JOURNAL OF MANAGEMENT AND ACCOUNTING STUDIES 2020(03)

Available online at http://journals.researchub.org

The impacts of Internet of Things (IOT) in Supply Chain Management

***Mohsen Gerami*[1*], *Samin Sarihi*[2]**

[1]*Faculty member of ICT Faculty-Tehran-Iran-Corresponding Author*

[2]*Islamic Azad University, Science and Research Branch- Tehran*

ARTICLE INFO

Article history:

Received 18 Jan 2020
Received in revised form 13 May 2020
Accepted 14 July 2020

Keywords:

Internet of things (IOT),
Supply chain management (SCM),
Smart SCM,
IOT challenges

ABSTRACT

The Internet of Things, a technologist who, in the future, will leave the human society, industry, services, and in general, the livelihood of human beings undergoing fundamental changes. One of these changes, which will have a significant impact on other parts, is supply chain management. With regard to what will discuss in this paper, the Internet of Things will increase productivity and efficiency by increasing speed and precision in decision making, reducing risk and increasing productivity and efficiency. In the future, due to the increase in the speed of life and the breadth of the Internet, the supply chain is also required to use the Internet of Things to meet the needs of the community. However, thanks to all the benefits that IOT has given us, we cannot ignore the challenges of implementing this technology. The most important of these challenges is information security. Given that the Internet of Things acts by collecting data from the environment (this information may include personal information of individuals). With these interpretations, the security of this volume of information in a way that does not reduce speed and efficiency is a serious and critical issue.

1. Introduction

Interne of Things (IOT) is a concept that aims to enhance the forms of communication that we have today. Currently, the Internet is a network tool that humans access using devices. IOT attempts to not only have humans communicating through the Internet but also have objects or devices. These things are to be able to exchange information by themselves over the Internet, and new forms of Internet communication would be formed: human-things and things-things (Tan & Koo, 2014). Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications. This is achieved by seamless large scale sensing, data analytics and information representation using cutting edge ubiquitous sensing and cloud computing (Gubbi et al., 2013).

SCM consists of the integration activities taking place among a network of facilities that procure raw material, transform them into intermediate goods and then final products, & deliver products to customers through a distribution system (Lee Hau & Billington, 1995). Information technology (IT) has been, and continues to be, an essential enabler for effective supply chain management (SCM) (Ross, 2016).

IOT takes supply chain communications to another level: the possibility of human to things communication and autonomous coordination among 'things' while being stored in a facility or being transported between different supply chain entities. These new capabilities offer tremendous opportunities to deal more effectively with SCM challenges. IOT provides new levels of supply chain visibility, agility and adaptability to cope with various SCM challenges (Ellis et al., 2015).

For this purpose, physical are equipped with specific technologies, so called automatic identification and data capture (AIDC) technologies, such as radio frequency identification (RFID) tags, telematics modules or sensor tags. Thus, such products gain intelligent characteristics, including identification, localization, communication, sensing or logical functions that enable innovative IOT services for supply chain management (SCM) (Atzori et al., 2010).

In this article, we will talk about the Internet of Things. We will then look into the security of this technology. We will continue to emphasize the importance of using the Internet of Things in Supply Chain Management and will tell how the Internet of Things will change the management of supply chain. Ultimately, we will examine the challenges of this technology.

1.1. About IOT

Kevin Ashton is accredited for using the term "Internet of Things" for the first time during a presentation in 1999 on supply-chain management (Ashton, 2009).

**Corresponding author:* Mohsen.Gerami@gmail.com
DOI: https://doi.org/10.24200/jmas.vol8iss03pp31-37

IOT tries to establish advanced connectivity among the devices or systems or services in order to make automation. All things are connected to gather and all information would be interacted to each other over standard and different protocol domain and applications (Giusto et al., 2010).

The IOT will connect the physical and digital worlds allowing the bidirectional communication between them (Lee, 2016).

A thing, in the Internet of Things, can be a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile that has built-in sensors to alert the driver when tire pressure is low — or any other natural or man-made object that can be assigned an IP address and provided with the ability to transfer data over a network (Udaya, 2014).

Many definitions for IOT have been presented, including the definition (Gubbi et al., 2013) that focuses mostly on connectivity and sensory requirements for entities involved in typical IOT environments. Whereas those definitions reflect IOT's basic requirements, new IOT definitions give more value to the need for ubiquitous and autonomous networks of objects where identification and service integration have an important and inevitable role (L.R., 2013).

Day by day more physical objects are equipped with emerging technologies that enable them to get, send, and receive information via fixed-wire or wireless communications connected to the Internet. The McKinsey Global Institute defines IOT devices as "those can monitor their environment, report their status, receive instructions, and even take action based on the information they receive" (McKinsey Global Institute, 2013).

Industrial IOT (IIOT) is another form of IOT applications favored by big high-tech companies. The fact that machines can perform specific tasks such as data acquisition and communication more accurately than humans has boosted IIOT's adoption. Machine to machine (M2M) communication, Big Data analysis, and machine learning techniques are major building blocks when it comes to the definition of IIOT. These data enable companies to detect and resolve problems faster, thus resulting in overall money and time savings. For instance, in a manufacturing company, IIOT can be used to efficiently track and manage the supply chain, perform quality control and assurance, and lower the total energy consumption (Vilajosana et al., 2015).

IOT covers a wide range of applications like healthcare, utilities, transport, agriculture etc (Sundmaeker et al., 2010). Although the definition of things has changed as technology evolved, the main goal of making computer sense information without the aid of human interference remains the same. A drastic development of the current Internet into a network of connected objects that not only gather information from the environment(sensing) and interacts with the physical world (command /control), but also uses existing Internet standards to provide services for information transfer, analytics, applications and communications (Buckley, 2006).

Another characteristic of IOT, which is highlighted in recent definitions, is "smartness." This distinguishes IOT from similar concepts such as sensor networks, and it can be further categorized into "object smartness" and "network smartness." (Da et al., 2014).

Another essential role of IOT is to build a collaborative system that is capable of effectively responding to an event captured via sensors, by effective discovery of crowds and also successful communication of information across discovered crowds of different domains (Dastjerdi & Sharifi, 2015).

IOT is also recognized by the impact on quality of life and businesses ,which can revolutionize the way our medical systems and businesses operate by: (1) expanding the communication channel between objects by providing a more integrated communication environment in which different sensor data such as location, heartbeat, etc. can be measured and shared more easily. (2) Facilitating the automation and control process, whereby administrators can manage each object's status via remote consoles; and (3) saving in the overall cost of implementation, deployment, and maintenance, by providing detailed measurements and the ability to check the status of devices remotely (L.R., 2013).

As adoption of IOT continues to grow, attackers and malicious users are shifting their target from servers to end devices. There are several reasons for this. First, in terms of physical accessibility, smart devices and sensors are far less protected than servers, and having physical access to a device gives the attackers an advantage to penetrate with less hassle. Second, the number of devices that can be compromised are far more than the number of servers. Moreover, since devices are closer to the users, security leads to leaking of valuable information and has catastrophic consequences. Finally, due to heterogeneity and the distributed nature of IOT, the patching process is more consuming, thus opening the door for attackers (Atzori et al., 2010; Babar et al., 2010).

1.2. IOT privacy and security

As devices become more connected thanks to the IOT, security and privacy have become the primary concern among consumers and businesses. In fact, the protection of sensitive data ranked as the top concern (at 36% of those polled) among enterprises, according to the 2016 Vormetric Data Threat Report. Cyber attacks are also a growing threat as more connected devices pop up around the globe. Hackers could penetrate connected cars, critical infrastructure, and even people's homes. As a result, several tech companies are focusing on cyber security in order to secure the privacy and safety of all this data (Meola, 2016).

The very rapid growth of Internet-connected devices, ranging from very simple sensors to highly complex cloud servers, shapes the *Internet of Things***,** where *Things,* in this context, refers to a wide variety of objects (e.g. smart bulbs, smart locks, IP cameras, thermostats, electronic appliances, alarm clocks, vending machines, and more). The resemblance between all IOT objects is the ability to connect to the Internet and exchange data. The network connectivity feature allows controlling objects remotely across the existing network infrastructure, resulting in more integration with the real world and less human intervention. The IOT transforms these objects from being classical to smart by exploiting its underlying technologies such as pervasive computing, communication capabilities, Internet protocols, and applications. Protocols are required in order to identify the spoken language of the IOT devices in terms of the format of exchanged messages, and select the correct bound- aries that comply with the various functionality of each device. Applications determine levels of granularity and specialty of the IOT device and how big are the data generated for analytics purposes. They also indicate the general scope of the IOT framework covering the context of the applied domain (Ammar, 2018).

Because of the massive amount of information that IOT and wearable technologies can gather, privacy and security-related concerns will grow as these devices and services proliferate (Thibodeau, 2014). Users enjoy the personalization and customization that IOT and wearable technologies offer, yet those same capabilities that are so hotly demanded also exacerbate digital privacy and data security risks that already existed for traditional online services and technologies (Singh & \ Powles, 2014).

These privacy- and security-related concerns can arise with regard to access to the device itself (i.e., what happens if it is lost or stolen); access to the information the device shares with nearby devices or systems (i.e., information shared over Wi-Fi or other wireless systems); or access to information transmitted to the cloud or to any remote storage system (Al Sacco, 2014).

This section will specifically explore how IOT technologies in general and wearables in particular challenge traditional privacy norms—both social and legal—and will explain why a more creative and flexible approach to dealing with these issues will be necessary. It is important that the privacy concerns regarding wearable technologies relate to both the users of those technologies and others in surrounding environments. For users, the privacy concern is that wearables allow a massive amount of data to be observed, gathered, and shared about them—potentially without their knowledge (ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 8/2014 ON THE ONRECENT DEVELOPMENTS ON THE INTERNET OF THINGS 4, 2014).

In turn, these new datasets might be used by third parties for marketing purposes, by employers for job-related purposes, or even by insurers to adjust user premiums. This possibility raises the specter of IOT and wearable devices and the datasets they generate being used in a supposedly discriminatory fashion (Thierer, 2015).

The potential for such ubiquity (billions to trillions of devices) of IOT seems like a foregone conclusion at this point. But there are multi-dimensional privacy challenges which must be surmounted if this truly is going to become a reality. To get ahead of these challenges the privacy engineering community (via National Institute of Standards and Technology) is currently involved in intense discussions as to how to "engineer in" the right privacy regime, which will provide users (consumers) with direct control over a wide range of their own personal privacy settings as well as creating auditing and measuring schemes to ensure compliance with both user settings as well as regulatory mandates. Privacy engineering is a very real challenge, and there are multiple paths in the IOT where a privacy regime must be monitored and maintained:

- The device (data generator, data receiver and aggregation point).
- The Internet (multi-directional data transport).
- The cloud (data manipulation and aggregation point).
- The machine (application services, big data repositories, analytics and more).

Each path requires appropriate privacy protections to be engineered into it, with user control wherever appropriate (device, machine and others) while being maintained along its entire length (virtual and physical). High levels of encryption, redundancy and security will be necessitated to counter threats in flight as well as at the endpoints. There will also be regulatory controls and adherence monitoring, which must be facilitated along these same pathways. Most of these will fall under the auspices of FTC (US), Data Privacy Act (EU), and other regulatory bodies and statutes across the world. In parallel with the need for comprehensive privacy, security and compliance capabilities, the IOT is entirely predicated on new business models, which disrupt conventional solutions. An enabler of this disruption is the cost model component, which dictates low inherent costs in the devices, and all other components of the value chain. These cost models will not be conducive to "out of band" controls via bolt on solutions. Engineering-in privacy as part of the device and other pathway structures will be the only path to success in which cost efficiencies are maintained while compliance is assured along the way (Taj Dini & Sokolov, 2017).

1.3. Why to Use IOT in SCM?

When someone mentions the Internet of Things (IOT), most people think of electronics or wearables – the types of technologies that are driving adoption of a highly personalized "smart" consumer lifestyle. But there's much more to the IOT story, and more specifically, its impact on the supply chain.

Research firm Gartner recently released a write-up highlighting what many supply chain professionals have been weighing for some time: the IOT trend is going to impact businesses, and in particular, it will disrupt the way we think about logistics. In the piece, Gartner says a thirty-fold increase in Internet-connected physical devices by the year 2020 will "significantly alter how the supply chain operates." Specifically, it notes the impact will relate to how supply chain leaders access information, among other things.

ERP and supply chain management (SCM) have gone hand-in-hand for quite some time, but the IOT revolution will allow us to enhance those solutions by intelligently connecting people, processes, data, and things via devices and sensors. Think of it as SCM 2.0. This deeper intelligence can come to life in many different ways when it comes to supply chain data and intelligence – from automation of the manufacturing process to improved visibility within the warehouse (Udaya, 2014).

Supply chains are operating under an ever-changing environment and are vulnerable to a myriad of risks at all levels. This environment is an ever-changing landscape because of many factors. Many supply chains extend over wide geographical areas and are vulnerable to many global risks (Butner, 2010). Customers are more and more demanding in terms of product customisation, price and level of service (Christopher, 2016). Products complexity is also increasing due to the high clock speed in many industries following the rapid changes in technology and the continuous introduction of new products to the market (Simchi-Levi et al., 2003). Furthermore, the external environment is highly dynamic due to economic (energy cost, prices and availability of raw materials, currency exchange rates), social (unrest, demanding customers) and natural factors (extreme weather conditions, earthquakes, tsunamis). In order to survive in such a complex environment, companies need to be extremely agile and build a high level of resilience and risk mitigation capabilities and structural flexibility that allow rapid response to these challenges. Christopher and Holweg define structural flexibility as the ability of the supply chain to adapt to fundamental changes in the business environment. However, flexibility and resilience come at an additional cost in the form of additional resources such as buffer inventory and extra capacity, and higher coordination cost (Christopher & Holweg. 2011). In order to balance the required level of resilience and flexibility and the cost of achieving it, firms need to have high visibility of the whole supply chain, the necessary velocity to respond quickly to changes and effective collaboration with suppliers and customers. Christopher summarised the principles that can guide supply chain managers into what he calls the '4Rs': responsiveness, reliability, resilience and relationships (Christopher, 2016).

The data emitted from smart objects, when effectively collected, analysed and turned into useful information, can offer unprecedented visibility into all aspects of the supply chain, providing early warnings of internal and external situations that require remediation. Responding to these signals in time can

drive new levels of supply chain efficiency. What was lacking so far is not the availability of information but rather the technologies for collecting and processing big data and the lag between data collection and action. IOT will allow the reduction in the time between data capture and decision-making that enables supply chains to react to changes in real time allowing levels of agility and responsiveness never experienced before (Ellis et al., 2015).

"The internet of things leads to a high transparency regarding the status of the supply chain and its nodes" (Akinlar, 2014).

Another perspective related with the supply chain "end-to-end" integration is the utilization of IOT for designing new services. "The Internet of Thinks envisions a multitude of heterogeneous objects and interactions with the physical environment."…"The vision of IOT relies on the provisioning of real-world services" (De wt al., 2011). IOT supports the integration of several technologies by "the result of synergic activities conducted different fields of knowledge, such as telecommunications, informatics, electronics, and social science" (Atzori et al., 2010).

Adner addresses innovations in ecosystems and emphasizes cooperations between firms in order to create valuable products. Because cooperation always entails risks, Adner proposes a management framework that is designed to assess these risks and to adjust a firm's innovation strategy accordingly (Adner, 2006). Moreover, Kapoor and Lee investigate the relationship between organizations and new technology investments in business ecosystems. Kapoor and Lee find that alliances, which facilitate coordination and cooperation, encourage investment in new and complementary technologies (Kapoor & Lee, 2013).

1.4. How IOT make SCM more efficient?

Information technology enables effective supply chain quality management; due to information sharing is crucial for timely quality management and control. The several cutting edge technologies which can be integrated as part of a supply chain quality monitoring system are (Kapoor & Lee, 2013): Service-oriented architecture, RFID, Agents, Workflow management, cross organizational integration.

The RFID, the technology associated with Internet of Things, can help improve the effectiveness of information flow in a supply chain. Partners in the supply chain will be able to access information and practice quality control based on the data shared through RFID and other technologies. This technology enables enterprises facilitating real-time traceability. This technology combined with Internet of Things enable integrating work processes better (Kapoor & Lee, 2013).

Lee (2016) selects three basic components that make a device able to get information from its environment, "think" and communicate: sensors, connectivity, and processors.

Lee (2016) also lists nine areas where IOT and SCM are currently coexisting successfully and provides examples: 1) transparency and visibility of the supply chain; 2) proactive replenishment; 3) predictive maintenance; 4) reduction in asset loss; 5) manufacturing flow management; 6) product development and commercialization; 7) risk management; 8) operational efficiency; and 9) improved fleet management. Being the top conclusion the improvement of transparency and visibility: "The transparency and end-to-end visibility afforded by IOT creates new opportunities that supply chain professionals can leverage in order to optimize supply chains and generate value" (Lee, 2016).

IOT promises an interconnected network of uniquely identifiable smart objects. This infrastructure creates the necessary backbone for many interesting applications that require seamless connectivity and addressability between their components. The range of IOT application domain is wide and encapsulates applications from home automation to more sophisticated environments, such as smart cities and e-government.

Industry-focused applications include logistics and transportation (Yuqiang et al., 2010), supply-chain management (Chaves & Decker, 2010), fleet management, aviation industry, and enterprise automation systems. Healthcare systems, smart cities and buildings, social IOT, and smart shopping are a few examples of applications that try to improve the daily life of individuals, as well as the whole society. Disaster management, environmental monitoring, smart watering, and optimizing energy consumption through smart grids and smart metering are examples of applications that focus on environment.

Monitoring devices via APIs can be helpful in multiple domains. The APIs can report power usage, equipment performance, and sensor status, and they can perform actions upon sending predefined commands. Real-time applications can utilize these features to report current system status, whereas managers and developers have the option to freely call these APIs without the need for physically accessing the devices. Smart metering, and in a more distributed form, smart grids, can help in identifying production or performance defects via application of anomaly detection on the collected data, and thus increase the productivity (Moreno et al., 2014).

When talking about billions of connected devices, methods for identifying objects and setting their access level play an important role in the whole ecosystem. Consumers, data sources, and service providers are essential parts of IOT; identity management and authentication methods applied to securely connect these entities affect both the amount of time required to establish trust and the degree of confidence (Perera et al., 2014).

Devices or objects in IOT have to be uniquely identified. There are various mechanisms, such as ucode, which generate 128-bit codes and can be used in active and passive RFID tags, and also Electric Product Code (EPC), which creates unique identifiers using Uniform Resource Identifier (URI) codes (Mainetti et al., 2011; Zorzi et al., 2010).

1.5. Challenges

Corporate finance professionals might agree when it comes to the Internet of Things (IOT). While this much-vaunted technological trend promises new operational efficiencies and revenue opportunities, IOT also poses significant transitional challenges across legacy supply chain management, data systems and departments within many organizations. Managing those challenges poorly could lead to losses or lower returns (Karen Lynch).

The promise of IOT in international supply chain management is high, in terms of both productivity and innovation, but it will be challenging for most companies to transition legacy supply chains to incorporate hundreds or even thousands of IOT devices and the data they deliver (Karen Lynch).

The study made by the companies PwC and Strategy& in 2015 in the German sector of manufacturing and engineering, automotive and process industries, is based on surveys of 235 German companies. The respondents expected that regarding to the digital transition will lead to a significant transformation of

their companies and they estimate that the share of investment will account for more than 50% of the planned capital investments for the next 5 years. Therefore, the first and the main challenge is the investment that means to apply Industry 4.0 solutions (Wegener, 2015).

Thus, the main challenges are the high investment levels and often the unclear business cases for the new industrial internet applications. As well as to have the sufficient skills to meet the needs of digital world. Moreover, binding standards must also be defined and tasks in the field of IT security have to be solved. It is clearly needed that companies, trade unions, associations and policy-makers cooperate in order to spread this fourth industrial revolution (Laura Domingo Galindo, 2016).

There is another challenge in the insufficient qualification of employees regarding the digital change, this will alter requirements for employees across all the steps of the value chain. Through the IOT and the growing digitalization, the need for employees with a foundation in data science and information technology in particular will increase. Policymakers should create the basis for the education needed. They need to encourage enthusiasm for technology from the early stage (Laura Domingo Galindo, 2016).

IOT offers unprecedented visibility into all aspects of the supply chain, providing early warnings of internal and external situations that require remediation.Therefore, IOT enables firms to respond quickly to changes through effective internal operations and collaboration with suppliers and customers. Current solutions and applications are still short of unlocking this potential. We only have piecemeal applications in isolated areas with limited work that addresses the entire supply chain (Ben-Daya et al., 2017).

The roots of IOT in logistics are not new. Using technology for the tracking of objects has been around for decades through various forms of information and communication technologies. Therefore, improvements brought by IOT to the logistics function can be viewed as a continuation to previous developments. The basic logistics functions are to transport 'the right goods in the right quantity and right quality at the right time to the right place for the right price' (Decker et al., 2008).

There are several gaps in the current literature dealing with IOT applications in SCM. These gaps can be summarized as follows (Ben-Daya et al., 2017):

• Lack of solid frameworks that provide guidance of IOT adoption in a supply chain context with clear guidelines and a roadmap. These would help in advising companies as to which process and where in the supply chain would they deploy IOT, given that supply chain partners may be at different stages of the IOT implementation. In addition, these frameworks would provide help with change management practices within the company and across the supply chain (Ben-Daya et al., 2017).

• Lack of models that address supply chain problems in an IOT environment. Management of smart supply chains is different from that of traditional supply chains. Decision-making in an IOT context requires new tools and models that take into account this new environment, such as the abundance of big data generated from sensors and connected things. IOT will affect procurement, production planning, the management of inventory, quality and maintenance, among other issues (Ben-Daya et al., 2017).

• There are several barriers to the implementation of IOT in SCM from both technological and managerial perspectives. A world where all things are connected opens the door for less security and privacy (Tadejko, 2015). This is especially true in a supply chain context where information sharing has always been a big challenge. Another challenge is interoperability. Research by McKinsey suggests that 40% of the value of the IOT will need to be unlocked via interoperability (Manyika et al., 2015). There is not much research addressing how to deal effectively with these challenges.

2. Conclusion

In this article, we first described the concept of the Internet of Things and briefly explained how this technology works. We outlined the basic requirements and requirements of this technology and then examined the effects and changes that this technology has made in the industry, treatment, services, and so on.

More precisely, supply chain management is one of the things that can dramatically change under the influence of Internet technology. In this regard, we specifically looked at the effects of the Internet of Things on Ethereal and the supply chain performance, and we saw that, the Internet of Things will change in which of the main components of supply chain management will evolve and how this transformation will improve the performance of the supply chain. After reviewing these factors, we looked at why we needed to use the Internet to manage supply chains, and we looked at each of these requirements. Like any other new technology, the Internet of Things faces various challenges. In the final section of this paper, we briefly described the challenge, and examined the core challenge of this technology, namely, information security.

Considering what was discussed in this article In the future, we will have to implement the Internet of Things in supply chain management. But we should keep in mind that information security is still our biggest challenge in this regard. That's a challenge to overcome the disaster that needs to be done and more effort is being made to secure information and cloud computing.

REFERENCES

J. Tan, S.G.M. Koo, A survey of technologies in internet of things, in: IEEE Computer Society, 2014: pp. 269–274. doi:10.1109/DCOSS.2014.45.

Gubbi, J., R. Buyya, S. Marusic, and M. Palaniswami. 2013. "Internet of Things (IOT): A Vision, A rchitectural Elements, and Future Directions." Future Generation Computer Systems 29 (7): 1645–1660.

Lee Hau L., and Corey Billington, "The Evolution of Supply-Chain-Management Models and Practice at Hewlett-Packard. Interfaces", (25), pp. 42-63, 5 September-October, 1995

Ross, D. F. 2016. Introduction to Supply Chain Management Technologies. Boca Raton, FL: St Lucie Press.

Ellis, S., H. D. Morris, and J. Santagate. 2015. "IOT-Enabled Analytic Applications Revolutionize Supply Chain Planning and Execution." International Data Corporation (IDC) White Paper. www.idc.com.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805.

Ashton K. That 'internet of things' thing. RFiD J 2009;22(7):97–114.

Gubbi J, Buyya R, Marusic S, Palaniswami M. Internet of Things (IOT): a vision, architectural elements, and future directions. Future Gener Comput Syst 2013;29(7):1645–60.

L.R. LLC. An introduction to the Internet of Things (IOT). http://www.cisco.com/c/dam/en_us/solutions/ trends/IOT/introduction_to_IOT_november.pdf; 2013.

Vilajosana X, et al. OpenMote: Open-source prototyping platform for the industrial IOT. In: Ad hoc networks. Springer International Publishing; 2015. p. 211–222.

Da Xu L, He W, Li S. Internet of Things in industries: a survey. Ind Inform IEEE Trans 2014;10(4):2233–43.

Dastjerdi AV, Sharifi M, Buyya R. On application of ontology and consensus theory to human-centric IOT: an emergency management case study. In: Proceedings of the eighth IEEE international conference on Internet of Things (iThings 2015, IEEE CS Press, USA), Sydney, Australia, Dec. 11–13, 2015.

L.R. LLC. An introduction to the Internet of Things (IOT). http://www.cisco.com/c/dam/en_us/solutions/ trends/IOT/introduction_to_IOT_november.pdf; 2013.

Atzori L, Iera A, Morabito G. The internet of things: a survey. Comput Netw 2010;54(15):2787–805.

Babar S, Mahalle P, Stango A, Prasad N, Prasad R. Proposed security model and threat taxonomy for the internet of things (IOT). Recent trends in network security and applications. Springer Berlin Heidelberg; 2010. pp. 420–429.

D. Giusto, A. Iera, G. Morabito, L. Atzori (Eds.), The Internet of Things, Springer, 2010. ISBN: 978-1-4419-1673-0.

H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé, Vision and challenges for realizing the Internet of Things, Cluster of European Research Projects on the Internet of Things - CERP IOT, 2010.

J. Buckley, ed., The Internet of Things: From RFID to the Next-Generation Pervasive Networked Systems, Auerbach Publications, New York, 2006.

Butner, K. 2010. "The Smarter Supply Chain of the Future." Strategy & Leadership 38 (1): 22–31.

Christopher, M. 2016. Logistics & Supply Chain Management. Harlow: Pearson. www.pearson.com.

Simchi-Levi, D., P. Kaminsky, and E. S. Levi. 2003. Designing and Managing the Supply Chain: Concepts, Strategies, and Case Studies. New York: McGraw-Hill.

Christopher, M., and M. Holweg. 2011. "'Supply Chain 2.0': Managing Supply Chains in the Era of Turbulence." International Journal of Physical Distribution & Logistics Management 41 (1): 63–82.

Adner, R. (2006) 'Match your innovation strategy to your innovation ecosystem', Harvard Business Review, April, 98–107.

Kapoor, R., & Lee, J. M. (2013). Coordinating and competing in ecosystems: How organizational forms shape new technology investments. Strategic Management Journal, 34(3), 274–296.

Yuqiang C, Jianlan G, Xuanzi H. The research of Internet of Things supporting technologies which face the logistics industry. In: International conference on computational intelligence and security (CIS); 2010. p. 659–663.

Chaves LWF, Decker C. A survey on organic smart labels for the internet-of-things. In: Seventh international conference on networked sensing systems (INSS); 2010. p. 161–164.

Moreno M, Úbeda B, Skarmeta AF, Zamora MA. How can we tackle energy efficiency in IOT based smart buildings? Sensors 2014;14(6):9582–614.

Perera C, Zaslavsky A, Christen P, Georgakopoulos D. Context aware computing for the internet of things: a survey. Commun Surv Tutorials IEEE 2014;16(1):414–54.

Mainetti L, Patrono L, Vilei A. Evolution of wireless sensor networks towards the internet of things: a survey. In: Nineteenth international conference on software, telecommunications and computer networks (SoftCOM); 2011. p. 1–6.

Zorzi M, Gluhak A, Lange S, Bassi A. From today's intranet of things to a future internet of things: a wireless-and mobility-related view. Wirel Commun IEEE 2010;17(6):44–51.

Lee, K. (2016). How the Internet of Things will change your world. *IDEABOOK 2015*, CSCMP's Supply Chain Quartelrly and DC Velocity. Retrieved June, 16, 2016 from:
http://digital.supplychainquarterly.com/supplychain/ideabook_2016/?folio=50&sub_id=Hxh5qJH8aRP9&pg=1#pg1

McKinsey Global Institute. (2013). Disruptive technologies: Advances that will transfor life, business and the global economy. Retrived June 16, 2016, from: http://www.mckinsey.com/business-functions/business-technology/our-insights/disruptive-technologieshttp://digital.supplychainquarterly.com/supplychain/ideabook_2016/?folio=50&sub_id=Hxh5qJH8aRP9&pg=1#pg1

Akinlar, S. (2014). Logistics 4.0 and challenges for the supply chain planning and IT. *Fra unhofer IML*. R etrieved June 16, 2016, from:
http://www.iis.fraunhofer.de/content/dam/iis/tr/Session%203_5_ession%203_5_Logistics_Fraunhofer%20IML_ Akinlar.pdf

De, S., Barnaghi, P., Bauer, M., & Meissner, S. (2011, September). Service modelling for the Internet of Things. In *Computer Science and Information Systems (FedCSIS), 2011 Federated Conference on* (pp. 949-955). IEEE.

Atzori, L., Iera, A., & Morabito G. (2010).The internet of things:A survey. *Computer networks, 54*(15), 2787-2805.

Andrew Meola.(2016).what is the internet of thing(IOT)?.Retrieved Des, 19, 2016, from: http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8

Margaret Rouse.from: http://internetofthingsagenda.techtarget.com/definition/Internet-of- Things-IOT

Udaya shanker.(2014).How the Internet of Things impacts Supply Chain?. Retrived August 04, 2014, from: https://www.inboundlogistics.com/cms/article/how-the-internet-of-things-impacts-supply-chains/

Decker, C., M. Berchtold, L. W. F. Chaves, M. Beigl, D. Roehr, T. Riedel, M. Beuster, T. Herzog, and D. Herzig. 2008. "Cost-Benefit Model for Smart Items in the Supply Chain." The Internet of Things Lecture Notes in Computer Science 4952: 155–172.

Mohamed Ben-Daya, Elkafi Hassini & Zied Bahroun. (2017) "Internet of things and supply chain management": a literature review, International Journal of Production Research.

Tadejko, P. 2015. "Application of Internet of Things in Logistics–Current Challenges." Economics and Management 7 (4): 54–64.

Manyika, J., J. Woetzel, R. Dobbs, M. Chui, P. Bisson, J. Bughin, and D. Aharon. 2015. The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute.

Wegener, D. (2015). Industry 4.0 - vision and mission at the same time. *Industry 4.0-*

Opportunities and challenges of the industrial internet .

Laura Domingo Galindo. 2016. "The Challenges of Logistics 4.0 for the Supply Chain Management and the Information Technology". Master Thesis Spring 2016. Norwegian University of Science and Technology.

Karen Lynch. "Internet of Things Poses Transition Challenges for Global Supply Chain Managers".from: https://www.americanexpress.com/us/content/foreign-exchange/articles/IOT-poses-transition-challenges-on-supply-chain-management/

Mahmoud Ammar, Giovanni Russello , Bruno Crispo. " Internet of Things: A survey on the security of IOT frameworks". Journal of Information Security and Applications 38 (2018) 8–27

See Patrick Thibodeau, *The Internet of Things Could Encroach on Personal Privacy*, COMPUTERWORLD (May 3, 2014, 7:45 AM), http://www.computerworld.com/s/article/9248086/The_Internet_of_Things_could_encroach_on_personal_privacy.hhtml, *archived at* http://perma.cc/QNX5-4BXE; Jaikumar Vijayan, *The Internet of Things Likely to Drive an Upheaval for Security*,COMPUTERWORLD (May 2, 2014, 7:07 AM), http://www.computerworld.com/s/article/9248069/The_Internet_of_Things_likely_to_drive_an_upheaval_for_security.html, *archived at* http://perma.cc/C46Z-MYHX.

See Jat Singh & Julia Powles, *The Internet of Things—The Next Big Challenge to Our Privacy*, GUARDIAN (July 28, 2014), http://www.theguardian.com/technology/2014/jul/28/internet-of-things-privacy , *archived at* http://perma.cc/4MA2-TA8D ; Alexander Suarez, *Wearable Fitness Device Privacy Concerns Abound*, JDSUPRA (Sept. 11, 2014), http://www.jdsupra.com/legalnews/wearable-fitness-device-privacy-concerns-17278 , *archived at* http://perma.cc/HS7A-DV3H .

Al Sacco, *Fitness Trackers Are Changing Online Privacy—And It's Time to Pay Attention*, CIO (Aug. 14, 2014, 8:31 AM), http://www.cio.com/article/2465142/wearabletechnology/fitness-trackers-are-changing-online-privacy-and-its-time-to-payattention.html, *archived at* http://perma.cc/X7H6-7FWP .

See ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 8/2014 ON THE ONRECENT DEVELOPMENTS ON THE INTERNET OF THINGS 4 (2014), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/ files/2014/wp223_en.pdf, *archived at* http://perma.cc/ZM36-XZ7M

Adam Thierer, *The Internet of Things and Wearable Technology:Addressing Privacy and Security Concerns without Derailing Innovation*,21 RICH. J.L. & TECH. 6 (2015), http://jolt.richmond.edu/v21i2/article6.pdf.

Mahyar Taj Dini, V. Yu. Sokolov.(2017)"INTERNET OF THINGS SECURITY PROBLEMS".