International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 3 ǁ 2021 ǁ PP. 36-39

IoT Applications Challenges Privacy and Security

Naveena.K.S [1], Poorana senthilkumar S[2]
[1]*PG Student, Department of Computer Science, Dr.N.G.P Arts and Science College, Tamil Nadu, India*
[2]*Assistant Professor, Department of Computer Science, Dr.N.G.P Arts and Science College, Tamil Nadu, India*

ABSTRACT
Now a day's Internet of Things (IoT) gained an excellent attention from researchers, since it becomes a crucial technology that promises a sensible person life, by allowing a communications between objects, machines and IoT represents a system which consists things within the world , and sensors attached to or combined to those things, connected to the web via wired and wireless network structure. The IoT sensors can use various connections like RFID, Wi-Fi, Bluetooth, and ZigBee, additionally to allowing wide area connectivity using many technologies like GSM, GPRS, 3G, and LTE. IoT enabled things will share information about the condition of things and therefore the surrounding environment with people, software systems and other machines. The present IoT enabling technologies have been improved within the recent years, there are still numerous problems that need attention. Privacy and security are among the many challenges of the internet of Things (IoT).This highly interconnected global network structure referred to as Internet of Things will enrich everyone's life However, this new reality (IoT) built on the idea of Internet, contains new quite challenges from a security and privacy perspective. IoT infrastructure consists of resource constrained devices like RFIDs and wireless sensor nodes. Therefore, a versatile infrastructure is required capable to affect security and privacy issues in such a dynamic environment. This paper presents a summary of IoT, security and privacy challenges and therefore the existing security solutions and identifying some open issues for future research during this paper we review an idea of the many IoT Technologies and future possibilities for brand spanking new related technologies.

KEY WORDS: *Internet of Things; privacy and security challenges, applications of internet of things*

Date of Submission: 09-03-2021 Date of acceptance: 23-03-2021

I. INTRODUCTION

The Internet of Things (IoT) refers to an idea of connected objects and devices of every type over the internet wired or wireless [1].The popularity of IoT or the online of Things has enlarged speedily. IoT introduced the hyper connectivity thought that suggests organizations and people IoT has improved the life-style of individuals by introducing machine-driven services. Most of the protection professionals think about IoT as a result for the purpose of cyber attacks as a result of weak security protocols and policies. IoT enabled devices are utilized in industrial applications and for multiple business are created to existing ones. Think about the latest advances among the 5G network, for example. 5G is expected to play vital for new technologies emerge, among the IoT systems and applications [2].It's obtaining the researchers attention and curiosity regarding the attainable security and privacy risks, with its high frequency and information measure. The internet of Things (IoT) started with Machine to Machine (M2M) communication. M2M communication indicates 2 machines human action with each other, typically while not human involvement. The communication platform is not outlined, and may be each wireless and wired communication. The term M2M stems from telecommunications, the different endpoints ought to exchange info between one another, rather like the identity of the caller. Sources By developing the IoT technology, testing and deploying product and implementing sensible environments by 2020.[5]In future, storage and communication services are about to be extremely distributed: individuals, machines, sensible objects, encompassing house and platforms connected with wired/wireless sensors, RFID tags can produce a extremely decentralized resources interconnected by a dynamic network .The IoT communication are going to be supported practical protocols, Finally the internet can terminate by a conclusion of the general sections.

Fig.1 *Example of applications*

II. INTERNET OF THINGS APPLICATIONS

Internet of things has many applications in human life, and making life easier, safe and smart. There are many applications like smart cities, homes, transportation, energy and smart environment.

A. Smart Cities

Many major cities were supported by smart projects, like Singapore, Dubai. Smart cities may still be viewed as cities of the future and smart life, and by the innovation rate of creating smart cities today's, it will became very feasible to enter the IoT technology in cities development.[6] Smart cities demand requires careful planning in every stage, with support of agreement from governments, citizens to implement the web of things technology in every aspect. By the IoT, cities are often improved in many levels, by improving infrastructure, enhancing public transportation reducing traffic jam,and keeping citizens safe, healthy and more engaged within the community of all systems within the cities like transportation ,healthcare system, weather monitoring systems and etc.., additionally to support people by the web in every place to accessing the database of airports, railways, transportation tracking operating under specified protocols, cities will become smarter by means of the internet of things.

B. Smart Home and Buildings

Wi-Fi's technologies in home automation are used primarily because of the networked nature of deployed natural philosophy wherever electronic devices like TVs, mobile devices, etc.., are typically supported by Wi-Fi. Wi-Fi have started changing into a part of the house information science network and due the increasing rate of adoption of mobile computing devices like good phones, tablets, etc.., for instance a networking to supply on-line streaming services or network at homes, could give a mean to manage of the device practicality over the network.[8] At identical time mobile devices make sure that customers have access to a transportable 'controller' for the natural philosophy connected to the network. each varieties of devices is used as gateways for IoT applications several corporations are considering developing platforms that integrate the building automation with diversion, care observation, energy observation and wireless device observation within the home and building environments By the idea of the internet of things, homes and buildings could operate several devices and objects well, of the foremost fascinating application of IoT in good homes and buildings are good lighting, good environmental and media, air management and heating, energy management and security.

III. INTERNET OF THINGS CHALLENGES

The fact that internet of things applications and eventualities printed on top of are terribly fascinating that provides technologies for good each thing. However there are some challenges to the applying of the internet of Things thought in value of implementation [10].The expectation that the technology should be on the market at low value with an oversized range of objects. IoT are sweet-faced with several different challenges:

Scalability: net of Things includes a huge thought than the standard net of computers, attributable to things is cooperated among associate degree open atmosphere. Basic practicality like communication and repair discovery thus got to operate equally expeditiously in each tiny scale and huge scale environments. The IoT needs a replacement functions associate degreed ways so as to realize an economical operation for measurability.

Self-Organizing: good things mustn't be managed as computers that need their users to tack and adapt them to explicit things[12].Mobile things, that are usually got to establish connections and ready to be organizing and tack themselves to suit their explicit atmosphere.

Information volumes: Some application eventualities of the web of things can involve to infrequent communication, and gathering information's type device networks, or type supplying and huge scale networks, can collect an enormous volumes of information on central network nodes or servers. The term represent this phenomena is huge information that is needs several operational mechanism additionally to new technologies for storing, process and management.

Computer code complexity: Iot of intensive computer code infrastructures are required on the network and on background servers so as to manage the good objects and supply services to support them. That as a result of the computer code systems in good objects can need to operate with stripped-down resources, as in standard embedded systems.

Security and privacy: additionally to the protection and protection aspects of the web such in communications confidentiality, the believability and trustiness of communication partners, and message integrity, different necessities would even be vital in a web of Things. There's a desire to access bound services or stop from communication with different things in IoT and additionally business transactions involving good objects would want to be protected against competitors' prying eyes.

Wireless communications: From associate degree energy purpose of read, established wireless technologies like GSM, UMTS, Wi-Fi and Bluetooth are so much less suitable; newer WPAN standards like ZigBee et al still below development might have a narrower information measure, however they are doing use considerably less power

IV. SECURITY FOR INTERNET OF THINGS

If one factor will forestall the internet of things from reworking the means we live and work, it'll be a breakdown in security. The interconnected nature of IoT devices means each poorly secured device that's connected on-line probably affects the safety and resilience of the Internet globally.[8] This implies that rights and respect for user privacy expectations are integral to making sure user trust and confidence within the net, connected devices, and connected services. IoT brought users large benefits; but, some challenges come back together with it. Cyber security and privacy risks area unit the first issues of the researchers and security specialists cited. These 2 area unit movement a substantial difficulty for several business organizations likewise as public organizations. Prevailing high-profile cyber security attacks have incontestable the vulnerabilities of IoT technologies.[7] This result of the interconnectivity of networks within the internet of Things brings on accessibility from anonymous and untreated internet requiring security solutions of all the challenges that area unit noted, none of them encompasses a additional vital influence on IoT Adaptation, like security and privacy. It is, however, unfortunate that the users don't typically have the specified acknowledgment of the safety impacts till the time once has occurred, inflicting huge damages like loss of crucial knowledge.[6]With the continued security that have compromised the privacy of users, the appetence of the shoppers for poor security is currently declining.

V. SECURITY

The IoT is numerous from ancient computers and computing devices, an excellent example of this is often sensors. Usually, the preparation of IoT contains of a group of alike or nearly identical appliances that similar characteristics. Similarly, several establishments have come back up with guides for risk assessment physical phenomenon. This step means that the probable range of links interconnected between the IoT devices new.[4] It is additionally clear that several of those devices will establish connections and communicate with alternative Devices mechanically in associate irregular method. These entail thought of the accessible tools, Techniques, and techniques that are associated with the safety of IoT. Even with the difficulty of security within the sector of knowledge and technology not being new, IoT implementation has bestowed distinctive challenges that require to be addressed. The customers are needed to trust the internet of Things devices and therefore the services are terribly secure from weaknesses, significantly as this technology continues turning into additional passive and incorporated in our everyday lives[5]. With protected of IoT gadgets and services, this is often one Knowledge the info the information of users by going away data streams not protected adequately.

VI. PRIVACY

The perspective of the quality of the IoT depends on however well it will respect the privacy of individuals. Issues relating to the privacy and also the potential harms that return at the side of IoT could be important in holding back the complete adoption of IoT. The connected Device, and connected services[9]. IoT is redefining the privacy problems such things because the increase of work and following. The rationale for the privacy issues is due to the present intelligence integrated artifacts wherever the sampling method and also the data distribution within the IoT could also be done nearly in anywhere. The ever present property via the net access is additionally an important issue that helps in understanding this downside as a result of internet of things.

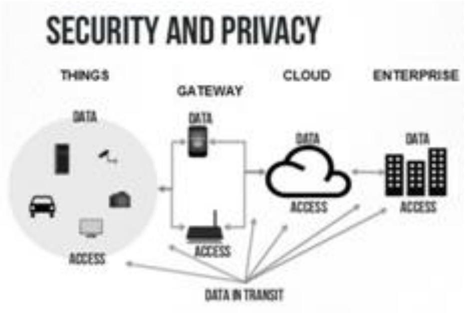

Fig.2 examples of privacy and security

VII. CONCLUSION

This paper aims to provides the reader a basic summary concerning internet of Things, the most important security and privacy challenges due to its exponential growth and what reasonably security primitives and approaches are being taken to form communication secure and to safeguard the user's information. The IoT devices support the collaboration with the stakeholders and facilitate in understanding the business necessities and outcomes. IoT-based analytics and processing will enhance the productivity and efficiency of commercial infrastructures. As a lot of and a lot of analysis studies are conducted, new dimensions to the IoT processes, technologies concerned and also the objects which will be connected, still emerge, additional method for more application functionalities of IoT. the actual fact that IoT is therefore expansive and affects much all areas of our lives, makes it a major analysis topic for studies in numerous connected fields like data technology and applied science. The paper highlights numerous potential application domains of the internet of things and also the connected analysis challenges. Different current problems, like address restriction, automatic address setup, security functions like authentication and cryptography, and functions to expeditiously can most likely be affected in implementing the conception of the net of things however by current in technological developments these challenges are going to be overcome. The internet of things guarantees future new technologies once associated with cloud, fog and distributed computing, big data, and security problems. By desegregation of these problems with the internet of things, smarter applications are going to be developed as before long. This paper surveyed a number of the foremost vital applications of IoT with explicit specialize in addition to the challenges implementation the internet of things conception, and also the different future technologies create the conception of IoT possible.

REFERENCES

[1]. M. A. Ezechina, K. K. Okwara, C. A. U. Ugboaja. The Internet of Things (Iota): A Scalable Approach to Connecting Everything. *The International Journal of Engineering and Science* 4(1) (2015) 09-12.

[2]. http://www.meraevents.com/event/iot-workshop

[3]. http://www.nxp.com/assets/documents/data/en/white-papers/INTOTHNGSWP.pdf

[4]. Sarnia C. M., Nitha K. P., Analysis of Security methods in Internet of Things. *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume 3, Issue 4; April 2015.

[5]. Sapandeep Kaur, Ikvinderpal Singh. A Survey Report on Internet of Things Applications. *International Journal of Computer Science Trends and Technology* Volume 4, Issue 2, Mar - Apr 2016.

[6]. S. V. Zanjal and G. R. Talmale, "Medicine reminder and monitoring system for secure health using IOT," Procedia Computer Science, vol. 78, pp. 471–476, 2016.

[7]. R. Jain, "A Congestion Control System Based on VANET for Small Length Roads", Annals of Emerging Technologies in Computing (AETiC), vol. 2, no. 1, pp. 17–21, 2018, DOI: 10.33166/AETiC.2018.01.003.

[8]. S. Soomro, M. H. Miraz, A. Prasanth, M. Abdullah, "Artificial Intelligence Enabled IoT: Traffic Congestion Reduction in Smart Cities,"

[9]. Liu, X.; Zhao, M.; Li, S.; Zhang, F.; Trappe,W. A security framework for the internet of things in the future internet architecture. Future Internet **2017**, 9, 27. [CrossRef]

[10]. Ali, S.; Bosche, A.; Ford, F. Cybersecurity Is the Key to Unlocking Demand in the Internet of Things; Bain and Company: Boston, MA, USA, 2018.

[11]. Benjamin Kleine, Bethany Lobo, Amanada Levendowski March 2015 Internet of Things: The new frontier for data security and privacy (Part 1).

[12]. Gartner's Hype Cycle Special Report for 2015,Gartner Inc.,2015. http://www.gartner.com/technology/ research/ hype-cycles/