International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 4

ISSN: 2454-4248
131 – 134

Analysis of Data Aggregation Techniques of IOT

Loveneet Singh
Software Engineering/Computer Science
Chandigarh University, India
loveneetsandhu1994@gmail.com

Er. Manjot Kaur
Computer Science Department
Chandigarh University, India
manjot.cse@cumail.in

***ABSTRACT* :-**The internet of things is the self configuring network in which sensor nodes can join or leave the network when they want. The security, data aggregation are the two major issues of IOT. In the previous years various techniques are designed to improve data aggregation rate of IOT. The clustering is the technique which can increase data aggregation rate and reduce lifetime of the network. In this paper, various techniques are reviewed to improve lifetime of the network and increase data aggregation rate

KEYWORDS*:-IOT, Data Aggregation, RFID*

*****

1. INTRODUCTION

The internet of things is the technology that allows users to achieve deep analysis, integration and automation within the system. In this technology sensor nodes sense the information from the environment and pass that information to base station. That gathered information than uploaded to the main server. When sensors change their positions handoff mechanism is installed. With the help of this accuracy and reach to the area of the system can be improved. In order to sense the network and robotics various technologies are emerged. It also exhibits the modern advance in the software technology as well as in hardware. Major changes can be seen in the exiting elements when the new advancements are done in product delivery, goods and services, economically and socially [1]. This concept was established from the member of Radio Frequency Identification (RFID) development community. In today's world everyone are connected to each other through internet over public or private Internet Protocol (IP) networks where they can sense the sense the environment, communicate and share information. All the interconnected objects collect the information from surroundings and analyzed that data to initiate the action in order to provide management and decision making.

It is defined as a network of physical objects. It is not the interconnection between the networks but it also evolved into a network of various types and sizes cameras, medical instruments and industrial systems, animals, people, buildings and so on. All these are interconnected to provide the communication and sharing of information to achieve smart reorganizations, positioning, process control & administration. IoT can be defined into three parts such as it is people to people, people to machine and machine to machine where interaction takes place through internet. It is a concept that considers a persistent presence in the environment for various objects in order to achieve the same goal through wired or wireless connection. Hence its applications are wide that create the development challenge to be huge [2]. It is a world where all the digital and virtual things has been utilized for the convergence of smart environment including transport, energy, cities and many more. It recognized as the general idea of things where everyday objects that can be controllable via internet irrespective of the communication devices such as wired or wireless networks.

RFID stands for the Radio-Frequency Identification and it is known to be the main object within the IoT. The building of global infrastructure for RFID tags which is known to be a wireless layer present on the top of Internet. The communication is made amongst network of interconnected objects and the interconnected computers. At some instants there are different Internet Protocol locations for the objects. These objects are embedded within the complex systems. Various sensors have been utilized to gather the information related to temperature, and other aspects present in the surroundings [3]. The sensors present near to each other transfer the gathered information in order to provide further processing as per the requirements of the current applications. All the aggregated information by the others objects or the components of complex devices can be accessed by the internet of things. The main objective of the Internet of Things is to communicate with any device anywhere using various paths and services.

The importance of IoT can be understood before we know the differences between the Internet and the World Wide Web. The Internet is the physical layer or network made up of switches, routers, and other equipment. The transportation of the information from one place to another place safely and reliably is the prime objective of IoT. The operation of the web is on the top of the internet that is

 ISSN: 2454-4248
131 – 134

application layer. It provides an interface that makes the information flowing across the Internet usable.

1.2 Characteristics of IoT

a. Interconnectivity: Internet of things enables to connect various devices and share information over the internet. With the help of global information and communication infrastructure huge number of things can be connected to each other.

b. Heterogeneity: The IoT technology can be applied on the various heterogeneous devices and networks. Different network platforms utilized for the communication with other devices [4]. A major issue which arises here is the communication that is to be provided amongst the devices.

c. Dynamic changes: There are dynamic changes in the state of the devices such as connected or disconnected as well as change in their speed or location. There is dynamic change in most of the devices.

d. Enormous scale: In order to mange number of devices and their connection with each other must be at least larger than an order of magnitude as compared to connected devices to internet currently. [5].

e. Safety: The safety of our personal data is very important for the safety of our physical well- being. The security paradigm can be created for the endpoints security, connected networks and moving data.

f. Connectivity: This feature allows processing of data traffic and their accessibility within the IoT. The common ability to consume and produce data is provided by the compatibility and the accessibility passes it to the network. The connection between the heterogeneous devices can be established using this.

1.3 Challenges and Barriers to IoT

The development potential of IoT is slowdown by the various challenges [6]. When the IoT technology is deployed in the systems, there are various challenges that arise amongst which some are explained below:

a. Deployment of IPv6: Previously world working on the IPv4, that slows down the potential of IoT's progress due to requirement of unique IP address to the each sensor. The management of network becomes easier with the help of IPv6 as it provides the auto configuration capabilities and offers improved security features.

b. Security: Security within these systems is always a major concern as there are numerous systems involved during the communication being held. Thus, the data involved within these systems is to be made secure.

c. Privacy: One of other major concerns within these systems is the violation of privacy of data present in them. In order to ensure that only the authorized users are given access to the private information.

d. Cost versus Usability: The physical objects can be connected to the internet using IoT technology. The cost of components must be inexpensive in near future for which support is required for the purpose of tracking, sensing and controlling in order to grow the adaptability of IoT.

e. Interoperability: The most basic core value in the traditional internet was interoperability [7]. The basic requirement of the interconnectivity is to connect with systems that operate on the same protocols and encodings. To support different application various standards has been utilized by huge number of industries. These diverse entities become important due to the use of standard interfaces where large amount of data and Heterogeneous devices are embedded.

f. Data Management: It is very difficult to manage such large amount of data hence it is considered as the critical aspect in the Internet of Things. When daily exchange of data is numerous and the objects are connected from world wide than it becomes difficult challenge for internet of things to provide optimal results.

g. Scalability: As the things are in cooperated within the open environment the Internet of things becomes the major concept as compare to the conventional Internet of computers [8]. Therefore, it is required to function equally in the basic functionality such as communication and service discovery.

1.4 Security issues

There is several security issues that exists within the IoT network that need to be in consideration. Some of them given below:

a. Unpredictable Behavior – The behavior of the internet of things are unpredictable due to the complete volume of deployed devices and enabling technologies they have. There is no prediction about how systems works when it interact with others hence is required a specific system that is well designed and within the control of administration [10].

b. Device Similarity –They are uniform in their nature. Internet of things utilized the same components and connection technology. All the present nodes in the network have the same specification for the transfer of data from source to destination. If one system or device suffers from the same issue other devices also show vulnerability and did not perform well.

 ISSN: 2454-4248
131 – 134

c. Problematic Deployment – The placement of networks and analytics is the main goal of the IoT at the place where it is not possible to go physically. Hence, it becomes a problem to secure the devices that are placed in the unknown and accessible area.

d. Longevity of devices –Longevity is one of the benefits of IoT device that means they may live longer than their device support them. Traditional systems are now obsolete as they are no longer in use.

e. No Upgrade Support – There is no modification or up gradation is allowed by many IoT devices such as in case of small devices. Many up gradation are offered that are ignored by the user or not recognized. Hence, up gradation of a system from time to time is very essential in IoT.

f. Web interface vulnerability: In order to circumvent access controls by hackers this is security vulnerability in web applications. Some security issues are vulnerable weak sessions, poor credentials management and cross-site scripting. This becomes major issue as large number of devices uses the cloud for the access.

g. Poor or No Transparency – According to their functionality many IoT devices fail to provide transparency. The user not aware of the internal processing of the system hence fails to access and observer the functionality of devices. There is no control of user on the unnecessary functions or data collection. It becomes more difficult to update the devices when more unwanted functions are applied [10].

h. No Alerts – This is the issue that occurs at the user end due to the lack awareness of user. User has no access to devices even they are unaware when something went wrong. Therefore, the main goal of the IoT is to provide the advanced functionality that provide all the data if the user is not present physically. Security violate can persevere over long periods without detection.

2 Literature Review

Daemin Shin, et.al (2016) presented PMIPv6 security protocols do not support the secure route optimization involved when communication of mobile node with external IoT devices in these services [11].The security and performance is ensured by the path of MNs and the IoT devices, the trust amongst the PMIPv6 domain and smart home is utilized in the newly proposed protocol. On the basis of simulation result, it is demonstrated that the RO issue within the PMIPv6 is resolved and the handover latency is minimized due to which the transmissions provided by proposed algorithm are highly secure in comparison to existing protocols.

Shuai Zhang, et.al (2017) presented a secure analytical framework, through which the delay and secrecy of the network are to be characterized. In order to enhance the performance of the network, a low-complexity secure on-off mechanism is proposed [12]. The delay and secrecy performances can be enhanced here with the help of secure on-off mechanism. On the basis of simulation results, the effects caused by the secure on-off scheme are seen in terms of the performance results on delay and secrecy of the IoT systems.

Dr. ReshmaBanu, et.al (2016) presented that the traditional security mechanisms cannot handle the newly derived IoT systems which include advanced properties, techniques and issues within them. Therefore, it is necessary to propose a new secure IoT mechanism with the involvement of biologically inspired models which help in security the IoT paradigms in much better way [13]. For different robust and computationally efficient security methods present in IoT, the research gaps are proposed in this paper along with the numerous biologically inspired algorithms that have used to improve the security of these techniques.

MinelaGrabovica, et.al (2016) presented major issue within the IoT is the data security. There is various communication technologies used within IoT that utilize the security protocols which are studied in this paper. The most commonly used protocols are RFID, Bluetooth, Wireless network and ZigBee [14]. The cryptography and security measures are provided on MAC layer by the ZigBee. On the basis of 128 bit keys and AES encryption, ZigBee provides access control, encryption, integrity of frame as well as the sequential freshness. The numerous techniques are compared and an analysis of these techniques amongst each other is presented in this paper.

ZimuGuo, et.al (2016) presented the connection between the endpoint devices and physical objectsthat are connected to Internet within the Internet of Things (IoT), hence it is require to ensure the security within the IoT systems [15]. However, there are various security issues as well which have been faced by the users. The convenience as well as security of IoT applications needs to be enhanced which is provided by the biometrics. The advantages as well as disadvantages related to the biometrics present within IoT are to be considered in this paper. The novel biometrics is combined with the system-level obfuscation techniques so that the unauthorized users cannot access the IoT devices. With the help of this technique the security of IoT devices is improved

José L. Hernández-Ramos, et.al (2015)presented a mechanism in which smart objects utilized the present information to make decision that provides security. The so-called context-aware security present on the IoT systems is

 ISSN: 2454-4248
131 – 134

computed by taking this gathered data as first priority. Amongst the various components related to security of framework, the interactions are provided by this method. This helps in generating awareness amongst the systems by providing envisioned security methods. As per these methods, the security decisions are adapted by this system

Conclusion

In this paper, it is concluded that internet if things is the type of network which sense the information and pass it to base station. The energy consumption, security are the major issues of the IOT. In this review paper, various techniques are reviewed which improve security and energy consumption. The techniques which are already proposed are compared in terms of certain parameters

References:

[1] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," Elsevier Future Generation Computer System, Vol. 29, No. 7, pp. 1645–1660, 2013.

[2] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on Internet and underlying issues," Ad Hoc Networks, vol. 28, pp. 68–90, 2015.

[3] O. Said and M. Masud, "Towards internet of things: survey and future vision," International Journal of Computer Networks, vol. 5, no. 1, pp. 1–17, 2013.

[4] R. M. Cardoso, N. Mastelari, and M. F. Bassora, "Internet of Things Architecture in the Context of Intelligent Transportation System – A Case Study Towards a Webbased Application Deployment," in 22nd International Congress of Mechanical Engineering (COBEM 2013), 2013, pp. 7751–7760

[5] J. S. Kumar and D. R. Patel, "A survey on internet of things: Security and privacy issues," International Journal of Computer Applications, vol. 90, no. 11, 2014.

[6] L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. Carbone, M. Marotta, and J. J. C. de Santanna, "Internet of things in healthcare: Interoperatibility and security issues," in Communications (ICC), IEEE International Conference on. IEEE, 2012, pp. 6121–6125.

[7] T. Abels, R. Khanna, K. Midkiff, "Future Proof IoT: Composable Semantics, Security, QoS and Reliability", in Proc. of IEEE Topical Conference on Wireless Sensor & Sensor Networks (WiSNet), pp. 1-4, 2017.

[8] Keyur K Patel1 , Sunil M Patel2, "Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges", IJESC, 2016.

[9] Kim Thuat Nguyen, Maryline Laurent, NouhaOualha, "Survey on secure communicationprotocols for the Internet of Things", Ad Hoc Network, vol. 7, pp. 5-15, 2015.

[10] Chen Chen, Honghui Zhao, Tie Qiu, Mingcheng Hu, Hui Han, Zhiyuan Ren, "An efficient power saving polling scheme in the internet of energy", Journal of Network and Computer Applications 89 (2017) 48-61

[11] [Daemin Shin, Vishal Sharma, Jiyoon Kim, Soonhyun Kwon, and Ilsun You, "Secure and Efficient Protocol for Route Optimization in PMIPv6-based Smart Home IoT Networks", 2016, IEEE

[12] Shuai Zhang, Jianhua Peng, Kaizhi Huang, Xiaoming Xu and Zhou Zhong, "Physical Layer Security in IoT: A Spatial-Temporal Perspective", 2017, IEEE

[13] Dr. ReshmaBanu, Dr. G. F. Ali Ahammed, NasreenFathima, "A Review on Biologically Inspired Approaches to Security for Internet of Things (IoT)", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016

[14] MinelaGrabovica, DraženPezer, SrdanPopic, Vladimir Kneževic, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey", 2016, IEEE

[15] ZimuGuo, NimaKarimian, Mark M. Tehranipoor and Domenic Forte, "Hardware Security Meets Biometrics for the Age of IoT", 2016, IEEE

[16] José L. Hernández-Ramos, Jorge Bernal Bernabe, Antonio F. Skarmeta, "Managing Context Information for Adaptive Security in IoT environments", 2015 29th International Conference on Advanced Information Networking and Applications Workshops