International Journal of
Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: http://dx.doi.org/10.31695/IJASRE.2018.32763

Volume 4, Issue 6
June - 2018

The Evolution and Issues Related to the Internet of Things

Ms. Savita Singh [1] and Ms. Supriya Sharma[2]

Assistant Professor [1-2]

Department of Computer Application

IPEM Group of Institution

Ghaziabad , Uttar Pradesh

India

ABSTRACT

The Internet of Things (IoT) is a technology which has the power to connect the enormous number of devices or objects and the capability to change to way we live and work. The fast growth in the number of devices is giving birth to various issues related to the authentication, authorization, security, and privacy of user data or personal information, over the most vulnerable medium, i.e. Internet. A significant number of these are specialized, including interoperability and scalability, as billions of heterogeneous gadgets will be associated, however choosing how to put resources into the IoT is a test for business, and there are additionally real social, legitimate and moral difficulties, including security and protection of information gathering, which must be settled. In this paper, we focus on the evolution of IoT, and the issues which are generated due to increase in the number of devices over the IoT.

KEYWORDS: *Internet of Things, Connectivity, Device Management, Security, Privacy.*

---

1. INTRODUCTION

As it has been already said, after making huge increase in address space of IPv6's- " it will turn out to be anything & become very easy to assign an IPV6 address to every atom on the surface of the earth". This turns into an imperative factor in the improvement of the Internet of Things[1].

The name of the concept of IoT has been coined in the 1999, by Kevin Ashton. Not much awareness has seen in the field IoT in the year 2004-2006, but now days the word is buzzing the Internet.

IoT incorporates everything from Personal Digital Assistants (PDA's), espresso creators, clothes washers, earphones, lights, wearable gadgets (like smart watches, smart shoes, Fitbit bands, e-skin etc.) and nearly whatever else you can consider. In short, we can state Internet o Things is Goliath system of associated things. An expansion in the number of brilliant hubs, and also the measure of upstream information the hubs create, is relied upon to raise new worries about information protection, information power and security. This idea picked up prevalence for its capacity to associate the detached – physical-first questions once unfit of producing, transmitting and getting information unless enhanced or controlled.

Internet of Things

Internet of Things is the Subset of the Internet of Everything, it is a projection of scenario "When we expand the correspondence and availability capacities of a protest, say sensors, any day by day life things; which can have an IP Address, and ready to produce, transmit, and devour information, with least human mediation".

Figure1. Internet of Things IOT

The Main Core Elements/system components of IOT:

- People: They are the end –users/consumers associated over the web for sharing information and activities.
- Things: It can be anything like the bed, TV, chair, A.C, smart refrigerator, smart thermometer etc). A thing is an Actuators or an embedded device/system, physical sensors, gadgets which can receive and transmit data from different sources over the network. while selecting a "thing' in IoT, we should consider the few points- memory size of the thing, number of i/o pins it has, and most importantly consider the peripheral communication it can do, and the communication capabilities(like it can connect with Ethernet, Bluetooth, etc).
  The "Thing" may give following services:[2]-

  a)Identification and info storage(RFID tags, MAC address)

  b)Information collection (Sensor networks, store sensor values)

  c)Information processing(Understanding commands, filtering data)

  d)Communications (Transmit and receive messages)

  e)Actuation (Switch control, motor control)

- Information: It covers crude data bust down and ready into valuable information for encouraging sensible decisions and management instruments. For instance: temperature logs changed into a standard number of high-temperature hours every day for the assessing room cooling necessities.
- Procedures: It implies utilizing network among info, people and things to incorporate esteem.

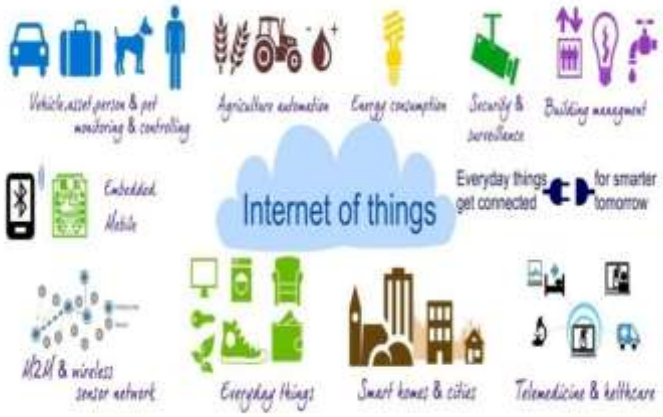

Figure 2. Basics of IOT [1]

Need of IOT

We know that IOT is changing our lives too. It becomes very easy to switch on-off the A.C in homes, to turn-on the lights in the room, to manage the ambiance etc. All these functions or capabilities of IoT, can see, hear and notice the world for themselves, in

DOI: 10.31695/IJASRE.2018.32763

all its irregular radiance. It is able to track and tally everything thus it will lessens the season of individual, lost of things and it likewise spare money. IOT empowers gadgets/items to watch, distinguish and comprehend a circumstance or the surroundings without being reliant on human help. The development and connection of knowledge, procedures and things on the net would create such associations a lot of applicable and significant, creating a lot of open doors for people, organizations and businesses.

Key concepts of the Internet of Things [6]:

a) Sensors/Device – In this first step the data is collected from the environment ,by the sensors or devices. This is as simple as measuring temperature , sensing human touch on the smartphone screen to on & off display screen light etc. System first has to gather the data from the "point of activity". The sensing **will be** done via biometric, biological, environmental, visual or **perceptible**, many more.
b) Communication / Cloud Based Capture -After collecting data ,the second step is to connect with cloud through variety of methods like WiFi, WAN , LPWAN etc. to store and process data.
c) Processing– After the data has been collected on cloud , the software's will perform of processing on it.
d) Delivery of Information/User interface - We can say that, this could be the last stage , when the usefull information is delivered to the end user. This requires the use of some end point interface like tablet, iPad , email, some alert msg, etc. Last but not the least, in IoT it is not the one way process. Because , in IoT the user may also affect and control the device by giving input from the interface. This is similar to seting temperature in AC, etc.

Issues that are being faced by Internet of Things:

In this paper, our focus is on the issues which Internet of Things is facing these days. If we talk about issue, an Issue is a topic of concern , an important matter in any field. As IoT is collection of huge number of devices, which are connected and capable of gathering, processing and transferring data . So for this hundreds of devices a connecting to IoT every days. When the amount of devices increases , this will generate some important issues like how can these devices to named, identified, how they can be authorized & authenticated and most importantly how can we safe guard the personal data of a customer . For this it requires some legal legislation given in the constitution.

"Device Management Issues"

IoT platform uses different devices which have various sensors such as temperature sensor, IR sensor, capacitive sensor, chemical sensor , smoke sensor, gas sensor , motion detector sensor etc.

IoT stages work and convey various kind of intelligence and data using a variety of sensors(mentioned above).They serve to collect data, pushing it and sharing it with a whole network of connected devices. These devices help companies integrate, organize, monitor and remotely manage internet-enabled devices at scale, offering features critical to maintaining the health, connectivity and security of the IoT devices along with their entire lifecycles.

Any object either physical, mechanical or anything could become the IOT device , if it can be connected to network wirelessly and able to transmit data. Embedded with technology, these devices can communicate and interact over the internet, and they can be remotely monitored and controlled.

These devices can be categorized into three main groups:

Devices	Description
Consumer	This include smart TVs, smart speakers, toys, wearables and smart appliances, Smart meters, commercial security systems and smart city technologies.
Enterprise	Like smart sensors located in a conference rooms , to adjust the temperature and the lights accordingly.
Industrial	These devices can help in monitoring but also automate many of complex process. Such as Inventory management, Quality control, Packaging Optimization etc.

Device management includes features like:

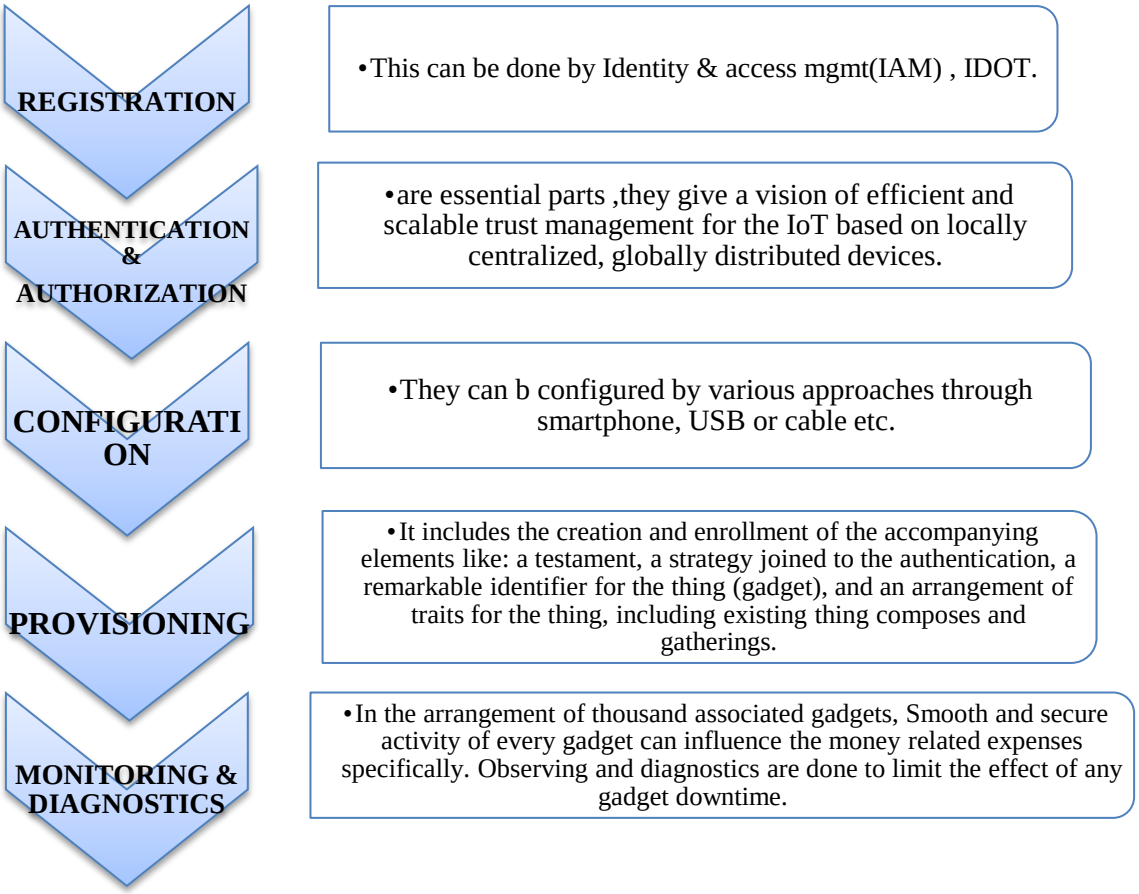

Fig-3: Features of Device Management

"Legal Security Issues"

Many times we see , that the common people are unaware from most of the constitutional legislations, which they should know for their benefit. That's why a large population of our country is also unaware of the legal security legislations present in our constitution-to give security ,privacy, & authentication to the user's data which has been collected and stored at the service provider's databaseWith a specific end goal to guarantee the security and assurance of the information gathered, the IoT specialist co-op can have particularly drafted protection arrangement specifying the private data that is gathered by the specialist organization. Because of the shortage of enactment and mindfulness in such manner, the legitimate issues relating to an IoT specialist organization can be completely tended to just by drafting and executing understandings consolidating significant arrangements to protect the enthusiasm of both the IoT specialist co-op and the IoT client.

IoT is something where enormous devices talking to each other via a network (i.e. Internet), so the potential for a security rupture is to a great degree high and as more IoT gadgets are presented after some time, this will turn out to be more convoluted further.

"Data Privacy & Protection Issues"

The data privacy and security issues is mostly ignored by the people, but it is most important. Because whenever we download some application or login on some website or device (i.e. IoT device) we always share some credentials or persona information. Like we permit applications to share contacts, pictures and area data and so forth. So the lawful enactment in information security and insurance will limit the sellers or specialist co-ops to make any abuse of client data.

There are some provisions present in our Indian constitution related to data protection of individual personal information is covered under the:

DOI: 10.31695/IJASRE.2018.32763

- **Information Technology Act, 2000 ("ITA")[7]**

Area 43A of the ITA-manages insurance of information in electronic medium and gives that right when a body corporate is indiscreet in executing and keeping up 'sensible security practices and procedure's in association with any 'fragile individual data or information' that it deals, has or handles in a PC asset that it claims, works or controls and such indiscretion makes wrongful disaster or wrongful increment any individual, such component ought to be committed to paying hurts by strategy for pay to the individual so affected.

- **Section 72 of the ITA[3]**- enunciates penalty for breach of the confidentiality and privacy of the data collected.

Liability and Data Ownership-

Today, an IoT service provider has to deal with an all-time increasing volume of data, the number of stakeholders involved in IoT, which is likely to increase more in the coming years.

Because of the association of numerous partners/ IoT clients , the IoT service provider (data controller) at all times should ensure that the line between the data controller and data processor does not get obscured and being the data collector would fundamentally choose the augmentation degree, way and explanation behind the use of the individual data.

Since, if the client information gets broke, which gathering will bear the danger of any mischief caused to the customer of IoT.

Privacy and authentication Issues:

We know that 'privacy' and 'authentication' is the most important issue, in this widely connected and unsecured world of devices. For Instance, when we go to open/unlock our associated auto with our cell phone, we need to be consoled that exclusive we, the proprietors/owner, are approved to do as such – went before by fruitful 'verification'. Because the user must not be masquerade (i.e. when some unauthorized entity pretends to be the other authentic entity) ,the user has to be assured about his/her information.

This implies guaranteeing the clients of a gadget (as well as record) are who they say they are and have the approved qualifications to get to the data from there on, helping structure the center reason for securing the correspondence of and with a gadget inside these broad systems.

Connectivity issues-

If the area is small the connectivity of IOT devices is easy task. However deploying IOT app on a large scale which are having thousands or even millions of users is very difficult task.

However the internet is not just one network , it can include enormous number of different networks, including fast connectivity, firewalls , proxy servers etc. that can disrupt connectivity of different devices of IOT.

The connectivity in IOT itself contain 5 big issues[5]. These are as follows,

1. Security or Hacking Threats[6] :

- Security is a tremendous task, yet it's principal in Internet of Things network. The specific area related with security are authorization, encryption and open port. Authorization is to make sure the available devices in IOT has proper authorization to send and receive that stream of data. In case of IOT we require end to end encryption between IOT devices. IOT is vulnerable at the point when it's sitting and tuning in to an open port out to the Internet.

2. Signalize :

Reliable bidirectional communication is required for collecting and routing data between connected IOT devices. Devices may take data from any devices or servers but we need to be sure that the stream of data is going and arriving at its destination on time.

3. Bandwidth, Cost & power supply :

When the IOT comes into cellular network , the bandwidth becomes expensive. Sometimes the taxed rate are so high that cannot be handled. Power disruption in one are can also disturb from locations miles away.

4. Implementing Detection :

The IOT relies on instant communication and fast updates. The big issue in connectivity is the monitoring of your own devices as a small disruption can generate threats and it can be really very difficult to find out in real time our own device and what is happing within the network itself. That means it can take months in detecting basically where was the problem lies.

5. Consumer Demand:

At the point when clients begin seeing various decisions and difference inside the decisions, the market might be constrained to bad-to-the-bone tech individuals as it were. Shoppers get disappointed with changes after they've effectively invested energy taking in a particular manner to complete things, and the IoT may turn out to be excessively troublesome, making it impossible to pitch to the normal individual right at this point.

Monitoring Issues

The devices utilized as a part of the Internet of Things will require administration and checking . As in the IOT as the number of devices increases , the available tools for IOT should be able to manage and monitor a huge number of devices. IT infrastructure is becoming complex day by day. Almost Every network need monitoring for its proper working . As IOT includes a million of devices so each devices need better IT support. Internet of Things Network Monitoring gives a chance to specialist organizations to be more pertinent and better address the issues of associated customers with a developing number of devices in their lives. As the development of the IoT proceeds with, IT experts, incorporation organizations, equipment producers and other specialist co-ops should discover better approaches to screen, oversee and investigate the gadgets that they arrange and supply.

CONCLUSION

The Internet of Things (IoT) is a technology which has the power to connect enormous number of devices or objects. But the fast growth in the number of devices is giving birth to various issues related to the authentication, authorization, security and privacy of user data or personal information, over the most vulnerable medium which is Internet. This paper discuss about these various issues which are being generated by connection of millions of devices. Though the IOT has these issues but it has the capability to change to way we live and work, like there are Legal Security Issues but these can be overcome if he/she have the knowledge about constitutional legislations. Similarly, in connectivity issues we should focus on issues like signaling, bandwidth and customer demand.

REFRENCES

[1] Prajwal Fernandes, Avinash Monteiro and Suman Antony Lasrado," EVOLUTION OF INTERNET OF THINGS (IOT): SECURITY CHALLENGES AND FUTURE SCOPE", International Journal of Latest Trends in Engineering and Technology Special Issue SACAIM 2016, e-ISSN:2278-621X.

[2] Kwok-Yan Lam, Chi-Hung Chi," Identity in the Internet-of-Things (IoT): New Challenges and Opportunities", K.-Y. Lam et al. (Eds.): ICICS 2016, LNCS 9977, pp. 18–26, 2016.

[3] Ebraheim Alsaadi, Abdallah Tubaishat "Internet of Things: Features, Challenges, and Vulnerabilities", IJACSIT, Vol. 4, No. 1, 2015, ISSN: 2296-1739.

[4] Mirza Abdur Razzaq, Muhammad Ali Qureshi, Sajid Habib Gill, Saleem Ullah," Security Issues in the Internet of Things (IoT): A Comprehensive Study", IJACSA, Vol. 8, No. 6, 2017.

[5] Abha Kiran Rajpoot, Mukul Varshney, Aparajita Nailwal, "Security and Privacy Challenges in the Internet of Things", IJCSMC, Vol. 5, Issue. 6, June 2016.

[6] https://www.pddnet.com/blog/2015/03/4-key-elements-iot

[7]http://www.mondaq.com/india/x/691560/Data+Protection+Privacy/Legal+Issues+Pertaining+To+Internet+of+Things+IOT

DOI: 10.31695/IJASRE.2018.32763