trustworthy manner would require redundancy on several levels and an ability to automatically adapt to changed conditions.
- **Power supply:** Things needs to move around and are not connected to a power supply, so their smartness requires be powered from a self-sufficient energy source. Although passive RFID transponders do not require their own resource of energy, functionality and communications range are very few. In many situations, batteries and power packs are problematic due to their size and weight, and especially because of their maintenance requirements. Energy saving is a factor not only in hardware and system architecture, but also in software like the implementation of protocol stacks.

 ISSN: 2454-4248
113 – 116

There are already some battery-free wireless sensors that can transmit their readings a short distance.

- **Interaction and short-range communications:** Wireless communication over very short distances will be sufficient, for example, if an object is in contact with another object or users hold their mobile against it. For such a short distances very little power is required, and the addressing is also simplified. Further there is no risk of being overheard by others. NFC is one example of this type of communication which uses inductive coupling as RFID. For the communication one partner is requires to be in active mode and the other will be in passive mode. Active units of NFC are small enough therefore it can be used in mobile phones; whereas passive units are significantly smaller, cheaper and do not need their own power source.
- **Wireless communications**: From an energy point of view, GSM, UMTS, Wi-Fi and Bluetooth established wireless technologies which are far less suitable. Recently WPAN standards such as ZigBee and others are still under development and may have a narrower bandwidth, but they do use significantly less power.

CONCLUSION

IoT ensures innovative, fully consistent "smart" world, with associations between matter and their environment. The vision of the Internet of Things as a ever-present array of devices bound to the Internet power primarily change how people imagine about what it means to be "online". While the potential ramifications are noteworthy, a number of potential challenges may stand in the way of this hallucination mostly in the areas of security; privacy; interoperability and principles; legal, authoritarian, and rights issues; and the inclusion of budding economies. The Internet Society cares about IoT because it represents an increasing characteristic of how people and institutions are likely to interact with and integrate the Internet and network connectivity into their personal, social, and economic lives. Solutions to maximizing the reimbursement of IoT while minimizing the risks will not be set up by engaging in a polarized debate those depths the promises of IoT against its possible perils. Rather, it will take knowledgeable engagement, dialogue, and collaboration across a series of stakeholders to plot the most effective ways frontward.

REFERENCES

[1] Sudip Mishra, "https://onlinecourses.nptel.ac.in /noc18_cs46/unit? unit=5&lesson=8".

[2] Somayya Madakam, "Internet of Things: Smart Things," International Journal of Future Computer and Communication, Vol. 4, No. 4, August 2015

[3] https://www.internetsociety.org/iot

[4] Friedemann Mattern and Christian Floerkemeier, "From the Internet of Computers to the Internet of Things,"

[5] John A. Stankovic, "Research Directions for the Internet of Things," IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3-9, Feb. 2014

[6] Ashvini Balte, Asmita Kashid, Balaji Patil, "Security Issues in Internet of Things (IoT): A Survey," International Journal of Advanced Research in Computer Science and *Software Engineering*, Volume 5, Issue 4, 2015