Security and Trust Issues on Digital Supply Chain

Haibo ZHANG
Kyushu University
Japan
zhang.haibo@inf.kyushu-u.ac.jp

Toru NAKAMURA
Advanced Telecommunications Research Institute International
Japan
tr-nakamura@atr.jp

Kouichi SAKURAI
Kyushu University
Advanced Telecommunications Research Institute International
Japan
sakurai@inf.kyushu-u.ac.jp

***Abstract*—This exploratory investigation aims to discuss current status and challenges, especially in aspect of security and trust problems, of digital supply chain management system with applying some advanced information technologies, such as Internet of Things, cloud computing and blockchain, for improving various system performance and properties, i.e. transparency, visibility, accountability, traceability and reliability. This paper introduces the general histories and definitions, in terms of information science, of the supply chain and relevant technologies which have been applied or are potential to be applied on supply chain with purpose of lowering cost, facilitating its security and convenience. It provides a comprehensive review of current relative research work and industrial cases from several famous companies. It also illustrates requirements or performance of digital supply chain system, security management and trust issues. Finally, this paper concludes several potential or existing security issues and challenges which supply chain management is facing.**

***keywords*—digital supply chain, security management, trust issues, IoT, cloud computing, blockchain**

I. Introduction

Supply chain has a long history as a traditional supply-demand model from manufacturing raw materials to processing and producing, then selling final products to end customers. Traditional supply chain system can provide services to humans life within a relatively safe environment, however, its not much easy to satisfy ever-increasing diversified types of goods and complicated customers demands which require supply chain to high-efficiently and less-costly work within a more complex consuming information network.

By enabling technical methods to traditional supply chains daily management work for gathering, processing, analyzing, storing and sharing large amount of information in a real-time manner, information technology (IT) has become a necessary component of supply chain management system for information collaborating and performance improving [1]. Various IT techniques, i.e. internet of things (IoT) technologies for information capturing and processing; cloud computing for big data processing; blockchain for transportation visibility and data-provenance for activities and responsibility tracking, have been applied to traditional supply chain management system by many enterprises to achieve the management systems maximum-efficiency and minimum-cost.

The reminder of this paper is organized as follows: section II introduces general histories and definitions of the supply chain and related technologies which have been applied or are potential to be applied to supply chain management systems with purpose of facilitating its security and convenience; section III demonstrates requirements of digital supply chain systems, and provides a comprehensive review of current relevant research work and industrial cases from several famous companies; section IV analyzes security issues resulted by applying current information technologies, and how those information technologies could be utilized on supply chain security management; section V illustrates existing trust problems from certain third-party service provider which could give rise to damage to supply chain system's assets, and how those IT technologies could be applicable for managing the trust problem of digital supply chain; section VI discusses potential or existing security challenges to which supply chain management is facing; section VII concludes a brief discussion on the perception and future work.

II. History and Definition

A. Traditional supply chain

Traditional supply chain has long history over than 100 years. A supply chain can be regarded as a network of all individuals, organizations, resources, activities and technologies involved in the creation, delivery and sale of a product [2]. A supply chain is linked together through physical flows, which involves the production, transportation, movement, and storage of goods and materials, as well as information flows, which allows the various supply chain members to coordinate their long-term plans and control the daily flow of goods and materials up and down the supply chain [3].

B. Digital supply chain

Digital supply chain does not have an explicit starting time in its development history, that could be regarded as starting from the first application of information technology on supply chain system which might be the first network

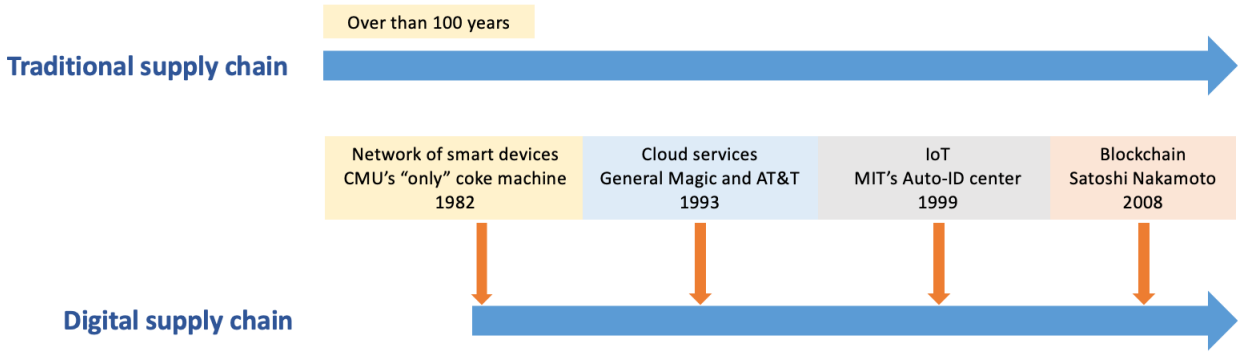

Fig. 1. Histories.

of smart devices, CMU's "Only" coke machine in 1982 [4]. Digital supply chain means applying advanced information technologies to traditional supply chain, including internet of thing, cloud computing and blockchain.

1) Internet of Things (IoT): The first idea of network of smart devices was applied on Carnegie Mellon Universitys modified Coke machine which was able to report its inventory and whether the loaded drinks were cold or not in 1982. However, the first proposal of Internet of Things was formally proposed by MITs Auto-ID Center in 1999 [4]. Benabdessalem et al. [5] defined IoT as a network of objects within which all objects were able to be identified by certain trustful mechanisms and connected, either with each other internally or to the internet externally through combining with IoTs necessary technologies like RFID, sensors, GPS chips and mobile phone to provide integrated services.

2) Cloud computing: The term cloud was firstly proposed by General Magic and ATT as platforms for distributed computing to describing their Telescript and PersonaLink technologies as early as 1993, while cloud computing became popular sine Amazons Elastic Computer Cloud released in 2006 [6]. Cloud computing refers to a super calculating model to distribute computing tasks into a remote data center with thousands of computer and servers connected to the computer cloud to assign different resources, like storage space, computing power and all kinds of software services, for various computing requirements [7].

3) Blockchain: Haber and Stornetta [8] firstly proposed the idea of cryptographically secured chain architecture for their tamper-proof time-stamp mechanism in 1990. Blockchain was formally proposed by a person or a group named Satoshi Nakamoto in 2008 as a core component of his cryptocurrency system bitcoin [9]. Blockchain refers to a decentralized architecture consists of increasing numbers of cryptographically linked blocks each of which stores the hash value of previous block [10]. Blockchain was able to protect the information among the network against any breached or vulnerable device through verifying identities and rejecting malicious parties by other members. The data stored in a block is immutable which is extremely hard to be tampered (tamperproof) which means that hackers must manipulate all blocks data until the head block to achieve cyberattacks, which is impossible in a real blockchain world.

III. Digital Supply Chain

A. Requirements of Digital Supply Chain

1) Cost control: The first important purpose of enabling IT technologies to traditional supply chain system is to lower its cost as much as possible in an economic manner. For instances, gathering and sharing information through IoT devices or cloud computing server could reduce time cost spent on communicating in circuity way including sending messages through many middle nodes and waiting for a long time, as well as money cost by improving the whole chain system performance in terms of speed of processing, transforming, decision making and plan coordinating.

2) Traceability: Traceability is a core feature an efficient supply chain management system should own for tracking products status and conditions in a real-time, especially in cold, food and agriculture chain in terms of temperature, power, storage and light. High-efficient traceability was able to allow supply chain members to make decisions and coordinate plans flexible and fast. A high-efficient traceability can also help organizations to manage their whole transportation network with lower cost.

3) Transparency: Transparency refers to the ability of determining such information as what actions and the time as well as locations cross the whole supply chain life cycle. True transparency allows auditing and inspecting of data sets in real-time refers to a level of transparency which makes activities and operations highly visible [19].

4) Accountability: For some unexpected incidents, the ability of tracing back to the responsible members or processes, by analyzing the evidence record of their activities, would be much useful for problems solving. Supply chain system can work normally with accountability whenever the incident happened.

B. Related existing work

1) IoT: One of the most necessary and important properties for digital supply chain is to achieve its high-efficiency traceability in some fields, i.e. cold chain, food supply chain, health

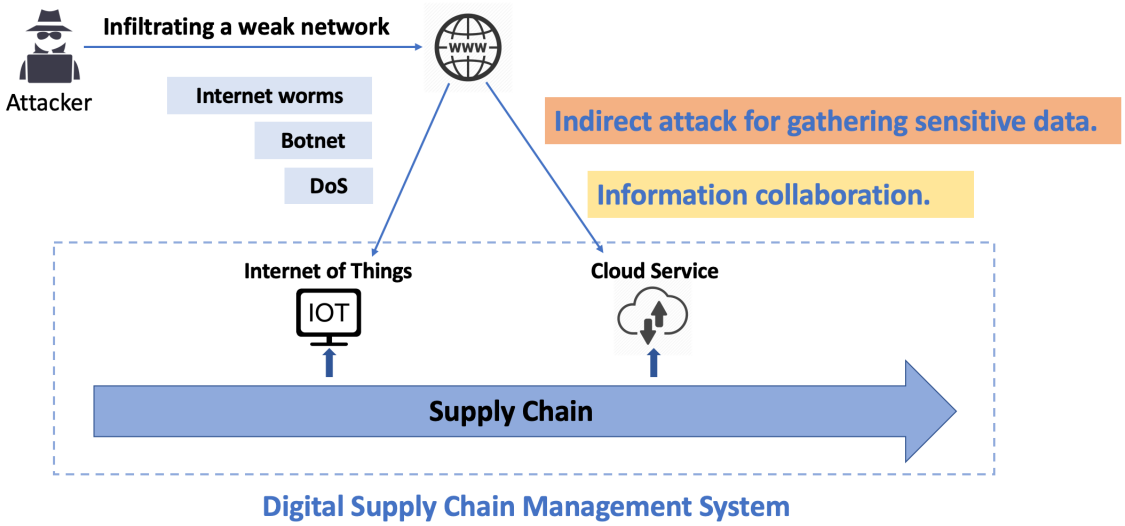

Fig. 2. Attack method on digital supply chain.

care, and pharmaceutical industries for preventing against some transportation or productions condition accidents like food poisoning which could cause some serious health effects on consumers [3]. The combination between IoT and supply chain would enhance the traceability especially in cold chain and food manufacturing. Mousavi et al. [11] proposed a practical system framework, which could trace the whole process of meat producing from the individual animal to individual prime cuts in the boning hall, with technologies such as bar code scanning and RFID. Regattieri et al. [12] provided a practical system framework for food manufacturing supply chain traceability with tracing functions, which could identify products self-information, track products status and data by utilizing traceability tools and route relevant information. Abad et al. [13] demonstrated an example of using RFID tags for tracking products status and conditions in the fresh fish cold chain in which multiple sensors were enabled to capture the real-time information in terms of temperature, humidity, power and light. The information thus collected are stored and can be further analyzed.

2) Cloud computing: Information sharing problem of supply chain management system have been an important research topic in areas of information integrity and security. Cloud computing could provide supply chain management providers an opportunity to take advantage of new processes related to ethereal space [14]. With applying cloud computing on supply chain management system, the inventory information would be updated instantly without users having to wait for central organizations or servers to populate information across a supply network [15].

Jain and Dhaka [16] researched on supply chain management in cloud computing environment and divided the history of supply chain into three parts, which were focused on administrative processes, core and rather complex processes covered in cloud. For industrial cases, Maziliauskaite [17] demonstrated companies could use cloud computing for real-time data sharing of inventory and products sales information which would allow the supply chain management providers get more integrate information and improve the ability of data analysis across whole supply chain members. Cao et al. [18] studied on a managerial perception in terms of using cloud computing technologies in supply chain management, especially on how cloud computing impacts information sharing among supply chain partners, the impact of trust in cloud information sharing and the impact of cloud computing on supply chain performance.

3) Blockchain: Blockchains architecture of distributed ledger can ensure a decentralized and transparent transaction mechanism in supply chain management system in industrial and business. Blockchain can help supply chain organizations and consumers to track products origins and whole processes during the whole transportation. Abeyratne and Monfared [19] proposed an architecture about how blockchain can manufacture supply chain system with factors of registrars, standards, certifiers, producers and consumers.

The application of blockchain in supply chain has been employed in industrial area widely by business companies. Alibaba worked with AusPost, Blackmores and PwC to explore the ability of combining blockchain with food supply chain for food fraud fighting such as selling low-quality foods. The purpose of their team is to develop a Food Trust Framework to improve the integrity and traceability on the global supply chains [20]. Walmart built a system for providing a service to monitor the pork production in the U.S. and China with blockchain enabling the digital tracking on individual pork products in a few minutes compared to many days taken in the past [20].

C. Hybrid Industrial Cases

1) IBM: IBMs Watson Supply Chain applied artificial intelligence on their supply chain system, and trained in supply

chain through machine learning, to provide comprehensive, end-to-end visibility and insights. They provide a personalized dashboard with 360-degree viewing angle for easy understanding and prioritizing critical issues in real-time. Users can use Watson to rapidly assemble the right team to collaborate and manage incidents and resolve disruptions quickly.

2) Wal-Mart: Wal-Marts integrated supply chain is the key enabler of its growth from a small retailer to a global leader. Wal-Mart has become the leading retailers because of having a powerful decision-making system that relied on data analysis through a barcode scanning system, a point-of-sale system, and real time data collection through current RFID technology. They enabled some advanced inventory technology like automated recording system for real-time data recording to the database.

3) Cisco: Cisco began to process its supply chain digitization initiative eight years ago. For the first three years, they focused on their systems and processes foundation. They upgraded their enterprise resource planning and product data management systems. Cisco also combined multiple processes and systems into a single system. They used technology such as collaboration, internet of things, mobility, big data and cloud services, to provide real-time visibility.

IV. Security Management

A. Security issues

While the enablement of information technology can provide an efficient information collaboration for supply chain networks, it also reduced or removed the protection barrier of traditional supply chain system. Traditional supply chain system was separated from external unstable cyberattacks environment due to its disconnecting with the internet. Connecting with the internet would allow various external or internal risks to enter into supply chain system resulting in unexpected problems. In this way, system flaws and vulnerabilities, especially from devices provided by third party providers like IoT devices or cloud computing server, would be exploited by network attackers to also increase supply chain risks.

Figure 2 shows some attack methods which could happen to current digital supply chain system. One way that a hacker can infiltrate a network is by manipulating the devices or hardware which is connecting that network. They can do this by intercepting a delivery from a supplier and injecting malicious code directly onto the devices. Another method is, hackers could inject malware into the software itself by breaking into a developer's infrastructure. The hacker get access to the developer's network by phishing or email-based attacks, then uses an internal vulnerability in the network.

Table II and Table III provides some attack cases, including software attack, i.e. stealing customers' sensitive data from end devices through the internet, or inserting malicious code into users' software or application for processing malicious behaviors, and hardware attack cases, i.e. modifying the blueprint in the phase of designing, or installing the spy chip into the hardware in the phase of development.

B. Management with information technology

Security management refers to a protective method to achieve the high-level system security by enabling related security methods such as identification, authentication, access control and defining security policies. Security management plays an important role in information technology environment for reliable data fusion and mining, as well as enhancing users privacy and information security, which allows systems to overcome perceptions of unexpected situation or risks.

The definition of security management on digital supply chain management system refers to manage potential risks such as privacy leakage and malicious members manipulation, which could happen to any part or process, appeared with enabling information technologies on supply chains.

1) IoT: Traditional tracking methods, such as periodic bar code scanning and check points, provide segmental information, that is incomplete. IoT technology is a kind of new technology which can enable supply chain traceability with complete information that traditional information technology cannot achieve. In recent years IoT technologies, such as RFID, enables an automatic supply chain tracking capability with the lowest operational cost. For example, many companies have started using RFID technology to track real-time inventory information and to monitor human resource activities [3]. Moreover, RFID could be used by retailers to facilitate the speed of returns, to manage warranty claims by manufacturers and improve the performance of post-sales support. Especially in pharmaceutical supply chain management system, RFID could cut down the counterfeiting of pharmaceutical drugs and insure the integrity of products purchased by consumers. RFID could also be used in the food supply chain to ensure that the foods are fresh by tracking food products real-time status and condition. Consumers can use RFID information to check all nodes of supply chains, especially in the cool supply chain. That is to say, goods attached by RFID would be traceable in the supply chain [21].

2) Cloud computing: The centralized cloud server architecture of cloud computing can manage and collaborate collected information between different systems in an efficient way, which could improve the performance of information sharing and collaboration across the whole supply chain system. While traditional supply chain management systems only focused on physical, in-person information management methods, cloud computing environment provided the on-demand access to information vital for procurement practices, store shelf optimization, sales and operations planning [18].

3) Blockchain: Blockchain as one current hottest research topic currently, its trustworthy architecture with distributed and decentralized ledger, as well as cryptographically linked blocks, can also provide an accurate way for measuring products quality during whole transportation on supply chain. For example, stakeholders in a supply chain can gather the location information about whether the product was in a wrong place or the whole journey from source to destination by analyzing collected data on the travel path and duration [20]. Other utilizing cases of this kind of capability are applying

TABLE I
ATTACK CASES (SOFTWARE)

Victim	Consequence	How
Target (Nov. 2013)	Data from 110 million customers and 40 million payment cards was stolen.	Hackers first broke into Target's network using passcode credentials stolen from a third-party provider, HVAC system.
Goodwill Industries (Sept. 2014)	Data from 868,000 payment card accounts was stolen.	The breach stemmed from malware used to compromise a third-party vendor used "to process credit card payments.
CCleaner (Aug. 2017)	More than two million customers downloaded the updated version with malicious backdoor.	Attackers found a way to insert malicious code into the CCleaner 5.33 update. That infected version was signed with a valid and authentic certificate and was available from the legitimate website of Avast, maker of CCleaner.

TABLE II
ATTACK CASES (HARDWARE)

Victim	Consequence	How
Modifying Blueprint (Design level)	Illegitimate privilege upgrade.	The authors modified the blueprint of a chip that causes its privilege level to be raised from user mode to super user mode after a certain sequence of instructions is executed on the processor.
Spy Chip (Deployment level)	Backdoor for sensitive data leakage, privilege upgrade, and providing connecting method for software threats.	Chip manufacturers inserted tiny spy chips into the mainboard to be triggered after a sequence of instructions is executed on the processor.

blockchain technology on cold supply chain for food products environment monitoring, especially for temperature, and on food supply chain for food healthcare which could lead to serious health risks without enough attention.

V. TRUST ISSUES

Another considerable issues about current digital supply chain management system should be the trust problem. Trust issues have been researched for not a short time, however, not any efficient solution proposed yet. How can users trust the service provided by third parties, how can service providers trust identities submitted by users, or how can downstream firms trust the service provided by their upstream firms, high-efficient method should be proposed.

Yasaman et al. [22] proposed a trust model for supply chain management system which incorporates trust factors specific to supply chain management system, represented in probabilistic and utility-based terms. This kind of trust model is grounded in probabilistic game theory. In this model, trust can be obtained through direct interactions, and/or by requiring information from other trustworthy agents.

We could also think about utilizing information technologies to manage supply chain trust issues:

A. IoT

Yan et al. [23] defined objectives of trust management on IoT systems, which could be applicable on IoT-enabled supply chain system, with regard to trust relationship and decision, data perception trust, privacy preservation, data fusion and mining trust, data transmission and communication trust, quality of IoT services, system security and robustness, human-computer trust interaction and identity trust. To provide a trust environment of a supply chain management system, IoT technologies and services enabled on supply chain should be enforced as many as better to achieve above objectives as standard measurement of IoT trust management systems.

B. Cloud computing

To achieve the trust management of supply chain under a cloud service environment, cloud service providers provide many technologies such as standardization technology, virtualization technology, data management technology, platform management technology [7]. The standardization technology can be applied to provide an interface which is for accessing cloud service providers and relating to alliance master formed real information interchanges on supply chain. The central cloud server could be regarded as a middleware which is in service and server cluster to provide the management service. The virtualization technology providers of cloud computing services can provide a same virtual software interface for different supply chain enterprises or systems who own different physical interfaces, in order to improve the efficiency of information collaboration, program collaboration and interface collaboration.

C. Blockchain

Blockchain can also play an important role on improving the performance of trust management by reducing the risk possibility since blockchain need to validate the identities of individual participating in transactions, which means only members who are mutually accepted in the network can engage in transactions.

VI. Challenges

For current digital supply chain management systems, an important security challenge is how to face those security risks which are also rigorous for enabled information technologies. While enabling above technologies on supply chain systems, some inherent security problems within themselves or between collaborations would be long/short-term challenges for digital supply chain system.

- IoT devices still face the unstable or untruthful internet environment with unexpected cyberattacks, so the information collaboration between IoT and data-provenance would be vulnerable to such risks.
- The limitations of blockchain would limit the development on supply chain as well, i.e. the global supply chain operates in a complicated environment which requires various parties to comply with diverse laws, regulations and institutions [20].
- Big data is another important factor for digital supply chain for appropriate data gathering, processing, storing and sensitive information protection, which could be consumer or retailers privacy, with the increasing scale of world-wide supply chain management system. Inefficient data processing and storage would allow some risks like sensitive information leakage to malicious parties.
- A new type of cyberattack between third-party service providers and end users is called software supply chain attack. Attackers target software developers and suppliers, seeking access to source codes and modify them, hide malware or backdoor in building and update processes.

Moreover, trust doesnt mean security, security also doesnt mean trust. More advanced solutions or solving plans, with regard to design a secure and trust supply chain management system, should be researched on.

VII. Conclusion

This paper discusses current situation and environment of supply chain management systems with various information technologies enablement for improving the performance corresponding to diversified demands. While working advantages of those information technologies, supply chain must face various security risks and challenges which are needed to be solved in the future research work. That would not be a short-term work to enhance the trust management of supply chain management system.

Acknowledgement

This research was partially supported by Collaboration Hubs for International Program (CHIRP) of SICORP, Japan Science and Technology Agency (JST).

References

[1] Smith, G. E., Watson, K. J., Baker, W. H., Pokorski Ii, J. A. (2007). A critical balance: collaboration and security in the IT-enabled supply chain. International journal of production research, 45(11), 2595-2613.

[2] Janvier-James, A. M. (2012). A new introduction to supply chains and supply chain management: Definitions and theories perspective. International Business Research, 5(1), 194.

[3] Zhou, W., Piramuthu, S. (2015, June). IoT and supply chain traceability. In International Conference on Future Network Systems and Security (pp. 156-165). Springer, Cham.

[4] Madakam, S., Ramaswamy, R., Tripathi, S. (2015). Internet of Things (IoT): A literature review. Journal of Computer and Communications, 3(05), 164.

[5] Benabdessalem, R., Hamdi, M., Kim, T. H. (2014, December). A survey on security models, techniques, and tools for the internet of things. In Advanced Software Engineering and Its Applications (ASEA), 2014 7th International Conference on (pp. 44-48). IEEE.

[6] Qian, L., Luo, Z., Du, Y., Guo, L. (2009, December). Cloud computing: An overview. In IEEE International Conference on Cloud Computing (pp. 626-631). Springer, Berlin, Heidelberg.

[7] Jun, C., Wei, M. Y. (2011). The research of supply chain information collaboration based on cloud computing. Procedia Environmental Sciences, 10, 875-880.

[8] Haber, S., Stornetta, W. S. (1990, August). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.

[9] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[10] Bocek, T., Rodrigues, B. B., Strasser, T., Stiller, B. (2017, May). Blockchains everywhere-a use case of blockchains in the pharma supply chain. In Integrated Network and Service Management (IM), 2017 IFIP/IEEE Symposium on (pp. 772-777). IEEE.

[11] Mousavi, A., Sarhadi, M., Lenk, A., Fawcett, S. (2002). Tracking and traceability in the meat processing industry: a solution. British Food Journal, 104(1), 7-19.

[12] Regattieri, A., Gamberi, M., Manzini, R. (2007). Traceability of food products: General framework and experimental evidence. Journal of food engineering, 81(2), 347-356.

[13] Abad, E., Palacio, F., Nuin, M., De Zarate, A. G., Juarros, A., Gomez, J. M., Marco, S. (2009). RFID smart tag for traceability and cold chain monitoring of foods: Demonstration in an intercontinental fresh fish logistic chain. Journal of food engineering, 93(4), 394-399.

[14] Markim A (2015) 8 ways cloud technology is changing the game for supply chain management. http://www.forbes.com/sites/louiscolumbus/2014/02/12/where-cloud-computing-is-improving-supply-chain-performance-lessons-learned-from-scm-world/4ee64acd6a91. Accessed 16 Nov 2016

[15] Gray J (2015) Cloud computing and supply chain management. Procurement Sense http://blog.procurify.com/2015/03/05/cloud- computing-and-supply-chain-management/. Accessed 20 July 2015

[16] Jain, B., Dhaka, R. (july 2015). Implementation of Cloud Computing in Supply Chain Management. International Journal for Research in Applied Science Engineering Technology (IJRASET), 3(VII), 11-15.

[17] Maziliauskaite K (2015) The cloud-whats in it for supply chain managers? Inventory and supply chain optimization. http://www.inventory-and-supplychain-blog.com/cloud-whats-supply- chain-managers/. Accessed 20 July 2015

[18] Cao, Q., Schniederjans, D., Schniederjans, M. (2017). Establishing the use of cloud computing in supply chain management. Operations Management Research, 10(1), 4763.

[19] Abeyratne, S., Monfared, R. (2016). Blockchain ready manufacturing supply chain using distributed ledger. S.A. and MONFARED, R.P., 2016. Blockchain ready manufacturing supply chain using distributed ledger. International Journal of Research in Engineering and Technology, 05(09), pp. 1-10.

[20] Kshetri, N. (2018). 1 Blockchains roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

[21] Shen, G., Liu, B. (2011, May). The visions, technologies, applications and security issues of Internet of Things. In E-Business and E-Government (ICEE), 2011 International Conference on (pp. 1- 4). IEEE.

[22] Haghpanah, Y. desJardins M. (2010). A Trust Model for Supply Chain Management. Proceedings of the Twenty-Fourth AAAI Conference on Artificial Intelligence (AAAI-10).

[23] Yan, Z., Zhang, P., Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of network and computer applications, 42, 120-134.