Original Article

Print ISSN: 2321-6379
Online ISSN: 2321-595X
DOI: 10.17354/ijssI/2017/73

The Challenges Facing with the Internet of Things

Omid Helmi[1], Ehsankanani[1], Mohammad Akbarpour Sokeh[2], Ghodrat Sepidnam[3]

[1]MA Student of Software Engineering, Shirvan Branch, Islamic Azad University, Shirvan, Iran, [2]Computer PhD, Faculty Member of Shirvan University, [3]PhD in Electronic Engineering, Faculty Member in Ferdowsi University

Abstract

Internet of Things is one of the new technologies in the current era, but its functional challenges have not been fully analyzed yet. Internet of Things has attracted much attention and has become a controversial subject in this field after epidemic using of that(data analysis security and privacy is the head of that). Protection of IOT (Internet of Things) is complex and a difficult activity. Internet of Things requires mechanisms of confidentiality, integrity, authentication and access control accurately.This phenomenon will create hundreds of new security challenges that must be examined in detail.Another challenge that arises in this field is the fact that the Internet of Things will enhance and deepen the digital divide. Other challenges such as IPV6 and force sensors also arise. In this article we have an overview of the challenges facing the Internet of Things.

Key words: Internet of things, Internet of things security, IPV6, Data analysis

INTRODUCTION

The Internet of Things (IOT) which is related to the instruments, objects and virtual display in a web-like structure is uniquely identifiable, was proposed in 1998 for the first time. In the last years, the concept of the Internet of Things is known by some applications such assmart electrical reading, expression of the green houses, remote health monitoring and smart transportation. Generally, IOT has four main components including sensation, heterogeneous access, processing of data, applications and services andin addition, factors such as privacy and security. Today IOT is widely known as an inaudible word.Secondary industrial applications related to IOT are used for cyber transportation systems, cyber-physical systems, and telecommunications device to device.Now, in discussing the implementation of the Internet of Things, we are facing with the challenges that can slow IOT. In this article we have 5 sections: Security challenge in the Internet of Things, large network of Internet of Things, Inefficiency of the standard of the Internet of Things, Insufficiency of IPV6 implementation, intensifying challenge of the digital divide. Each section includes many issues.

Access this article online

IJSS
www.ijss-sn.com

Month of Submission : 06-2017
Month of Peer Review : 06-2017
Month of Acceptance : 07-2017
Month of Publishing : 07-2017

CHALLENGES OF INTERNET OF THINGS

Many standards have been proposed for the Internet of Thingsto have an impact on the implementation and the ease and efficiency of that. Various groups are created for providing the protocols to support the Internet of thingsincluding Microsoft leadership Web Consortium, the Internet Engineering Task Force (IETF), Institute of Electrical and Electronic Engineering Institute and Telecommunication Standards Europe. In general, with the development of IT technology, the debate about the challenges facing them is presented; what challenges must be overcome and how and in what way these should take place. In fact, the challenge is said to concept that hinders the development of a technology but in the Internet of Things, these challenges need to be resolved with the regard to the scope of this technology from industry to medical science. In the other tasks performed previously, this work has been sporadically done but not enoughbecause they are not just integrated. Realization of the Internet of Things version is not an easy job, because of many challenges that have been discussed. For example, the confidentiality and security play a significant role in all world markets. Alsoevaluating the performance of Internet of Things services is a key challenge (1). Most identified challenges are reported in (2), (3), (4), (5) and (6) studies. There areresearch

Corresponding Author: Omid Helmi, MA Student of Software Engineering, Shirvan Branch, Islamic Azad University, Shirvan, Iran.
E-mail: omid_helmi@yahoo.com

projects such as IOT6, PERUM (7) and PELYonIT that examine the challenges and shortcomings of the Internet of Things and offer guidelines for these solutions.

SECURITY IN THE INTERNET OF THINGS

Security challenge in the Internet of Things is as a growing number thatintroducing the security threats is very important among all types of devices connected to the network Internet of Things. Although the company's productivity and enhance the quality of life improves the Internet of Things but at different levels they put the Internet of things at the attack of hackers and other cyber criminals. A recent study by Hewlett-Packard (HP) (2014) showed that 70% of IOT devices that are used may be experiencing the serious vulnerabilities. IOT devices are vulnerable due to the lack of transfer encoding, unsecure web interface and insufficient protection of software. On the average, each unit consists of 25 holes.

Presenting devices on the Internet of Things as usual are used without data encoding techniques. Some Internet of things applications support critical infrastructure and strategic servicessuch as smart networks and facility protection.The other Internet of Things applications increasingly produce large amounts of personal information about families, health and financial status that the companies will be able to convert it to a leverage for their business. Possible security challenges can be deceased by training to the developers and customers and combined security solution (For example, intrusion prevention systems, firewalls) and products and encouraging the users to use Internet of things security features that are available on the devices.

Although academic research on the topic of security in the Internet of Things is still in its early stages, but there is a considerable amount of researches that examine thepresenting challenges and possible protecting work. It is thought the internet of things architecture studies a crowd of millions things that are interactedwith each other and other entities such as humans or virtual entities (8)&(9). But the security of all the cases should in a way that prevents information and providing the service to the agents involved.However protect the Internet of Things work is complex and difficult.However, the Internet of Things protect is complex and difficult work.The word security has in a whole range of different concepts such as authentication, integrity, non-repudiation and availability. In the case of the Internet of Things, the security should focus on the required security systems and also on the perception of the overall system and how to implement security functionalities (8).

Today, with the increasingly rapid development of Internet of Things in the world the need for security in these systems has increased in the visible form. Various mechanisms are also explored for them.

LIMITED RESOURCES AND THE HETEROGENEOUS RELATIONSHIP OF SOURCES

Networks with limited resources and Powerful Internet are a challengebecause the heterogeneity of both networks complicate the protocol design and operation of the system. The Internetof thingsnetwork is faced with resource limitation that relies on lossy channels with low bandwidth for connectionamongsmall groups and considering the processor, memory and energy budget. This property directly affect threatens and designing the security protocols for the Internet of Things scope.Using the small packages may lead to fragmentation of greater packagesof the security protocol.On the other hand, fragmentation of package usually reduces performance rank of overall system due to the waste of piece and need to resend (1).

IDENTITY AND AUTHENTICATION

Authentication is necessary and inevitable task that how identity management and authentication on the Internet of things is not quite done (10). It must bedefined the mechanisms for that to prevent impersonation. Once we mention these security works, we have considered some inherent security things. In architecture of the Internet of Things, some of these challenges are natural (1).

Access Control

The access challenge means that given to the extensive network and different entities that are in the existing network, it can be possible to prevent from unauthorized access that occurs in the network of the internet of things by hackers or external factors. Challenges associated with access control are also closely related to those that are seen in distributed system. A special service with the community of several services and data sources of different situations and contexts is built. All these information providers will have the information license and the special policies for access control. There are certain issues that must be managed (1).

Privacy

In Internet of things, Privacy is an undeniable issue. As we know, the individuals' data in the hands of companies providing the Internet of things service can lead to the misuse of customers' information.Some solutions are done In this case.

Privacy at the sensors means ensure of data accuracy and integrity against external attacks and unauthorized access to the system. There are 10 sensors in the smart home that personal information put at the disposal of particular individuals or groups, even people are controlled by spy agencies. This is a severe and hard blow on technology body. A lot of people do not like their personal information be shared with the others, but Internet of Things sensors with not well security allow this.

Chaos

Due to the large volume of information and variety of available information, a reasonable structure should be built that available information to be used correctly and avoid the chaos of data. Recently some efforts have been done at global levels that server companies should create the contracts with their clients and with regulate some legislations, assure their customers that their information will not be abused and the other organizations do not use them. On the other hand, in limit sensors discussion and for example in smart homes, this point is given to the customer that can prevent from transmitting of the information.

Security Terms

Now, it is not paid attention to security law and regulations and there is no specific standard of IOT. IOT relates to national security information, trade secrets and privacy of individuals. As a result, countries need to create some laws thatrules and regulations are required. In this aspect, we have a long way to do it (11).

But according to the standards established among service companies in the field of the Internet of Things, the hope is that pervasive and more comprehensive laws be created that could help the Internet of things.

Reliability

Reliability refers to the proper functioning of system based on its characteristics (12). The objective of reliability is to increase the delivery of IOT. It is closely related to the availability; because we guarantee the reliability, the availability of data and services over the time. When it comes to the field of applications with emergency response, the reliability is even more critical and has more stringent requirements (13). In these systems, a vital part is the communication network that should be flexible in the face with defectsto fulfill distribution of the reliable information. Reliability should be implemented in all layers of hardware and software IOT.Communications should be reliableIn order to have efficient IOT (13&14).

Security and Privacy

Because of the lack of architecture and standards for the Internet of Things security, Security is considered as a considerable challenge for the Internet of Things. In heterogeneous networks such as the Internet of Things, assurance of the users' security and privacy is not an easy task (15).The main work of the Internet of Things for exchange of information among billions of objects is based on Internet connection.An open issue about the Internet of Things that is not considered in standards is the distributions of keys among the services. Secure of data exchange to avoid losing or compromising of confidentiality is required.Increasing the number of smart things around us with sensitive data of control management provide an easy and transparent access.

LARGE NETWORK OF INTERNET OF THINGS

One of the big challenges facing with the Internet of things need to interact among thousands objects at any time and in any place. IOT scale is much larger compared to the other systems.The larger sizes of the network make it complex and more difficult creating a logical structure like a tree structure. In addition, it increases the technique to broadcast a message to an entire network.However, due to breadth of the network, we are faced with challenges such as Data analysis. The availability of the Internet of Things should be done at the hardware and software levels to provide services for customers anywhere and anytime. Availability of software pointes out the ability of Internet of Things applications to providesimultaneously services for all in different locations.Availability of hardware refers to the devices at all times compliant with the Internet of things protocols and functions.

DATA MANAGEMENT

It is difficult the relationship of billions or trillions of smart tools for service providers; including difficult issues to manage aspects of fault, configuration, performance and security of these tools.This management's efforts requires the new protocols design to manage potential concerns of management thatcan be potentially achieved by the deployment of the Internet of Things in the coming years. The management of smart tools and applications can be an effectiveness factor for growing the deployment of the Internet of Things (16).

Management effort requires new protocols designed to manage potential concerns of management.The potential for the deployment of Internet of Things can be achieved in the coming years. The management of Smart tools and applications can be an effective factor in the deployment of the Internet of Things growing (16).

The management of data is essential and if it is not properly done, the systems are faced with data redundancy. Internet of Things sensors and developing devices are faced with massive amounts of data that needs processing and storage. The current architecture of the data center is not ready to deal with the heterogeneous nature and the big volume of personal and the company information (Gartner, 2014). Companies are able to invest enough in data storage and collect all the data from homes by the Internet of Things network.As a result, they prioritize the data for operations or backup version based on need and value. Data centers efforts to improve processing efficiency and response time of IOT devices are widely usedand more bandwidth is consumed.

THE CHALLENGE OF BIG DATA AND CLOUD COMPUTING

Connect a large number of physical objects such as humans and animals, personal computers equipped with sensors to the Internet is what named Big data. It is obvious that connected devices need to have mechanisms for storage, processing and retrieval of data;but big data are such massive thatover the capabilities of the hardware environments and software tools to acquire, manage and process them that is acceptable in a limit time.Emerging and growing technology of cloud computing by the National Instituteand Standards and Technology NIST shared as an access model of network on demand ofcomputing resources is defined configurable such as networks, servers, storage, and applications and services (17).Cloud services allows individuals and companies that use hardware and software components from a long-distance. Cloud computing enables the researchers and businesses use and maintain lot of resources secure and with low cost from long distance. Internet of things uses from a large number of embedded devices such as sensors that create big data required complex calculations and extracting the knowledge (18). Therefore, computing resources and cloud storage is the best choice for the Internet of Things for storing and processing of big data.

Data Analysis

Data analysis is the discovery of useful, potential, interesting and new patterns from large data sets and applying new algorithms to extract hidden information (19). Many other terms are also used for data analysis. In fact, the goal of any data analysis process is to create a descriptive or predictive efficient model of huge volumes of data (20).

When it comes to Internet of things and big data, the great challenges occursthat the quantity of data is big and quality of data is low and the data are from different data sources and inherently have many different types and shapes and generally unstructured (21).

Using the data analysis tools is a necessity as the available data for further processing and analysis. The data includes not only the traditional discrete data, but also the transmission of data generated by digital sensors in industrial equipment, automotive, electrical and transport boxes.The data is about the location, motion, vibration, temperature, humidity, and even chemical changes in the air.There is a shortage of qualified data analysts along with the need for advanced data analysis tools to extract data from sensor networks and video (22).

A. The first challenge is the access of extracting large-scale data from multiple locations of storage data. We have to deal with multiple heterogeneous data and data noise; the big challenge is finding the faults andcorrection the data is even more difficult task.In the areas of data analysis algorithms how to modify the traditional algorithms with big data environment is a major challenge (21).
B. The next challenge is how finding incomplete and uncertain data to use big data. In data analysis, a security and effective solution to share the data between different systems and applications is one of the most important challenges because a lot of sensitive information such as banking transactions and medical records should be concerned (21).

RELIABILITY AND HIDING THE INFORMATION

Each daily object deals with several different models of data that members of a family may submit it. There should be the ability to acknowledge the data and check out the accuracy. The system shouldnot be not able to provide not the access to the information. Suppose that the personal information of a patient is sent to another doctor to get tips now if in the meantime someone access to the information and change them, at that time false information is submitted to the doctor and cause the doctor makes the wrong decision (23).

Now this argument is proposed here that it should be solutions to identify people who have access to information or the use the encryption to be more confidence in the system. But since this is absolutely not the Internet of Things is a big challenge;but since this is absolutely is not done, it is a big challenge in the Internet of Things.

Scalability

The scalability of the Internet of Things points to the ability to add functions and new tools for customers without affecting negatively the quality of existing services. Adding the new operations and supporting the new tools is not easy especially in the presence of a variety of various hardware platforms and communication protocols.Internet of Things applications must be design again to provide extension services and operations (24).

INEFFICIENCY OF THE INTERNET OF THINGS STANDARDS

Since the proposed standards of the interment of things are not fully explained have some defects;Therefore, they have not paid special attention to the Internet of Things and on the other hand, there is no development in this part. As the various platforms are produced by different companies, there can be little hope of integrating these standards.It has become a business issue for companies. Now what will happen if there are no standards?

A- When there are different platforms is so that you use a local Internet network.In simple terms, the ability to adapt to different platform disappears and cannot work together easily.

B- If security platforms are different, their security is lower and there are moresecurity gaps. In this way, the credibility of the system gets cheap among the users.

CHALLENGE OF MOBILE COMMUNICATIONS

In ten years, millions of mobiles established the internet access via the Internet of things;but on the other hand, mobile security issue and the data are important discussions. Telegrams and phone hacking are some cases of that (23).

Architectural Structure

IOT remains stable during the entire period and security mechanism in each layer cannot reasonably implement a complete defense system. As a result, it has been a challenge and a lot of research areas to create a safe structure with combining data and control is required (25). It is clear that in such cases, it will be difficult data management.

As the data management is an important basis of secure mechanism, it is always an important research topic.It is also the most difficult aspect of security encryption. At the moment, the researchers have not found the ideal solution for this issue.Style encryption algorithm or higher performances of sensor node are not still applied. As a result, large-scale sensor network always remain applicable. More network security issues have been much considered and become an important point and create problems in the field of environmental research network (26&27).

Insufficient ofIPV6 Implementation

Given that IPV4 officially was excluded in February of 2010, but still there are many devices that cannot work with IPV6 (Internet protocol version 6) and require to be upgraded and updated In terms of hardware and software. As the security and large number of IP homes are needed to implement the Internet of things, so this problem should be resolved and the full use of IPV6 is required for that. IPV6 has the ability to have more addresses because the Internet of Things causes the internet network become larger;therefore, the materials relating to the Internet will be required several times and more IP addresses are used. On the other hand, network management needs much costs than past with the development of Internet of things. But it can be prevented by providing more IPV6 context. On the other hand, has 3 IPV6 addressing scheme which increase the security in the Internet of Things. Therefore, greater use of IPV6 in the systems that work with Internet is necessary and vital and if this is not done thoroughly, it gets a main obstacle in implementation of the Internet of Things. Other items that can be said are the default activation of IPV6 addresses and complicate the process of maintenance and management of smart systems.

Battery Power Insufficient of Wireless Sensors

The problem of storing energy in sensors should be solved to use the Internet of Things. Suppose that the battery millions of sensors around the world are to change, it is clearly impossible.Finding the natural ecological ways to power them is the only possible thing.

Operation Challenge

After the commissioning phase, the system gets into the operational phase.During the operational phase, the objects can be linked to the local information created during the startup. Phase to exchange the information securely.Here we investigate the aspects of communication and dynamic patterns and at this stage (1).

Mobility

Mobility is another challenge to implement the Internet of Things because it is expected the services to be delivered to mobile users.Continuously connecting users working to better serve is an important consideration in the Internet of Things. Not providing the service for mobile devices occurs when these tools transfers from a gate to another one (28). Mobile Source suggests that the two methods are supported. A large number of smart tools for IOT systems require efficient mechanisms for management. A reasonable approach presented in (29).

Operation

Evaluating the performance of Internet of Things services is a huge challenge because many of the components and performance depends on the type of technology. Internet of things like systems must constantly improve and design its services to meet customers' needs.Internet of things tools should be acceptable price and evaluated to provide the best performance for customers. Evaluating the performance of each technology and strict protocols such as BLE (32), RFID (31), RPL (30) have been reported in the literature application protocols. But the lack of accurate performance evaluation of applications for the Internet of Things is still an open issue.

Exacerbating the Digital Divide

Other concerns raised in the Internet of Things are increasing the digital divide. People who are not connected to a digital network or are reluctant to connect to this network, will be deprived of many services if the spread of the Internet of Things.Many scientists pointed to the unequal distribution of facilities and noted that there is the possibility of the formation of the social divide among those who have not the resources to pay the equipment, information literacy and skills to work in environments with sophisticated technology.This does not refers only to access difference to technologies among different people of society but to cultural, geographical differences and social structure.Internet of Things will create many benefits for people in developed countries, it also has the impact on utilities such as water and electricity and power. It is worth noting this technology help lower to developing countries with development approaches (33). Today the wearable electronic devices used to control the employees in the workplace.Doing this gets much easier in the future with technological advances. Thus it is possible by 2025, when outbreak of the Internet of things, the privacy will get weak. There are two types of gap arises from the lack of IOT development as two sides of a coin. The digital divide points to differences in demographic characteristics (such as age, income, gender, education, etc.) and access to ICT within or among the countries. Another gap as or knowledge gap, points to the lack of skill and strength to use automatic transactions and manage these transactions between objects and activities of IOT.Those who do not adapt to the development of new technologies, they are face with the risk of losing knowledge and skills.Digital divide is considered as one of the greatest challenges in development of IOT;although this technology is partly imposed on people. Access and distribution of IOT technology will vary according to geographical area and will penetrate in working patterns, daily activities political and civic activities.According to the influence of IOT in all aspects of life, people's threat by malware is a concern. IOT distributed control creates issues in the field of accountability and responsibility, where it is possible to trace the origin and destination transactions of data and this is also an example of the knowledge gaps caused by IOT.

Requirements for Emerging Applications

With WSN development, radio frequency identity (RFID), pervasive computing technology, network telecommunications technology and distributed real-time control theory CPShave found a form of IOT (34) & (35). In this system, high security is required to ensure system performance. As previously mentioned,IOT challenges are to meet the internet of things security. Creating safe-like structures are also very necessary.Basic management in sensor networks of real large-scale has always been a challenging problem and Laws and regulations related to the field of IOT is also a challenge.

REFERENCES

1. D. Uckelmann, “Performance measurement and cost benefit analysis for RFID and Internet of Things implementations in logistics,” in Quantifying the Value of RFID and the EPCglobal Architecture Framework in Logistics. New York, NY, USA: Springer-Verlag, 2012, pp. 71–100.
2. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, “Future Internet: The Internet of Things architecture, possible applications and key challenges,” in Proc. 10th Int. Conf. FIT, 2012, pp. 257–260.
3. A. Gluhak et al., “A survey on facilities for experimental Internet of Things research,” IEEE Commun. Mag., vol. 49, no. 11, pp. 58–67, Nov. 201.
4. Z. Sheng et al., “A survey on the IETF protocol suite for the Internet of Things: Standards, challenges, and opportunities,” IEEE Wireless Commun., vol. 20, no. 6, pp. 91–98, Dec. 2013.
5. J. A. Stankovic, “Research directions for the Internet of Things,” IEEE Internet Things J., vol. 1, no. 1, pp. 3–9, Feb. 2014.
6. S. Chen, H. Xu, D. Liu, B. Hu, and H. Wang, “A vision of IoT: Applications, challenges, and opportunities with china perspective,” IEEEInternet Things J., vol. 1, no. 4, pp. 349–359, Aug. 2014.
7. S.Ziegler etal.,IoT6-Moving to anIpv6-Based FutureIoT. New York, NY, USA: Springer-Verlag, 2013.
8. AUTO-ID LABS. http://www.autoidlabs.org/. Online, last visited 30. June 2011.
9. BACnet. http://www.bacnet.org/. Online, last visited 30. June 2011.
10. M. Dworkin. NIST Special Publication 800-38B. NIST Special Publication, 800(38B):38B, 2005.
11. Z. H. Hu, “The research of several key question of internet of things,” in Proc. of 2011 Int. Conf. on Intelligence Science and Information Engineering, pp. 362-365..
12. D. Macedo, L. A. Guedes, and I. Silva, “A dependability evaluation for Internet of Things incorporating redundancy aspects,” in Proc. IEEE 11th ICNSC, 2014, pp. 417–422.
13. N. Maalel, E. Natalizio, A. Bouabdallah, P. Roux, and M. Kellil, “Reliability for emergency applications in Internet of Things,” in Proc. IEEE Int. Conf. DCOSS, 2013, pp. 361–366.
14. J. Kempf, J. Arkko, N. Beheshti, and K. Yedavalli, “Thoughts on reliability in the Internet of Things,” in Proc. Interconnecting Smart Objects Internet Workshop, 2011, pp. 1–4.
15. I. Ishaq et al., “IETF standardization in the field of the Internet of Things (IoT): A survey,” J. Sens. Actuator Netw., vol. 2, pp. 235–287, 2013.
16. M. A. Rajan, P. Balamuralidhar, K. P. Chethan, and M. Swarnahpriyaah, “A self-reconfigurable sensor network management system for Internet of Things paradigm,” in Proc. ICDeCom, 2011, pp. 1–5.
17. B. Rao, P. Saluia, N. Sharma, A. Mittal, and S. Sharma, “Cloud computing for Internet of Things and sensing based applications,” in Proc. 6th ICST, 2012, pp. 374–380.
18. R. Bryant, R. H. Katz, and E. D. Lazowska, “Big-data computing: Creating revolutionary breakthroughs in commerce, science, and society,” Comput. Commun. Consortium (CCC), Washington, DC, USA, 2008.
19. H. Jiawei and M. Kamber, Data Mining: Concepts and Techniques, MorganKaufmann, 2011..
20. J. Zhang, P. Deng, J. Wan, B. Yan, X. Rong, and F. Chen, “A novel multimedia device ability matching technique for ubiquitous computing environments,” EURASIP Journal on Wireless Communications and Networking, vol. 2013, no. 1, article181,12pages,2013.
21. Hui Suo et al, (2018).”Security in the Internet of Things: A Review”.

22. C.-W. Tsai eat al, (2014), “Future internet of things: openissuesandchalleng es,”WirelessNetworks, vol.20, no.8, pp.2201–2217, 2014.
23. A Survey Report on: Security & Challenge in Internet of Things.
24. D.Uckelmann, M.Isenberg, M.Teucke, H.Halfar, andB.Scholz-Reiter, “Autonomous control and the Internet of Things: Increasing robustness, scalability andagility inlogistic networks,” UniqueRadio Innovation for the 21st Century, pp. 163–181, 2010.
25. C. Ding, L. J. Yang, and M. Wu, “Security architecture and key technologies for IoT/CPS”, ZTE Technology Journal, vol. 17, no. 1, Feb. 2011.
26. G. Yang, J. Xu, W. Chen, Z. H. Qi, and H. Y. Wang, “Security characteristic and technology in the internet of things,” Journal of Nanjing University of Posts and Telecommunications (Natural Science), vol. 30, no. 4, Aug 2010..
27. T. Polk, and S. Turner. “Security challenges for the internet of things,” http://www.iab.org/wp-content/IAB-uploads/2011/03/Turner.pdf.
28. F. Ganz, R. Li, P. Barnaghi, and H. Harai, “A resource mobility scheme for service-continuity inthe Internet ofThings,”in Proc.IEEEInt. Conf. GreenCom, 2012, pp. 261–264.
29. H. Fu, P. Lin, H. Yue, G. Huang, and C. Lee, “Group mobility management for large-scale machine-to-machine mobile networking,” IEEE Trans. Veh. Technol., vol. 63, no. 3, pp. 1296–1305, Mar. 2014.
30. M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, “How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4,” in Proc. IEEE WCNCW, 2012, pp. 232–237.
31. D. Uckelmann, “Performance measurement and cost benefit analysis for RFID and Internet of Things implementations in logistics,” in Quantifying the Value of RFID and the EPCglobal Architecture Framework in Logistics. New York, NY, USA: Springer-Verlag, 2012, pp. 71–100.
32. M. Siekkinen, M. Hiienkari, J. K. Nurminen, and J. Nieminen, “How low energy is Bluetooth low energy? Comparative measurements with ZigBee/802.15.4,” in Proc. IEEE WCNCW, 2012, pp. 232–237.
33. SY, P. (2015). Defending Privacy e Dark Side of IoT, Automating Cryptography.
34. J. F. Wan, H. Suo, H. H. Yan, and J. Q. Liu, “A general test platform for cyber-physical systems: unmanned vehicle with wireless sensor network navigation,” in Proc. of 2011 Int. Conf. on Advances in Engineering, Nanjing, China, December, 2011.
35. J. H. Shi, J. F. Wan, H. H. Yan, and H. Suo, “A survey of cyber-physical systems,” in Proc. of the Int. Conf. on Wireless Communications and Signal Processing, Nanjing, China, November, 2011.

How to cite this article: The Challenges Facing with the Internet of Things Helmi O, Ehsankanani, Sokeh MA, Sepidnam G. Int J Sci Stud 2017;5(4):527-533.

Source of Support: Nil, **Conflict of Interest:** None declared.