Internet of Things: Extracting Latest Challenges and Solutions

Hesham M. Allam and Ahsan A. Chaudhri
Higher Colleges of Technology, Dubai, 16062, UAE
Email: {hallam, achaudhri}@hct.ac.ae

Abstract —IOT is an evolving technology and expected to bring the next phase of revolution in it industry by connecting any device anywhere by any available means. The potential of IOT applications is abundant allowing users to have real-time feeds from surrounding and distant objects helping in making intelligent decisions. Despite the potential benefits of IOT, there several challenges that needs to be address for IOT to harvest its potential benefits. This paper tackles recent challenges and proposes some solutions concerning IOT. We followed a systematic review of the latest literature covering IOT and extracted nine distinct categories of challenges including standardization and harmonization, connectivity, power management, security, privacy, trust, complexity, evolving scenarios, socio-ethical considerations, network technology, complexity, and rapid evolution. Further, the paper discusses the latest solutions evolved ranging from flexible radio standards, wireless sensor networks, wireless battery charging technology, ipv6/6lowpan protocols, privacy broker techniques, flexible IP protocol, to wireless identification and sensing platforms.

Index Terms—IoT, privacy, security, trust, identification, RIFD, network, ubiquitous, challenges

I. Introduction

MIT Auto-ID Centre is considered to be the originator of phrase of "Internet of Things"[1]. The center has been involved in developing identification technologies for use in industry as well as the development of Internet of Things including hardware and software required. International Telecommunications Union (ITU) in 2005 prepared a comprehensive report on IoT bringing it in a greater limelight. ITU called IoT a truly ubiquitous network– "anytime, anywhere, by anyone and anything" [2]**.** This is graphically depicted in Fig. 1.

The components IoT applications is composed of a "metamorphosis of objects" ranging from simple artifacts that are simple and may be hand manufactured to machines objects that are complex requiring main power sources, and from products that are mass manufactured and finally from gizmos that are unstable, modifiable by the user, programmable, and short-lived) [3].

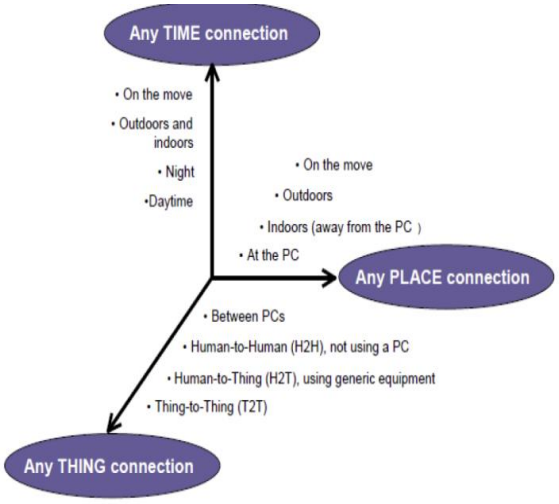

Fig. 1. IoT [2]

Now, IoT is looked at as the next technical revolution that will "connect inanimate objects and things to communication networks" [2]. IEEE defined IoT as "A network of items—each embedded with sensors—which are connected to the Internet" [4]. Further, IoT is regarded as the third wave of evolution in IT industry [4].

IoT leverages internet technology to create an intelligent network fabric that senses and enables various devices to communicate with each other. The widespread deployment of IoT could utilize hundreds of billions of devices and sensors that would interact with one another using numerous applications to provide seamless service to millions of users. As per some estimates the number of connected devices using IoT is expected to be 50 billion by 2020 [5]. This could generate data in size of unprecedented scale and allow things to be managed and controlled from remote locations leading to serious issues including security, privacy, complexity, socio-ethical issues and many more.

The seamless interconnection and communication between such large numbers of devices is full of challenges for researcher working on IoT technology. This paper looks into some of the evolving challenges in IoT technology and the solutions that have been proposed to resolve these challenges.

II. Challenges

Any modern technology faces many challenges till it matures and put to use. IoT, which involves seamless

Manuscript received May 23, 2017; revised September 19, 2017.
doi:10.12720/jcm.12.9.538-542

working of anything situated anywhere, and communicating using Internet, faces many challenges that are worth highlighting. Some of the key challenges have been detailed in the following section.

A. Standardization and Harmonization

Standardization is one of the key pre-requisite of a successful technology development because it creates interoperability among devices that are manufactured by different vendors, supplier, and countries which allows the technology to gain commonality and popularity among users. Since IoT operates with multiple devices, it makes sense to have common standards among these devices to operate together and to gain market popularity. For instance, the popularity of mobile phone is attributed to standards such as GSM, TCP/IP, IMT-2000 etc. [2]

One of the main challenges facing IoT is to ensure global interoperability especially with technology that use radio spectrum. Example of radio spectrums that were allocated for broadcasting purposes are AM, FM, digital audio broadcasting, analogue terrestrial television, digital terrestrial Television. Other radio spectrum were allocated to cater for communication purposes are mobile telephony, citizen-band radio, emergency services communications, wireless internet, short-range radio. However, many frequency band allocations are not unified across different regions of the world and some of them are specified for particular regions to server particular purposes [6]. This creates disharmony between devices and hence could diffuse the potential benefits of IoT. Attempts to resolve such a challenge by relocating the radio spectrum could be difficult and would require lengthy time to get government bodies, international agencies, and regional entities to agree on one unified radio spectrum that can work for all. In the meantime, efforts should be dedicated to allow IoT devices using radio spectrum to work on multiple protocols and multiple frequencies to minimize the possible disruption effect on users of such devices [7]. This could take place if a Memorandum of Understanding (MOU) could be established to act as platform for communication and collaboration to avoid interference in each other's process of standardization. For that reason, Telecommunications Standards Institute (ETSI) along with GS1 and CEN aims to define standards related to spectrum, physical objects, infrastructure for communication, security and privacy issues etc. [8]. The standardization activities for IoT have taken a decent shape with close co-ordination among various organizations to make it a success. For example, ETSI's Machine-to-Machine Workgroup and Internet Engineering Task Force (IETF) are working on a Low power Wireless Personal Area Networks (6LoWPAN) for use with IP6 as an initiatives to standardize IoT [9]. ISO, on the other hand, is involved in handing technical issues such as modulation schemes, protocol, and radio spectrum [8].

B. Connectivity

Although the potential of IoT in connecting anything anywhere is promising, it adds a key challenge with regards to IoT devices connectivity. The devices can be stationary or moving and may use several types of technology for communication. Thus, the system cannot use single connectivity solution. Rather, wide varieties of wired and wireless standards will be involved to provide connectivity. A real challenge will be to make different standards communicate with one another seamlessly to establish the targeted connectivity [5].

One of the key technology to be used for connecting various devices in IoT is Wireless Sensor network (WSN). However, when used for IoT, the WSN is also be connected to Internet [10]. The challenge for existing scheme proposed to provide security in WSN must provide security from Internet as well. The device heterogeneity in IoT also requires special techniques for workload distribution in WSN to maintain system quality of service. The sheer volume of devices using WSN may undergo a revamp of current protocols to handle these volumes and traffic. Further, the nodes in WSN may also need management of their configuration settings [10].

C. Power Management

Devices that operate IoT are likely to be powered using small batteries or using energy harvesting techniques to make them self-sustaining. Changing batteries in battery powered devices could be a challenges task especially when the number of devices is numerous requiring charging batteries of all the devices that connected to system. The IoT system would require effective power management techniques to address power related issue as well as conserve the energy requirements [5]. Although still in its primitive stage, battery wireless charging technology is one of the potential options to manage such a challenge.

D. Security

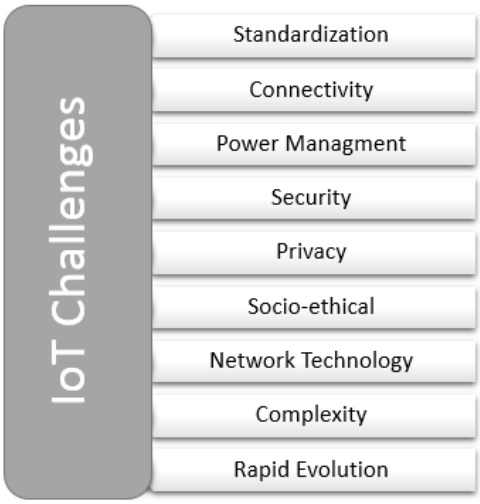

Fig. 2. Graphical representation of challenges in Internet-of-Things

Security is considered a major issue for the adoption of IoT technologies. In order to adopt IoT, users need system level confidentiality, privacy and authenticity. Since IoT aims at connecting various devices, it is vulnerable to possible attacks from leaving wireless

devices unattended and from the wireless network that is connecting the devices. It should be noted that some IoT devices come with low cost components and limited technical capabilities making it difficult to implement complex security scheme to enforce security and privacy [8]. Other IoT security issues can originate from mobile and sensor network and can lead to access control and authentication, data integrity, information management and storage and many more [2], [11]. Moreover, in the absence of authentication infrastructure, it could be difficult to provide authentication with exchange of message to the devices. For example, the number of message that can be exchanged in RIFD tags is limited and beyond the requirements of authentication server message exchange [8]. Fig. 2 depict some challenges facing the implementation of IoT.

It should be noted that the IoT system need specialized solution to ensure data confidentiality due to the potential huge data generation leading to scalability issues and to the requirement of dynamic access control due constantly changing scenarios [12]. Number of schemes have been proposed to take care of dynamic situation. One such scheme is called CADS, short for Continuous Authentication on Data Streams which ensures the authentication of information constantly once transmitted by data owner to the service provider [13], [14].

One solution was suggested by Bagci *et al*. [15] as they proposed a secure storage and communication framework based on IPv6/6LoWPAN protocols. This protocol ensures using an encryption and authentication procedures of transmitted data packets. For instance, before the storage takes place, the author uses cryptographic methods and data formats which is defined by ESP for data processing. This encrypted data must be stored in ESP compatible over network which can be achieved by using IPsec as a base for communication and storage, and the existing key exchange mechanisms defined for IPsec can be reused for the storage element of the framework. IV. D [15]

E. Privacy

Similar to current health tracking tools on mobile phone or watches, IoT devices can avail significant amount of personal data on IoT users' location and movements, health conditions, and purchasing preferences. This can invade personal privacy for individuals using IoT technology. Although IoT service providers may seek to protect personal privacy, they are sacrificing a massive data that can improve the quality of people's lives and decreasing service providers' costs by streamlining operations. In spite of the overall benefits for general public, individuals still prefer to protect their own privacy even it means sacrificing the overall public benefit. According to the 2014 eTRUST Internet of Things Privacy Index, only 22% of Internet users agreed that the benefits of smart devices outweighed any privacy concerns [16]. While the IoT continues to gain popularity through smart home technology and wearable devices, confidence in and acceptance of the IoT will depend on the protection of users' privacy.

Whatever the solution for privacy is, it has to conceal personal information and control what happens with the information collected [12]. Substantial number of schemes has been proposed for privacy of RFID and can be broadly categorized into two types: schemes that limit physical access and schemes that use passwords [11]. The physical based scheme uses methods such as deactivate tag [16], clip tags [17], block tags [18], shield tags [19] etc. In most of these schemes the tag is disabled after its final use. For example, after user pay for item, the tag gets automatically disabled to avoid tracking the user. The password based schemes use encryption and include schemes such as hash chain [20], noisy tags [21], anonymous ID [22] etc.

Providing privacy in areas where sensor networks are deployed is more challenging as the person entering the area has no control over data being collected related to an individual [8]. The personal data collected need to be used only by authorized service provider for authorized services. The use of system called privacy broker has been suggested for this [23]. In this system, a proxy is used that interacts with user who can set the access setting for a service provider. This allows the service provider to access only the data that is authorized for their service. But this system may not scale to IoT requirements. Another solution being considered is the use of system that allows digital forgetting which means that data get automatically deleted after certain instance [8].

F. Socio-ethical Considerations

The wide spread use of IoT due to use of ubiquitous communication, sensors, RIFD and smart object can have an effect on society in many ways [2]. The prevalence of IoT can affect the quality of life by providing a high level of convenience in people's day to day operations. The technology can help monitoring elderly and kids at home especially for working couples. At the same time, this convenience can lead to fears of constant surveillance from the numerous IoT devices surrounding people. This is likely to create heightened anxiety when making choices and decisions. Further, the automation of normal human activity may not be desirable. IoT technology can be a cause for isolating individuals from human contact leading to psychological issues. The authenticity of information being decimated via numerous devices is another issue. Notably, the plethora s of IoT objects, if left without any regulation or interference, might give rise to a genuine, extensive surveillance society. Each individual would spontaneously document his life by complementing factual information on his journeys, locations and transactions, which are today aggregated, with the micro-events of his day-today intimate life [12]. Thus, while enjoying the benefits of IoT, researchers and industry leaders should consider the negative impact on individuals and society as the technology continues to in complexity and availability [2].

G. Network Technology

The IoT deployment requires developments in network technology which is essential for IoT to live up to its expected vision to connect to objects and bring them into the Internet. Technology such as RFID, short-range wireless technologies and sensor networks are enabling this, while for example IPv6, with its expanded address space, allow that all objects or things to be connected, and be tracked. To make this possible, the network technology must be affordable and viable to connect all these devices together. Further, since protocol gateways translation can be complicated for such devices, current IP solutions provides end to end communication between these devices without intermediate protocol. New scalable architectures designed specifically for the ubiquitous sensor networks communications would allow for networks of billions of devices. Improvements in techniques for secure and reliable wireless communication protocols would also enable mission critical applications for ubiquitous sensor networks based on wireless identifiable devices [12].

H. Complexity

One of the main challenges encountering IoT adoption is that it will require connection with a wide array of objects many of which were not exposed to the networks before. In other words, IoT design and development initiatives must be simple and neutral enough to accept large number of devices that cater to the potential benefits of IoT. IoT design and development must be simplified in order to increase the number of connected devices. This can be done in a number of ways [24]:

- Better design of wireless capability by providing modules, reference designs, on-chip Internet connectivity software stack and comprehensive development environment
- Making the device set-up simple enough to allow average user to be able to use without efforts.

I. Rapid evolution

IoT is still in its dawn stage and is constantly changing and evolving. The uncertainties of unknown devices being added, unknown applications being developed, and unknown use being added, make IoT's full spectrum of challenges hard to identify [5]. Further, the devices connected range from small ones with very limited capabilities and energy to large range with high performance and processing capabilities. The connectivity technology is still evolving all the time in wired as well as wireless fields. The sensing technologies are integrated with passive RF tags to provide new applications especially in areas of e-health. Solutions such as wireless identification and sensing platforms (WISP) are being proposed [8]. Every day new types of sensors with different capabilities are being added and require interface, communication and power management for efficient interface to IoT [5].

III. Conclusion

In IoT the seamless interconnection and communication between billions of devices is a challenging task. Handling of sheer volume of devices itself is a challenging task whether its identification, privacy or networking. The challenges are technological, evolving as well as socio-ethical. The technological challenges include those related to standardization and harmonization, connectivity, power management, security, privacy, trust, complexity, evolving scenarios, socio-ethical considerations, network technology, complexity, and rapid evolution. Tackling these challenges require development of a strong frame work for each aspect and use of advance technologies that are efficient as well as lightweight. The automation of human activity without human interaction can have serious socio-ethical problems in the society if the IoT technology is not regulated and controlled. The system complexity and constant evolution of device, techniques make IoT a very challenging task and require further research and continuous investigation.

References

[1] G. Santucci, "The internet of things: Between the revolution of the internet and the metamorphosis of objects," in *Vision and Challenges for Realising the Internet of Things*, Brussels, Cluster of European Research Projects on the Internet of Things, 2010, pp. 11-23.

[2] ITU, "ITU internet reports: The internet of things," ITU, Geneva, 2005.

[3] R. Minerva, A. Biru, and D. Rotondi, "Towards a definition of the Internet of Things (IoT)," *IEEE*, 2015.

[4] H. D. Ma, "Internet of things: Objectives and scientic challenges," *Journal of Computer Science and Technology*, vol. 26, no. 6, pp. 919-924, 2011.

[5] Chase, "The evolution of the internet of things," *Texas Instruments*, Texas, 2013.

[6] Preishuber-Pflügl, "Standardisation issues challenges on RFID and a future IoT," in *Vision and Challenges for Realising the Internet of Things*, Brussels, Cluster of European Research Projects on the Internet of Things (CERP-IoT), 2010, pp. 129-136.

[7] H. Sundmaeker, P. Guillemin, P. F. Riess, and S. Woelffe, *Vision and Challenges for Realizing the Internet of Things*, Brussels: European Commission - Inform, 2010.

[8] Atzori, A. Iera and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787-2805, 2010.

[9] Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals," IETF RFC 4919, 2007.

[10] 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, 2009.
[11] Q. Jing, A. V. Vasilakos, J. W. J. Lu, and D. Qiu, "Security of the internet of things: Perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, p. 2481-2501, 2014.
[12] D. Miorandi, S. Sicari, F. D. Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Elsevier: Ad Hoc Networks*, vol. 10, pp. 1497-1516, 2012.
[13] S. Papadopoulos, Y. Yang and D. Papadias, "CADS: continuous authentication on data streams," in *Proc. 33rd International Conference on Very Large Data Base (VLDB'07)*, Vienna, Austria, 2007.
[14] A. M. ElTabakh and C. Nita-Rotaru, "FT-RC4: A robust security mechanism for data stream systems," Purdue University, Technical, 2005.
[15] B. S. Rasa, T. Chung, U. Roedig, and T. Voigt, "Combined secure storage and communication for the internet of things," in *Proc. IEEE International Conference on Sensing, Communications and Networking*, New Orleans, LA, 2013.
[16] E. Trust. (2014). Internet of things privacy index-US. Trust. [Online]. Available: http://www.truste.com/resources/
[17] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels, "Security and privacy aspects of low-cost radio frequency identification systems," *Security in Pervasive Computing*, vol. 2802, pp. 201-212, 2004.
[18] M. Chen, S. Gonzalez, Q. Zhang, and V. Leung, "Codecentric RFID system based on software agent intelligence," *IEEE Intelligent Systems*, vol. 25, no. 2, pp. 12-19, 2010.
[19] Blaskiewicz, M. Klonowski, K. Majcher and P. Syga, "Blocker-type method for protecting customers' privacy in RFID systems," in *Proc. IEEE International Conference on Cyber-enabled Distributed Computing and Knowledge Discovery (CyberC)*, 2013.
[20] S. Spiekermann and O. Berthold, "Maintaining privacy in RFID enabled environments," in *Privacy, Security and Trust within the Context of Pervasive Computing*, Berlin, Springer., 2005, pp. 37-146.
[21] Juels, R. Pappu and S. Euros, "Privacy protection RFID-enabled banknotes," in *Proc. Seventh International Financial Cryptography Conference*, 2003.
[22] Castelluccia and G. Avoine, "Noisy tags: A pretty good key exchange protocol for RFID tags," in *Proc. Smart Card Research and Advanced Applications*, Berlin, Springer, 2006, pp. 289-299.
[23] S. Kinos, F. Hoshino, T. Komuro, A. Fujimura, and M. Ohkubo, "Nonidentifiable anonymous-ID scheme for RFID privacy protection," in *Computer Security Symposium*, 2003.
[24] G. Bedi, G. Venayagamoorthy, and R. Singh, "Navigating the challenges of Internet of Things (IoT) for power and energy systems," in *Proc. Clemson University Power Systems Conference (PSC)*, Clemson, SC, 2016.

Hesham M. Allam is a faculty member with the Department of Computer and Information Science at the Higher College of Technology, Dubai Women's Campus. He received his interdisciplinary Ph.D. from Dalhousie University, Halifax, Canada, in 2013 combing computer science, business administration, and information management. Dr. Allam is specialized in social computing, business intelligence, and data mining. He has published some of his research results in highly reputed international conferences, and served as a reviewer for multiple premier conferences in IS. Prior to joining HCT, he worked as adjunct faculty at Dalhousie University teaching both undergraduate and graduate degrees at the Faculty of Computer Science, School of Business Administration, and School of Information Management. Dr. Allam also worked as researcher at Dalhousie University, a faculty member of information technology at YIC, KSA, and an instructor of IS at California State University Sacramento (CSUS). He received his MBA in MIS from CSUS, and B.A in Education from Tanta University. Dr. Allam is a member of ACM and IEEE.

Ahsan Chaudhri holds BB(IT) from Curtin University, Australia and PGC, MBA , MBUS(IT) , Master of Education &Leadership, from Auckland University of Technology , New Zealand. He holds more than 15 years of combined experience in academia and industry at senior positions. He has published in many leading journals and attended conferences in Australia, New Zealand, Malaysia, Thailand, and UAE. His research interest includes domains of business and information systems. Currently he is working as an "Academic Director' at Alpha Education Institute in New Zealand. His previous position was a business faculty member at Higher Colleges of Technology, UAE