# INTERNET OF THINGS: ISSUES AND CHALLENGES

[1]YASEEN ABDULLAH ABDULRAHMAN, [2]MASSILA KAMALRUDIN, [3]SAFIAH SIDEK,
[4]MAHADI ABU HASSAN

[1, 2] Faculty of Information and Communication Technology,
[2, 3, 4] Innovative Software Systems and Services Research Group
Universiti Teknikal Malaysia Melaka,
Locked Bag 1200, Hang Tuah Jaya, 75450 Ayer Keroh, Melaka.

E-mail: yaseeno994@gmail.com, massila@utem.edu.my, safiahsidek@utem.edu.my,
mahadi@utem.edu.my

## ABSTRACT

Substantial research attention has been paid to the Internet of Things (hereafter abbreviated to IoT) since the dawn of the new millennium. IoT is very much perceived as being a major component of the Internet of the future. The composition of the Internet of the future will be billions of intelligent things that communicate through a variety of connected devices and it will become a means of enabling the realization of new capabilities of the 'things' that are connected. This paper presents a review of the related research relating to IoT. Further, issues associated with IoT particularly standardisation, security and privacy are also discussed. The discussion provides valuable information for future research in IoT.

**Keywords**: Internet of Things, RFID, Security, Privacy, Data Protection.

## 1. INTRODUCTION

Internet of Things (IoT) is seen as the 'Next Big Thing' after the Internet by the worldwide information industry, both in technological and economic terms. The IoT perception is that of an intelligent network that connects all things to the Internet and allows information exchange, as well as communication, through sensing devices while complying with standard protocols.

According to Stankovic [1], the IoT succeeds in attaining the aims of intelligent identification, location, tracking, monitoring and management of things. Pretz [2] considered IoT to be a things-connected network, in which the things are connected wirelessly through smart sensors. Furthermore, he predicates that IoT does not require human intervention to interact. By its inherent ability of permitting human and human, to human and things, or between things and things, IoT both expands and extends Internet-based network communications. The IoT hypothesis means many objects that surround us can be hooked up to networks in one form or another. In this context, a plethora of applications will have Radio-Frequency Identification (RFID), sensor and other smart technologies embedded into them.

In certain fields, applications that take advantage of IoT technology have already been developed: These include healthcare, transportation and the automotive industries, as well as home management ([3];[4];[2]). In addition, the cloud-based Internet has been seen as new developments in the integration of objects with sensors ([5]; [4];[2]).

Although there has been rapid advancement in the developments of IoT products, but the issues regarding IoT still exist and thus requiring appropriate solution and improvement. These include infrastructure, protocols and standards as well as the issues associated with IoT over privacy, security and protection. This review will look at the latest research in IoT development thus far and attempt to identify topics for future research into IoT.

This paper develops an insight of the value of knowledge as well as issues regarding IoT explored from different articles which previous authors didn't explore till recent year 2016. Previous review paper discussed on the major IoT application in industries, IoT research trends and some IoT challenges.

## 2. DEFINITION OF IOT

Several definitions of IoT have been proposed by researchers since the term and concept of IoT was first instigated by Kevin Ashton in 1999. Back then in hundreds of presentations he gave to corporate leaders, he proffered the idea that the IoT is connected uniquely to identifiable and interoperable objects by the use of RFID technology. But an exact definition of IoT remains in the formative stage, and is subject to perceptions ([5]; [4]; [2]).

The IoT European Research Cluster [6] and others ([7]; [8]; [9]) gave a general definition of the IoT as a "dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols; physical and virtual 'things' in an IoT have identities and attributes and are capable of using intelligent interfaces and being integrated as an information network". In essence, according to the European Telecommunications Standards Institute [10], the IoT can be considered as a superset of connecting devices that are uniquely identifiable by existing near-field communication (NFC) techniques.

Disregarding disagreements on the definition of IoT, discussions have been widespread, and quick development of consequent technologies by diverse bodies has occurred ([11]; [5]; [12]; [13]; [2]): some of the best examples are techniques used for intelligent sensing and wireless communication that have become part of IoT, giving rise to new challenges and research vistas ([14]; [15]).

While the definition of IoT may vary according to technologies used in implementation, the basic tenet of IoT demands that objects within the IoT can be uniquely identified when virtually represented. Built into IoT is that all things are able to exchange data and where necessary, process the data collated in relation to pre-defined standard.

## 3. LITERATURE REVIEW

The Internet of Things (IoT) [16] contends that the goal of linking together "everything" that carries a bare minimum of both computational power and storage capability is a new perspective, whereby things connected in such a way can cooperate at any time regardless of location or form. Such collaboration will occur with applications designed to cover a variety of fields, for example in social and personal arenas, the monitoring of services and utilities, transport and business enterprises ([17]; [18]).
Estimates made in 2013 indicated that the number of IoT devices in existence exceeds 30 billion, which make more than 200 billion intermittent connections between them [19]. By the year 2020, it is anticipated that over 700 billion Euros of revenue will be created from such connections [20]. Due to the rise in popularity of mobile communications that utilize wireless sensor networks (WSNs) and RFID technologies, plus an abundance of small hardware where storage and operational computing requirements are reduced to a minimum, there has been a corresponding increase in connectivity of such IoT gadgets [21]. These factors, when combined with efforts to standardize communication protocols like Machine-to-Machine (M2M), MQ Telemetry Transport (MQTT) v. 3.1, Extensible Messaging and Presence Protocol (XMPP) and others Saint-Andre, Smith, Tronon means that the worldwide vision of the IoT per se is now facilitated for the majority of industry and the markets they serve. Where reliability becomes a critical issue in such global uses, these may demand a minimum degree of system specification accuracy combined with a high level of reassurance in respect of properties that are non-functional like privacy, protection and security [22]. In this regard, formal analysis techniques must be used to guarantee as much unambiguity as achievable: the specifications derived will lead to applications that are strong and dependable.

The pervasive computing technologies of today mean that daily activities of many of us are tracked by smartphones in use: increasingly, more everyday things in use are connected to the Internet [23]. This generates a sea change in interactions, lifestyle and the way people work. In turn, this has given rise to 'smarter' cities being possible. However, complexity of the urban environment as well as the people living in it means that the design, development and implementation of computing projects and innovations is particularly challenging.

In the field of mechatronics, the latest developments in the IoT have compelled those working with mechatronics to reconsider the manner in which mechatronic systems and components are contrived, designed and made. Issues like machine ethics, user interaction, and also those concerning security of data and the individuals using mechatronic smart objects need to be considered because the structure of an IoT based system is defined by context. The inherent challenges presented by the IoT are driving forward new approaches to design and education in mechatronics [24].

A line type dismantling system for end-of-life vehicles (ELV) dismantling plants was proposed by Hwa-Cho Yi and Jung ([25]; [26]). The implementation used remote real-time monitoring using IoT technology. Identification data of the ELV such as the vehicle identification number (VIN) stored on a server enables identification of the ELV by match of a RFID tag on the car being loaded. Workstations are able to identify the vehicle via a RFID reader, request the ELV's weight through Zigbee communication and receive a dismantling worksheet generated from the server. The result of the dismantling is displayed on the PC screen and also stored on the server. Authorized users can enquire what status each workstation is at and view the work history via Internet and/or the work history of each ELV directly from the server. It is suggested that this research could be the foundation for more complex monitoring systems that include downstream recyclers like shredding and anti-slip regulation (ASR) treatment.

Over the last ten years, RFID-based identification has seen wide use in the fields of logistics, retail management, pharmaceuticals and health care [27]. Due to the advances made since 2010 in intelligent sensors, sensor network technology and low energy wireless communication, an increasing number of 'things' can be networked as IoT ([28]; [29]; [30]; [31]; [32]; [33]).

Technical standards relative to specification of data exchange, processing and intra-network communication should be designed for IoT to provide high quality services to end-users and applications alike [34]. Factors affecting the success of IoT include standardization on a global scale that will deliver inter-operability, compatibility, dependability and operational effectiveness. Objects in an IoT have to possess the ability of autonomous communication and exchange of data ([35]; [36]; [37]). Once millions, or even billions, of things can be seamlessly and effectively integrated, IoT becomes capable of widespread application over innumerable areas ([38]; [4]; [39]; [40]).

Both developed and developing nations have recognized the importance of IoT and its future potential. Many have formulated proposals for national strategies to investigate enabling technologies for IoT. As a few examples, in the UK, the government launched a £5 million project on IoT technology and innovation ([41]; [42]). The IoT European Research Cluster (IERC) has sponsored a number of cooperative projects in fundamental research pertaining to IoT: applications and end-users supply specific requirements to push forward the theoretical studies in these projects. One of these is the project of Internet of Things Architecture (IoT-A), aimed at developing a reference model and architecture of IoT to satisfy specific needs of the applications. Simultaneously, the European Telecommunications Standards Institute (ETSI) has the responsibility of developing policies related to IoT ([43]; [44]; [29]).

Moving westwards, in the US the Information Technology & Innovation Foundation (ITIF) advocated that new information and communication technologies (ICT) can be an effectual means to improve traditional and information technology infrastructure that will have a greater positive impact on productivity and innovation. The concentrated areas of ICT developments in the US are energy, broadband technologies, rural utility services, and health information technology ([45]; [46]).

In the Far East, Japan proposed "u-Japan x ICT" and "i-Japan strategies" in 2008 and 2009 - these projects aimed at deploying IoT in all areas of daily life. South Korea ran RFID/USN and "New IT Strategy" programs to advance IoT infrastructure development. In China, the government officially launched the "Sensing China" project in June 2010; the goal of this project was to develop the technologies so that objects in an environment have identity tags which are able to broadcast information, and such information could be accessed through the Internet. People can be tracked within the IoT and any conditional variables monitored so that the performance of the networked systems can be optimized to reduce waste and costs.

## 4. ISSUES RELATED TO IOT

Many cross-layer protocols exist for Wireless Networks ([10]; [6]), Wireless Mesh Networks (WMNs) [41] or Ad Hoc Networks (AHNs) [47]. Nevertheless, they cannot be applied to the IoT because of several reasons. First of all, the diversity of the IoT, caused by things having largely different hardware configurations, Quality of Service (QoS) requirements, functionalities, and objectives. By contrast, nodes in a Wireless Sensor Network (WSN) usually have similar hardware specifications, comparable communication requirements, and shared aims. Second, the Internet is involved in the IoT, from which IoT inherits a centralized and hierarchical architecture. Contrastingly, WSNs, WMNs and AHNs have comparatively flat network architectures: nodes in them communicate in a multi-hop fashion without

Internet involvement.

Despite significant research efforts in the development of IoT, there remain several major outstanding issues in terms of technical challenges. An example is the design of a service-oriented architecture (SoA) for IoT which is still considered as a big challenge, whereby service-based things may suffer in terms of their performance, including cost. Added to this, the automated service composition based on the requirements of applications is still unresolved. From a network standpoint, IoT is a complicated diverse network that includes connections between various types of networks through differing communication technologies. Devices and methodologies to counter problems with things management is an outstanding challenge. Also from the viewpoint of service, the lack of commonly accepted service descriptions makes service conflicts in different implementation environments. Furthermore, a powerful service discovery and searching engine should be very helpful to advance IoT technology. Since IoT operates in an ICT environment, all connected things could adversely affect it. The challenge of integrating IoT with current ICT systems is therefore an outstanding issue.

The absence of agreed standards is an argumentative factor for a decrease in the competitiveness of IoT products ([48]; [49]; [43]; [44]; [50]; [51]; [52]; [53]; [54]). Over the last ten years, a number of technical standards have been developed by various organizations; these constitute a more and more important role to the success of IoT [55]. Standards for middleware and interfaces are considered to be extremely important. Research efforts include: (1) designing policies and distributed architecture; (2) ensuring privacy and protection of users; (3) realizing the trustworthiness, acceptability, and security of networks; (4) developing standards; (5) exploring new enabling technologies such as micro-electronic mechanical system (MEMS) devices and ubiquitous localization ([51];[52][53]). Standards in IoT have attracted a great deal of attention in many countries. Internationally, the ITU, Electronic Product Code global (EPCglobal), International Electrotechnical Commission (IEC), International Organization for Standardization (ISO), and IEEE have provided a set of standards to identify, capture, and share data using RFID technologies. ([48]; [49]; [43]; [44]; [50]; [51]; [52]; [53]).

The standardization of IoT takes the efficacy and readiness of specifications into account ([47]; [56]; [57]). Although many organizations are working on primary standards for IoT, global collaboration between standards bodies is essential to deal with the lack of consistency among standards bodies and the standards; the World Standards Cooperation (WSC) needs to be able to manage the relationships between the international standards bodies and regional standards bodies [58]. Worthy of note is the importance of standards for the technological development of IoT. On the one hand, standards help developers and users define the best technical rules for applications and services in IoT. On the other hand, standardization of technologies in IoT is considered to be important and urgent: this can and will accelerate the spread of IoT technology [59].

Standardization is vitally important in the development of IoT. Its goals include lowering the entry barriers to new service providers and users; improvement of interoperability; and to enable products or services to compete for better outcomes at a higher level ([60]; [61]; [62]; [63]; [64]). Standardization of IoT is difficult due to its rapid growth. Particular problems experienced in IoT standardization include interoperability, radio access level, semantic interoperability, plus security and privacy issues [65]. Open standards of IoT, such as those of security, communication and identification, may prove to be several key enablers for expansion of IoT technologies [66].

Two other very important issues have arisen in IoT: those of security and privacy. IoT connectivity depends upon the ability of smart tags or sensors to both sense the environment they are in and to exchange data between devices. The information drawn from such elements like RFID tags, intelligent sensors, Bluetooth Low Energy (BLE) that are integrated into devices within this ‘sensing layer’ demands technologies that must be effective in providing security and protection of privacy of these data over a wide range of activities, be they personal or business in nature. ([67]; [68]; [69]; [70]). IoT applications could be disturbed by persistent threats of RFID tag attacks or even data leakage [71]. There are a number of security schemes and protocols for authentication proposed to counteract threats to security [72], an example of which is the “block tag” method to guard against unauthorized tracing [35]. When considering exchange of data, low cost symmetric key cryptography algorithms, for example Advanced Encryption Standard (AES) and Tiny Encryption Algorithm (TEA) have been expounded as protection. From the security point of view, low cost RFID tags have implemented elliptic curve cryptography using asymmetric key algorithm for authentication purposes. It is also possible to integrate security protocols already developed for WSNs as a fundamental part of IoT. Further studies are required into a) adoption of existing Internet standards for interoperable protocols in IoT, and b) assuring security of compassable services.

In IoT, it is of particular importance to label and give an address to each and every object (thing) that is connected. But connections between things could possibly give rise to security issues that have never arisen before [73]. Thus strong security measures are essential to preclude both attacks and malfunctions. [74]. Established networks like the Internet utilize security protocols and privacy settings are generally the means of protecting communication and individual privacy, but sadly it is a fact that these techniques fall short of the requirements of IoT [75]. Such mechanisms need improvement before they can be applied to IoT [76].

In addition, frameworks for legal and technical issues are required. With the complexity, dynamic nature and many uncertainties involved in IoT, protection of millions of things that are diverse and intelligent in nature represents a daunting task [77]. This very diversity has a significant effect on security of networks that could suffer threats. Things themselves might also be subject to a multitude of dangers like leakage of data or threats from external networks. The demand on security technologies to offer robust protection for all system components at all stages is high: from sensing layer to interface layer, in ID through provision of services, and from RFID tags to IT infrastructure [78]. Furthermore, information must be secured from the moment of collection to the end of its life cycle, or cradle to grave. Privacy of information ranks as one of the most sensitive areas for IoT [79]. In personal services, the requirement of ease of data accessibility poses the challenge of protecting the information [80]. In designing privacy protection methods, certain factors have to be considered: as one example, user authentication concurrently involves development of access control and trust management ([81]; [82]; [5]).

Public acceptance of new IoT technology and services depends largely on how trustworthy the information is and how well private data is protected. Despite a number of development projects aimed at security and protection of privacy, a dependable solution for these issues is still outstanding in respect of data confidentiality, privacy and trust [83]. From a technical perspective, the following concerns need addressing: defining security and privacy from social, cultural and legal standpoints: trust mechanism: security of communications: privacy of user data and communications; and last but not least, security of applications and services.

## 5. CONCLUSIONS

Nowadays Internet of Things has received much attention from many researchers and developers who have been working on how to integrate it on the large number of proposed technologies. This paper reviewed the current related research and development on IoT. Although there has been an increase usage of IoT in healthcare, social networks and industrial application, issues such as standardization, security and privacy have become among the main concerns in the field of IoT.

Public awareness on the three major IoT issues is showing a sign of anxiety which need to be solved right away. This is related to the public trustworthy in order to be persistence in accepting IoT. However, this is actually a promising opportunity to those researchers and developers in IoT field to keep experimenting for the better methods of solution to the related IoT issues.

## FUTURE RESEARCH

IoT is definitely an emerging and appealing technology that requiring lots of improvement from day to day in term of developing the effectiveness of the system application. Therefore, an update review on the changes in the development and usage of IoT together with the related issues provide a valuable platform for future research in IoT.

## 6. ACKNOWLEDGEMENT

We would like to thank the financial support from the Ministry of Higher Education Malaysia and the Universiti Teknikal Malaysia Melaka for their assistance in this research. All authors acknowledge the support of the FRGS grant: FRGS/1/2015/SS06/PBPI/02/F00206.

## REFERENCES

[1] J. A. Stankovic, “Research directions for the Internet of Things,” *IEEE Internet Things*, vol. 1,no.1, pp. 3–9, 2014.

[2] K. Pretz, “The Next Evolution of the Internet.,” *IEEE Inst.*, pp. 1–4, 2013.

[3] L. He, W., Yan, G., & Xu, “Developing vehicular data cloud services in the IoT environment.,” *IEEE Trans. Ind. Informatics.*, 2014.

[4] S. W. Joshi, G. P., & Kim, "Survey, nomenclature and comparison of reader anti-collision protocols in RFID," *IETE Tech. Rev.*, 2013.

[5] D. Hepp, M., Siorpaes, K., & Bachlechner, "Harvesting Wiki consensus: using wikipedia entries as vocabulary for knowledge management.," *IEEE Internet Comput.*, no. 11(5), pp. 54–65., 2007.

[6] IERC, "Coordinating and building a broadly based consensus on the ways to realise the internet of things in Europe," 2013.

[7] D. Kirtsis, "Closed-loop PLM for intelligent products in the era of the internet of things," *Comput. Des.*, no. 43(5), pp. 479–501, 2011.

[8] J. Li, S., Xu, L., Wang, X., & Wang, "Integration of hybrid wireless networks in cloud services oriented enterprise information systems.," *Enterp. Inf. Syst.*, no. 6(2), pp. 165–187, 2012.

[9] Y. Li, Y., Hou, M., Liu, H., & Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things.," *Inf. Technol. Manag.*, no. 13(4), pp. 205–216, 2012.

[10] ETSI, "The European Telecommunications Standards Institute," 2013.

[11] Z. Guo, J., Xu, L. D., Xiao, G., & Gong, "Improving multilingual semantic interoperation in cross-organizational enterprise systems through concept disambiguation," . *IEEE Trans. Ind. Informatics*, no. 8(3), pp. 647–658, 2012.

[12] ITU, "The internet of Things, International Telecommunication Union (ITU)," *Internet Rep.*, 2013.

[13] X. Li, S., Xu, L., &Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Trans. Ind. Informatics*, no. 9(4), pp. 2177–2186, 2013.

[14] B. Hunter, D., Yu, H., Pukish, M., Kolbusz, J., & Wilamowski, "Selection of proper neural network sizes and architectures-a comparative study.," *IEEE Trans. Ind. Informatics*, no. 8(2), pp. 228–240, 2012.

[15] B. Wilamowski, "Challenges in Applications of Computational Intelligence in Industrial Electronics," *Proc. IEEE Int. Symp. Ind. Electron. (IEEE ISIE 2010)*, pp. 15–22., 2010.

[16] M. Gubbi, J., Buyya, R., Marusic, S., Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions," *Futur. Gener. Comput. Syst.*, pp. 1645–1660, 2013.

[17] G. Atzori, L., Iera, A.,&Morabito, "The Internet of Things: A survey," *Comput. Networks Elsevier*, no. 54 (2010), pp. 2787–2805, 2010.

[18] J. Bandyopadhyay, D., Sen, "Internet of Things - Applications and Challenges in Technology and Standardization," *Wirel. Pers. Commun.*, 2011.

[19] P. Vermesan, O., Friess, "Internet of things converging technologies for smart environment and integrated Ecosystems," *River Publ. Ser. Commun.*, 2013.

[20] S. Mazhelis, O., Warma, H., Leminen, "Internet-of-Things Market, Value Networks, and Business Models: State of the Art Report," *Tech. Rep. TR*, no. 39 (2013), 2013.

[21] M. Palattella, M.R., Dohler, "Internet of Things in the 5G Era:Enablers, Architecture and Business Models," *IEEE J.*, no. 0733–8716, 2016.

[22] B. Aziz, "A formal model and analysis of an IoT protocol," *Ad Hoc Networks 36 49–57. 1570-8705/© 2015 Elsevier B.V*, 2016.

[23] U. Salim, F.,Haque, "Urban computing in the wild: A survey on large scale participation and citizen engagement with ubiquitous computing, cyber physical systems, and Internet of Things," *Int. Journal.Human-Computer Stud.*, no. 81(2015), pp. 31–48,1071–5819, 2015.

[24] Bradley,D.,Russell,D.,Ian,F.,Isaacs,J.,Allan, M., White, "The Internet of Things–The future or the end of mechatronics," *Mechatronics 27 57–74. 0957-4158/_ 2015 Elsevier Ltd*, no. 27 (2015), pp. 57–74. 0957–4158, 2015.

[25] Hwa-Cho Yi and Jung Whan Park., "Design and Implementation of an End-of-Life Vehicle Recycling Center based on IoT (Internet of Things) in Korea.," in *The 22nd CIRP conference on Life Cycle Engineering.Procedia CIRP 29 ( 2015 )*, 2015, pp. 728 – 733.

[26] H.-C. Y. Jung, W. P., "A Monitoring System Architecture and Calculation of Practical Recycling Rate for End-of-Life Vehicle Recycling in Korea," *Int. J. Precis. Eng. Manuf. Technol.*, vol. 1, No. 1, pp. 49–57, 2014.

[27] S. He, D., Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," *IEEE INTERNET THINGS J.*, vol. VOL. 2, NO, 2015.

[28] J. Li, L., & Liu, "An efficient and flexible web services-based multidisciplinary design optimisation framework for complex engineering systems.," *Enterp. Inf. Syst.*, no. 6(3), pp. 345–371, 2012.

[29] G. Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., & Borriello, "Building the internet of things using RFID: the RFID ecosystem experience," *IEEE Internet Comput.*, no. 13(3), pp. 48–55, 2009.

[30] E. Kranenburg, R., & Anzelmo, "The Internet of Things," *1st Berlin Symp. Internet Soc.*, 2011.

[31] T. Malatras, A., Asgari, A., & Bauge, "Web enabled wireless sensor networks for facilities management.," *IEEE Syst. J.*, no. 2(4), pp. 500–512, 2008.

[32] I. Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, "Internet of things: vision, applications and research challenges," *Ad hoc Networks*, no. 10(7), pp. 1497–1516, 2012.

[33] M. P. Oliveira, R.R., Cardoso, I.M.G.,Barbosa, J.L.V., Costa, C.A., Prado, "An intelligent model for logistics management based on geofencing algorithms and RFID technology," *Expert Syst. Appl.*, no. 42 (2015), pp. 6082–6097, 2015.

[34] N. Nguyen, K.T.,Laurent,M.,Oualha, "Survey on secure communication protocols for the Internet of Things," *Ad Hoc Networks*, no. 32 (2015), pp. 17–31, 2015.

[35] A. Juels, "RFID security and privacy: a research survey.," *IEEE Sel. Areas Commun.*, no. 24(2), pp. 381–394, 2006.

[36] A. S. Mitrokotsa, A., Rieback M. R., & Tanenbaum, "Classifying RFID attacks and defences," 2013.

[37] R. and Sikdar, "A Survey of MAC Layer Issues and Protocols for Machine-to-Machine Communications.," *IEEE INTERNET THINGS J.*, vol. VOL. 2, NO, 2015.

[38] EPCglobal, "Radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications," *860– 960 MHz, Version 1.2.0, http//www.gs1.org/gsmp/kc/epcglobal/*, 2013.

[39] L. Li, "Technology designed to combat fakes in the global supply chain," *Bus. Horiz.*, no. 56(2), pp. 167–177, 2013.

[40] C. Mutti, C., & Floerkemeier, "CDMA-based RFID systems in dense scenarios: Concepts and challenges," in *IEEE Int. Conf. on RFID, Las Vegas, NV*, 2008, pp. 215–222.

[41] E. Fleisch, "What is the Internet of things?," 2013.

[42] R. Klair, D. K., Chin, K.-W., & Raad, "A survey and tutorial of RFID anti-collision protocols.," *IEEE Commun. Surv. Tutorials*, no. 12(3), pp. 400–421, 2010.

[43] M. Floerkemeier, C., Roduner, C., & Lampe, "RFID application development with the Accada middleware platform," *IEEE Syst. J.*, no. 1(2), pp. 82–94, 2007.

[44] D. Gama, K., Touseau, L., & Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware.," *Comput. Commun.*, no. 35(4), pp. 405–417, 2012.

[45] L. He, W., & Xu, "Integration of distributed enterprise applications: a survey," *IEEE Trans. Ind. Informatics*, no. 10(1), pp. 35–42, 2014.

[46] L. Xu, "Enterprise systems: state-of-the-art and future trends.," *IEEE Trans. Ind. Informatics*, no. 7(4), pp. 630–640, 2011.

[47] W. Marry, "Disruptive civil technologies six technologies with potential impacts on us interests out to 2025," 2013.

[48] H. Broll, G., Rukzio, E., Paolucci, M., Wagner, M., Schmidt, A., & Hussmann, "Perci: pervasive service interaction with the internet of things," *IEEE Internet Comput.*, no. 13(6), pp. 74–81, 2009.

[49] F. Dada, A., & Thiesse, "Sensor applications in the supply chain: the example of quality-based issuing of perishables.," *LNCS*, no. 4952, pp. 140–154., 2008.

[50] E. Ilic, A., Staake, T., & Fleisch, "Using sensor information to reduce the carbon footprint of perishable goods.," *IEEE Pervasive Comput.*, no. 8(1), pp. 22–29, 2009.

[51] E. Karpischek, S., Michahelles, F., Resatsch, F., & Fleisch, "Mobile sales assistant – an NFC-based product information system for retailers," *Proc. First Int. Work. Near F. Commun. 2009, Hagenberg, Austria,* pp. 20–23, 2009.

[52] S. Li, L., Li, S., & Zhao, "QoS-aware scheduling of service oriented Internet of Things.," *IEEE Trans. Ind. Informatics*, 2014.

[53] T. Li, S., Oikonomou, G., Tryfonas, T., & Chen, "A distributed consensus algorithm for decision-making in service-oriented Internet of Things.," *IEEE Trans. Ind. Informatics.*, 2014.

[54] M. B. Spring, "The Future of Standardization: Are We Destined to Repeat History?," *IEEE Comput. Soc. Y*, 2016.

[55] K. Lee, I., Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *J. Bus. Horizons*, no. 2015( 58), p. 431—440, 2015.

[56] J. Vilamovska, A. M., Hatziandreu, E., Schindler, H. R., Oranje-Nassau, C. V., Vries, H., Krapels, "Study on the requirements and options for RFID application in healthcare Identifying areas for Radio Frequency Identification deployment in healthcare delivery: a review of relevant literature.," *Dir. Gen. Inf. Soc. Media, Eur. Comm. St. Monica, CA, USA RAND Corp.*, 2012.

[57] E. Borgia, "The Internet of Things vision: Key features, applications and open issues," *J. Comput. Commun.*, no. 54 (2014), pp. 1–31, 2014.

[58] S. Li, S., Li, D.Xu., Zhao, "The Internet of Things. A survey.," *Inf. Syst. Front*, pp. 243–259, 2015.

[59] L. Dave, B., Kubler, S., Främling, K., Koskela, "Opportunities for enhanced lean construction management using Internet of Things standards," *J. Autom. Constr.*, no. 61 (2016), pp. 86–97, 2016.

[60] Y. Jiang, H., Zhao, S., Zhang, Y.,&Chen, "The cooperative effect between technology standardization and industrial technology innovation based on Newtonian mechanics," *Inf. Technol. Manag.*, no. 13(4), pp. 251–262, 2012.

[61] Y. Jiang, H., Zhao, S., Qiu, S., & Chen, "Strategy for technology standardization based on the theory of entropy," *Inf. Technol. Manag.*, no. 13(4), pp. 311–320, 2012.

[62] Z. Jiang, H., Zhao, S., Wang, X., & Bi, "Applying electromagnetic field theory to study the synergistic relationships between technology standardization and technology development," *Syst. Res. Behav. Sci.*, no. 30(3), pp. 272–286, 2013.

[63] B. Chen, S., Wang, H., Xu, H., Liu, D., Hu, "Vision of IoT: Applications, Challenges, and opportunities with China Perspective," *IEEE INTERNET THINGS J.*, vol. VOL. 1, NO, 2014.

[64] C. L. Rose, K., Scott, E., "The Internet of things, an overview, understanding the issues and challenges of a more conected world," *internet Soc. J.*, 2015.

[65] H. Keoh, S. L., Kumar, S. S., Tschofenig, "securing the Internet of Things: A Standardization Perspective," *IEEE INTERNET THINGS J.*, vol. VOL. 1, NO, 2014.

[66] C. Soumya, K. D., Da Costa, R. F., Bonnet, "Resource Discovery in Internet of Things: Current Trends and Future Standardization Aspects," *IEEE J.*, 2015.

[67] C. Tan, W., Xu, W., Yang, F., Xu, L., & Jiang, "A framework for service enterprise workflow simulation with multi-agents cooperation," *Enterp. Inf. Syst.*, no. 7(4), pp. 523–542, 2013.

[68] X. Wang, F., Ge, B., Zhang, L., Chen,Y., Xin,Y.,&Li, "Asystems framework of security management in enterprise systems.," *Syst. Res. Behav. Sci.*, no. 30(3), pp. 287–299, 2013.

[69] L. Xing, Y., Li, L., Bi, Z., Wilamowska-Korsak, M., & Zhang, "Operations research (OR) in service industries: a comprehensive review.," *Syst. Res. Behav. Sci.*, no. 30(3), pp. 300–353, 2013.

[70] R. Vucˇinic, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., Guizzetti, "OSCAR: Object security architecture for the Internet of Things.," *J. Ad Hoc Networks*, no. 32 (2015) 3–16, pp. 1570–8705, 2015.

[71] W. Henze, M., Lars, H., Daniel, K., Roger, H., Rumpe, B., Klaus, "A comprehensive approach to privacy in the cloud-based Internet of Things.," *Futur. Gener. Comput. Syst.*, no. 56 (2016), pp. 701–718, 2016.

[72] R. H. Weber, "Internet of things: Privacy issues revisited.," *J. Comput. law Secur. Rev.*, no. 31 ( 2 0 1 5 ), pp. 618–627, 2015.

[73] J. Roman, R., & Lopez, "Integrating wireless sensor networks and the internet: a security analysis.," *Internet Res.*, no. 19(2), pp. 246–259, 2009.

[74] A. Caron, X., Bosua, R., Maynard, S.B., Atif, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," *J. Comput. law Secur. Rev.*, no. 32 (2016), pp. 4–15, 2016.

[75] C. Kang, K., Pang, Z., Xu, L., Ma, L., & Wang, "An interactive trust model for application market of the Internet of Things," *IEEE Trans. Ind. Informatics.*, 2014.

[76] M. H. Weinberg, B.D., Milne, G. R., Yana, G. A., Fatima, "Internet of Things: Convenience vs. privacy and secrecy," *J. Bus. Horizons*, no. (2015) 58, pp. 615—624, Elsevier, 2015.

[77] A. Sicari, S., Rizzardi, A., Grieco L.A., Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *J. Comput. Networks*, no. 76 (2015), pp. 146–164, 1389–1286/_ 2014 Elsevier., 2015.

[78] M. U. Akgun, M., Cagˇlayan., "Providing destructive privacy and scalability in RFID systems using PUFs," *Ad Hoc Networks J.*, pp. 1570–8705/_ 2015 Elsevier, 2015.

[79] L. Lin, X. J., Sun, "Insecurity of an autonomous authentication for privacy preserving IoT target driven applications," pp. 1–8, 2013.

[80] A. Y. Perera, C., Ranjan, R., Wang, L., Khan, U. S., Zomaya, "Big Data privacy in the internet of things era," *IEEE Comput. Soc.*, pp. 1520–9202/15/© 2015 IEEE., 2015.

[81] R. N. Fielding, R. T., & Taylor, "Principled design of the modern web architecture.," *ACM Trans. Internet Technol.*, no. 2(2), pp. 115–150, 2002.

[82] J. Frenken, T., Spiess, P., & Anke, "flexible and extensible architecture for device-level service deployment.," *LNCS 5377*, pp. 230–241, 2008.

[83] L. Zheng, X., Martin, P., Brohman, K., & Xu, "CLOUDQUAL: a quality model for cloud services," *IEEE Trans. Ind. Informatics.*, 2014.