IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 4, Ver. V (Jul.-Aug. 2016), PP 117-121
www.iosrjournals.org

Internet of Things: An Overview

Sheetal S. Joshi [1], Ketki R. Kulkarni[2]

[1](*Computer Science, North Lake Community College, USA)*
[2](*Electronics and Telecommunication, K.K.W.I.E.E.R, India)*

Abstract: *The growth of smart applications is reaching a whole new level. This allows shopping, banking and numerous everyday activities resulting in a comfortable life. The credit goes to the IoT (Internet of Things). It comprises capabilities of detecting and connecting numerous physical objects into an integrated system. This paper outlines the concept of Internet of Things and the technologies involved in it. The later section provides in brief the applications of Internet of Things in different domains along with risks associated in it.*
Keywords: *Internet of Things , RFID, WSN, Bluetooth and Wi-Fi ,network, risk, security*

I. Introduction

The Internet of Things (IoT) is a developing research area of technical, technological, socioeconomic effect. This innovation includes an extensive variety of networked products, frameworks, and sensors, actuators taking advantages of advances in web and interconnections giving new services not previously possible.

With the assistance of IoT objects are associated with Internet to change our working, living, and playing .The future will be changed to increase new dimension by making machines to converse with different machines for the benefit of individuals through IoT. IoT helps things to convey virtual identity and virtual personalities working in smart environment to speak with the users straightforwardly or might be through different things by insightful interfaces .Statistical investigation uncovers that there are between 10 to 20 billion things that are as of now associated with the Internet and in not so distant future assessed scope of associated articles by 2020 will be 40 to 50 billion [1].

Internet of Things; as name recommends it is things associated with internet. Internet is interconnection vital for correspondence though ; things are really data of things or information connected with things. Along these lines IoT offers data about things (counting area, status) empowering its access remotely through web [2]. IoT joins the physical world and data world expanding the extension for present day wireless communication. With expansive progression in the field of IoT, physical gadgets which can be called things can be associated and controlled from any place remotely [2]. IoT application horizon reaches out from object tracking to smart environmental control applications. IoT makes it possible to connect gadgets smartly [3]. There is no application area where IoT can't be applied.

Significant application areas of IoT incorporates healthcare for monitoring improvement of patient , in smart structures or homes for proficient power usage, in smart business for tracking merchandise, inventory administration, in mobiles empowering web checking at the travel times and picking routes ,giving data about traffic, pollution specifically territory, in smart Cities for environment checking application, in savvy car to decrease mischance via independent basic leadership diminishing human blunders, in banking sector, ,in instructive field actualizing brilliant classrooms by IoT, in mechanization commercial enterprises and many more[4],[5] as shown in figure 1.

II. Technologies In IOT

IoT requires taking data from objects or things, remarkably distinguishing a thing, setting up the association between two things or amongst thing and human and transmitting this information. For overcoming any issues between physical universe of things and data, sensors which can track things are required. Sensing paradigms which are every now and again utilized are RFID, WSN, Bluetooth and Wi-Fi. RFID innovation gives automatic identification of objects, their area and status data making it mainstream to use as object tracker.

RFID labels can be either passive, dynamic or battery assisted passive. A dynamic tag has an onboard battery while a battery helped passive has a little battery on board and is actuated within the sight of a RFID reader. Its scope of operation is 10cm to 200m.WSNs empower the accumulation, processing, analysis, and dispersal of gathered information. It additionally assumes imperative part in urban detecting applications. Bluetooth is another wireless technology for trading information over short distances. It utilizes short wavelength radio transmissions as a part of the ISM band from 2400–2480 MHz from fixed and portable devices. Its scope of operation is 1100m.Wi-Fi is a technology that permits an electronic device to trade information remotely. It utilizes radio waves over a PC system through fast Internet connections. It works at

frequency2.4 GHz, 3.6 GHz and 4.9/5.0 GHz groups and its scope of communication is normally up to 100m and can be broadened.

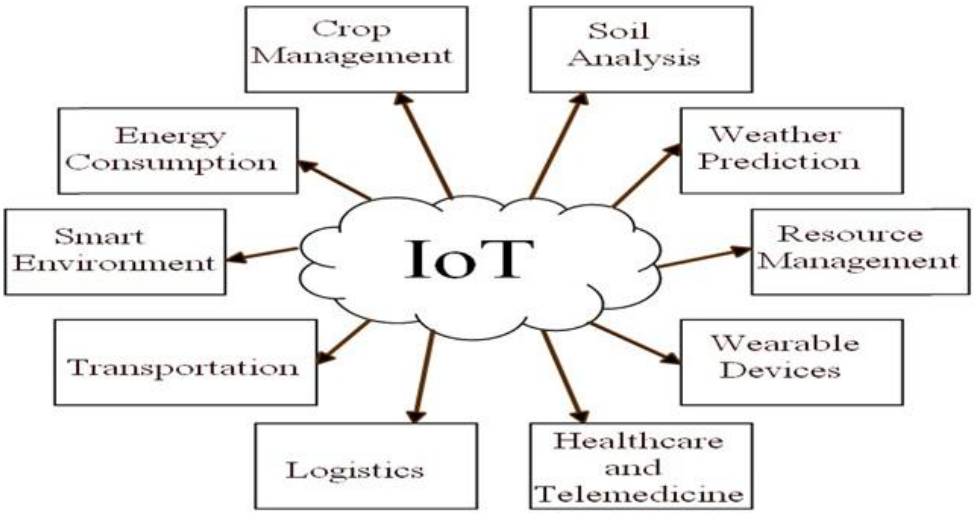

Fig1. Application Domains in IoT

Once the thing to be monitored is sensed, it should be addressed uniquely for making IoT successful. Unique addressing of things allows identification of numerous things and controlling them remotely without hampering device functionality. IPv4 and IPv6 provide solution to this problem. IPv4 has limitation in providing addresses which can be overcome by IPv6 providing 2128 unique addresses which can represent 2 Billions of Billions addresses per square millimetre of surface of earth. IPv6 also allows addressing mobile objects which makes it extremely suitable for using in IoT. Thus IPv6 serve as communication between devices through internet.

User Datagram Protocol (UDP) and Transmission Control Protocol (TCP/IP) are the two protocols that are used for sending messages that is datagrams on internet Protocol network (IP). IPv6 packets are compressed, encapsulated with header and sent or received on IEEE 802.15.4 based network using IPv6 over Low power Wireless Personal Area Network abbreviated as 6LoWPAN [6].

III. Applications In IOT

Possibilities offered by the IoT allow the advancement of countless, of which just a little part is at present accessible to our general public. There are many areas and environments in which new applications would likely enhance the nature of our lives: at home, at medical centres, at work etc. These domains are presently equipped with objects having very basic knowledge, the majority of times without any communication abilities among them. This ability gives a wonderful result like deploying numerous applications. These can be assembled into the following domains:

1) Healthcare
2) Transportation and logistics
3) Social
4) Smart environments

Among the possible applications, we can distinguish them as straightforwardly applicable or near to our current living habitudes. In the accompanying subsections we give a survey of some applications.

1. Healthcare domain

IOT provides numerous benefits to the medicinal area. And the subsequent applications can be grouped into:

i. Programmed data accumulation and sensing
ii. Identification and authentication of individuals iii. Keeping track of staff and patients

The IOT advances, for example, WSN, RFID etc., could convey different advantages in the healthcare area. For example, the health status of any person could be deduced from the RFID tags or from wearable medicinal gadgets. Furthermore, the application can be sorted into programmed data sensing [7], staff and patients tracking, authentication and identification proof of individuals, and remote healthcare. In the remote healthcare framework [8], every day blood glucose level, human blood oxygen level are gathered automatically

by the sensor nodes, transmitted remotely to the base station and showed contrasted with time on the screen. Additionally by associating the base station with an arranged home individual PC, specialists may check the information to check whether the outcomes are ordinary or not. The information can be exchanged to specialist cell phones through the GSM short message from the home base station. This framework offers advantages to clinic or remote human services at homes.

2. Transportation and Logistics Domain

The transportation like trains, buses, bikes, and cars are getting advanced with actuators, sensors, and also with processing power. Moreover transported merchandise and streets themselves can send imperative data to the traffic control sites. Also it can provide the transportation information to the traveler, and monitor the status of the goods being transported.

3. Social domain

The applications under this area are the ones that allow the user to interact with other individuals to keep up and build social connections. Without a doubt, naturally people exchange their messages with each other like meeting some common mates playing soccer, moving from/to our home/office, touring and travelling. In future urban communities, robot taxis swarm together, moving in groups, giving administration where it is required in an opportune and productive way. The robot taxis react to real time movement of traffic in city, and are adjusted to diminish congestion at bottlenecks in the city and to provide services in all most frequent areas. With or without a human driver, they weave all through activity at ideal velocities, keeping away from mischance through proximity sensors, which repulse them magnetically from different objects. These taxis can be called from the side of the road by indicating a cell phone at them or by utilizing hand signals. The client's location is consequently followed by means of GPS and empowers clients to ask for a taxi to be at a specific area at a specific time by simply calling attention to out on a detailed map. On the rare events when they are not being used, the taxis head for 'pit stops' the place where they consequently stack themselves into tight bays which are equipped with sensors where actuators set off recharging batteries, carry off simple maintenance tasks and clean the cars. The pit stop ensures the guarantee of no over or underutilization by communicating with each other [9].

4. Smart environments domain

A savvy situation is that making its "job" simple and agreeable on account of the knowledge of contained articles, be it an office, a home, a modern plant, or a recreation environment. Workplaces and home sensors and actuators, can make our life more agreeable in a few viewpoints: the room lighting can change as per the daylight, room warming can be adjusted to our inclinations and to the climate, the automatic switch off the electric equipments results saving energy, and local incidents can be controlled with proper alarm systems. We may consider energy suppliers as another example that utilizes dynamically changing energy costs to impact the general energy consumption in a way that smoothes load peaks. Throughout the day automation logic can optimize the consumption of power costs. This is done by observing the prices provided by an external web service and are according to the current energy production and consumption, of different home appliences like battery charger, refrigerator, ovens.

To improve the automation in industrial plants, smart environment can help with deployment of RFID tags which are related to the production parts. In a general situation, the tag will be read by the RFID reader as production parts reach the processing point. The RFID reader creates an event with some important data like RFID number which is stored on the network. The notification then goes to the robot or specific machine which picks up the production part. In parallel, to check the vibrations a wireless sensor is mounted on the machine. An event gets created promptly if the vibrations exceed a particular limit or threshold. The devices reacts with the emergency event if it occurs. The robot immediately stops the operation after getting the emergency event. The plant supervisor likewise promptly sees the status of the supposed Enterprise Resource Planning (ERP) orders [10], [11].

IV. Risks Associated With IOT

This section describes various risks associated with the perception layer, network layer, middleware layer and application layer.

1. Perception Layer Challenges

Even if there are number of accomplishments in the research field of IoT, the open risks cannot be ignored. The next passage will explain various risks associated with the IoT.

i. Spoofing Attack

Spoofing attack is a situation where the hacker or attacker shows wrong information to the RFID systems which makes it showing up from the original

ii.. Jamming Of Radio Frequencies : With the denial of service attacks (DoS) the RFID tags can also be traded off by the hacker. With an abundance of noise signals the actual radio frequency signals is interrupted.
iii.. Cloning Of RFID Tags : As mentioned above the RFID tags or data associated with it can be easily read or altered by the hacker, also it can be cloned with some hacking strategies. The cyber criminals can make a copy of the tags in such a way that the reader cannot recognize the unique and the traded off tag.
iv. Unauthorized Access to the Tags: The RFID tags can be easily accessed by someone without authorization due to the lack of proper authentication. Even though the data can't just read however it can be deleted or edited by the hacker [12].

2. Network layer Challenges

Network layer comprises of the Wireless Sensor Network (WSN) which transmits the information from the sensor to its destination with dependability. There are several issues related with the security. Following are some risks associated with it:
i. Sybil Attack: Sybil is a sort of attack in which the attacker controls the hub to exhibit numerous personalities for a solitary hub because of which an impressive part of the system can be traded off bringing about false data about the redundancy.
ii. Sinkhole Attack: It is a sort of attack in which the hacker makes one node look appealing. As a result the information flow from a specific node is redirected towards the new compromised node. Hence the traffic get silenced by believing that the information has been gotten on the other side.
iii. Sleep Deprivation attack: The sensor nodes within the WSN have poor lifetime batteries. Hence in order to extend the lifetime these sensor nodes follows certain sleep schedule. At this point sleep deprivation attack takes place. In this type of attack the sensor nodes stay alert or awake constantly, and generate more battery utilization. As a result all of the sensor nodes are forced to cease.
iv. DoS Attack: The DoS attack takes place when the system is overflowed by the hacker with numerous requests. This action exhausts the original resources resulting in the unavailability of the network to its users.
v. Malicious Code Infusion: In this type of attack the hacker hacks a node which infuses pernicious code into the system. As a result of this inappropriate action the hacker get full control over the network.

3. Middleware Layer Challenges
i. Malicious Insider: This sort of attack happens when somebody from within alters the information for individual advantages or the advantages of any outsider. The information can be effectively extricated and afterward modified intentionally from within.
ii. Unauthorized Access: To store the data as well as applications various interfaces are provided by the middle ware layer. The hacker can simply tricks the system by deleting the existing information. This obstructs the access to the related services resulting in damaged system.
iii. Denial of Service Attack: This is the DoS attack which makes the services and resources unavailable to the users as discussed above.

4. Application Layer Challenges:
Some of the security concerns are given below:
i. Malicious Code Injection. **:** In this type of attack, the hacker can influence the attack on the framework from end-client with some hacking methods that permit the hacker to infuse any sort of malignant code into the framework to take some sort of information from the client.
ii. Sniffing Attack: In this type of attack the attacker focuses on the framework by bringing a sniffer application into the framework, which could pick up system data bringing about defilement of the framework.
iii. Spear-Phishing Attack: It is an email spoofing attack in which casualty, a high positioning individual, is baited into opening the email through which the foe accesses the qualifications of that casualty and afterward by a misrepresentation recovers more delicate data.
iv. Denial-of- Service (DoS) Attack: DoS attack can take place in any or all layers. The hacker or the attacker makes constant requests for the resources resulting in network unavailability for other end users.

V. Conclusion

Considering the current growth of IT, in near future it can be inferred that IoT will expand more and more. In this paper, we provide an overview of Internet of Things with various technologies like RFID, WSN, Bluetooth, Wi-Fi. Moreover, various application areas are discussed along with examples. By using various standards and protocols we can implement numerous IoT applications. Privacy and security issues are the main hurdle in the way of the IoT development. Security at all the levels of IoT is expository to the functioning of IoT. As of now there has been numerous research accomplishments in the IT security concerns

and for powerful execution of a security framework for IoT, these accomplishments should be further extended rather off centering the consideration towards the new possible security arrangements.

References

[1]. S. DuBravac, C. Ratti ,The Internet of Things: Evolution or Revolution?, Part1 series 1, Consumer Technology Association

[2]. Y. Huang and G. Li, A Semantic Analysis for Internet of Things, IEEE International Conference on Intelligent Computation Technology and Automation,2010,pp. 336-339

[3]. L. Coetzee and J. Eksteen, The Internet of Things – Promise for the Future? An Introduction, IST-Africa, Conference. Proceeding, IIMC International Information Management Corporation, 2011, pp.1-9

[4]. Lu Tan and Neng Wang, Future Internet: The Internet of Things, IEEE 3rd International Conferenc. on Advanced Computer Theory and Engineering(ICACTE),,2010, vol.5, pp. 376-380

[5]. M H Asghar, N Mohammadzadeh and A Negi, Principle Application and Vision in Internet of Things (IoT), IEEE Internationa. Conference on Computing, Communication and Automation (ICCCA), 2015,pp. 427-431

[6]. https://postscapes.com/internet-of-things-technologies/

[7]. J. Tan., G. Simon., and M. Koo., A Survey of Technologies in Internet of Things, 2014 IEEE International Conference on Distributed Computing in Sensor Systems, pp. 269 – 274.

[8]. A. Vilamovska., E. Hattziandreu., R. Schindler., C. Van Oranje., H. De Vries., and J. Krapelse., RFID Application in HealthcareScoping and Identifying Areas for RFID Deployment in Healthcare Delivery. RAND Europe, February 2009.

[9]. Y. Liu and G. Zhou, Key Technologies and Applications of Internet of Things, ICICTA, 2012, Intelligent Computation Technology and Automation, International Conference on, Intelligent Computation Technology and Automation, International Conference on 2012, pp. 197-200, doi:10.1109/ICICTA.2012.56

[10]. L. Atzori., A. Iera., and G.Morabito., The Internet of Things: Survey, Computer Networks Journal 54(2010), pp.27872805.

[11]. https://iotanalytics.com/10internetofthingsapplications/

[12]. A M.U. Farooq ,M Waseem ,A Khairi , S Mazhar , Critical Analysis on the Security Concerns of Internet of Things (IoT) , International Journal of Computer Applications (0975 8887) Volume 111 - No. 7, February 2015