WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Internet of Things (IOT): Key Challenges and Issues

Nidhi Chadha, Ramandeep Kaur

Assistant Professor, Arya Kanya Mahavidyalya,India

A B S T R A C T

This paper presents the key challenges in the domain of IoT. The key challenges associated with the development of IoT , industry as well as government, Industrial IoT systems, the related security and privacy challenges has been reviewed and presented. Vulnerability of Internet of Things systems have been improved with the advent of new computational systems for IoT. However, the current design of IoT does not effectively address the higher security requirements posed by those vulnerabilities. Many recent attacks on IoT systems have shown that novel security solutions are needed to protect this emerging system.

Keywords: IOT, Review, Key Challenges

1. Introduction

The Internet of Things is an emerging topic of technical, social, and economic significance. To realize a strong vision of Internet of Things, communication, storage and sensing capabilities of sensors must be efficient with growing ubiquity. Haller et al. [1] have provided the following definition.

"A world where physical objects are seamlessly integrated into the information network, and where they, the physical objects, can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues."

Internet of things consists of sophisticated sensors, actuators and chips embedded in the physical things that around us by making them smarter than ever. Abundant of data is exchanges between sensors and other digital components without any human intervention [2].

[3] A number of challenges are in the way of IoT. There exist constraints related to shortage of time, memory, processing, and energy efficiency. In emerging areas of healthcare, smart cities, education, architect and various other fields these limitations need to be addressed.

2. Review

Various perspectives related to issues and challenges involved in dealing with data management in IoT have been presented in this paper. Handling varied amount of data is a big challenge that also includes a series of issues related to a particular category of data. Sensors stores abundance of information about the connected objects and people, security information and every other information associated with the system. From last many years problems and issues associated with sensors and other embedded devices have been studied and various authors and researchers have proposed optimum solutions in different contexts.

* *Corresponding author.*

E-mail address: nidhibhatia006@gmail.com

In Industrial IoT systems, the related security and privacy challenges, and an outlook on possible solutions towards a holistic security framework for Industrial IoT systems have been presented. Some distinguished features of IoT and generic architecture has been described in previous research. Need of standardization, security and governance in the field of Internet of Things has been focused. The table given below presents the review of various issues related to IoT over the span of last seven years.

Table-2.1 Challenges and Issues of Internet of Things-A Review

S.NO	AREA	Related Issues	Meaning
1	[4] Database Management in Internet of Things	Size ,Scaling and Indexing	Indexing is a major challenge in the world where all the objects are identified using IP address.
		Query Language	It is really difficult to have standard uniform structure of data in such a heterogeneous environment.
		Process Modeling and transactions	Applicability of ACID properties and two phase locking becomes difficult in Internet Of Things
		Heterogeneity and Integration	Issues related to Heterogeneity and Integration arises because of different types of platforms and data.
		Time Series Aggression	The problem revolves around the ability to select the optimal sampling period for continuous data.
		Archiving	Archiving data is a technique that involves
		Data Protection	Data protection becomes a complex task because of availability of data in large quantity.
	[5]cross organization inter- action,	Network Foundation	Limitations of the current Internet architecture in terms of mobility, availability, manageability and scalability are some of the major barriers to IoT.
		Security, Privacy and Trust	(a) Securing the architecture of IOT - security to be ensured at design time and execution time (b) Proactively identifying and protection of IOT from arbitrary attacks from malicious software.
		Managing heterogeneity	In addition to the above major challenges, some of the other challenges are: (a) managing large amount of information and mining large volume of data to provide useful services, (b) designing an efficient architecture for sensor networking and storage, (iii) designing mechanisms for sensor data discov- ery, (iv) designing sensor data communication protocols - senor data query, publish/subscribe mechanisms, (v) developing sensor data stream processing mechanisms, and (vi) sensor data mining - correlation, aggregation filtering techniques design.
	[6] academia, industry as well as government	Naming and Identity Management	The IoT will connect billions of objects to provide innovative services. Each object/sensor needs to have a unique identity over the Internet. Thus, an efficient naming and identity man- agement system is required that can dynamically assign and manage unique identity for such a large number of objects
		Interoperability and Standardization	The standardization of IoT is very important to provide better interoperability for all objects and sensor devices.
		Information Privacy	Different types of identification technologies like RFID and barcodes us be prevented from unauthorized access.
		Objects safety and security	The IoT consists of a very large number of perception objects that spread over some geographic area, it is necessary to prevent the intruder's access to the objects that may cause physical damage to them or may change their operation
		Data confidentiality and encryption	Enhancing data integrity on arrival of information is one of the core issues that have to be taken as utmost priority. Embedded sensors must guarantee these parameters to be fulfilled and guard the data.
		Spectrum	Limited spectrum availability and dedicated spectrum to transmit data over the wireless medium are the major requirements.
		Network security	Large number of data packets is transmitted during sensor and real time communication over wired or wireless transmission network. This data need to be secured that may contain high level confidential credentials of

			users. Network security is the most important concern these days in order to maintain the trust level and security of IoT users.
		Greening of IoT	Increasing number of very high data transfer has raised the requirement of optimum energy consumable network. Energy efficiency playa a major role in efficient data transmission. Thus, green technologies need to be adopted to make the network devices as energy efficient as possible.
	[7]Distributed IoT systems	**Identity** management, **Authorization and authentication, Trust and governance, Fault tolerance**	Protocol and network security service must be implemented I Internet of things. Problem of **identity** management exist due to availability of billions of heterogeneous objects. **Authorization and authentication** of these objects is highly required. Real time communication and high amount of data is a big threat to privacy that necessitates availability of high end privacy tools. **Trust and governance** is affected because of size and heterogeneity of IoT. **Fault tolerance** is also necessary due to vulnerability of system.
	[8]	RFID Collision	In order to avoid RFID Collision, it is required to ensure RFID privacy protection and trust management. WSN 's security is also top priority that include cryptographic algorithms in WSN , key management in WSN, Secure routing protocols for WSN network layer and trust management of nodes in WSN. The problem of heterogeneity is also described as one of the core issues.
	[9]	Technical and managerial challenges	It consists of **Data Management** issues related to processed and stored data. Response time and process efficiency are the major challenges in Internet of Things. **Data Mining** Challenges requires advanced data mining tool to mine streaming data. Protecting **privacy** is the key of improving data quality. Lack of Security makes it difficult for firms to deal with sensitive data and infrastructure. **Chaos** need to be prevented in hyper connected Iot World and reduce other types of complexities like Security, Privacy and Trust.
	[10]Industrial Internet of Things	Security Goals and Requirements	Protection against denial-of-service attacks is the foremost necessity in order enhances unnecessary delay in production and generates revenues. It is most important to prevent unauthorized access and availability of information.
		Attacks on Industrial	In current scenario, IoT systems are vulnerable to a variety of cyber attacks. Countermeasures against cyber attacks often followed integration of IT components with some delay
		Attack Surfaces	To break security chain in highly secured and trusted systems, various attack surfaces are infused For example cyber physical production systems (CPPS).
	[11]	Internet of Robotics	Many issues are to be fully addressed by the scientific communities in the field of Internet of Robotics. One of the key benefits of IoRT is the capability of **shared- offloading** of computationally intensive asks to the IoT cloud for execution. Optimization is very necessary to deal with **computational challenge**. **Security and trust** are the major issues in robotics. Especially, when it is the case of IoRT where cloud involvement is a must we shall face two major security challenges. This is another key issue where robotics is striving to bet through since its inception. Ethical issues are the major concern in IoRT.
	[12]	Edge computing	Edge computing or fog computing is the process of data processing at the edge of the network. In this process data volume reduction and

			latency reductions should be considered. There is plethora of challenges related to Big Data in real time environment. Networking protocols for Internet of Things solutions can be divided in smart device networks and traditional networks that are designed primarily for high data rates. Issue for the development of a generic smart home solution is the cost associated with integrating smart home devices.
	[13]	Access control in the Internet of Things:	Applications of light weight security tools are required where integration of various internet and data oriented tools and objects are required. In **centralized environment** issues related to Possibility to reuse existing technologies, Ease to manage access control policies, End to end security, Single point of failure ,Expensive management , Trust Foreign entities exist. In distributed environment -Data management and privacy, Cost , User involvement in security mechanisms configuration , Complex security mechanism , difficulties to manage and update access control policies are the major challenges
	[14]	Open issues in IoT	Highlighted various key challenges such as integration of cyber world with physical world, Compatibility of Heterogeneous devices and communication, limited capabilities of IoT devices, threats to privacy of people, security challenges are the major issues described in this paper
	[15]	Internet Of Things Security	The challenges have been described in ths paper in following categories **Smart Grids->**Heterogeneity of communication standards and information system technologies in smart grids. • Scalability issues• Vulnerabilities related to information system technology• Data sensitivity and privacy **Healthcare->** Resources limitations• Mobility • Heterogeneity **Transportation systems->** Diversity of attacks' sources • High mobility• Heterogeneity **Smart cities->**Very high level of heterogeneity• Scalability• Data management issues. **Manufacturing->**Security Challenges • Cyber-Physical attacks: • Scalability issues• Lack of standardization• Resources limitation• Safety challenges
	[16]	Challenges and Security Issues in Underwater Wireless Sensor Networks	Various challenges and issues related to Underwater Wireless Sensor Networks are threats of active and passive attacks, limited hardware resources, security issues related to Underwater Wireless Sensor Networks etc.

3. Conclusion

Internet of Things paradigms and infrastructure is associated with large number of objects and technologies and applicable in wide number of diverse field. It contains particular field specific issues too. Achieving a standardized platform and protocol architecture for highly secured and efficient system is a big deal. It requires eradicating the issues related to performance of objects, associated technologies, network and specific limitations of those application areas. The end user requirements and satisfaction is the foremost essential standard for IoT. The main objective of this paper is to provide analysis of Internet of Things. Although ,there are some issues in IoT. These issues can be removed in near future. With such a rapid growth, the day is not too far that we can decide our dinner even before reaching home on the way.

References

[1] S. Haller, S. Karnouskos, and C. Schroth, "The Internet of Things in an enterprise context", in Future Internet Systems (FIS), LCNS, vol. 5468. Springer, pp. 14-8., 2008.

[2] Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, pro- tocols, and applications. IEEE Communications Surveys & Tutorials, 17(4):2347–2376, 2015.

[3] Qi Jing , Athanasios V. Vasilakos , Jiafu Wan, Jingwei Lu , Dechao Qiu, "Security of the Internet of Things: perspectives and challenges", Springer Science+Business Media New York , 2014.

[4] D. Christin, A. Reinhardt, P. S. Mogre, and R. Steinmetz, ''Wireless sensor networks and the Internet of Things: Selected challenges,'' in Proc. 8th GI/ITG KuVS Fachgespräch 'Drahtlose Sensornetze', Hamburg, Germany, pp. 31–34, 2009

[5] C. JOSHUA, J. ANNE, "Challenges for database management in the Internet of things [J]", *IETE Technical Review (Institution of Electronics and Telecommunication Engineers India)*, vol. 26, no. 5, pp. 320-324, 2009.

[6] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," Wireless Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011.

[7] Rafiullah Khan, Sarmad Ullah Khan, Rifaqat Zaheer, and Shahid Khan, "Future Internet: The Internet of Things Architecture,Possible Applications and Key Challenges", in the proceedings of 10th International Conference on Frontiers of Information Technology, Islamabad, Pakistan, 17-19 December, 2012.

[8] R. Roman, J. Zhou, J. Lopez, "On the features and challenges of security and privacy in distributed internet of things", Comput. Networks 57 (10) 2266–2279, 2013

[9] Lee I, Lee K , " The internet of things (IoT): applications, investments, and challenges for enterprises". Bus Horiz 58:431–440, 2015.

[10] adeghi1. Ahmad-Reza, Wachsmann2. Christian, Waidner1. Michael, "Security and Privacy Challenges in Industrial Internet of Things", *DAC ' '15 June 07 – 11 2015 San Francisco CA USA Copyright 2015 ACM ACM 978-1-4503-3520-1/15/06.\$15.00*, [online] Available: http://dx.doi.org/10.1145/2744769.2747942.

[11] Ray PP. ,"Internet of robotic things: concept, technologies, and challenges. IEEE Access "; 4: 9489–9500, 2016.

[12] Stojkoska, B. L. R., & Trivodaliev, K. V. (2017). A review of Internet of Things for smart home: Challenges and solutions. *Journal of Cleaner Production*, *140*, 1454–1464.,2017.

[13] A. Ouaddah, , Mousanif, H, *et al*. access control model in the Internet of Things: the road ahead. In the proceeding of the Proceeding of the 12th ACS/IEEE International Conference on Computer Systems and Applications (AICCSA),2017.

[14] K. Sha, W. Wei, T. A. Yang, Z. Wang, W. Shi, "On security challenges and open issues in internet of things", *Future Gener. Comput. Syst.*, vol. 83, pp. 326-337, 2018.

[15] Kouicem, D. E., Bouabdallah, A. & Lakhlef, H.,"Internet of things security: a topdown survey", Computer Networks.,2018

[16] Yang, G.; Dai, L.E.; Si, G.N.; Wang, S.X.; Wang, S.Q. Challenges and Security Issues in Underwater Wireless Sensor Networks. In Proceedings of the International Conference on Identification, Information & Knowledge in the Internet of Things, Beijing, China, 19–21 October 2018. in press.