Winter 12-6-2015

Effects Of The Internet Of Things (IoT): A Systematic Review Of The Benefits And Risks

Paul Brou

Marijn Janssen

EFFECTS OF THE INTERNET OF THINGS (IOT): A SYSTEMATIC REVIEW OF THE BENEFITS AND RISKS

Brous, P., Delft University of Technology, Delft, The Netherlands, p.a.brous@tudelft.nl
Janssen, M., Delft University of Technology, Delft, The Netherlands, M.F.W.H.A.Janssen@tudelft.nl

ABSTRACT

The Internet of Things (IoT) might yield many benefits and can be transformative in nature, yet has been given scant attention in e-commerce literature. The IoT describes a situation whereby physical objects are connected to the Internet and are able to communicate with, and identify themselves to other devices. These devices generate a huge amount of data. When it is possible to combine data from devices and other systems, new insights may be created which may provide important benefits to e-commerce. The duality of technology predicts that the accomplishment of benefits might also cause risks. In this paper we conduct a systematic review of literature to create an overview of perceived benefits and risks of IoT. The results confirm the duality that IoT has a variety of expected political, strategic, tactical and operational benefits as well as interrelated risks attached to its adoption. However, risks regarding the adoption of IoT also occur at all levels. Accomplishment of benefits requires that possible risks need to be mitigated in concert.

Keywords: Internet of Things, IoT, adoption, open data, e-commerce, smart cities, impediments, barriers, challenges, benefits, advantages

INTRODUCTION

The term, the Internet of Things (IoT) refers to the increasing network of physical objects that feature an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems [8][21][33]. IoT makes it possible to access remote sensor data and to monitor and control the physical world from a distance, allowing many physical objects to act in unison, through means of ambient intelligence [33]. These devices, and the communication between these devices, can benefit e-commerce by providing enough quality data to generate the information required to make the right decisions at the right time.

IoT can be used to enrich e-commerce by enabling a technology-mediated relationship between stakeholders. According to Daniel, Wilson, and Myers (2002), e-commerce encompasses not only "the buying and selling of information, products and services via computer networks" [24 p.254] but also, the use of Internet technologies to exchange or share information within the organization or with external stakeholders. IoT can have important implications for e-commerce to improve the client experience and ensure reliable product delivery. The data may be combined in new, creative ways to be used for commercial gain.

Research in the sociology of technology suggests that the evolution of new applications is a process of social interaction between multiple agents [2]. The duality of technology theory [28] describes technology as assuming structural properties whilst being the product of human action. Technology is *physically* constructed by actors in a social context, and *socially* constructed by actors through the different meanings they attach to it. A crucial aspect of human action is that it is knowledgeable and reflexive. According to Orlikowski (1992), agency refers to capability not intentionality, although action taken by actors may have unintended consequences. As such IoT implementations may also bring with them unintended consequences such as the misuse of surveillance or telecom data which disregards personal privacy, or on the positive side, the use of sensor data in "Big Data" applications which provide insight into issues other than those for which the sensor was placed in the first place. The dual nature suggests that IoT might have positive impacts and it could also exert negative effects when not designed properly. We will view this as the risks that might occur.

The methodology used in this research is described in section two. On the basis of state of the art literature an initial list of benefits and risks will be derived in section three. The potential benefits of IoT will be presented followed by the risks. The results show that IoT has a variety of potential strategic, tactical and operational benefits and risks. This implies that IoT enables effective knowledge management, sharing and collaboration between domains and divisions at all levels of the organization, as well as with external partners. However, these benefits do need to be weighed against the potential risks of IoT adoption. Finally, conclusions will be drawn in section four.

RESEARCH METHOD

The common benefits and risks of IoT were identified from a rigorous review of literature. In August 2015, the keywords: "Internet of Things", ("benefits" or ("impediments" or "barriers")) and "e-commerce", returned four hits within the databases Scopus, Web of Science, IEEE explore, and JSTOR, of which three were considered relevant to this research. This confirmed the limited amount of e-commerce literature addressing this topic. The query [all abstract: "internet of things" "benefits" "impediments" "barriers" "e-commerce"] searching between 2000 and 2015 returned five hundred and thirty-nine hits in Google Scholar. We then filtered these results and performed a forward and backward search and selected thirty-three relevant articles based on the criteria that they specifically referred to potential benefits or risks with regards to the use or implementation of IoT within potential e-commerce applications. The resulting risks and benefits found in the literature were perceived benefits and risks and it was not clear if they actually could be found in practice and how the benefits and risks are

interrelated. In the literature benefits and risks are often assumed to occur, but there was no systematic account of the evaluation in practice and if they were actually accomplished. The expected benefits and risks of the IoT for e-commerce are expressed in italics within this paper.

LITERATURE REVIEW

The main enabling factor for the IoT is the blending integration of several technologies and communications solutions such as identification and tracking technologies, wired and wireless sensor and actuator networks, enhanced communication protocols (shared with the Next Generation Internet), and distributed intelligence for smart objects [3], Radio Frequency Identification technology, Electronic Product Code technology, and ZigBee technology [10]. By installing apps on a mobile phone or tablet the device can become a sensor in a large network. For example, accelerometers can be used to detect potential potholes when persons are cycling or driving. Cameras and microphones can be used to collect evidence when there is a robbery or a riot and devices can measure the concentration of fine particles. Sensors can be used for enabling public safety and compliance to regulations for example. In this way it may provide a more effective control mechanism [3][7][10][11][17].

Potential Benefits

IoT results in a large amount of big data. Literature shows that this might have two important benefits for e-commerce [9]. Firstly, making data and information available to the public greatly improves government transparency [9]. Increased openness and transparency helps ensure proper oversight and reduces government waste. Secondly, enabling consumer self-service in this way can empower citizens and business to take decisions through better access to information by making use of the vast amount of data collected by IoT and the collective wisdom of the crowds [3][7][10][14][17][21] [12]. The IoT gives intelligent advice to users. For example, in intelligent transportation systems such as in-car intelligent driving systems and smart highways, route planning assists drivers by considering constraints related to traffic, time, and cost [21][33].

Fleisch (2010) identifies seven value drivers for the IoT which result in potential business benefits: 1. The "simplified manual proximity trigger" increases job satisfaction, empowers consumers by enabling consumer self-service, reduces labor costs and improves data quality [5]; 2. the "automatic proximity trigger" reduces fraud related costs, process failure costs, and labor costs, and provides high granularity data for improved efficiency through process improvement; 3. the "automatic sensors trigger" helps improve service quality by providing individual and prompt process control, increases process efficiency and effectiveness, and provides an additional level of data quality for identifying potential areas for further process improvement; 4. automatic product security reduces cost of process failure due to fraud, reduces the cost of process security and helps increase consumer trust; 5. simple, direct user feedback improves service efficiency and effectiveness by helping processes become more accurate, more flexible, and faster; 6. extensive user feedback improves trust by ensuring new customer contact, providing new advertising opportunities and supporting additional service revenues; 7. mind changing feedback allows for the identification of trends, enabling new product features and new services, and enables an active selection of attractive customer segments [14].

Another view of possible IoT application classification is provided by [11]. Chui et al. (2010) define two broad categories for IoT applications, Information and Analysis and Automation and Control. In Information and Analysis, decision making services are improved by receiving better and more up to date information from networked physical objects which allows for a more accurate analysis of the current status-quo with regards to tracking, situational awareness, and sensor-driven decision analytics. In Automation and Control, outputs received from processed data and analysis are acted upon to improve efficiency, effectiveness and to enforce compliancy.

Haller et al. (2009) draw on the work of Fleisch et al. (2006) and identify two major paradigms from which business value can be derived: real-world visibility, and business process decomposition. Haller et al. (2009) believe that with real-world visibility, sensors make it possible for a company to better know what actually is happening in the real world. The use of automated identification and data collection technologies such as RFID enables an increased accuracy and timeliness of information about business processes and provides competitive advantages through improved service efficiency in terms of process optimization [39]. This may allow for more system flexibility in which the system is better able to react to dynamic changes [39].

According to Harrison (2011), the benefits of IoT technologies for commerce and e-commerce are primarily derived from the availability of more granular information which is automatically collected and readily shareable soon after it is generated [20][41]. This provides better analysis of track and trace information, and helps balance supply and demand [20]. Ubiquitous computing and grid computing can be applied to network manufacturing resources [5]. Data can be acquired promptly and readily shared by all decision-making units.

In short, IoT can deliver a variety of benefits related both to the real-time measurement and analyses of sensor data efficiency of services, improved effectiveness of services, and improved flexibility of services as to trend analysis of historical data over time. We list the possible benefits of IoT according to strategic/political, tactical and operational divisions. This is a popular divisioning [1][23], suitable for e-commerce research. Possible benefits of the IoT are: 1. Political and Strategic - improved forecasting and trend analysis, promoting government transparency, improved citizen empowerment; 2. Tactical - improved planning with regards to management and maintenance, more efficient enforcement of regulations, improved health and safety

measures, cost reduction, new revenue streams; 3. Operational - improved efficiency of services, improved effectiveness of services, improved flexibility of services.

Potential Risks

Organizations are increasingly turning to the IoT as new sources of data, which are derived from continuously monitoring a wide range of things within a variety of situations, become available. However, there are several technological and regulatory challenges that need to be addressed. Scarfo (2014) believe that the most important of them are related to data ownership such as security, privacy and the sharing of information [36]. It is clear that the implementation of IoT for e-commerce faces a variety of impediments. Skarmeta et al. (2014) consider security and privacy to be the main obstacles for a full acceptance of IoT. The sensitivity levels of the information are a crucial aspect to be considered by the access control mechanism. Disclosure of user data could reveal sensitive information such as personal habits or personal financial information. The unauthorized access to this information can severely impact user privacy [13][22][25][36][37][43][44]. In this way, IoT requires novel approaches to ensure the safe and ethical use of the generated data [35], requiring a strong data governance [16][22][36][40][43]. A weak form of data governance can impede the safe and ethical use of data generated by IoT devices.

According to Misuraca (2009), IoT brings with it a wealth of new business opportunities. There is enormous scope for developing applications and selling new services [26]. But a lack of, or poorly coordinated, policy and regulations regarding IoT can also greatly impede the implementation and application of IoT. Organizations need to develop policy and regulations and position themselves carefully within this arena [19][40][43]. In this regard, organizations should consider the role they play in enabling IoT development very carefully. Market forces of supply and demand can play substantial roles in the success or failure of IoT [13][26][32][42]. For example, according to Qiao et al. (2012) the IoT industry will demonstrate an inevitable outbreak growth at the growth stage of the Industry Lifecyle Theory [4].

Although reduction in overall costs is an often cited benefit of IoT for e-governance [8], many researchers also cite high development and implementation costs as an important impediment to the implementation and application of IoT [13][19][27][32][43]. According to Yazici (2014), high maintenance costs are often rated as the largest impediments to IoT implementation. A fully functional IoT system based on RFID technology can be substantial. By way of example, Yazici (2014) quotes Wal-Mart's vendors as having spent US$1 to US$3 million on a RFID implementation.

Furthermore, the Internet of things is more than one device, application or network. In order to ensure sustainable connectivity, all interfaces and communication protocols require unified industry standards [13]. However, Fan et al. (2014) believe that the large number of standards-setting organizations has led to a situation in which the top standard has not yet been set. Vendors are free to choose which standard they find best fits their production line, leading to a wide variety of available types. This may impede interoperability and integration of data [6][13][19][36][40]. IoT requires that a large number of devices be integrated with the existing Internet. These devices can be diverse in terms of data communication methods and capabilities, computational and storage power, energy availability, adaptability, mobility, etc. Heterogeneity at the device level is a serious impediment to IoT adoption.

According to Zeng et al. (2011), Universal Plug and Play (UPnP) is currently the most popular solution for personal network implementation. However, there is no authentication protocol proposed for UPnP. All devices are allowed to configure the other devices on the personal network, without any user control. This can result in a critical security issue when the smart things become available on the Internet. The attention given to security by a number of authors [13][19][22][36][37][44] suggests that a lack of security standards is becoming a serious impediment to IoT implementation. Whilst there are many standard technologies and protocols to address many security threats, the severe constraints on the IoT devices and networks prevent a straightforward implementation of these solutions [37]. Furthermore, IoT devices generally have to work in harsh, uncontrolled environments, where they may be prone to attacks, misuse or malicious intentions [37].

According to Kranenburg et al. (2014), the success of user-centric services based on IoT technology depends primarily on people participating and sharing information flows [25]. Willingness on the part of people to participate in these systems is therefore required [13][16][27][29][38][42]–[44]. Kranenburg et al. (2014) believe that this willingness is predominantly dependent on the perception of people: the perceived trust and confidence in IoT and the perceived value that the IoT generates for them. The greater the trust of users in the IoT, the greater their confidence in the system and the more willing they will be to participate [25]. A lack of trust in the system can be a strong impediment to the effectiveness of IoT.

Operational barriers include human capital issues such as difficulty in employing qualified personnel, lack of specialists, and personnel skill shortage to operate new applications [38][43], [19], as well as insufficient IoT oriented training and educational activities [19]. Harris et al. (2015) also identify personnel reluctance to change or to learn new technology as a barrier. A lack of understanding about how IoT works, the possible benefits, and how to make the business case for IoT implementation were also found to be barriers by a number of researchers [30][34][38][43]. Reyes et al. (2012) includes calculating the return on investment and the payback period in this category [34]. Operational barriers also include technical issues such as limitations in information technology (IT) infrastructural capabilities [13][22][25][31][36][42]–[44].

Data management issues are also of concern. Organizations are often faced with a complex legacy of data and applications

when implementing IoT solutions [16]. Many organizations may have several generations of systems running in parallel, and much of the data fed into the system has been done manually, with associated risks in terms of data quality [6][16][40].

In short, IoT faces a variety of barriers related to the proper use (privacy and security for example) and proper management of the data collected by the vast number of interconnected things. Strategic/political barriers are: data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces. Tactical barriers include: costs, interoperability and integration issues, acceptance of IoT, and trust related issues. Operational issues are: a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues.

Table 1. Summary of Benefits and Risks

	Benefits	**Risks**
Strategic	Improved forecasting and trend analysis [11][14][20], Promoting transparency [3][7][9][10][17][21], Customers/citizen empowerment [3][7][9][10][12][14][17][21]	Data privacy [13][22][25][36][37][43][44], data security [13][19][22][25][29][36][37][43][44], Weak/uncoordinated data policy [19][26][40][43], Conflicting market forces[13][26][32][42], Non-compliance to regulations[16][22][36][40][43]
Tactical	Improved planning [7][14][21][33], more efficient enforcement of regulations [3][7][10][11][17], Improved health and safety measures [7][21], Cost reduction [5][14][18], New revenue streams [5][18]	Costs[13][19][27][32][43], interoperability and integration [6][13][19][36][40][42], Acceptance of IoT [13][16][25][27][38][42]–[44], Trust related issues [25][42][44]
Operational	Improved efficiency of services [7][11][14][18][20][21][33][41], Improved effectiveness of services[7][11][14][18][20][21][33][41], Improved flexibility of services [7][11][14][18][20][21][33][41] Real-time monitoring [14][15][20][21][33][41]	Lack of sufficient knowledge [38][43], IT infrastructure limitations [13][22][25][29][31][36][42]–[44], Data management issues[6][16][27][36][44] Incorrect data [22][36][40]

The literature emphasized the benefits of IoT and fewer risks were found. The benefits in the literature were often assumed benefits and whether or not they were actually accomplished was not clear.

CONCLUSION

The IoT makes it possible to access remote sensor data and to monitor and control the physical world from a distance. Furthermore, combining and analyzing captured data also allows organizations to develop and improve services which cannot be provided by isolated systems. Although there has been limited research in the field of e-commerce about IoT, our review shows the main focus has been anecdotal and till now has focused on the benefits. The research shows that benefits range from the political to the operational level. Specifically benefits for e-commerce can be attributed to improved efficiency, effectiveness and flexibility of services; reduction of costs; improved citizen empowerment; improved government transparency; more efficient enforcement of regulations; improved planning and forecasting; and improved health and safety measures. The IoT makes it possible to access remote sensor data and to monitor and control the physical world from a distance. There are the future consequences that can go beyond the accomplishment of the intended benefits. Specifically impediments can be attributed to data privacy issues, data security issues, weak or uncoordinated data policies, weak or uncoordinated data governance, and conflicting market forces, costs, interoperability and integration issues, acceptance of IoT, and trust related issues, a lack of sufficient knowledge regarding IoT, IT infrastructural limitations, and data management issues. It is clear that IoT will have a major impact on e-commerce services in the future and will bring a variety of benefits for e-commerce at all levels, but these needs to be carefully balanced with the risks and appropriate mitigation measures taken.

Many of the issues are interrelated; interoperability and integration issues have a direct impact on costs and on trust in the systems, and many issues can be resolved with sufficient knowledge and capabilities within the organization and the issues do need to be resolved in concert. It is important that organizations address dominant impediments, such as privacy and security issues, within policy and legal frameworks during the implementation of IoT. Similarly, technical and knowledge issues are very much interrelated with a lack of standards and impediments regarding interoperability and integration of data. Organizations should keep this dual perspective in mind when using and designing IoT applications.

ACKNOWLEDGEMENTS

We acknowledge and thank the people of the Rijkswaterstaat who gave of their time and expertise during the case study research. This research is funded by Rijkswaterstaat.

REFERENCES

[1] Ackoff, R.L. (1971) 'Towards a system of systems concepts', *Management Science*, Vol. 17, No. 11, pp. 661–671.

[2] Allen, J.P. (2003) 'The evolution of new mobile applications: A sociotechnical perspective', *International Journal of Electronic Commerce*, Vol. 8, No. 1, pp. 23–36.

[3] Atzori, L., Iera, A. & Morabito, G. (2010) 'The internet of things: A survey', *Computer networks*, Vol. 54, No. 15, pp. 2787–2805.

[4] Audretsch, D.B. & Feldman, M.P. (1996) 'Innovative clusters and the industry life cycle', *Review of industrial organization*, Vol. 11, No. 2, pp. 253–273.

[5] Bi, Z., Da Xu, L. & Wang, C. (2014) 'Internet of things for enterprise systems of modern manufacturing', *Industrial Informatics, IEEE Transactions on*, Vol. 10, No. 2, pp. 1537–1546.

[6] Blackstock, M. & Lea, R. (2012) 'IoT mashups with the WoTKit', *2012 3rd International Conference on the Internet of Things (IOT)*, pp. 159–166.

[7] Boulos, M.N.K. & Al-Shorbaji, N.M. (2014) 'On the internet of things, smart cities and the WHO healthy cities', *International journal of health geographics*, Vol. 13, No. 1, pp. 10.

[8] Brous, P. & Janssen, M. (2015) 'Advancing e-government using the internet of things: A systematic review of benefits', in Tambouris, E. Janssen, M. Scholl, H.J. Wimmer, M.A. Tarabanis, K. Gascó, M. Klievink, B. Lindgren, I. & Parycek, P. (eds.), *Electronic Government*, Springer International Publishing, Thessaloniki, pp. 156–169.

[9] Castro, D. (2008) 'Digital quality of life: Government', Social Science Research Network, Rochester, NY.

[10] Chen, X.-Y. & Jin, Z.-G. (2012) 'Research on key technology and applications for internet of things', *Physics Procedia*, Vol. 33, pp. 561–566.

[11] Chui, M., Löffler, M. & Roberts, R. (2010) 'The internet of things', *McKinsey Quarterly*, Vol. 2, No. 2010, pp. 1–9.

[12] Coetzee, L. & Eksteen, J. (2011) 'The internet of things - promise for the future? An introduction', *IST-Africa Conference Proceedings, 2011*, pp. 1–9.

[13] Fan, P.F., Wang, L.L., Zhang, S.Y. & Lin, T.T. (2014) 'The research on the internet of things industry chain for barriers and solutions', Vol. 441, pp. 1030–1035.

[14] Fleisch, E. (2010) 'What is the internet of things? An economic perspective', *Economics, Management, and Financial Markets*, No. 2, pp. 125–157.

[15] Fleisch, E., Sarma, S. & Subirana, B. (2006) 'High-resolution management', *IESE Alumni Magazine*, pp. 8–13.

[16] Gilman, H. & Nordtvedt, J.-E. (2014) 'Intelligent energy: The past, the present, and the future', *SPE Economics and Management*, Vol. 6, No. 4, pp. 185–190.

[17] Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013) 'Internet of things (IoT): A vision, architectural elements, and future directions', *Future Generation Computer Systems*, Vol. 29, No. 7, pp. 1645–1660.

[18] Haller, S., Karnouskos, S. & Schroth, C. (2009) 'The internet oftThings in an enterprise context', in Domingue, J. Fensel, D. & Traverso, P. (eds.), *Future Internet – FIS 2008*, Springer Berlin Heidelberg, pp. 14–28.

[19] Harris, I., Wang, Y. & Wang, H. (2015) 'ICT in multimodal transport and technological trends: Unleashing potential for the future', *International Journal of Production Economics*, Vol. 159, pp. 88–103.

[20] Harrison, M. (2011) 'The 'Internet of Things' and commerce', *XRDS: Crossroads, The ACM Magazine for Students*, Vol. 17, No. 3, pp. 19–22.

[21] Hounsell, N.B., Shrestha, B.P., Piao, J. & McDonald, M. (2009) 'Review of urban traffic management and the impacts of new vehicle technologies', *IET Intelligent Transport Systems*, Vol. 3, No. 4, pp. 419–428.

[22] Hummen, R., Henze, M., Catrein, D. & Wehrle, K. (2012) 'A cloud design for user-controlled storage and processing of sensor data', pp. 233–240.

[23] Ivanov, D. (2010) 'An adaptive framework for aligning (re)planning decisions on supply chain strategy, design, tactics, and operations', *International Journal of Production Research*, Vol. 48, No. 13, pp. 3999–4017.

[24] Kalakota, R. & Whinston, A.B. (1997) *Electronic Commerce: A Manager's Guide*, Addison-Wesley Professional, NY.

[25] Kranenburg, R.V., Stembert, N., Victoria Moreno, M., Skarmeta, A.F., Lopez, C., Elicegui, I. & S´anchez, L. (2014) *Co-Creation as the Key to a Public, Thriving, Inclusive and Meaningful EU IoT*.

[26] Misuraca, G. (2009) 'Futuring e-government: governance and policy implications for designing an ICT-enabled knowledge society', *Proceedings of the 3rd International Conference on Theory and Practice of Electronic Governance*, ACM, New York, NY, USA, pp. 83–90.

[27] Nam, T. & Pardo, T.A. (2014) 'The changing face of a city government: A case study of Philly311', *Government Information Quarterly*, Vol. 31, Supplement 1, pp. S1–S9.

[28] Orlikowski, W.J. (1992) 'The duality of technology: Rethinking the concept of technology in organizations', *Organization science*, Vol. 3, No. 3, pp. 398–427.

[29] Ortiz, P., Lazaro, O., Uriarte, M. & Carnerero, M. (2013) 'Enhanced multi-domain access control for secure mobile collaboration through Linked Data cloud in manufacturing', *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, pp. 1–9.

[30] Pedro M. Reyes & Patrick Jaska. (2007) 'Is RFID right for your organization or application?', *Management Research News*, Vol. 30, No. 8, pp. 570–580.

[31] Prasad, K.H., Faruquie, T.A., Joshi, S., Chaturvedi, S., Subramaniam, L.V. & Mohania, M. (2011) 'Data cleansing techniques for large enterprise datasets', IEEE, San Jose, USA, pp. 135–144.
[32] Qiao, H. & Wang, G. (2012) 'An analysis of the evolution in Internet of Things industry based on industry life cycle theory', in Chen, R. Sun, D. & Sung, W.P. (eds.), *Frontiers of advanced materials and engineering technology, Pts 1-3*, pp. 785–789.
[33] Ramos, C., Augusto, J.C. & Shapiro, D. (2008) 'Ambient intelligence-the next step for artificial intelligence', *IEEE Intelligent Systems*, Vol. 23, No. 2, pp. 15–18.
[34] Reyes, P.M., Li, S. & Visich, J.K. (2012) 'Accessing antecedents and outcomes of RFID implementation in health care', *International Journal of Production Economics*, Vol. 136, No. 1, pp. 137–150.
[35] Roman, R., Najera, P. & Lopez, J. (2011) 'Securing the internet of things', *Computer*, Vol. 44, No. 9, pp. 51–58.
[36] Scarfo, A. (2014) 'Internet of Things, the Smart X enabler', *2014 International Conference on Intelligent Networking and Collaborative Systems (INCoS)*, pp. 569–574.
[37] Skarmeta, A.F., Hernandez-Ramos, J.L. & Moreno, M.V. (2014) 'A decentralized approach for security and privacy challenges in the internet of things', *2014 IEEE World Forum on Internet of Things (WF-IoT)*, pp. 67–72.
[38] Speed, C. & Shingleton, D. (2012) 'An Internet of cars: Connecting the flow of things to people, artefacts, environments and businesses', pp. 11–12.
[39] Spiess, P. & Karnouskos, S. (2007) 'Maximizing the business value of networked embedded systems through process- level integration into enterprise software', pp. 536–541.
[40] Stephan, E.G., Elsethagen, T.O., Wynne, A.S., Sivaraman, C., Macduff, M.C., Berg, L.K. & Shaw, W.J. (2013) 'A linked fusion of things, services, and data to support a collaborative data management facility', *2013 9th International Conference Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom)*, pp. 579–584.
[41] Vesyropoulos, N. & Georgiadis, C.K. (2013) 'Web of things: Understanding the growing opportunities for business transactions', *Proceedings of the 6th Balkan Conference in Informatics*, ACM, New York, USA, pp. 267–274.
[42] Wiechert, T.J.P., Thiesse, F., Michahelles, F., Schmitt, P. & Fleisch, E. (2007) 'Connecting mobile phones to the internet of things: A discussion of compatibility issues between EPC and NFC', pp. 4436–4446.
[43] Yazici, H.J. (2014) 'An exploratory analysis of hospital perspectives on real time information requirements and perceived benefits of RFID technology for future adoption', *International Journal of Information Management*, Vol. 34, No. 5, pp. 603–621.
[44] Zeng, D., Guo, S. & Cheng, Z. (2011) 'The web of things: A survey', *Journal of Communications*, Vol. 6, No. 6, pp. 424–438.