International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Internet of Things (IoT) : Security, Applications, Challenges and Future Directions

Navjot Jyoti

Assistant Professor, Northwest Group of Institutions, Dhudike (Moga), Punjab, India

ABSTRACT

The IoT is made of billions of Internet-associated gadgets or things, every one of which can sense, communicate, compute, and potentially actuate, and can have intelligence, multimodal interfaces, physical/virtual identities, and attributes. This paper is basically focusing on IoT, Technology, Security, architecture, elements, applications and challenges.

Keywords : IoT, security, WSN, RFID, NFC

I. INTRODUCTION

At present, more than 20 billion IoT gadgets are sent on the Internet, and this number is relied upon to increment in scale throughout the following five to 10 years[1]. Kevin Ashton has used the term Internet of Things (IoT) for the first time, which is now gaining popularity. Current IoT gadgets generate immense measure of information named as large data, consequently we require a devoted computing framework to process this in close ongoing. An extensive variety of IoT applications incorporate transportation frameworks, Smart homes, Shrewd Industries, Media, and Medical and so forth.[2] The IoT organize helps in the data handling and control of these applications. Internet of Things are fundamentally physically associated objects. Every physical object associated with each different structures in an IoT makes IoT network. The associated physical gadgets are moreover implanted with various softwares, sensors and also have network connectivity which makes them able to share and access the information.

II. IoT SECURITY

The developing IoT arrange has approached with essential needs for influencing it to secure. A great deal of security issues have turned into a challenge for the IoT organize. These issues may incorporate security, genuineness, get to control and administration issues[3]. The primary issue is that in light of the fact that networking gadgets and different items is generally new, security has not generally been considered in item outline. IoT items are frequently sold with old and unpatched installed operating system and software. Besides, buyers regularly neglect to change the default passwords on new gadgets - or in the event that they do transform them, neglect to choose adequately solid passwords. To enhance security, an IoT gadget that should be straightforwardly available over the Internet, ought to be divided into its own particular network and have organize get to limited. The system fragment should then be checked to recognize potential bizarre traffic, and move ought to be made if there is an issue[4].

Security experts have warned of the potential risk of large numbers of unsecured devices connecting to the Internet since the IoT concept was first proposed

in the late 1990s. In December of 2013, a researcher at Proofpoint, an enterprise security firm, discovered the first IoT botnet[5]. According to Proofpoint, more than 25 percent of the botnet was made up of devices other than computers, including smart TVs, baby monitors and other household appliances.

III. ARCHITECTURE OF INTERNET OF THINGS

More than 25,000,000,000 gadgets are relied upon to be interconnected by 2020 [6] which is an extensive number so the current design of Internet with TCP/IP conventions can't deal with a system as large as Internet of Things, consequently to help that enormous IoT arrange we require another engineering that has a capacity to deal with different Quality of Service (QoS) and security issues moreover it has additionally capacity of taking care of a current system application. Without tending to reasonable protection guarantee, Internet of Things isn't relied upon to be endorsed by many. In this manner security of information and isolation of clients are vital difficulties for Internet of Things.

For propel development of Internet of Things, various "multilayered security models" are proposed. Wang Chen has proposed a 3 level design of Internet of Things [7] while Hui Suo proposed a 4 level engineering [8]. Miao Wu has proposed a 5 layered engineering utilizing Internet and Telecommunication administration systems designs in light of TCP/IP and TMN models separately. Likewise a 6 layered design was additionally anticipated in view of the system various leveled structure [9]. So essentially it has six Layers as appeared in the Fig. 1.

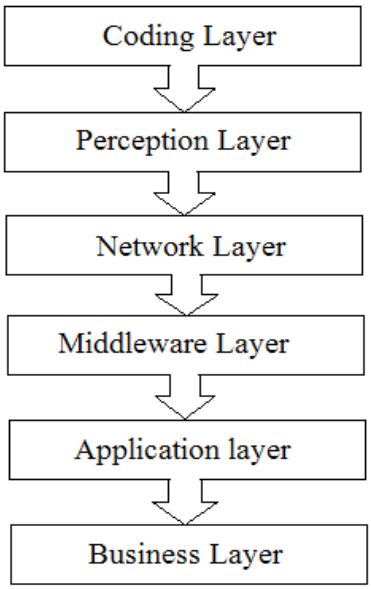

Fig1: Six-Layer IoT Architecture

i. Coding Layer

Coding layer is the base of Internet of Things which gives fundamental distinguishing proof to the gadgets that are a piece of Internet of Things. In this layer, every gadget are assigned with "novel ID" which makes it simple to recognize the gadgets.

ii. Perception Layer

Perception layer of Internet of Things, which gives a physical importance to every gadget. It comprises of information sensors in different structures which could detect the dampness, temperature, area and speed of the gadget. This layer gathers the data of the gadget from the sensor associated with them and makes an interpretation of the data into advanced signs which is at that point conveyed onto the Network Layer for propel activity.

iii. Network Layer

The goal of Network Layer is acknowledge the helpful data as computerized signals from the Perception Layer furthermore, exchange it to the handling frameworks in the Middleware Layer through the trans-mission mediums like Bluetooth, WiFi, Zigbee, WiMaX, 3G, GSM, and so on with conventions like IPv6, IPv4, DDS, MQTT, and so forth [10].

iv. Middleware Layer

Middleware layer forms the information anticipated from Network Layer [11]. It contains the innovations like Ubiquitous registering, Cloud processing which gives an immediate access to the database to record all the fundamental data in it.

Utilizing some Intelligent Processing Equipment, the data is handled and a completely computerized move is made based on the handled result of the data.

v. Application Layer

Application layer perceives the uses of Internet of Things for a wide range of generation, in light of the controlled information. Applications advance the propel improvement of Internet of Things so this layer is exceptionally helpful in the enormous scale advancement of Internet of Things organize. The Internet of Things applications could be smart transportation, smart homes, brilliant planet and so on.

vi. Business Layer

Business Layer controls the administrations of Internet of Things and application and is at risk for all the investigation identified with Internet of Things. It makes distinctive plans of action for various business models.

IV. APPLICATIONS OF IoT

A large portion of the applications in this day and age are keen however they are not equipped for speak with each other. By enabling those applications, they have a capacity of speak with each other and ready to utilize shared data to make a huge scope of new inventive applications. These creating applications with some selfdirected abilities would absolutely propel the nature of our lives. A couple of utilizations are as of now accessible in the showcase [12], Google Car is a standout amongst other IoT application in the market. It has a capacity of a self-driving with realtime movement, it additionally investigations a climate, street conditions and other data . In future there will be a Hugh number of Internet of Things applications which will change our lives for better. In this area, few number of applications are depicted.

1) Smart home

Smart Home obviously emerges, positioning as most noteworthy Internet of Things application on every deliberate channel. More than 60,000 individuals as of now look for the expression "Brilliant Home" every month. This isn't an astonishment. The IoT Analytics organization database for Smart Home incorporates 256 organizations and new companies. A larger number of organizations are dynamic in savvy home than some other application in the field of IoT. The aggregate sum of subsidizing for Smart Home new companies as of now surpasses $2.5bn. This rundown incorporates noticeable startup names, for example, Nest or AlertMe and additionally various multinational enterprises like Philips, Haier, or Belkin.

2) Smart City

Brilliant city traverses a wide assortment of utilization cases, from activity administration to water appropriation, to squander administration, urban security and ecological observing. Its ubiquity is filled by the way that numerous Smart City arrangements guarantee to lighten genuine agonies of individuals living in urban communities nowadays. IoT arrangements in the territory of Smart City take care of movement blockage issues, lessen commotion and contamination and help make urban areas more secure.

3) Wearables

Wearables remains an intriguing issue as well. As purchasers anticipate the arrival of Apple's new savvy in April 2015, there are a lot of other wearable developments to be amped up for: like the Sony Smart B Trainer, the Myo signal control, or LookSee wrist trinket. Of all the IoT new companies, wearables creator Jawbone is presumably the one

with the greatest subsidizing to date. It remains at the greater part a billion dollars!

4) Connected car

The associated auto is coming up gradually. Inferable from the way that the advancement cycles in the car business commonly take 2-4 years, we haven't seen much buzz around the associated auto yet. Be that as it may, it appears we are arriving. Most huge vehicle creators and additionally some overcome new companies are chipping away at associated auto arrangements. Also, if the BMWs and Fords of this world don't present the cutting edge web associated auto soon, other understood goliaths will: Google, Microsoft, and Apple have all reported associated auto stages.

5) Connected Health (Digital health /Telehealth /Telemedicine)

Associated wellbeing remains the resting giant of the Internet of Things applications. The idea of an associated medicinal services framework and savvy therapeutic gadgets bears huge potential, not only for organizations likewise for the prosperity of individuals when all is said in done[13].

6) Business Services

A facility services company uses their multi-device IoT application to enable support personnel to receive alerts about service issues and take immediate action. By aggregating data from thousands of sensors in places like coffee machines, soap dispensers, paper towel dispensers and mouse traps rather than manual checks, the application has significantly cut costs and improved service levels.

V. IoT ELEMENTS

In this section I have listed and discussed on some key elements for IoT and IoT based applications. It can be as followed:

(i) Hardware
(ii) Middleware
(iii) User End Visualization

Hardwar constitutes of various sensors, actuators, embedded devices and other communication devices. ***Middleware*** constitutes of various tools used for on demand storage of data collected by sensor devices and processed by embedded devices and various computing tools used for data analytics. ***User End Visualization*** consists of various data visualization and interpretation tools which can be accessed on various diverse platforms which aids the end user to keep a track of various events driven by those data collected by various sensory hardwares.

Wireless Sensor Network (WSN): The propels in low power incorporated circuits and remote interchanges has made it a plausibility of making accessible effective, minimal effort, low power smaller than normal gadgets for use in remote detecting applications. These variables has enhanced the practicality and possibility of using a sensor organize comprising of a substantial number of shrewd sensors, empowering the accumulation, handling, investigation and dispersal of profitable data, assembled in an assortment of environments[14]. The information gathered by different sensor hubs are sent to either circulated frameworks or brought together frameworks (in light of need) for additionally preparing and examination that aides in different basic leadership forms and for mechanization forms basic leadership. The leap forward advances accomplished in improving equipment segments to a more noteworthy degree has expanded the life time of sensor hubs with enhancement at equipment level and at convention level.

Radio Frequency Identification (RFID): A radio-frequency identification proof framework utilizes labels, or names joined to the items to be recognized. Two-way radio transmitter-recipients called questioners or perusers send a flag to the tag and read

its reaction. The perusers by and large transmit their perceptions to a PC framework running RFID programming or RFID middleware. There are two sorts of RFID labels: Active Tags and Passive Tags. passive RFID labels are not battery fueled and they utilize the energy of the peruser's cross examination flag to impart the ID to the RFID peruser. This has brought about numerous applications especially in retail and inventory network administration. The applications can be found in transportation and access control applications also. The uninvolved labels are as of now being utilized as a part of numerous bank cards and street toll labels which is among the primary worldwide arrangements. Dynamic RFID perusers have their own particular battery supply and can instantiate the correspondence. Of the few applications, the principle utilization of dynamic RFID labels is in port compartments for checking cargo. The operating frequency range is: 120–150 kHz (LF), 13.56 MHz (HF), 433 MHz (UHF), 865-868 MHz (Europe)902-928 MHz (North America) UHF, 2450-5800 MHz (microwave), 3.1–10 GHz (microwave) with a range of 10cm to 200m[15].

Near Field Communication (NFC): It is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 cm (2 inches) of each other. In other words NFC, is a form of contactless communication between devices like smartphones or tablets. Contactless communication allows a user to wave the smartphone over a NFC compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection. Near field communication maintains interoperability between different wireless communication methods like Bluetooth and other NFC standards.

VI. CHALLENGES IN DEVELOPING IOT

This segment talks about a portion of the real difficulties that should be tended to assemble the IoT. The answers for these issues should be originated from innovative, social, legitimate, money related, and business foundations with a specific end goal to get wide acknowledgment by the IoT people group.

1. Guidelines and interoperability

Guidelines are imperative in making markets for new advances. On the off chance that gadgets from various producers don't utilize similar benchmarks, interoperability will be more troublesome, requiring additional entryways to make an interpretation of starting with one standard then onto the next. Likewise, an organization that controls distinctive parts of a vertical market may overwhelm a market, smothering rivalry and making hindrances for littler players and business people. Varying information measures can likewise tend to bolt shoppers into one group of items: if purchasers can't without much of a stretch exchange their information when they supplant one gadget with another from an alternate producer, they will as a result lose any advantage from the information they have been amassing after some time.

2. Security

As the IoT associates more gadgets together, it gives more decentralized passage focuses to malware. More affordable gadgets that are in physically traded off districts are more subject to altering. More layers of programming, combination middleware, APIs, machine-to-machine correspondence, and so forth make greater multifaceted nature and new security dangers. Hope to see various procedures and merchants tending to these issues with arrangement driven ways to deal with security and provisioning.

3. Trust and Privacy

With remote sensors and observing a center utilize case for the IoT, there will be elevated affectability to controlling access and responsibility for. Compliance will keep on being a noteworthy issue in medicinal and helped living applications, which could have life and passing repercussions. New consistence systems to address the IoT's special issues will develop. Social and political worries around there may likewise frustrate IoT appropriation.

4. Complexity, confusion and integration issues

With different stages, various conventions and vast quantities of APIs, IoT frameworks coordination and testing will be a test no doubt. The disarray around advancing measures is certain to moderate reception. The fast advancement of APIs will probably devour unforeseen improvement assets that will reduce venture groups' capacities to include center new usefulness. Slower appropriation and unforeseen improvement asset prerequisites will probably slip plans and ease back time to incomes, which will require extra subsidizing for IoT ventures and longer -runways for new businesses. [16]

5. Evolving architectures, protocol wars and competing standards

With such a significant number of players required with the IoT, there will undoubtedly be progressing turf wars as inheritance organizations look to secure their restrictive frameworks points of interest and open frameworks defenders endeavor to set new gauges. There might be numerous norms that develop in light of various prerequisites controlled by gadget class, control necessities, abilities and employments. This presents open doors for stage sellers and open source backers to contribute and impact future models. [16]

VII. CONCLUSION

In not so distant future there will be a bunch of Internet of Things (IoT) applications which will greatly affect our life. The IoT applications will go from brilliant home to keen human services with propel innovation. In this paper I have centered on IoT Introduction, IoT Architecture and IoT Applications. Hugh measure of research is completed around there. Be that as it may I have not tended to the security worries with IoT applications. The general public need new, adaptable, perfect and secure answers for both the administration of the always wide, unpredictably arranged Internet of Things, and furthermore for the help of different plans of action.

VIII. REFERENCES

[1]. Hesham el-sayed , Sharmi Sankar et al. "Edge of Things: The Big Picture on the Integration of Edge, IoT and the Cloud in a Distributed Computing Environment," Received October 24, 2017, accepted November 19, 2017, date of publication December 6, 2017,

[2]. I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey,'' Comput. Netw., vol. 38, no. 4, pp. 393_422, 2002.

[3]. L. Coetzee and J. Eksteen, "The Internet of Things_Promise for the future? An introduction,'' in Proc. IST-Africa Conf., 2011, pp. 1_9.

[4]. S. Zahra et al. "Fog Computing Over IoT: Secure Deployment and Formal Verification", Received August 30, 2017, accepted October 12, 2017, date of publication November 22, 2017, date of current version December 22, 2017.Digital Object Identifier 10.1109/ACCESS.2017.2766180

[5]. http://internetofthingsagenda.techtarget.com/definition/IoT-security-Internet-of-Things-security

[6]. Gartner, Inc. It can be accessed at: http://www.gartner.com/newsroom/id/2905717
[7]. Wang Chen,"AN IBE BASED SECURITY SCHEME OF INTERNET OF THINGS," in Cloud Computing and Intelligent Systems (CCIS), 2012, pp. 1046, 1049
[8]. Hui Suo, Jiafu Wan, Caifeng Zou, Jianqi Liu,"Security in the Internet of Things: A Review," in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651
[9]. Miao Wu, Ting-lie Lu, Fei-Yang Ling, ling Sun, Hui-Ying Du, "Research on the architecture of Internet of things," in Advanced Computer Theory and Engineering (ICACTE), 2010, pp. 484-487
[10]. Ying Zhang,"Technology Framework of the Internet of Things and Its Application," in Electrical and Control Engineering (ICECE), 2011, pp. 4109-4112
[11]. Guicheng Shen and Bingwu Liu,"The visions, technologies,applications and security issues of Internet of Things," in E-Business and E-Government (ICEE), 2011, pp. 1-4
[12]. L.Atzori, A.Iera, G. Morabito,"The Internet of Things: A survey," in Computer Networks - Science Direct
[13]. https://iot-analytics.com/10-internet-of-things-applications/
[14]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless Sensor Networks: A Survey, Computer Networks 38 (2002) 393–422.
[15]. K.Yogitha, V.Alamelumangai ,"Recent trends and issues in IOT", (IJAER) 2016, Vol. No. 11, Issue No. I, January, e-ISSN: 2231-5152/ p-ISSN: 2454-1796
[16]. The internet of things challenges and opportunities. Retrieved from http://sandhill.com/article/the-internet-of-things-challenges-and-opportunities/