Recent Advances in Technology and Engineering (RATE-2017)
6th National Conference by TJIT, Bangalore

International Journal of Science, Engineering and Technology
An Open Access Journal

Impact Review on IoT, Applications and Avenues through Big data Analytics for Avoiding Possible Attacks

[1]Manjusha Kulkarni, [2]Annie S

Abstract

Internet of Things or IOT in short, is the idea of making devices and objects smarter by linking them to the internet. When we talk about linking, there comes wireless communication between sensors, actuators and various equipments those are nothing but "Things". The focus of this study is to review IoT, its applications, the some causes of attacks associated to internet of things, design for security and research on internet of things in future possible solutions as well scalability of IoT. Security issues which start from application environments where security concerns are important, connecting technology used for hardware devices and software as well as inbuilt security issues, manageability after increasing the network size related issues as in IoT large number of nodes(sensing ability) connected to the internet. The massive amount of data is provided by these sensors. This data is to be processed and utilized after interpretation. For reliable operation this massive network is made secure as the objects in the network are unsupervised.

Keywords: Internet of Things, applications of IoT, Key Technologies, Attacks, security,Communication, Face Recognition.

Introduction

The (IoT) internet of things is a novel model which has rapidly spread in the scenario of the emerging modern wireless communication. IoT represents a target and vision to extend the internet induced in entities which hold together all over, everyday Things as seen in [1]. The IoT comprises physical objects connected through web to act smart. These physical things can be anything such as TV remote controller, furniture, car and any device. The technology plays vital role to connect these physical world objects. This study is given by McKinsey global institute which also focuses on how IoT is diffused with interactive of human environment and that will be near future research agenda.

In study [2] authors have specified that main role is played by theses smart objects. Whereas the information and other communication technologies, embedded technologies would have potential to revolutionize the uses of this objects. Utility of things and objects. There [3] are sensors in the IoT network which senses information and sends data to other nodes in the network. This transmission to be done once the data is processed. To process the data each sensor should able to find and differentiate the data so that it can communicate to other objects with reference to the context .Each sensor node upgrade itself digitally for improving physical functionality as the digitally upgraded objects are added into the network . There are various domains where this application can be applicable and based on the functionality the connectivity of network of these physical objects is established and they are monitored remotely for gathering information from anytime to analyze the data as cloud smart device. IoT revolves around the interconnection capabilities among things, objects and people. It's a heterogeneous network environment and is enabled different communication and connection platforms and technologies are available based on the usage and architecture of IoT network e.g. WSN, RFID and wireless net connection..There are set of rules i.e. protocols defined for communication. Since IoT is heterogeneous collection of hardware and software devices and communication medium there is always security related issues are concerned while implementation. In [18] such security threats and measures are discussed including man in the middle attack, denial of service attack and replay Once the

deployment of network is done these security measures to be considered at the application level. The future of this technology [17] in terms of gadgets is having good extensions. The identification and tracking of these gadgets will be another threat in near future.

Big data is defined by authors in [16] as it's a collection of massive data gathered in variety of formats which is to be preprocessed before making decisions and optimization of process. Also data comes with high speed as the sources could be varying. Now in IoT there are RFID tags as well as sensors that are used to handle such massive data and its integration.

As we can find various definitions of the Internet of it are generally accepted as defined by the RFID group and there are standard protocols which addresses the connected objects and things in the network. [19].

Forecasts for the number of connected devices on the Internet of Things for the year 2020 vary considerably, from 26 billion (Gartner) [17], to 30 billion (ABI Research) [1], to 50 billion (Cisco) [5], to 75 billion (Morgan Stanley) [4]. Regardless of which prediction is closest to reality, the definition of IoT determines collection and connection of smart objects and there is a transmission of data between objects. The data collected by the sources in the network must be processed as it is not segregated in the required format because it is again categorized into the level in which the particular application is utilized such as industry, organization, society level or it is used by individually.

The location must be detected and tracked for moving objects which is mobile in nature for its environment and for the object which is stable, which should monitor its environment changes accordingly. On the other hand, stationary objects with sensor and control capabilities that are connected to the Internet of Things can monitor the surrounding environment, report conditions, alter its state depending upon predefined parameters, alter the state of connected things, and make changes to its surrounding environment. 75 billion objects with such functionality create tremendous opportunities for operational and strategic benefits for organizations that know how to take advantage of the technology. The effective management of this level of automation requires the collection, combination and analysis of massive collection of data which is unprocessed. The information in the IoT could be gathered from sensing node. The data can be a image, video or may be social media feeds. The information taken from satellites and location traced by GPS. This study paper organized as section I Introduction, section II application section III key technologies of IoT section IV Types of Attacks on IoT section V conclusion.

APPLICATIONS

The authors have categorized IoT based application depending on the usage such as whether it is applicable at mobile communication enterprise or for smart business. Also other applications could be as at smart home, in healthcare and other utilities. This can be categorized at smart building automation level. Hence there are total six levels of categories .Smart objects in smart home are communicated through house electricity which is powered by data usage of IoT devices. These smart objects are connected to things and they are used for saving energy of home utilities. Considering other levels of application these objects and things may vary such

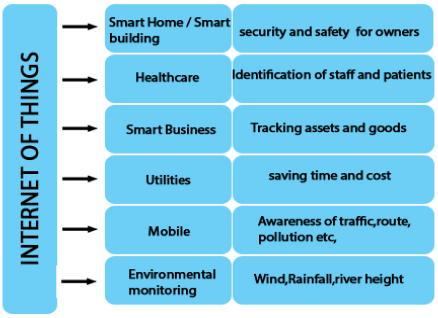

Figure 1.Application in IoT [68]

as data center and cloud is used. The physical world and virtual world is connected through such versatile and unique technologies which embedded together for making things and objects smart. These objects and things how they communicated and what technologies are to fill the gap are briefed as: Communication, Addressability, Identification objects, Sensing, Localization objects: For communication between objects in the IoT network different technologies can be utilized such as Wi-Fi, wsn e.g. GSM, Zigbee and specifically are the communication medium in IoT framework. Uniquely identification of objects can be done with the various technologies e.g. EPC,RFID which has electronic barcodes and these objects can be addressed by ONS(Object-Name-Service).This identification is cross verified with data collected by sensors and again sent it back to server. For capturing location of objects GPS data can be taken.

KEY TECHNOLOGY OF IoT

The definition of IoT comprises "things" and those things can be very small objects. That could be

"anything connected". Here the study specifies some of the technologies which are behind IoT building blocks. One of them is RFID tags (radio frequency identification).There is various scenarios are available which supports IoT concept. One scenario is EPC and it uses RFID technology for data transfer between authorized entities.

Figure2: The architecture of EPC network [68]

B. RFID Technology:

RFID is the technology which is basically meant for communication of wireless devices. It identifies the objects location. It has electronic barcode. Radio signals are used to find the objects. These objects are processing data after gathering information. RFID consists of the components such as sender, reciver.Here they are called as tags and tag reader. The communicating medium radio waves which are transmitted thought antennas and software installed on local server which manages data processing provides storage.

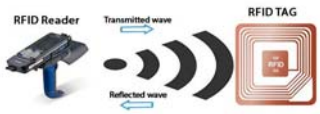

Figure 3: RFID Reader block diagram [68]

As discussed in one of paper, Radio waves are communication medium for sender and receiver of data [17].Radio signals between tag reader and tag are transmitted by antenna. Tags are the sender data and tag reader is the information received at destination. Based on the power supply these tags are divided into passive tags, active tag and semi active tags. The software manages all processing of data which is installed on local server and also permits data exchange with tag reader if needed. To handle massive data gathered by tag reader is handled by using RFID technology

TYPES OF ATTACKS ON IOT

As discussed in paper [69] there are three types of attacks:

A. Application based

There are various sensor technologies are available which processes massive quantity of data collected by them, making the application platform complex while feeding the data at backend storage timely.

B. Connection based

In the environment of IoT, objects are connected to IoT sensors for data transmission which changes the natural attributes of objects for the data transmission.

As we all know that IoT is the connection of smart objects through communication medium. Hence the communication medium i.e. internet and the connected devices both are not trustworthy and whole network can be breeched. And more over the recent technologies such as cloud computing and other storage platforms are having their own security threats while it comes to protecting data [7].

The scalability can be increased of the IoT network by deploying the devices and connecting them through web but that should be secure throughout the network i.e. end to end .This causes hybrid attacks as the network is made up of hybrid communication medium and hybrid devices.

The domain in which IoT is developed and how it is raising in the particular platform, based on that security issues are invoked and those are challenges in this filed.

4.1A framework to examine the adoption, Usage and impact of the Internet of Things [70]

Based on the usage of IoT at different environments the framework is prepared. Such as at industry levels how this works, at individual level how it works and its effectiveness at organizational and society level is verified and same is shown in below fig.

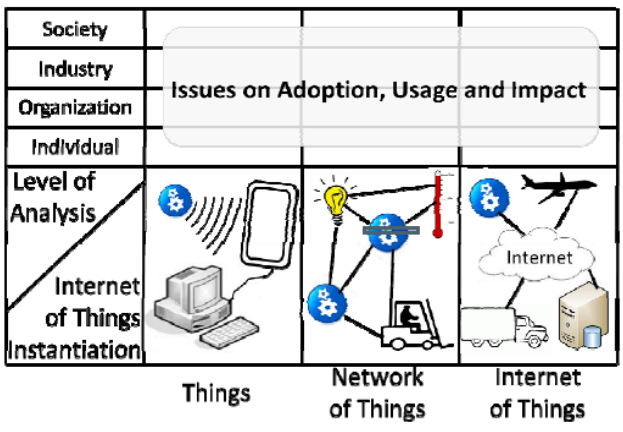

Fig. [68] Adoption, usage and impact framework: instances vs level of analysis [70]

The authors have made literature review to validate the framework by categorizing research done to date that has examined the non-technical behavioral, organizational, and business issues related to the IoT. The study gives wide range of ways for future enhancement in IoT for different levels using recent trends in technologies such as big data analytics

As study focuses on concept of Iot, introduction, the technologies behind it and security issues in IoT .Also highlights on research questions while adopting this technology based on the level it used. The level could be individual level, industry level or it could at social level. Authors have specified questioner at each level. Such as what type of privacy measures taken in the IoT based world and security issues are opened by IoT. Researchers need to find how the IoT using big data analytics will change the relationship between key stakeholders across the organization.

CONCLUSION

In this survey paper gives idea on basic concept of internet of things. The key technologies behind IoT architecture .The study highlighted on a framework based on the idea behind the IoT. IoT is evolved from observing "Things" surround us and forming "Networks of Things" and ultimately developed an "Internet of Things". The study tells about the framework that the assumption, usage and effect of these three terms of the Internet of Things can be seen from the individual, organizational, society levels and industry.

The authors have suggested a set of methodologies pertaining a number of ways available for doing research in field of IoT with the help of trending technologies such as big data analytics considering 4 levels based on usage of IoT as: organization, individual, society levels and industry. Also it focuses key components required for implementation of IoT. As IoT is defining as network of Things, it urges a framework which should be authorized and versatile which handle verticality, pervasive and preserves the culture of the IoT [12].

The study focuses on how in daily life IoT playing major role. IoT is capable for developing smart objects through communication process and these objects are used to build "anytime, anywhere, and anything"concept with the small, smart things. Authors have shown the IoT has the potential to feel the gap between physical world and virtual.

References

[1] D. Giusto, A.lera,G.Morabito,l.Atzori(Eds.)The Internet of Things, Springer ,2010. ISBN:978-1-4419-1673-0.

[2] McKinsey Global Institute "Disruptive technologies: Advances that will transform life, business, and the global economy". report by May 2013.

[3] Fleisch, E.: What is the Internet of Things? When Things Add Value. Auto-ID Labs White Paper WP-BIZAPP-053,Auto-ID Lab St. Gallen, Switzerland (2010).

[4] Schoenberger, C.R.: The internet of things. Forbes Magazine, March 18 (2002).

[5] European Commission: Internet of Things – An action plan for Europe. COM(2009) 278,http://eurlex.europa.eu/LexUriServ/site/en/com/2009/com2009_0278 en01.pdf (2009).

[6] A. Gluhak, S. Krco, M. Nati, D. Pfisterer, N. Mitton, T.Razafindralambo,A survey on facilities for experimental Internet of Things research, IEEE Communications Magazine 49 (2011) 58–67.

[7] H.S. Ning, Z.O. Wang, Future Internet of Things architecture: like mankind neural system or social organization framework? IEEE Communications Letters 15 (2011) 461–463.

[8] L. Atzori, A. Iera, G. Morabito, SIoT: giving a social structure to the Internet of Things, IEEE Communications Letters 15 (2011) 1193–1195.

[9] L. Atzori, A. Iera, G. Morabito, The Internet of Things: a survey, Computer Networks 54 (2010) 2787–2805.

[10].M.Vilamovska,E.Hattziandreu,R.Schindler,C.Van Oranje,H.De Vries,J. Krapelse, RFID Application in Healthcare-Scoping and Identifying areas for RFID Deployment in Healthcare Delivery,RAND Europe,February 2009.

[11]X,Li,R.X,LU,X.H,Liang,X.M.Shen,.M.Chen.X.D ,Lin,amart community:an internet of things application,IEEE Communication Magazine 49(2011)

[12] M, Yun,B Yunix,Research on the architecture and key technology of internet of things(IoT) applied on smart grid, in:Advance in Energy Engineering, ICAEE,2010

[13] H, Jun-Wei, Y,Shouyi, L. Lebio,Z zhen, W .Shaojum, A crop monitoring system based on wireless sensor network,Procedia Environmental Science 11(2011)

[14] Kumar, S .Ranganath, W.Huang ,K.Sengupta, framework for real-time behavior interpretation from traffic video, IEEE transaction on intelligent Transportation system (2005)

[15] David L. Brock, Integrating the Electronic Product Code (EPC) and the Global Trade Item Number (GTIN),Updated edition published November 1, 2001. Distribution restricted to sponsors until February 1, 2002,MIT auto-id center [16] Luigi Atzori, Antanio Lera,Giacomo Morabiti, The Internet of Things: Survey. July 2010ScienceDirect [17] Lu Yan ,Yan Zhang LaurenceT. Yang Huansheng Ning, The

internet of things--from RFID to the next-generation pervasive network system.2008

[17] N.Mahalle,B.Anggorojati, N.R. Prasad and R.Prasad, "Identity Authentication and capability based access control (IACAC) for the internet of Things," Journal of cyber security and Mobility, River Publishers, Vol 1, 2013, pp309-348.

[18] D.C. ZHU Shunbing, "Research on urban public safety emergency management early warning system based on technologes for the internet of things," 2012 International symposium on safety science and technology, Procedia Engineering Vol 45, 2012, pp 748-754.

[19] Z. Ying-Cong and Y. Jing, "A study on the fire IOT development strategy," Procedia Engineering, SciVerse ScienceDirect, Elservier, Vol 52, 2013, pp314-319.

[20] S.Raza, L.Wallgren and T. Voigt, "SVELTE:Real-time intrusion detection in the Internet of Things," Ad Hoc Networks Vol 11,2013, pp 2661-2674.

[21] P.Jappinen, R. Guarneri and L. M.Correia, "An

applications perspective into the future internet," Journal of network and computer applications, Elservier, Vol 36, 2013, pp249-254.

[22] S. Subashini and V.Kavitha, "A survey on security issues in service delivery models of cloud computing," Journal of network and computer applications, Elservier, Vol 34,

2011, pp 1-11.

[23] J.Yick, B. Mukherjee and D.Ghosal, "Wireless sensor network survey," Computer networks, Vol 52, 2008, pp2292-2330.

[24] Han,W. Qiu-xin and Li, "Secure solution of trusted Internet of Things based on TCM," The Journal of china universities of Posts and Telecommunications, 2013,pp47-53.

[25]Y.B.Saied,A.Olivereau,D.Zeghlache and M.Laurent, "Lightweight collaborative key establishment scheme for the internet of Things," Computer Networks, 2014, pp273-295.

[26] M.P. Narendra, "Identity management framework for internet of things,"Centre for Telefrastruktur & Aalborg University Denmark, 2013.

[27] P. Kassal, I. M. Steinberg and M. D. Steinberg, "Wireless smart tag with potentiometric input for ultra low-power chemical sensing,"Sensors and actuators Vol B 184,2013,pp 254-259.

[28] R. H.Weber, "Internet of Things-New security and privacy challenges," Computer law & security review, Vol 26,2010, pp 23-30.

[29] H. Suo, J. Wan, C. Ou and J. Liu, "Security in the internet of things: A review," 2012 International conference on computer science and electronic engineering.IEEE Computer Society, 2012, pp648-651.

[30] R. Roman, P. Najera and J. Lopez, "Securing the internet of Things," IEEE computer, Vol 44, No.9 , 2011, pp 51-58.

[31] F.Razzak, "Spamming the internet of Things: A possibility and its probable solution," Procedia computer science Vol 10,2012, pp 658-665.

[32] M.Aharan, "Critical success factors and challenges of implementing RFID in supply chain management,"Journal of supply chain and operations management,Vol 10, No.1,2012, pp144-167.

[33] ABI Research, "More Than 30 Billion Devices Will Wirelessly Connect to the Internet of Everything in 2020", 2013

[34] Atzori, L., Iera, A., and G. Morabito, "The Internet of Things: A Survey", Computer Networks, 54(15), 2010, pp.2787-2805.

[35] Beaty, D.L., "Internal It Load Profile Variability",ASHRAE Journal, 55(2), 2013, pp. 72-74.

[36] Business Insider, "Morgan Stanley: 75 Billion Devices Will Be Connected to the Internet of Things by 2020",2013.

[5]Cisco, "The Internet of Things", http://share.cisco.com/internet-of-things.html, accessed September 4, 2014.

[37] Curtin, J.P., Gaffney, R.L., and F.J. Riggins, "Identifying Business Value Using the RFID E-Valuation Framework", International Journal of RF Technologies: Research and Applications, 4(2), 2013, pp. 71-91.

[38] Curtin, J., Kauffman, R., and F. Riggins, "Making the 'MOST' out of RFID Technology: A Research Agenda for the Study of the Adoption, Usage and Impact of RFID",Information Technology and Management, 8(2), 2007, pp. 87-110.

[39] Datt, S., "The Information Explosion: Trends in Technology 2011 Review", The Journal of Government Financial Management, 60(4), 2011, pp. 46-51.

[40] Davenport, T.H., and D.J. Patil, "Data Scientist: The Sexiest Job of the 21st Century", Harvard Business Review 2012, pp. 70-76.

[41] H. Dutton, W., "Putting Things to Work: Social and Policy Challenges for the Internet of Things", info, 16(3),2014, pp. 1-21.

[42] Eu Fp7 Project Casagras, "Casagras Final Report: RFID and the Inclusive Model for the Internet of Things",2009.

[43] Fadlullah, Z.M., Fouda, M.M., Kato, N., Takeuchi, A., Iwasaki, N., and Y. Nozaki, "Toward Intelligent Machineto-Machine Communications in Smart Grid",Communications Magazine, IEEE, 49(4), 2011, pp. 60-65.

[44] Fichman, R.G., Santos, B.L.D., and Z. Zheng, "Digital Innovation as a Fundamental and Powerful Concept in the Information Systems Curriculum", MIS Quarterly, 38(2), 2014, pp. 329-354.

[45] Fosso Wamba, S., and A.T. Chatfield, "A Contingency Model for Creating Value from Rfid Supply Chain Network Projects in Logistics and Manufacturing Environments", European Journal of Information Systems, 18(6), 2009, pp. 615-636.

[46] Fowler, D., Pitta, D., and R.C. Leventhal,

"Technological Advancements and Social Challenges for One-to-One Marketing", Journal of Consumer Marketing, 30(6), 2013, pp. 509-516.

[47] Gartner, "The Importance of 'Big Data': A Definition", June 21, 2012, https://www.gartner.com/doc/2057415/ importance-big-data-definition, accessed June 12, 2014.

[48] Gartner, "Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units by 2020", December 12, 2013, http://www.gartner.com/newsroom/id/2636073 access September 4, 2014.

[49] Glenn, J.C., "Our Global Situation and Prospects for the Future", The Futurist, 48(5), 2014, pp. 15-20.

[50]Gubbi,J.,Buyya,R.,Marusic,S.,and Palaniswami, "Internet of Things (Iot): A Vision,Architectural Elements, and Future Directions", Future Gener. Comput. Syst., 29(7), 2013, pp. 1645-1660.

[51] Haller, S., Karnouskos, S., and C. Schroth, "The Internet of Things in an Enterprise Context", in (Domingue,J., Fensel, D., and Traverso, P., 'eds.'): Future Internet – FIS2008, Springer Berlin Heidelberg, 2009, pp. 14-28.

[52] Hsinchun, C., Chiang, R.H.L., and V.C. Storey,"Business Intelligence and Analytics: From Big Data to Big Impact", MIS Quarterly, 36(4), 2012, pp. 1165-1188.

[53] Knutsen, J., "Uprooting Products of the Networked City", International Journal of Design, 8(1), 2014.

[54] Mack, T.C., "Privacy and the Surveillance Explosion", The Futurist, 48(1), 2014, pp. 42-47.

[55] Ngai, E.W.T., Moon, K.K.L., Riggins, F.J., and C.Y. Yi, "RFID Research: An Academic Literature Review (1995-2005) and Future Research Directions", International Journal of Production Economics, 112(2), 2008, pp. 510-520.

[55] Ngai, E.W.T., and F.K.T. Wat, "A Literature Review and Classification of Electronic Commerce Research",Information & Management, 39(5), 2002, pp. 415-429.

[56] Riggins, F.J., "A Framework for Identifying Web- Based Electronic Commerce Opportunities", Journal of Organizational Computing and Electronic Commerce, 9(4),1999, pp. 297-310.

[57] Riggins, F.J., and S. Mitra, "An E-Valuation Framework for Developing Net-Enabled Business Metrics through Functionality Interaction", Journal of Organizational Computing and Electronic Commerce, 17(2), 2007, pp. 175-203.

[58] Riggins, F.J. and T. Mukhopadhyay, "Interdependent Benefits from Interorganizational Systems: Opportunities for Business Partner Reengineering", Journal of Management Information Systems, 11(2), 1994, pp. 37-57.

[59] Riggins, F.J., and T. Mukhopadhyay, "Overcoming EDI Adoption and Implementation Risks", International Journal of Electronic Commerce, 3(4), 1999, pp. 103-123.

[60] Rubinstein, I.S., "Big Data: The End of Privacy or a New Beginning?", International Data Privacy Law, 3(2),2013, pp. 74-87.

[60] Sarkar, S., Lovett, T., Bertuccelli, L., Vrabie, D.,Krucinski, M., and S. Mijanovic, "Smart Homes Green Cities", Mechanical Engineering, 135(12), 2013, pp. 5-17.

[61] Shakiba, M., Singh, M.J., Riggins, F.J., Sundararajan, E., Zavvari, A., and M.T. Islam, " Evaluating the Trend of RFID Technology Development Based on Academic Publications from 2001 to 2013", working paper, 2014.

[62] Sharda, R., Delen, D., and E. Turban, Business

Intelligence – a Managerial Perspective on Analytics, 3rd edition, New Jersey, 2014.

[63] Shrestha, R.B., "Big Data and Cloud Computing",Applied Radiology, 43(3), 2014, pp. 32-34.

[64] Skiba, D.J., "The Internet of Things (Iot)", Nursing Education Perspectives, 34(1), 2013, pp. 63-64.

[65] Tucker, P., "Mapping the Future with Big Data", The Futurist, 47(4), 2013, pp. 14-18.

[66] Wang, J., and Z. Wang, "A Survey on Personal Data Cloud", The Scientific World Journal, 2014.

[67] Watson, J., "The Requirements for Being an

Analytics-Based Organization", Business Intelligence Journal, 2012, pp. 4-6.

[68] Yonck, R., "Connecting with Our Connected World", The Futurist, 47(6), 2013, pp. 16-21.

[69] Mohsen Hallaj Asghar , Nasibeh Mohammadzadeh Atul Negi,"Principle Application and Vision in Internet of Things (IoT)" International Conference on Computing, Communication and Automation ,2015.

[70] Frederick J. Riggins, Samuel Fosso Wamba "Research Directions on the Adoption, Usage and Impact of the Internet of Things through the Use of Big Data Analytics", 48th Hawaii International Conference on System Sciences,2015.

[71] Attlee M. Gamundani," An Impact Review on Internet of Things Attacks", 978-1-4799-7707-9/15/$31.00 ©2015 IEEE.

Author's details

1Manjusha Kulkarni, Asst Prof., CSE, T John Institute Of technology,Karnataka,India,
manjushakulkarni@tjohngroup.com

2Annie S Asst Prof., CSE, T John Institute Of technology, Karnataka, annies@ tjohngroup.com