IoT - Supply Chain Forensics and Vulnerabilities

Venkata Venugopal Rao Gudlur
Center for Post Graduate Studies
Limkokwing University of Creative Technology
Cyberjaya, Malaysia
saigopal1123@gmail.com

Vikneswara Abirama Shanmugan
Department of Water and Environmental Engineering
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Malaysia
vikneswara.abirama21@gmail.com

Sundresan Perumal
Faculty of Science & Technology
Universiti Sains Islam Malaysia (USIM)
Nilai, Malaysia
sunderesan.p@usim.edu.my

Radin Maya Saphira Radin Mohammed
Department of Water and Environmental Engineering
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Malaysia
maya@uthm.edu.my

***Abstract*—The Supply Chain Forensics are latest revolution to save money and reduce the Risk. Supply chain management has been developed over many centuries ago from ancient civilization. The review of literature reveals that the current Digital Supply Chain industry is more connected to IoT devices which is latest revolution and future development such as gathering information and tracking goods, has evolved in to smart Supply Chain with RFID based tagging and sensor based technologies connected to IoT (Internet of Things).The use of these devices gives accurate organizational and operational outcome even though there may be unidentified procedural inconsistencies that may weakens the smooth operational procedures. This paper explains about the vulnerabilities related Supply Chain industry 4.0. Even though the application of IoT today not only tracks the goods and services but also predicts helps in future analysis for Supply Chain Industry. The entire digitalized process may help in protecting and reducing losses but there may be vulnerabilities will be identified by digital forensics. The problem really comes into focus when IoT devices are connected in unsecure Supply Chain environment. That may further concern is the fractured digital supply chains that they are relying on by modern industry experts.**

Keywords— SCF - Supply Chain Forensics, IoT - Internet of Things, RFID - Radio Frequency Identification

I. INTRODUCTION

Industry 4.0 - the utilization of the Internet of Things, the utilization of cutting-edge mechanical autonomy, and the use of cutting-edge investigation of enormous information in store network administration: put sensors in all things, make organizes all over the place, mechanize anything, and dissect everything to essentially enhance execution and consumer loyalty" [5]. In the course of the most recent thirty years, coordination's has experienced an enormous change: from a simply operational capacity that answered to deals or fabricating and concentrated on guaranteeing the supply of generation lines and the conveyance to clients, to an autonomous inventory network administration work that in a few organizations is now being driven by a CSO - the Chief Supply Chain Officer. In near future IoT will have greater impact on Supply chain industry in terms of technological changes with accurate information with in time frame. The focal point of the inventory network administration work has moved to timely arrangement forms, for example, systematic interest arranging or incorporated S&OP, which have turned out to be built up business forms in numerous organizations, while operational coordination's has frequently been redistributed to outsider LSPs. The store network work guarantees incorporated tasks from clients to providers.

Currently supply chains are working under ever changing condition and subsequently are helpless against an assortment of dangers. A few hazard factors influence this ever-evolving condition. Organizations are tested with discovering approaches to meet consistently rising client desires at a reasonable expense. The scope over wide topographies opens supply chains to dangers on worldwide scale (Butner 2010) [5]. The worldwide spread of supply chains is further being tested with critical increment in client mindfulness. Client today not just want auspicious conveyance, they likewise request and are exceedingly touchy w.r.t. item quality, cost and administration (Christopher 2016) [6]. With contribution of various and scattered players, overseeing vulnerability in the supply chain process represents a major test. Regardless of enormous logical improvements on a few parts of supply chains, various erratic and hard to control components can influence auspicious satisfaction of requests. Run of the mill regular elements causing late conveyances are activity and deficiency of stocks. IoT technology will give more Quick improvements in innovation has prompted similarly quick absence/ change of items which has additionally expanded the intricacy of supply chains (Simchi-Levi, Kaminsky furthermore, Levi 2003) [7]. Henceforth, Supply chain administration (SCM) has turned out to be basic and critical part of numerous ventures. To get by in such aggressive and testing condition, organizations need to fabricate a hearty however fundamentally adaptable, chance free and exceptionally responsive store network (Christopher and Holweg 2011) [8]. A great deal is being composed about the Internet of Things (IoT) furthermore, how it will influence about each worldwide industry— from retail to associated vehicles. A standout amongst the most energizing territories of effect is the worldwide inventory network. (Ross 2016) [9]. This has been accomplished through enhancing correspondence, gaining and transmitting information which empowers fast basic leadership and improving store network execution. Usage of Conceptual: Inventory network administration has been in presence [6].

II. LITERATURE REVIEW

IoT has fundamentally enhanced run of the mill difficulties of SCM like perceivability of the chain and in the meantime has improved dexterity and versatility of SCM (Ellis, Morris what's more, Santagate 2015) [10]. This report manages different components of production network what's more, its administration. The significance and difficulties of inventory network administration. The report gives an extensive survey of writing on store network administration, brief recorded point of view on the advancement of IoT and its mix in to

supply chain administration. Advance the report gives a detail record of IoT framework and the application frameworks. The IoT innovations utilized today in different supply chains administration are portrayed in detail. An exertion is made to give some contextual investigations on use of IoT in SCM.

As per Fig. 1 the technical description of IoT based forensic has been compared with in supply chain industry such as warehouse management, shipping, customer service and goods forwarding [1] [2] [3] [4]. What we finish up dependent on this examination is depicted in a nutshell. A book index of the references utilized for the examination are given toward the finish of this report [12]. Industry 4.0 makes an interruption and expects organizations to reconsider the way they structure their store network. A few advances have risen that are modifying conventional methods for working. Over this, uber patterns and client desires change the diversion. Other than the need to adjust, supply chains likewise have the chance to achieve the following skyline of operational viability, to use developing advanced store network plans of action, and to change the organization into a computerized inventory network. A few super patterns affect inventory network administration: there is a proceeding with development of the country regions around the world, with riches moving into locales that have not been served previously. Strain to diminish carbon discharges and directions of activity for financial reasons add to the difficulties that coordination's are confronting. In any case, changing socioeconomics prompt lessened work accessibility and expanding ergonomic prerequisites that emerge as the workforce age increments.

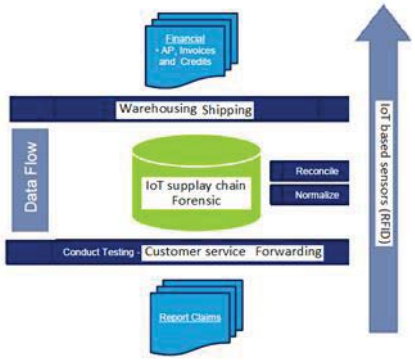

Fig. 1: IoT Forensic flow warehousing, Shipping, Customer service and Forwarding [1] [2] [3] [4]

III. IoT -Supply chain Forensic

A. *Related work: Future IoT -Supply chain Forensic.*

The digitization of the store network empowers organizations to address the new prerequisites of the clients, the difficulties on the supply side and in addition the rest of the desires in proficiency enhancement. Digitization achieves a Supply Chain 4.0, which will be quicker. New methodologies of item appropriation decrease the conveyance time of high sprinters to couple of hours. The reason for these administrations is worked by cutting edge gauging approaches, e.g., prescient investigation of inside (e.g., request) and outside (e.g., advertise patterns, climate, school excursion, development files) information and in addition machine status information for extra parts request, and gives a significantly more exact gauge of client request 3.1. Cloud Storage Characteristics. The more clarification on study will be depend on Realtime analogy of system which will interact with smart devises in supply chain industry. Arranging cycles and solidified periods are limited and arranging turns into a ceaseless procedure that can respond powerfully to changing necessities or requirements (e.g., constant creation limit criticism from machines). When the items are sent, expanded adaptability in the conveyance forms enables clients to reroute shipments to the most advantageous goal [13]. This scope of information gives a joint data premise to all levels of position and capacities in the store network. The joining of information of providers, specialist co-ops, and so forth in an "inventory network cloud" guarantees that all partners steer and choose dependent on similar actualities [14]. Digital waste prevents supply chains from leveraging the potential of Supply Chain 4.0

B. *Proposed IoT Supply Chain Forensic Model*

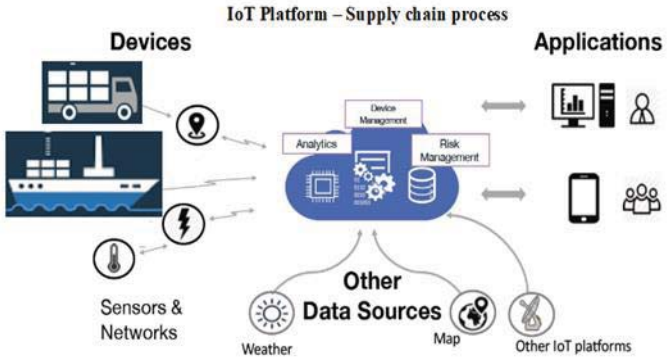

Fig. 2: Proposed Supply Chain Forensics Using Big Data to Identify and Fight Fraud

The "hatchery" is the seed of supply chain 4.0 I the association – quick, adaptable and productive [16].Detecting this chip-level tampering is analogous to finding a needle in a haystack of needles, according to a 2015 paper entitled Performance analysis of Hardware Trojan detection methods in the International Journal of Open Information Technologies [17].

C. *Advantages of IoT – Supply chain forensic industry 4.0*

Taking out the present computerized squander and embracing new advances is a noteworthy switch to build the operational viability of supply chains. The potential effect of Supply Chain 4.0 in the following a few years is colossal - up to 30 percent bring down operational expenses and a decrease of 75 percent in lost deals while diminishing inventories by up to 75 percent are normal, in the meantime expanding the dexterity of the supply chains essentially. Inventory network benefit/lost deals. Low client benefit is either determined by a wrong guarantee to the client (e.g., doubtful lead times), a wrong stock profile (requested items are not accessible), as well as an inconsistent conveyance of parts. Lost deals also happen if the required items are not accessible on the rack or in the framework - clients will choose to change to another brand. This is valid for both B2C and B2B conditions [14].

D. *Technical Process and Flow*

The user will display his finger to the sensor that captures the picture with face recognition, and this is known as the enrolment stage. The unique finger impression and face recognition sample are pre-processed to obtain permission to access data from the could database. whereas at the point when a client needs to login to get to applications on public cloud,

he gives his unique finger impression and face recognition to the mobile phone or sensor which catches the picture and plays out some pre-handling capacity to remove the highlights sent to the cloud server for validation check or process [17] [18] [19].The cloud data base will perform the matching function performs a comparison check and updates the user with access granted or denied. The access process can be set maximum tries depends on public network setting. The technical process can be implemented to retailers and suppliers when it comes to total scalability of the system example Walmart stock clearance and stock check all over the globe can be monitored and updates will be provided to relevant team members respective region such as retailers and suppliers.

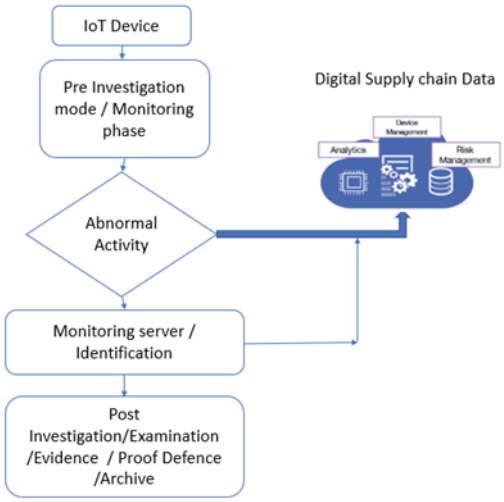

Fig. 3: Proposed flow chart of Research Model

As per Proposed IoT Model Pre investigation or monitoring phase will be active when it comes to any abnormal activity by IoT sensors during the manufacturing / supply data which has been recorded at respective server as mentioned IoT Sensor Technical Flow.

The IoT Sensor Technical flow consists of Sensor Module, Processing Module, Actuation Module, Communication Module and Energy Module as a main module as shown in Fig. 4.

However, 26.8 % report that they presently have no program set up to avert and distinguish those dangers and just 29.3 % utilize examination to alleviate store network misrepresentation and budgetary dangers [19]. As per above figure comparison model explain about IoT device forensic data collection and investigation process and understanding of proposed model. Most companies are doing at least some form of non-fraud-based risk assessment across their supply chains, they just need to extend that process to include the fraud piece." With continuous monitoring, we can identify those types of outliers and better protect the business without making people feel like you are watching them" [20].

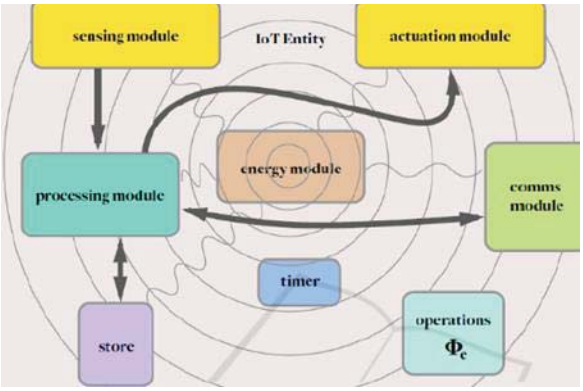

Fig. 4: IoT Model of Entity (Julian Rathke and Vladimiro Sassone 2010)

TABLE 1: COMPARISON FORENSIC MODELS WITH PROPOSED MODEL

IoT Supply Chain Investigation Models and Comparison	IoT Devices	Monitoring Phase	Abnormal Activity	Secure Location / IDS/IPS	Base Devise Identification	Examination	Evidence Analysis	Results
Venkata Venugopal current study	●	●	●	●	●	●	●	●
K.Kyei et al		●	●	●	●	●	●	
A.Agawal el al		●		●	●	●	●	
I.O Ademu el al				●	●	●	●	●
V.Baryamureeba and F.Tushabe		●	●	●	●	●		

IV. SECURITY AND PRIVACY RISK IN IOT SUPPLY CHAIN FORENSIC

i. Inconsistent data across procurement-related systems
ii. Data quality issues relating to spend data and vendor data
iii. Lack of transparency of procurement data
iv. Lack of controls around use of preferred vendors, negotiated contracts
v. Low compliance with corporate preferred buying guidelines
vi. Buying power not fully leveraged due to lack of reporting/knowledge of historical spend
vii. Multiple instances of the same vendor within master file
viii. Inconsistent vendor payment terms across the organization
ix. Lack of controls around vendor creation and management
x. Failure to actively manage high-risk vendor relationships
xi. Duplicate payments
xii. Inefficient invoice processing
xiii. Failure to optimize cash flow and payment terms to vendors and suppliers
xiv. Limited segregation of duties involving payments, credits, and reconciliation of vendors

V. FUTURE WORK

"The most important part of this is the supply chain and procurement people working with the business requesters – sales or operations – to make sure they have done enough due diligence to add these third parties to the supply chain" [21]. The year 2020 will see a stunning 25 billion devices connected to the Internet of Things. Simply envision the potential outcomes of using Realtime data from all connected devices. The financial service sector in supply chain industry is also impacted by the intelligence devices. There may be better innovation and smooth operations with zero errors when they deal with supply chain industry 4.0 [22] [23]. The Internet of Things will change and transforming Supply chain financial services. Many supply chain industry experts would preferably choose not to see to store network extortion over to let it be known's occurring inside their association [24] [25] [26].

VI. CONCLUSION

There are no best practices available which can be mapped to the practice of unorganized sector east or west in the globe. There are no formal information systems available in and process flow of future connectivity with IoT devices. Mostly, the information flow is informal, and the material flow is disorganized and may involve low level of mechanization/automation. Still some companies are using money flow is also using traditional methods [27] [28]. The extent of e-commerce or payment gateways may not be there. However, the industry 4.0 with IoT supply chain will give a big challenge to the future world and users which involves a huge amount of manpower with technical skills. Their supply chain is also an opportunity for mass employment generation. Therefore, the challenge is to manage human flow appropriately. Thus, supply chain in emerging economies offer an altogether different domain for modelers and analysts with industry 4.0 and IoT connectivity [29][30].

ACKNOWLEDGMENT

I would like to thanks to Putra Intelek International college for financial support to publish this paper and my supervisor who always encourages with technical knowledge.

REFERENCES

[1] Qiu, X., Luo, H., Xu, G., Zhong, R., & Huang, G. Q. (2015). Physical assets and service sharing for IoT-enabled Supply Hub In Industrial Park (SHIP). International Journal of Production Economics, 159, 4-15.

[2] Kwon, D., Hodkiewicz, M. R., Fan, J., Shibutani, T., & Pecht, M. G. (2016). IoT-based prognostics and systems health Management for industrial applications. IEEE Access, 4, 3659-3670.

[3] Solic, P., Blazevic, Z., Skiljo, M., Patrono, L., Colella, R., & Rodrigues, J. J. (2017). Gen2 RFID as IoT enabler: Characterization and performance improvement. IEEE Wireless Communications, 24(3), 33-39.

[4] Shim, J. P., Avital, M., Dennis, A. R., Rossi, M., Sørensen, C., & French, A. (2019). The transformative effect of the internet of things on business and society. Communications of the Association for Information Systems, 44(1), 129-140

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

[6] Christopher, M. 2016. Logistics and Supply Chain Management. Harlow: Pearson.

[7] 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.

[8] 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.

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

[10] 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.

[11] Brezmes T, Gorricho J-L, Cotrina J. Activity Recognition from Accelerometer Data on a Mobile Phone. In: Omatu S, Rocha M, Bravo J, Fernández F, Corchado E, Bustillo A, et al., editors. Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Notes in Computer Science. Berlin Heidelberg: Springer; 2009. p. 796–9.

[12] Kamp I, Kilincsoy U, Vink P. Chosen postures during specific sitting activities. Ergonomics. 2011; 54 (11):1029–42.

[13] de Waard D, Westerhuis F, Lewis-Evans B. More screen operation than calling: the results of observing cyclists' behaviour while using mobile phones. Accid Anal Prev.2015; 76:42–8. doi: 10.1016/j.aap.2015.01.004 PMID: 25590920.

[14] Lian, J. W. (2015) 'Critical factors for cloud based einvoice service adoption in Taiwan: An empirical study', International Journal of Information Management, 35(1), pp. 98-109.

[15] European Commission: European Cloud Computing Strategy.

[16] ENISA: Good Practice Guide for securely deploying Govern Mental Clouds. practice-guide-for-securely deploying governmental-clouds.

[17] Shawish, A., M. Salama, 2014. Cloud computing: paradigms and technologies. In FXhafa, & M. Salama (Eds.), Intercooperative collective intelligence: Techniques and applications (pp: 39e67). Berlin: Springer-Verlag.

[18] Singh, S., D. Chand, 2014. Trust evaluation in cloud based on friends and third party's recommendations. In Engineering and Computational Sciences (RAECS), 2014 Recent Advances in (pp: 1-6. IEEE).

[19] Anil K. Jain, Fellow, IEEE, Arun Ross, Member, IEEE, and Salil Prabhakar, Member, IEEE An Introduction to Biometric Recognition IEEE Transactions on Circuits And Systems For Video Technology,Vol. 14, No. 1, JanuarY 2004

[20] Abdullah A. Albahdal and Terrance E. Boult, Problems and Promises of Using the Cloud and Biometrics ResearchGate publications, 17th November 2015.

[21] Kaul, V.; Bharadi, V.A.; Choudhari, P.; Shah, D.; Narayank hedkar, S.K," Security Enhancement for Data Transmission in 3G/4G Networks", IEEE sponsored 1st International Conference on Computing, Communication, Control, and Automation (ICCUBEA), February 2015, pg. 95 – 102.

[22] Sutherland, Iain; Theodoros Spyridopoulos; Huw Read; Andy Jones; Graeme Sutherland and Mikhailia Burgess. (2015). Applying the ACPO Guidelines to Building Automation Systems. In Human Aspects of Information Security, Privacy, and Trust, pp. 684-692.

[23] Joshi, R.C., Pilli, Emmanuel S. (2016). Fundamentals of Network Forensics, Springer- Verlag London 2016

[24] Morrison L., Read H., Xynos K., Sutherland I. (2017) Forensic Evaluation of an Amazon Fire TV Stick. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII. Volume 511 of the series IFIP Advances in Information and Communication Technology pp. 63-379, Springer, Berlin, Heidelberg

[25] Liu C., Singhal A., Wijesekera D. (2017) Identifying Evidence for Cloud Forensic Analysis. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics XIII. 410 of the series IFIP Advances in Information and Communication Technology pp. 111-130, Springer, Berlin, Heidelberg

[26] Edward, E. (2017), US supreme court to hear appeal in Microsoft warrant case, The IRISH TIMES, 2017. [Online].

[27] Ryder, S., Le-Khac, N-A. (2016), The End of effective Law Enforcement in the Cloud? To encrypt, or not to encrypt, 9th IEEE International Confer ence on Cloud Computing, San Francisco, CA, USA, June 2016.

[28] Richard, G., Le-Khac, N-A., Scanlon M., Kechadi M-T., (2016), Analytical Approach to the Recovery of Data from CCTV File Systems, The 15th European Conference on Cyber Warfare and Security, Munich, Germany, July 2016.

[29] Perumal, S., Norwawi, N. M., & Raman, V. (2015). Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) (pp. 1923). IEEE.

[30] Julian Rathke and Vladimiro Sassone, 2010. Cyber Security in the internet of things. Cryptology and Information Security Series, 4, pp.109–124.