International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

AN OVERVIEW OF SIX LAYERED ARCHITECTURE, SECURITY AND PRIVACY CHALLENGES OF IOT

Revathi Gangisetty[1],
[1]Assistant Professor,
Department of CSE,
BVRIT,
Narsapur, India.

May 23, 2018

Abstract

Internet, a dynamic development, is constantly changing into some new kind of hardware and software making it unavoidable for anyone. The type of correspondence that we see now is either human-human or human-device, however the Internet of Things (IoT) guarantees an extraordinary future for the internet where the sort of correspondence is machine-machine (M2M). This paper proposed to give a detailed outline towards IoT situation and specifies its empowering advancements and the sensor networks. Likewise, it portrays a six-layered architecture of IoT and calls attention to the related key challenges.

***Key Words*:**WSN, RFID, IOT architecture, IoT applications, IoT Vision, Internet of Things, IoT security.

1 Introduction

With the persistent progressions in innovation a potential development, IoT is descending the street which is prospering as a pervasive worldwide registering network where everybody and everything

will be associated with the Internet [1]. IoT is constantly developing and is a hot research theme where openings are unending. Creative energies are vast which have put it nearly reshaping the present type of internet into an altered and coordinated variant. The quantity of devices benefiting internet administrations is expanding each day and having every one of them associated by wire or wireless will put an intense wellspring of data readily available. The idea of empowering collaboration between canny machines is a front line innovation yet the advancements creating the IoT are not something new for us [2]. IoT, as you can figure by its name, is the approach of meeting information got from various types of things to any virtual stage on existing Internet infrastructure [3]. The idea of IoT goes back to 1982 when an altered coke mama chine was associated with the Internet which could report the beverages contained and that whether the beverages were cool [4]. Afterward, in 1991, a contemporary vision of IoT as omnipresent registering was first given by [5]. However in 1999, Bill Joy provided some insight about Device to Device correspondence in his scientific classification of internet [6]. In the extremely same year, Kevin Ashton proposed the expression "Internet of Things" to portray an arrangement of between associated devices [7]. The essential thought of IoT is to permit independent trade of valuable data between undetectably implanted diverse remarkably identifiable genuine devices around us, energized by the main technologies like Radio-Frequency IDentification (RFID) and Wireless Sensor Networks (WSNs) [2] which are detected by the sensor devices and further prepared for basic leadership, based on which a mechanized activity is performed [1].

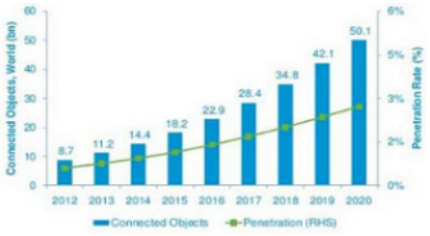

FIGURE 1 Expected penetration of connected objects by the year 2020, according to Cisco

The paper is sorted out as takes after. Area 2 dissects the

vision of the IoT. Section 3 depicts the bland architecture of the IoT. Section 4 examines the advances that IoT is made out of. Section 5 estimates the future applications. Section 6 talks about the privacy and security challenges postured by IoT and at last Section 7 concludes the paper.

2 VISION

In 2005, ITU revealed about an omnipresent networking period in which every one of the networks are interconnected and everything from tires to clothing types will be a piece of this immense network [8]. Envision yourself doing an internet look for your watch you lost some place in your home. So this is the primary vision of IoT, a domain where things can talk and their information can be prepared to perform wanted errands through machine learning [9]. A useful implementation of IoT is shown by a destined to be discharged Twine, a minimized and low-control equipment cooperating with ongoing web software to make this vision a reality [10]. However unique individuals and associations have their own particular diverse visions for the IoT [11].

An article distributed in Network World uncovered IoT methodologies of best IT merchants, they did a few meetings from the key IT sellers. As of HP's vision, they see a world where individuals are associated with their substance. Cisco has confidence in the mechanical mechanization and meeting of operational innovation. Intel is focused on enabling billions of existing devices with knowledge. Microsoft does not think about IoT as any modern innovation; they trust that it as of now exists in the present effective devices and that the devices simply should be associated for a lot of information which could be useful. In spite of having distinctive visions, they all concur about a network of interconnected devices along these lines more advancements inside the coming decades are relied upon to be seen including that of another merged data society [13].

3 ARCHITECTURE

In excess of 25 Billion things are required to be associated by 2020 [14] which is a colossal number so the current architecture of Internet with TCP/IP conventions. Without a legitimate privacy confirmation, IoT isn't probably going to be received by numerous [17]. In this way assurance of information and privacy of clients are key challenges for IoT [18].

[21] proposed a five layered architecture utilizing the best highlights of the architectures of Internet and Telecommunication administration networks in view of TCP/IP and TMN models separately. Similarly a six-layered architecture was likewise proposed in light of the network various leveled structure. So for the most part it's partitioned into six layers as appeared in the Fig. 2.

The six layers of IoT are depicted beneath:

A. Coding Layer

In this layer, each object is specified with one kind of ID which makes it simple to observe the objects.

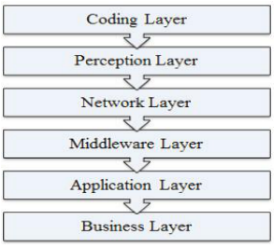

Figure 2 IoT : Six-Layered Architecture

B. Perception Layer

It is a device layer of IoT towards physical importance to each object. It comprises of information sensors in various structures like RFID labels, IR sensors or other sensor networks which could detect the temperature, dampness, speed and area and so forth of the objects. This layer accumulates the valuable data of the objects from the sensor devices connected with them and proselytes the data into computerized signals.

C. Network Layer

The motivation behind this layer is get the valuable data as advanced signs from the Perception Layer and transmit it to the preparing frameworks in the Middleware Layer.

D. Middleware Layer

This layer forms the data got from the sensor devices [2]. It incorporates the innovations like Cloud registering, Ubiquitous figuring which guarantees an immediate access to the database to store all the fundamental data in it. Utilizing some Intelligent Processing Equipment, the data is prepared and a completely auto-mated move is made in view of the handled aftereffects of the information.

E. Application Layer

This layer understands the applications of IoT for a wide range of industry, in light of the prepared information. Since applications advance the improvement of IoT so this layer is exceptionally useful in the substantial scale improvement of IoT network. The IoT related applications could be brilliant homes, savvy transportation, shrewd planet and so on.

F. Business Layer

This layer deals with the applications and administrations of IoT and is responsible for all the examination identified with IoT. It produces diverse business models for powerful business procedures [1].

4 TECHNOLOGIES

The development of a pervasive processing framework where digital objects can be exceptionally recognized towards objects to gather information based on which automated moves are made, requires the requirement for a mix of new and successful innovations. In this segment we examine the applicable innovations that can help in the vast scale development of IoT.

A. Radio Frequency IDentification (RFID)

RFID is the key technology for making the objects extraordinarily identifiable. It is a handset microchip like a cement sticker which could be both dynamic and uninvolved, contingent upon the kind of application. Dynamic tags have a battery connected to them because of which they are constantly dynamic and in this manner persistently produce the information signals while Passive tags simply get enacted when they are activated. RFID system is made out of perusers and related RFID tags which discharge the identification, area or some other specifics about the object, on

get-ting activated by the age of any fitting signal.

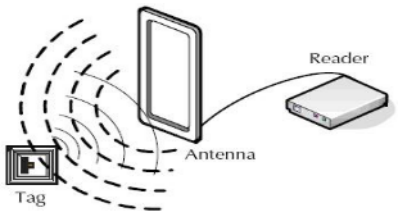

Figure 3 RFID Scenario

Contingent upon the kind of application, RFID frequencies are partitioned into four unique frequencies ranges, which are given beneath:

1. Low frequency (135 KHz or less)
2. Ultra-High Frequency (862MHz 928MHz)
3. High Frequency (13.56MHz)
4. (4)Microwave Frequency (2.4G , 5.80)

Bar Code is additionally an identification technology which has nearly an indistinguishable capacity from a RFID yet RFID is more viable than a Bar Code because of some of its advantages. Also, a RFID can fill in as an actuator to trigger diverse occasions and it has even change capacities which Bar codes plainly don't have.

B. Wireless Sensor Network (WSN)

WSN is a bi-directional wirelessly connected network of sensors in a multi-jump mold, worked from a few hubs scattered in a sensor field each connected to one or a few sensors which can gather the object particular information, for example, temperature, dampness, speed and so forth and then pass on to the handling hardware [16]. The detecting hubs convey in multi-jump Each sensor is a handset having a radio wire, a miniaturized scale controller and an interfacing circuit for the sensors as a correspondence, activation and detecting unit individually alongside a wellspring of energy which could be both battery or any vitality gathering technology. However [2] has proposed an extra unit for sparing the information, named as Memory Unit which could likewise be a piece of the detecting hub.

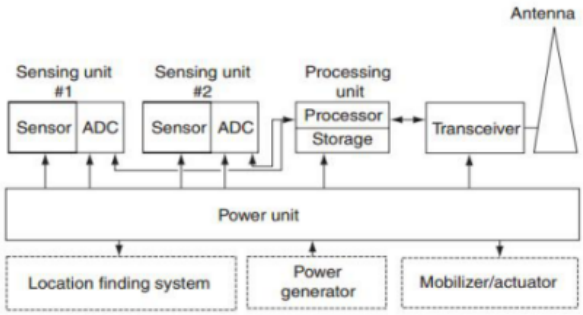

FIGURE 4 A typical sensing node

Wireless Sensors Network technology and RFID technology when joined together opens up potential outcomes for significantly more savvy devices, for which various arrangements have been proposed. A case arrangement is given by the Intel Research Labs as Wireless Identification Sensing Platform (WISP). WISP is a latent wireless sensor network with builtin light, temperature and numerous different sensors [5].

The innovations that empowers the reconciliation of WSN with the IOT are a hot research point, numerous arrangements have been proposed for that including that of a 6LOWPAN standard [8], that enables IPv6 packets to be transmitted through the networks that are computationally confined. Likewise there's ROLL routing standard for end-to-end routing arrangements [15].

C. Cloud Computing

With a huge number of devices anticipated that would stop by 2020 [14], the cloud is by all accounts the main technology that can break down and store every one of the information adequately. It is an intelligent computing technology in which number of servers are united on one cloud platform to permit sharing of assets between each other which can be gotten to whenever and wherever [18]. Cloud computing is the most essential piece of IoT, which meets the servers as well as procedures on an expanded preparing power and investigates the helpful information got from the sensors and even give great stockpiling limit [13]. Be that as it may, this is only a start of releasing the genuine capability of this technology. Cloud computing interfaced with keen objects utilizing conceivably a huge number of sensors can be of colossal advantages and can

help IoT for an expansive scale development so looks into are being done since IoT will be absolutely reliant on the Cloud Computing.

Figure 5 A typical Cloud Computing Scenario

D. Networking Technologies

These technologies have an imperative part in the accomplishment of IoT since they are in charge of the association between the objects, so we require a quick and a successful network to handle countless devices. For wide-run transmission network we commonly utilize 3G, 4G and so on yet As we probably am aware, versatile movement is such a great amount of unsurprising since it just needs to play out the standard undertakings like making a call, sending an instant message and so on. so as we advance into this cutting edge period of omnipresent computing, it won't be unsurprising any longer which requires a need of a super-quick, super-proficient fifth era wire-less system which could offer significantly more bandwidth [17]. Correspondingly for a short-extend correspondence network we utilize technologies like Bluetooth, WiFi and so on.

E. Nano Technologies

This technology acknowledges littler and enhanced form of the things that are interconnected. It can diminish the utilization of a sys-tem by empowering the development of devices in nano meters scale which can be utilized as a sensor and an actuator simply like an ordinary device. Such a nano device is produced using nano segments and the subsequent network characterizes another networking worldview which is Internet of Nano-Things [18].

F. Micro-Electro-Mechanical Systems (MEMS) Technologies

MEMS are a blend of electric and mechanical segments cooperating to give a few applications including sensing and inciting which are as of now being financially utilized as a part of numerous field as transducers and accelerometers and so on. MEMS ombined with Nano technologies are a financially savvy answer for ad libbing the correspondence system of IoT and other advantages like size decrease of sensors and actuators, incorporated ubiquitous computing devices and higher scope of frequencies and so on [19].

5 APPLICATIONS

The vast majority of the day by day life applications that we ordinarily observe are al-prepared smart however they can't speak with each other and empowering them to speak with each other and offer utilize full information with each other will make an extensive variety of innovative applications [11]. These rising applications with some self-governing capacities would absolutely enhance the nature of our lives. A couple of such applications are as of now in the market [22], we should take the case of the Google Car which is an activity to furnish a self-driving auto involvement with continuous movement, street conditions, climate and other information trades [12], all because of the concept of IoT. There are various conceivable future applications that can be of extraordinary advantage. In this segment, we display few of these applications:

A. Smart Traffic System

Movement is an essential piece of a society along these lines all the related issues must be legitimately tended to. There is a requirement for a system that can enhance the movement circumstance in light of the activity information acquired from objects utilizing IoT technologies [23]. For such an intelligent activity observing system, acknowledgment of an appropriate system for programmed identification of vehicles and other movement factors is critical for which we require IoT technologies as opposed to utilizing basic picture handling techniques [4]. The intelligent movement observing system will give a decent transportation encounter by facilitating the clog. It will give highlights like robbery recognition, announcing

of auto collisions, less environmental contamination. The streets of this smart city will give preoccupations with climatic changes or unforeseen roads turned parking lots because of which driving and strolling courses will be advanced [21]. The traffic lighting system will be climate versatile to spare vitality. Benefit capacity of parking spots all through the city will be available by everybody.

B. Smart Environment

Forecast of cataclysmic events, for example, surge, fire, quakes and so on will be conceivable because of inventive technologies of IoT. There will be an appropriate observing of air contamination in the environment.

C. Smart Home

IoT will likewise give DIY answers for Home Automation with which we will have the capacity to remotely control our apparatuses according to our requirements. Legitimate observing of utility meters, vitality and water supply will help sparing assets and identifying sudden over-burdening, water spills and so forth. There will be legitimate infringement identification system which will anticipate robberies. Cultivating sensors will have the capacity to gauge the light, dampness, temperature, dampness and other planting vitals, and in addition it will water the plants as per their necessities.

D. Smart Hospitals

Healing centers will be furnished with smart adaptable wearable inserted with RFID tags which will be given to the patients on entries, through which not simply specialists but rather medical attendants will likewise have the capacity to screen heart rate, circulatory strain, temperature and different states of patients inside or outside the premises of doctor's facility [15]. There are numerous medicinal crises, for example, heart failure yet ambulances set aside some opportunity to achieve tolerant, Drone Ambulances are as of now in the market which can travel to the scene with the first aid pack so because of legitimate observing, specialists will have the capacity to track the patients and can send in the automaton to give speedy restorative care until the point when the rescue vehicle arrive.

E. Smart Agriculture

It will screen Soil nourishment, Light, Humidity and so forth and enhance the green lodging background via programmed change of temperature to expand the creation. Exact watering and treatment

will help enhancing the water quality and sparing the composts separately [16].

F. Smart Retailing and Supply-chain Management

IoT with RFID gives numerous advantages to retailers. With RFID prepared items, a retailer can undoubtedly track the stocks and recognize shoplifting. It can monitor every one of the things in a store and to keep them from leaving stock, it puts in a request consequently. Besides the retailer can even produce the business diagram and charts for viable methodologies.

6 RESULT

IoT makes everything and individual locatable and addressable which will make our lives significantly simpler than previously; however without an absence of certainty about the security and privacy of the client's information, it's all the more probably not going to be received by many [17]. So for its universal reception, IoT must have a solid security infrastructure. A portion of the conceivable IoT related issues are as taken after:

A. Unauthorized Access to RFID

An unapproved access to tags that contains the identification information is a noteworthy issue of IoT which can uncover any kind of private information about the client so it should be tended to. Not only the tag can be perused by a reprobate peruser yet it can even be altered or potentially be harmed. In this specific situation, [17] condensed a portion of the genuine threats of RFID which includes RFID Virus, Side Channel Attack with a cell-phone and SpeedPass Hack.

B. Sensor-Nodes Security Breach

WSNs are helpless against a few sorts of assaults since sensor hubs are the piece of a bi-directional sensor network as talked about in Section 4.2, which implies other than the transmission of information, air conditioning acquisition of information is likewise conceivable. [18] portrayed a portion of the possible assaults that includes Jamming, tampering, Sybil, Flooding and some other kinds of assaults, which are abridged as taken after:

1. Jamming deters the whole network by interfering with the frequencies of sensor hubs.

2. Tampering is the type of assault in which the hub information can be extricated or changed by the assailant to make a controllable hub.

3. Sybil assault guarantees numerous pseudonymous personalities for a hub which gives it a major influence. Flooding is a kind of a DOS assault caused by a lot of movement that outcomes in memory depletion.

C. Cloud Computing Abuse

Cloud Computing is a major network of joined servers which permit sharing of assets between each other. These common resources can confront a great deal of security threats like Man-in-the-middle assault (MITM), Phishing and so forth. Steps must be taken to guarantee the total security of the clouding platform [19]. Cloud Security Alliance (CSA) proposed some conceivable threats among which few are Malicious Insider, Data Loss, Accounts Hijacking and Monstrous utilization of Shared Computers and so forth [20] which are outlined as taken after:

1. Malicious Insider is a danger that somebody from the inside who have an entrance to the client's information could be involved in information mama nipulating.

2. Data Loss is a risk in which any villain client who has an unapproved access to the network can change or erase the existing information.

3. Man-in-the-middle (MITM) is a kind of Account Hijacking risk in which the aggressor can modify or intercept messages in the correspondence between two gatherings.

4. Cloud computing could be utilized as a part of a gigantic ways in light of the fact that if the assailant gets the opportunity to transfer any malignant software in the server e.g. using a zombie-armed force (botnet), it could get the aggressor a control of many other connected devices.

7 CONCLUSION

With the incessant burgeoning of the emerging IoT technologies, the idea of Internet of Things will soon be inexorably developing

on a vast scale. This emerging worldview of networking will influence all aspects of our lives ranging from the computerized houses to smart well being and environment monitoring by embedding intelligence into the objects around us. In this paper we talked about the vision of IoT and exhibited an all around defined architecture for its arrangement. Then we featured different enabling technologies and few of the related security threats. And finally we talked about various applications resulting from the IoT that are relied upon to encourage us in our day by day lives. Looks into are as of now being done for its wide range selection, however without addressing the challenges in its development and providing secrecy of the privacy and security to the client, it's exceedingly far-fetched for it to be an omni-introduce technology. The organization of IoT requires strenuous endeavors to handle and present answers for its security and privacy threats.

References

[1] Stankovic, John An. Exploration Directions For The Internet Of Things. IEEE Internet Things, 2014.

[2] Cecchinel, Cyril, Matthieu Jimenez, S' ebastien Mosser, Michel Riveill. An Architecture To Support The Collection Of Big Data In The Internet Of Things. IEEE 10Th World Congress On Services, 2014.

[3] Journal, RFID. That 'Web of Things' Thing - RFID Journal. [online] Rfidjournal.com. Accessible at: http://www.rfidjournal.com/articles/view?4986,2015.

[4] Atzori, Luigi, Antonio Iera, Giacomo Morabito. The Internet Of Things: A Survey. Computer Networks, 2010.

[5] Li, Shancang, Li Da XU, and Shanshan Zhao. The Internet Of Things: A Survey. Springer Science, Business Media New York, 2014.

[6] Guoru Ding, Long Wang, Qihui Wu. Huge Data Analytics In Future Internet Of Things. National Natural Science Foundation Of China, 2013.

[7] Sulayman K sowe, Takashi Kimata, Mianxiong Dong, Koji Zettsu. Managing Heterogeneous Sensor Data On A Big Data Platform: Iot Services For Data-Intensive Science. IEEE 38Th Annual International Computers, Software And Applications Conference Workshops, 2014.

[8] Antonio J. Jara, Dominique Genoud,Yann Bocchi. Big Data In Smart Cities: From Poisson To Human Dynamics. 28Th International Conference On Advanced Information Networking And Applications Workshops, 2014.

[9] Stephen Kaisler, Frank Armor, J. Alberto Espinosa, William Money. Huge Data: Issues And Challenges Moving Forward. 46Th Hawaii International Conference On System Sciences, 2013.

[10] Gartner. Enormous Data Management and Analytics. [Online]. Accessible: http://www.gartner.com/innovation/points/huge data.jsp, 2015.

[11] nformationWeek. At the point when Internet Of Things Meets Big Data - InformationWeek. [online] Available at: http://www.informationweek.com/huge information/enormous information examination/when-web of-things-meets-huge information/a/d-id/1298137, 2014.

[12] Lu Tan, Neng Wang. Future Internet: The Internet Of Things. 3Rd International Conference On Advanced Computer Theory And Engineering (ICACTE), 2010.

[13] Shashank Agrawal, Dario Vieira. A Survey On Internet Of Things. Abakos, 2013.

[14] Innova.com.tr, (2015). Innova conveys shrewd home and brilliant office administrations for TTNET — Innova. [online] Available at: http://www.innova.com.tr/en/news-detail.asp?haber=777C888F-C922-8822-EEE2-BBB222FF333C, 2015.

[15] Smart Health. Strolling Fit. [online] Available at: http://smarthealthusa.com/strolling fit, 2015.

[16] Bidnessetc.com. Web Of Things: Connecting (And Disrupting) Your Universe. [online] Available at: http://www.bidnessetc.com/business/web of-things-interfacing and-upsetting your-universe,2014.

[17]]Smartpharma.co.za. Welcome to Smart Pharmaceuticals. [online] Available at: http://www.smartpharma.co.za, 2015.

[18] Jasper Tan, Simon G. M. Koo. A Survey Of Technologies In Internet Of Things. IEEE International Conference On Distributed Computing In Sensor Systems, 2014.

[19] Charu C. Aggarwal, Naveen Ashish, Amit Sheth. The Internet Of Things: A Survey From The Data-Centric Perespective, Managing And Mining Sensor Data. Springer Science, Business Media New York, 2013.

[20] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, M. Palaniswami. Internet Of Things (Iot): A Vision, Architectural Elements, And Future Directions. Future Generation Computer Systems, 2013.

[21] Khaled Salama, Abbas El Gamal. Examination Of Active Pixel Sensor Readout Circuit. IEEE Trans. Circuits System, 2003.

[22] Abhisek Ukil. Towards Networked Smart Digital Sensors: A Review. IEEE, ABB Corporate Research, Switzerland, 2008.

[23] CRC Press, (2015). Biosensors in Food Processing, Safety, and Quality Control. [online] Available at: http://www.crcpress.com/item/isbn/9781439819852googlePreviewContainer, 2015.