I J C T A, 9(37) 2016, pp. 377-384

Handling the Unstructured Data in IOT

Sunil Kumar Mishra M*

Abstract: The Internet of Things (IoT) is a new trend of connecting different devices to the Internet with no or minimal human involvement. This is also known as Machine to Machine (M2M) communication, a widely increasing area in the world of electronic and computing which gives ability to different devices to exchange their information autonomously through networks including Internet, Wireless Sensor Networks (WSNs), etc. IoT has various applications in transport, logistic, industrial management, health care, supply chain management, asset tracking, smart environment, energy, defense, and agriculture domains. However, there are several challenges associated with IoT such as standardization, interoperability, integration with other networks, *Security* and the most important is the handling of heterogeneous sensors and there data. Large amount of data will be formed from billions of devices and to store, handle and making the data secured is surely not an easy task. In this paper, we have discussed about the general information, Architecture, security background of IoT And continued with maintenance of the Unstructured data using various techniques. Finally, we have also discussed some research directions that could be the future work for the solutions to the data related challenges for IOT.

Keywords: Internet of things; NoSQL; Sensors; Big Data**.**

1. INTRODUCTION

What is "IoT"? Till many years group of researchers and organizations tried to know and understand for the exact definition for IOT. Haller et al. proposed a definition of IoT with "*A world where physical objects are seamlessly integrated into the information network, and where the physical objects can become active participants in business process*." [1].Whereas Sarma et al. defines the "Things" from physical objects to virtual objects which represents as the identities with Internet connectivity [2]. IOT is characterized by the introduction of M2M applications with no or minimal human involvement [3]. It is the new field of "ubiquitous computing" [4] or "ambient intelligence"[5] which has enhanced the intelligence of the objects around us by combining the computing capabilities to the physical context. Although IEEE IoT Initiative is proceeding to draft a white paper for the formal definition of IoT, that there are still no common agreements for the definition of IoT. In this paper we describe "THING" as any physical object which can connect to the internet and can communicate with different objects as well. When the growth of the IOT increases, the security problem also becomes very important for the heterogeneity and large scale of the objects. [20] As the connection of the object increases, the security should also be taken care. The security problem for the "Things" is created by vulnerabilities produced by careless program design; this creates opportunities for malwares or backdoors installation [6]. In this paper we are going to discuss various challenges which are faced in the field of IOT.

2. ARCHITECTURE OF IOT

To build the architecture of IoT is not at all an easy task. There are lots of devices of various sizes and to combine then for a working model is very big task. A. Zanella Has told that because of very large variety of devices it's very complex task to build a general architecture for IoT based services [16]. Moreover

* Sunil Kumar Mishra M, Department of Information Technology, SRM University, Kattankulathur, Singara garden, Old Washermenpet Chennai, India. *Email: Skmsunil55@gmail.com*

the basic architecture of IoT consists of three layers namely sensing layer, network layer and application layer.

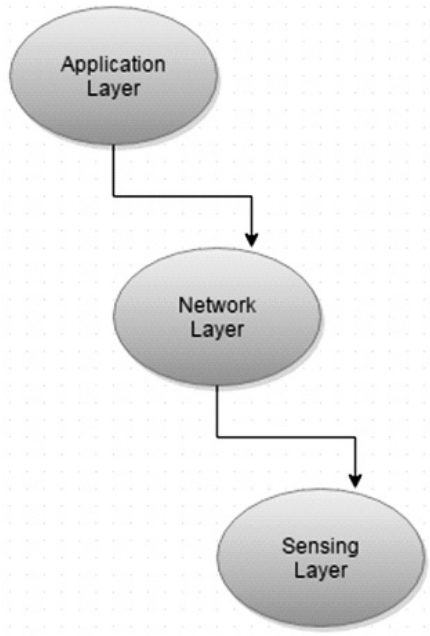

Figure 1: Architecture of Internet of Things

A. Application layer: The objectives of the application layer are to provide the method which shows us that how the user is going to use the information services. Application layer in IoT architecture is the place where IoT and industry technologies converge and make real-time applications of different industries such as production control, transportation, smart girds, public safety and health care. However, these applications are not limited to industries only.

B. Network Layer: This layer is on the middle of the Internet of Things architecture. The main purpose of the network layer is to perform the functions of transmission, information processing, through the network connected like LAN, WAN, etc.

C. Sensing Layer: The main objectives of sensing layer are to identify, acquire and collect data by sensing physical properties of the objects of environment. The sensing layer gathers in-formation from RFID tags, sensors, 2D Bar codes, actuators and terminals, etc. The collected information is converted into digital signals.

The generic architecture of IoT is simple and gives brief insight into the purposes and functions of the individual layers. However, this generic architecture does not address the issues of security and privacy which is a major concern in IoT. Since IoT is being used in large numbers of applications, the architecture must provide the security for tags, communications, network transmissions, storages and processing. IoT architecture must handle the privacy issues such as public cryptography, authentication, authorization and aggregation. These points are further discussed later in this pap. Integration of IOT with Other Networks.

Integration of IOT with Other Networks

A. Connecting WSNs to the Internet is possible in the three main approaches mentioned by [9], differing from the WSN integration degree into the Internet structure. Currently adopted by most of the WSNs accessing the Internet, and presenting the highest abstraction between networks, the first proposed approach for WSN (Figure 2) consists of connecting both independent WSN and the Internet through a single gateway.

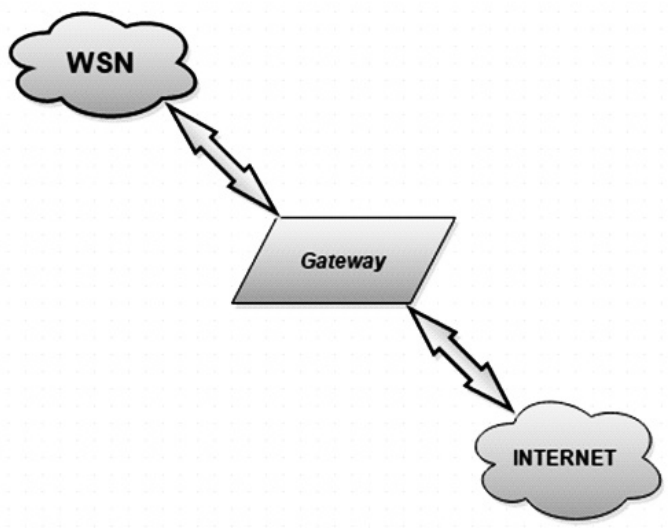

Figure 2: Independent Network

Showing an increasing integration degree, the second approach (Figure 2) forms a hybrid network composed of both considered.

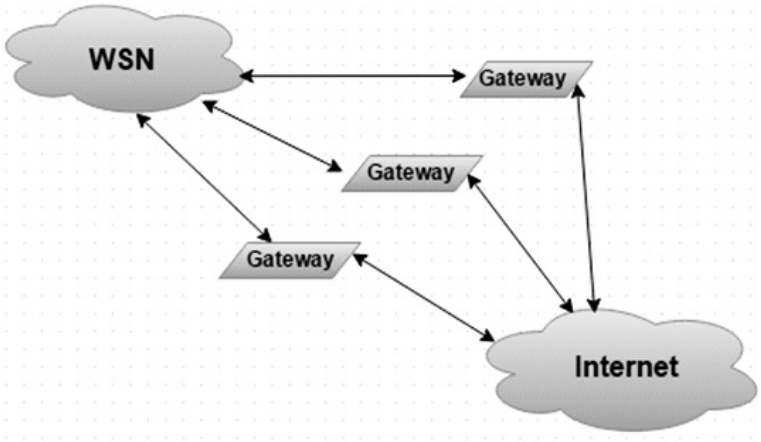

Figure 3: Hybrid Network

Whereas the connection showed in Figure 4, is inspired from WLAN structure which forms a dense 802.15.4 access Point network and can join multiple sensor nodes with Internet in one hop.

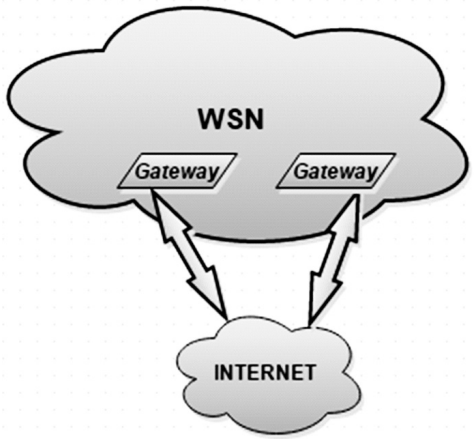

Figure 4: Access point Network

B. Wireless Local Area Network (WLAN): The last approach is inspired from current WLAN structure and forms a dense 802.15.4 access point network, where multiple sensor nodes can join the Internet in one hop. IEEE 802.11, also known as WLAN, is a wireless network which connects two or more objects/devices through a wireless (radio) connection.

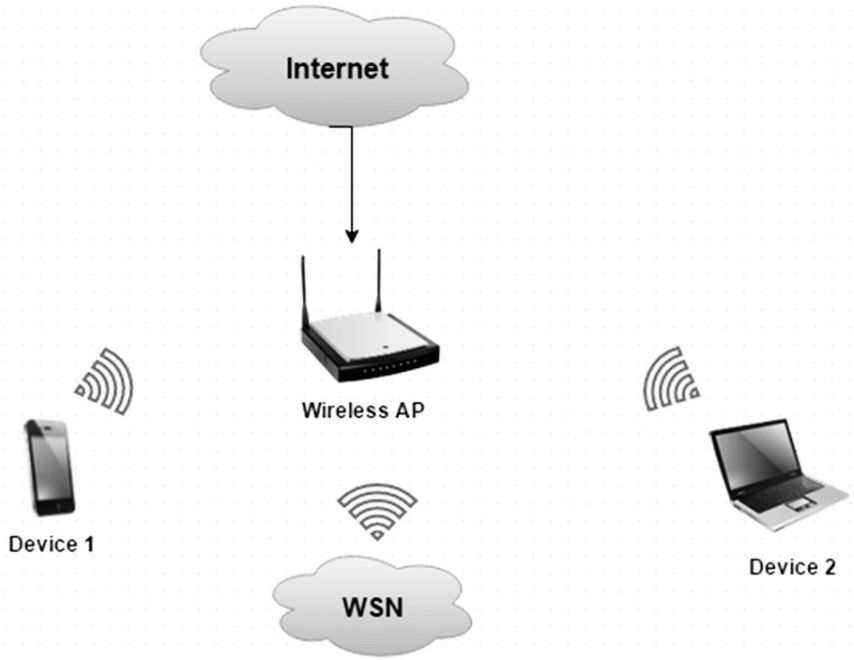

Figure 5: Wireless Local Area Network

In this section, we discuss different technologies and networks that are involved for the integration of the Internet of Things such as Radio Frequency Identification (RFID), Wireless Sensor Network (WSN), Wireless Personal Area Network (WPAN) and Wireless Local Area Network (WLAN).

C. Radio Frequency Identification: RFID consists of RFID tags and reader. The objects are uniquely identified by RFID technology and their unique identification information is stored in a tag. The tag consists of an antenna, small memory and Electronic Product Code (EPC). RFID reader reads unique identification code to identify the devices. It is the ideal technology for the recognition of the things in the IoT environment.

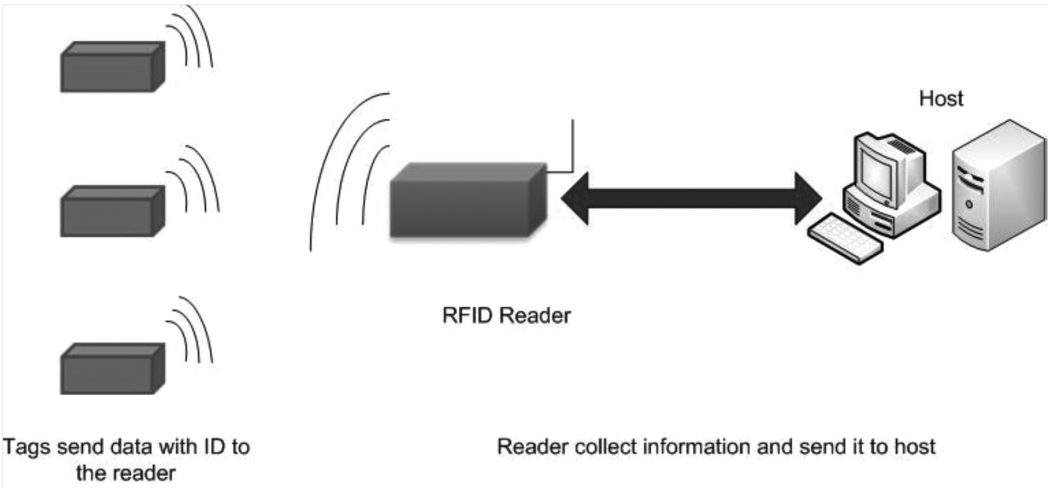

Figure 6: Radio Frequency Identification

3. SECURITY CHALLENGES FOR IOT

According to various reports there are more than 20 billion devices at present, and to connect so many devices is not at all an easy task. As the applications of IoT are increasing, the challenges in the IoT field are also in-creasing. IoT is considered to bring along multiple technological, economical and social challenges. Developing technologies and solutions for enabling the IoT vision is a major challenge. Various standards of wireless networking empower the Internet of Things technologies for rapid development, but these developments also present some major challenges of security, performance and scalability [7]. In security, the privacy is most common issue. For example, in the e-mails, war, enemies or hackers can send false information to us through wireless sensors by intruding wireless sensor network. To highlight and discuss the challenges emerging from such novel responsibility assignment, researcher's has discovered three potential tasks that the sensor nodes would have to accomplish: Security and quality of service (QoS) management, and network configuration. [8]. In general, the main challenges of IoT are related to formalization, standardization and data. Formalization means that obtained data must be complete and reliable. For example, the equipment must be accurately and widely arranged in such manner that in case of breakdown, other components should be replaced. There is need of international standards and communication protocols for the development of IoT applications. To enable the communication of different "things" or "objects" with Internet, they all need communication standards. Network address data, descriptive data, position and environmental data, sensor data, historical data, physical model, RFID and command data are some of the data. Therefore, received data must be accurate and sent by the authenticated user. Moreover, it should be scalable and received within proper time lines. Large-scale heterogeneous network integration and management is also a major challenge for IoT. This requires building automatic or intelligent net-work management system to adapt to this challenge. The current challenges faced by IoT can be summarized as follows.

- For the identification and authentication of technologies at global scale development of convergence and interoperability are needed.
- Need for standard architectures to maximize interoperability among heterogeneous systems and distributed resources.
- Integration of various technologies and their applications within complete end-to-end systems.
- Hardware adaptation and parallel processing in ultra-low power multi-processor system.
- Technologies for searching and discovering distributed resources to handle their capabilities, location and information they can provide.
- And most important of them the Security of the data or the information which they have to keep it very confidential [23].

4. DATA IN IOT

Moreover the major challenge to deal in IoT is to deal with the heterogeneous sensors. [15] Argues how efficiently we can use, manage heterogeneous sensors data and store the data of those sensors on big data platform. Today everyone focuses on smart lightening, smart city, smart classrooms, home automation, etc. therefore to make all the things go smart we need lots of sensors. To do so we will be dealing with heterogeneous sensors which will generates large amount of Data. For example in home automation large number of the devices will be connected together to make it fullest automated, so that there should be less human interfere. So to make such automation, large number of sensors will be required to connect all the devices. Like connecting doors, windows, lights, fans, AC etc with each other using sensor. As anyone enters the door automatically gets opens and as soon as someone enters the sensors should sense using motion

senor or any other and lights and fan automatically gets switched on. So just imagine every time a person enters, sensors sense the data and if there are 4-5 members are in that home, and even enters in that room twice a day then how much the data will be produced in one month. Many of things in the IoT world had started being implemented in real time. Once we achieve the task we should not stop there. Now comes the Security, managing all the data of the sensors form getting vulnerable, we have to handle it very carefully. [24] Gives example of some real time threats and breaches which have happened. Whereas [26] argues different types of barriers which may arise while delivering the values of Big data and IoT like standards, Security and privacy and network, data centre infrastructure, analytics tools and skills. For example if he achieved home automation then next thing is to make it secure, so that above listed threat can be neglected. For that we can install voice recognition system, eye scanner, finger scanner, CCTV etc. and again for all this type of making secure again going to take lots of dat. CCTV takes the most, because it has to record everything for 24 hours. So where are we going to store all those data? The 3 different techniques argued by [25] can make the IoT more secure, where he shows Big Data can play a major role.

According to [12], around 80% of the todays data are Unstructured data compared to Structured data which includes satellites images, Scientific data, photograph, video, social media data, website content etc. so these data cant be stored in the normal SQL format. As we are going to deal more with sensors, so here we are going to NoSQL. NoSQL database is used to storage and retrival of data which is stored in means other than tabular relations other than relation database[13]. NoSQL consits of different databases to provide consistency and relliablity to the developers, some of the popular database are Hadoop/ Hbase, Cassandra, MongoDb etc[19].

5. PROPOSED ARCHITECTURE

As we are going to use various devices to communicate with each other, lots of complexity may occur and we may need big storage place to store the data or the information from the devices as well as from the human beings which are nothing but the objects. Internet of Things will compromise “Billions of Things” including humans that can sense communicate, compute, and potentially actuate, as well as have intelligence, multimodal interfaces, physical/virtual identities, and attributes [17]. At present there are more 26 billion devices, we started connecting devices, then there will be lots of data will be collected from these devices and to store such a huge amount of data we may need Big data in the Future. Because of high flexibility, dynamicity, the objects (like sensors) can penetrate into each and every real time applications like industries, health care, agriculture, business, and many more[21] large amount of data generated through those objects. So to deal with such a huge amount of data we need Big Data. To combine or using of big data with IOT it will be huge challenge but once if this challenge achieved then it will reduces lots problem and complexity. For example a plant with temperature sensors record the temperature for whole day and then the next day, the whole week and even a month so that it can generate water or protect it from the sun rays. So just imagine how much data the sensors are capturing and where all those are storing. So we need a big database to store that data. Not only for storing the data but also we can analyze the data we can produce more efficient, convenient and QoS for the users. [18] [22] discusses different types of analytics tools which will be used to analyze the data generated through different types o sensors. This can be achieved through by using various technologies like NoSQL, HBase, MapReduce, etc; can also become major factor in the development of IoT. Once the Big data is combined with IoT, after that we have to go for the security. The data from the sensors has been obtained, they are successfully stored in big data, is the work got over? No, we don’t know how much secure our data is, after adding in big data. We have to be very careful with the data; it should not get vulnerable at any point of time. [25] Explains how will be the security of IoT depending on Big data while [27] explains us how can we secure our data by using various techniques.

6. CONCLUSION

Every new technology faces many problems during its development stages, so does the IoT. It has several challenges related to standardization, architecture, interconnection and integration between environment and other wireless networks. In this paper, we have identified the challenges related to IoT applications, architecture, and Data storage. And proposed an architecture where the IOT meets the Big Data which may solve various problem of the IOT.

References

1. S. Haller, S. Karnouskos, and C. Schroth, 2009, "*The Internet of Things in an Enterprise Context*," in *Future Internet – FIS 2008 Lecture Notes in Computer Science*, Vol. 5468, pp 14-28.
2. A. C. Sarma, and J. Girão, 2009, "*Identities in the Future Internet of Things*," in *Wireless Personal Communications 49.3*, pp. 353-363.
3. PhD Student QUEST Nawabshah, Internet of Things: Architecture & Integration with Other Networks. First International Conference on Modern Communication & Computing Technologies (MCCT'14)
4. Weiser, M. September 1991. The Computer for the Twenty-First Century. Scientific American 265(3), pp. 94-104,
5. Ahola J (2001) Ambient Intelligence, ERCIM News, No 47, October 2001. A available in: http://www.ercim.org/pubilcation/Ercim□News/enw4//intro.html.
6. Zhi-Kai Zhang, Michael Cheng Yi Cho, Chia-Wei Wang, Chia-Wei Hsu, Chong-Kuan Chen, Shiuhpyng Shieh, 2014
7. "*IoT Security: Ongoing Challenges and Research Opportunities*" 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications. *IEEE Fellow* Department of Computer Science National Chiao Tung University Hsinchu, Taiwan (2014)
8. Vangelis Gazis, Konstantinos Sasloglou, Nikolaos Frangiadakis and Panayotis Kikiras, 2012 "*Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things*", 16th Pan-Hellenic Conference on Informatics, pp. 276-282,.
9. Delphine Christin, Andreas Reinhardt, Parag S. Mogre, Ralf Steinmetz "*Wireless Sensor Networks and the Internet of Things: Selected Challenges*" Multimedia Communications Lab, Technische University at Darmstadt Merckstr. 25, 64283 Darmstadt, Germany
10. R. Roman and J. Lopez, 2009. "*Integrating Wireless Sensor Networks and the Internet: a Security Analysis*," Internet Research: Electronic Networking Applications and Policy, Vol. 19, No. 2,
11. http://techcrunch.com/2015/01/25/what-happens-to-privacy-when-the-internet-is-in-everything
12. John A. Stankovic, 2014. Life Fellow, IEEE INTERNET OF THINGS JOURNAL, VOL. 1, NO. 1, FEBRUARY 2014Research Directions for the Internet of Things John A. Stankovic, Life Fellow, IEEE
13. http://www.dummies.com/how-to/content/unstructured-data-in-a-big-data-environment.html
14. https://en.wikipedia.org/wiki/NoSQL
15. C. Cecchinel, M. Jimenez, S. Mosser, and M. Riveill, 2014. "*An architecture to support the collection of big data in the internet of things*," in Services (SERVICES), IEEE World Congress on. IEEE, 2014, pp. 442–449
16. Sulayman K. Sowe*, Takashi Kimata, Mianxiong Dong, Koji Zettsu, 2014 Information Services Platform Lab. Universal Communication Research Institute, NICT, 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.
17. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, 2014. "*Internet of things for smart cities*," *Internet of Things Journal, IEEE*, vol. PP, no. 99, pp. 1–1.
18. A. Zaslavsky, 2003. "*Internet of things and ubiquitous sensing*," *Computing Now*, vol. Guest Editor's Introduction.
19. https://gigaom.com/2013/01/31/data-for-dummies-5-data-analysis-tools-anyone-can-use/
20. http://nosql-database.org/
21. Miorandi D, Sicari S, Pellegrini FD and Chlamtac I. 2012. "*Internet of Things: Vision, Applications and Research Challenges*". *Ad Hoc Networks*, Vol. 10, pp. 1497-1516.
22. http://www.forbes.com/sites/howardbaldwin/2014/03/28/big-datas-big-impact-across-industries/

23. http://www.kdnuggets.com/2014/06/top-10-data-analysis-tools-business.html.
24. Mir Saleemullah Jamali1, Pardeep Kumar2 and Umair Ali Khan, 2014. Internet of Things: Architecture & Integration with Other Networks First International Conference on Modern Communication & Computing Technologies (MCCT'14).
25. http://www.datasciencecentral.com/profiles/blogs/big-data-iot-and-security-oh-my.
26. http://www.ibmbigdatahub.com/blog/big-data-s-potential-helping-secure-internet-things.
27. http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power.
28. http://www.oracle.com/us/technologies/big-data/securing-big-data-life-cycle-2543085.pdf.